

Partizipationsmeeting

Elektronische Identität und
Vertrauensinfrastruktur

08.05.2025

La version française
est disponible sur
GitHub.

The English version
is available on
GitHub.

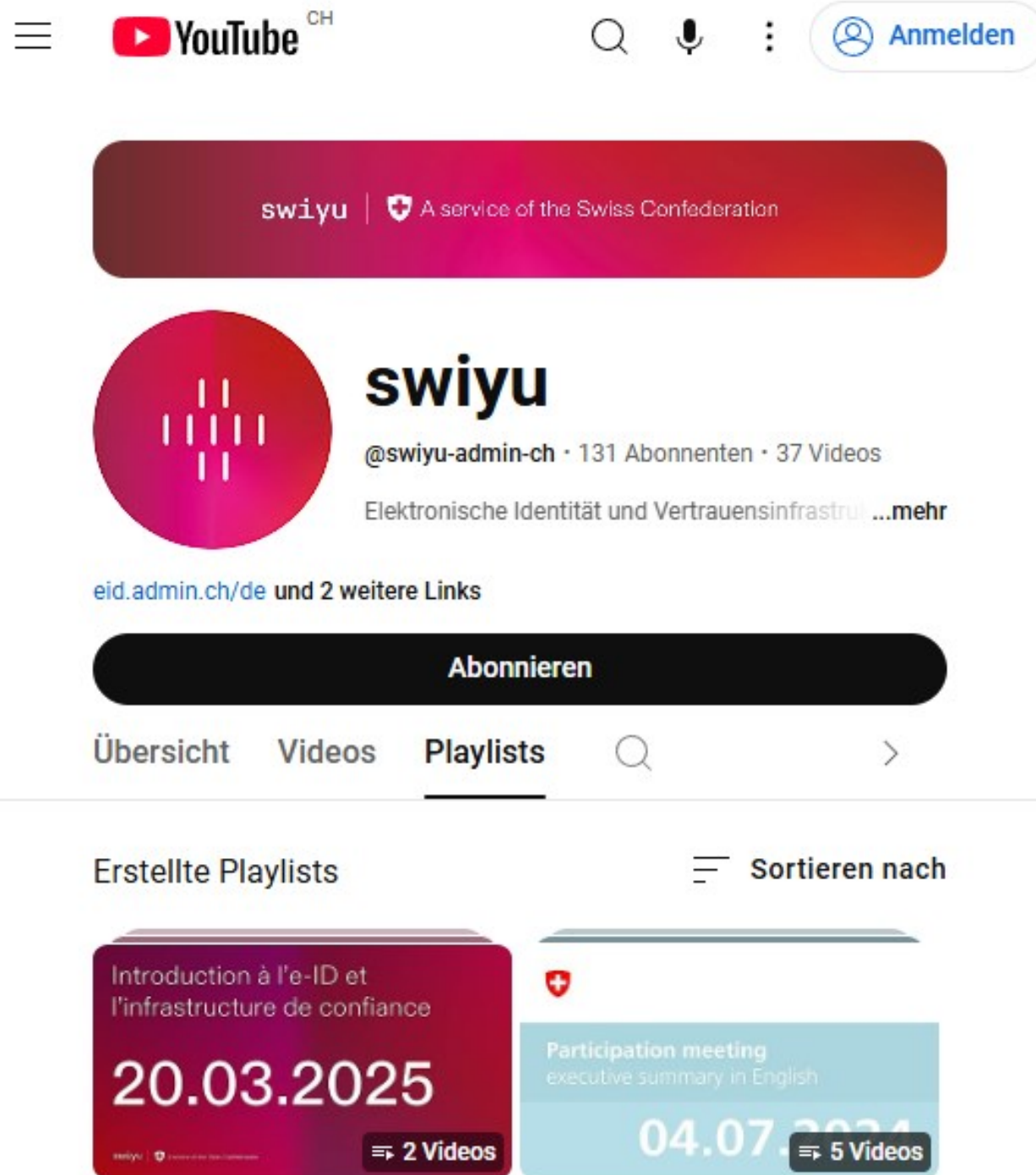


Agenda


- Begrüssung und Agenda
- Offene Stellen
- Global Digital Collaboration on Wallets and Credentials
- Gesetzgebung – Stand und Ausblick
- Public Beta
 - Stand und Ausblick
 - Erste Rückmeldungen aus der Privatwirtschaft
 - User-Testing
- Unverknüpfbare e-ID: Batch-Issuance und Renewal-Key-Konzept
- Fragen aus dem Publikum
- Executive Summary in English (18 Uhr)

Aufzeichnung

Das Partizipationsmeeting wird aufgenommen und auf YouTube publiziert.




The screenshot shows the YouTube channel page for 'swiyu'. At the top, there's a navigation bar with the YouTube logo, a search icon, a microphone icon, and a 'Anmelden' button. Below this is a banner for 'swiyu' with the text 'A service of the Swiss Confederation'. The channel's profile picture is a red circle with white vertical bars. The channel name 'swiyu' is displayed, along with the handle '@swiyu-admin-ch', 131 subscribers, and 37 videos. The channel description is 'Elektronische Identität und Vertrauensinfrastruktur ...mehr'. Below the description, there's a link to 'eid.admin.ch/de' and '2 weitere Links'. A large black button labeled 'Abonnieren' is prominent. Below the button are tabs for 'Übersicht', 'Videos', 'Playlists', and a search icon. The 'Playlists' tab is selected. Under the 'Playlists' tab, there's a section titled 'Erstellte Playlists' with a 'Sortieren nach' dropdown. Two playlists are shown: 'Introduction à l'e-ID et l'infrastructure de confiance' dated '20.03.2025' with '2 Videos', and 'Participation meeting executive summary in English' dated '04.07.2024' with '5 Videos'.


swiyu |  A service of the Swiss Confederation


swiyu
@swiyu-admin-ch • 131 Abonnenten • 37 Videos
Elektronische Identität und Vertrauensinfrastruktur ...mehr

eid.admin.ch/de und 2 weitere Links

Abonnieren

Übersicht Videos **Playlists** 

Erstellte Playlists  Sortieren nach

Introduction à l'e-ID et l'infrastructure de confiance
20.03.2025
swiyu |  A service of the Swiss Confederation **2 Videos**

Participation meeting executive summary in English
04.07.2024
5 Videos

Hinweise zu Fragen und Antworten

- Bitte unser Informationsangebot nutzen!
 - www.eid.admin.ch
 - <https://www.youtube.com/@swiyu-admin-ch>
 - <https://github.com/swiyu-admin-ch>
- Spezifische Fragen bitte via Chat stellen – sie werden via Chat beantwortet.
- Fragen, die für alle interessant sein könnten, bitte via Mikrofon stellen.
- Wir führen hier keine politischen Diskussionen.

Offene Stellen

Der Fachbereich e-ID sucht neues Personal

- ICT Consultant e-ID-Ökosystem Marketing
- ICT Consultant e-ID-Ökosystem Integration
- ICT Consultant Technology Scouting und Interoperability

[Mehr Informationen und Bewerbungen via www.stelle.admin.ch](http://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

Informationen zur Konferenz

Agenda

- 1. Juli: Geografischer und sektorieller Überblick im Plenum
- 2. Juli: Deep dives parallel in 15 unterschiedlichen Räumen
- Konferenzsprache ist Englisch

Teilnahme

- Teilnahme ist kostenlos
- Anmeldung auf www.lu.ma/gc25 via DIDAS oder Digitale Gesellschaft (Digital Society)

Gesetzgebung

Stand und Ausblick

e-ID-Gesetz: Referendum zustande gekommen

- Innerhalb der Referendumsfrist wurden 55 638 Unterschriften gegen das Bundesgesetz vom 20. Dezember 2024 über den elektronischen Identitätsnachweis und andere elektronische Nachweise (E-ID-Gesetz, BGEID) eingereicht. Die Überprüfung durch die Bundeskanzlei hat ergeben, dass 55 344 der eingereichten Unterschriften gültig sind.
- Damit ist das Referendum formell zustande gekommen.
- Der Bundesrat muss mindestens 4 Monate vor dem Abstimmungstermin die Abstimmungsthemen bestimmen.
- Nächste Abstimmungstermine sind 28. September und 30. November 2025.

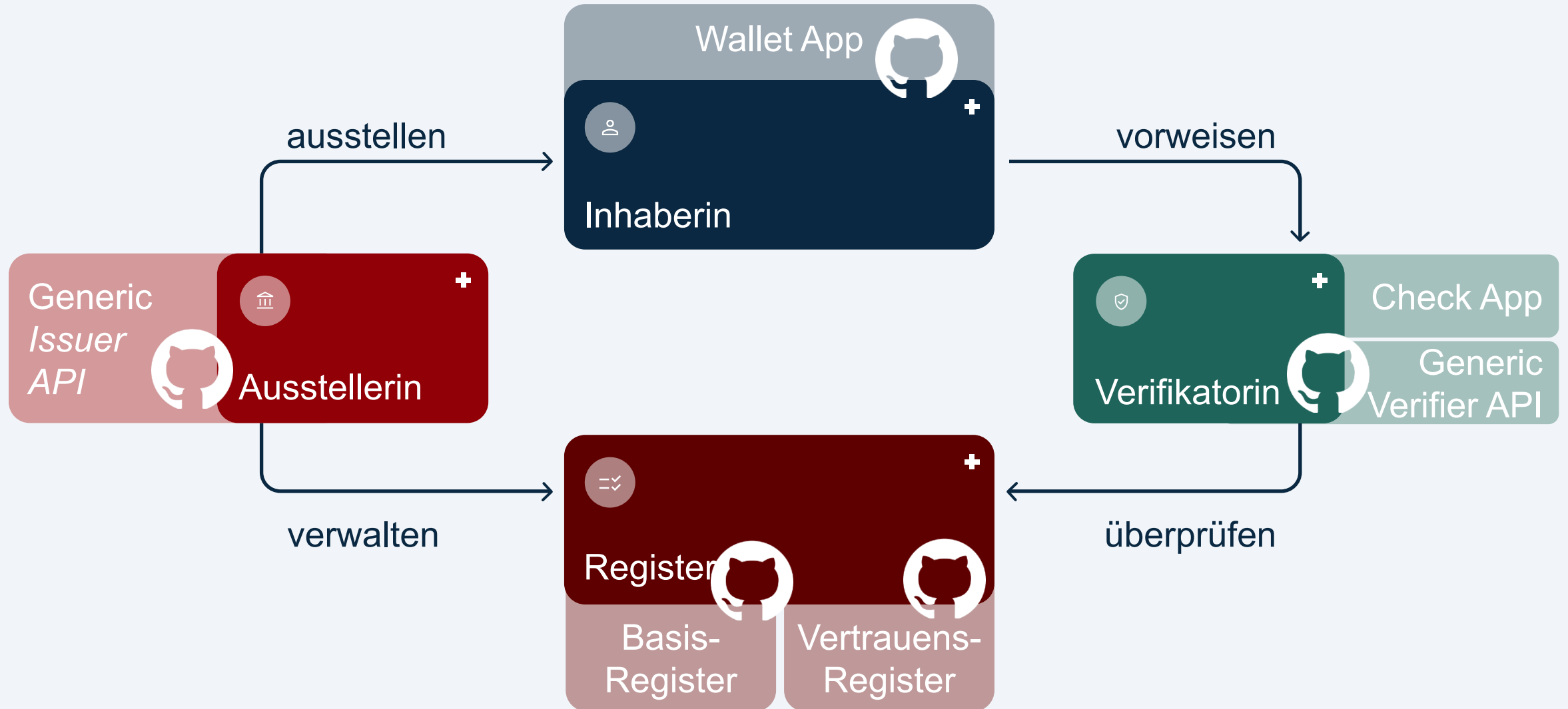
Vernehmlassung zur Verordnung

- Die Arbeiten an der Verordnung schreiten plangemäss voran.
- Die Vernehmlassung der Verordnung wird voraussichtlich noch vor der Sommerpause eröffnet.

Public Beta

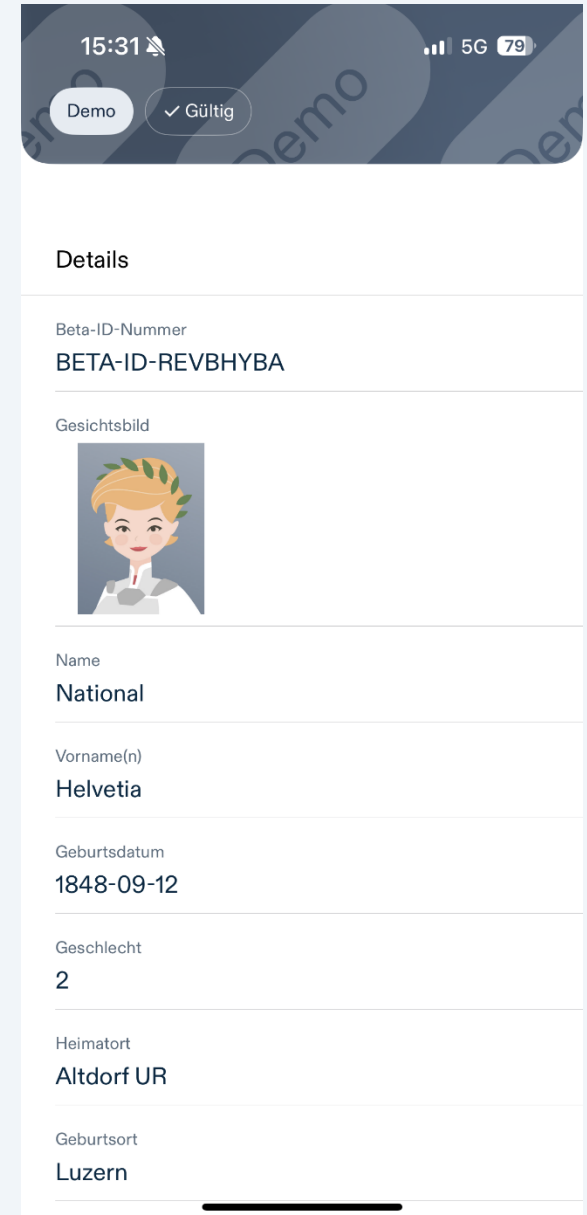
Stand und Ausblick

Public Beta-Komponenten



Beta-ID

- Datenfelder sind mit den Datenfeldern der e-ID identisch:
 - Vorname(n), Nachname, Geburtsdatum, älter als 16/18/65, Nationalität, AHV-Nummer etc.
 - Ebenso die weiteren Daten wie: Dokument-Nummer, Verifikationsprozess-Typ, Gültig bis etc.
- Das Format der Beta-ID ist SD-JWT, gemäss Definition im swiss-profile (GitHub)
- Halterbindung ist vorhanden (wo möglich Hardware-Binded, sonst Software-Binded)
- Die Benutzer können den Inhalt selber definieren.



Erste Zahlen zu Public Beta

Nutzerinnen und Nutzer

- swiyu-Downloads: +11'000
- Beta-ID-Ausstellungen: +9'000
- Verifikations-Links: +5'000
- Verifikationen: +1'500
- Revokationen: +350
- Business-Partner auf dem e-Portal: +125
- Trustregistereinträge: 16

Infrastruktur

- CPU-Nutzung: unter 2%

GitHub

- Generic Verifier: +450 Downloads der Docker Images
- Generic Issuer: +600 Downloads der Docker Images
- Issues und Anfragen im Diskussionsforum: +30

Public Beta

Erste Rückmeldungen aus der Privatwirtschaft

Public Beta

User-Testing

Unverknüpfbare e-ID

Batch-Issuance und Renewal-Key-Konzept

Ausgangslage

Was ist Unverknüpfbarkeit?

- 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)
- Dies kann anhand der **Inhalte**, beim Kommunikationsaufbau entstehende **Randdaten** oder der **kryptographischen Daten** erfolgen
- [Blogpost zur Unverknüpfbarkeit](#)




Inhaltliche Verknüpfbarkeit der e-ID

✓ Gültig

Details

Foto



Amtlicher Name
Schweizer Sample

Vorname(n)
Helvetia

Geburtsdatum
01.08.1995

Heimatort
Bern

Nationalität
Schweiz

Ausgestellt am
03.02.2023

Übermittelter Inhalt

- Schweizer Sample
- Helvetia
- 01.08.1995

Technische Daten

(für Unverknüpfbarkeit relevant)

- Issuer Signatur des VCs
- Disclosures (Salted/Hashed Claims)
- Public Key des Holders
- Revokationsinformation


Verifier

Technische Verknüpfbarkeit der e-ID

✓ Gültig

Details

Foto



Amtlicher Name

Schweizer Sample

Vorname(n)

Helvetia

Geburtsdatum

01.08.1995

Heimatort

Bern

Nationalität

Schweiz

Ausgestellt am

03.02.2023

Übermittelter Inhalt

- älter als 18

Technische Daten

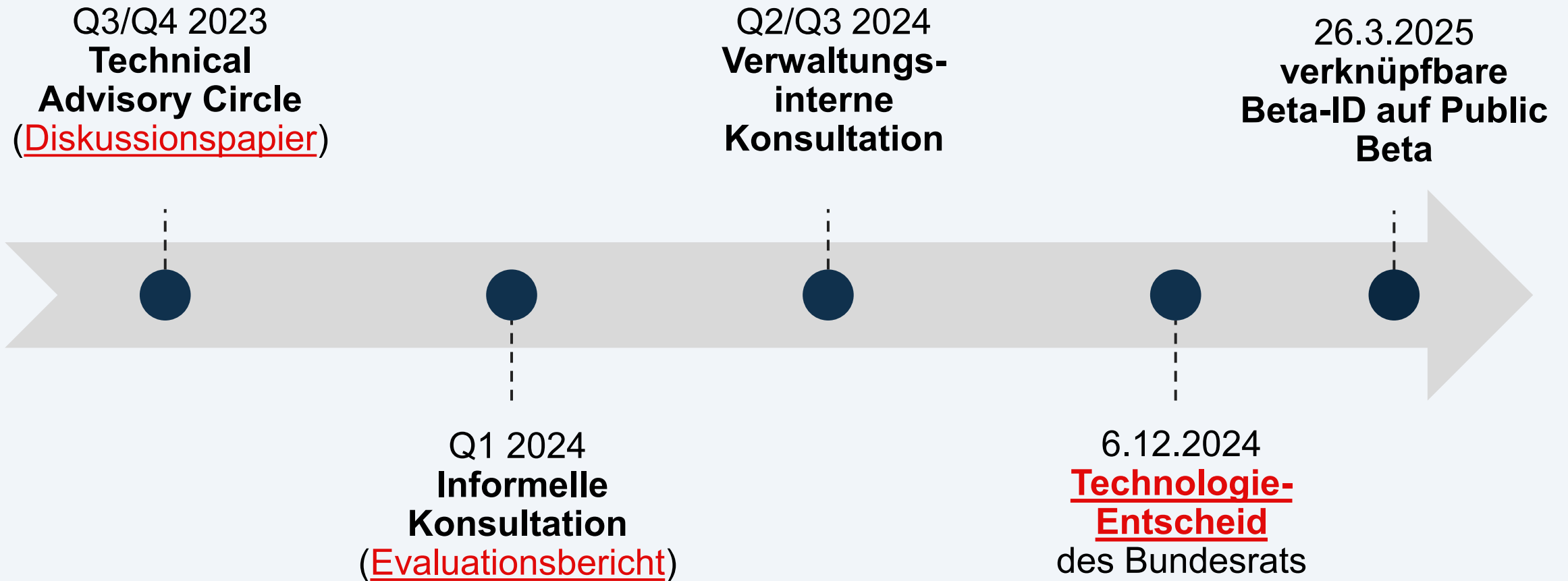
(für Unverknüpfbarkeit relevant)

- Issuer Signatur des VCs
- Disclosures (Salted/Hashed Claims)
- Public Key des Holders
- Revokationsinformation

Auch wenn SD-JWTs kryptografisch nicht verknüpfbar sind, könnten **Randdaten** zur **Verknüpfung** missbraucht werden. Nutzerinnen der Wallet können zusätzlich aktiv Fingerprinting und IP-Korrelation vermeiden.

Verifier

Rückblick Unverknüpfbarkeit im Programm e-ID



Technologie-Entscheidung Dezember 2024

- **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 gekoppelt
- Es werden dedizierte **Mittel und Team-Ressourcen** eingesetzt, um das Thema voranzutreiben



The screenshot shows the 'News Service Bund' website. The header includes a navigation bar with 'Alle Schweizer Bundesbehörden' and a language selector 'DE'. Below the header is the 'News Service Bund' logo and the text 'Das Portal der Schweizer Regierung'. The main content area displays a news article titled 'E-ID: Bundesrat trifft Technologie-Entscheidung', dated 'Veröffentlicht am 6. Dezember 2024'. The article text states that the Federal Council has decided on the principles for the technical implementation of the new electronic identity (E-ID) at its meeting on December 6, 2024. It also mentions that the implementation will be done in two steps and that the Federal Council has decided on the name of the trust infrastructure: 'SWIYU'. The article concludes by stating that the new E-ID is planned for implementation in 2026 and that the Federal Council has decided on the principles for the technical implementation.

Alle Schweizer Bundesbehörden DE

 News Service Bund
Das Portal der Schweizer Regierung

Veröffentlicht am 6. Dezember 2024

E-ID: Bundesrat trifft Technologie-Entscheidung

Bern, 6.12.2024 - Der Bundesrat hat an seiner Sitzung vom 6. Dezember 2024 die Grundsätze der technischen Umsetzung der neuen elektronischen Identität des Bundes (E-ID) festgelegt. Die Umsetzung soll in zwei Schritten erfolgen. Gleichzeitig wurde der Bundesrat über den künftigen Namen der Vertrauensinfrastruktur informiert: Die elektronische Briefftasche des Bundes heisst SWIYU.

Derzeit ist geplant, die neue E-ID des Bundes im Jahr 2026 einzuführen. Um diesen Zeitplan einhalten zu können, arbeitet der Bund bereits jetzt an der technischen Umsetzung. Die Umsetzung beinhaltet sowohl die Entwicklung der E-ID als auch den Aufbau der für den Betrieb notwendigen Vertrauensinfrastruktur. An seiner Sitzung vom 6. Dezember 2024 hat der Bundesrat die Grundsätze für die technische Umsetzung festgelegt.

Go-Live e-ID 2026

Ab Einführung: Unverknüpfbare e-ID dank Batch-Issuance

Durch die Ausstellung mehrerer gleich aussehender VCs (Batch-Issuance) wird die kryptographische Unverknüpfbarkeit **ab der Einführung** der e-ID ermöglicht.

- ! Verknüpfbarkeit auf Basis vorgewiesener Attribute oder anfallender Randdaten kann nicht verhindert werden.



Eckpunkte von batched e-ID-VCs



e-ID-VC Gültigkeit: Gültigkeit des zugrundeliegenden Ausweisdokuments oder max. 5 Jahre



Batch Grösse: 25 e-ID-VCs pro Batch



Batch-VC Nutzung:

- Einmalige Nutzung, automatisierter Bezug zusätzlicher e-ID-VCs nach Einwilligung
- Zufällige Nutzung, bei abgelehnter Einwilligung oder fehlgeschlagener Erneuerung



Bezug eines neuen Batches:

Wenn noch 2 ungenutzte Nachweise in der Wallet vorhanden sind



Revokation:

Bezug eines neuen Batches führt nicht zur Revokation → nur erneuter erfolgreicher e-ID Antrag führt zur Revokation aller e-ID-VCs
Wenn möglich die e-ID mehrerer Personen gebündelt revozieren (Herden-Revokation)

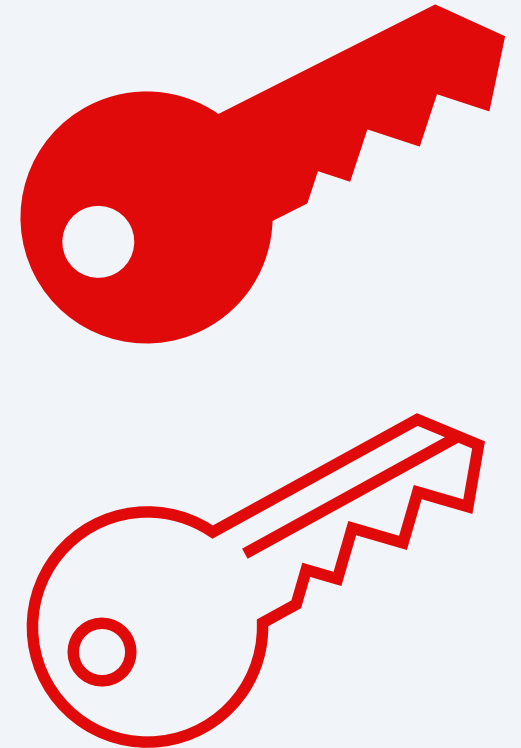
Renewal-Key-Konzept

Bindung an die Inhaberin

- Wenn die e-ID-VCs «verbraucht» sind, soll die Inhaberin oder der Inhaber resp. die Wallet einen **neuen Batch beziehen** können.
- Das heisst, es muss wieder eine **sichere Verbindung** zwischen der Wallet und der Ausstellerin der e-ID (fedpol) **aufgebaut werden**.
- Bei der Erstausstellung der e-ID ist die **Identifikation der Person** (online oder am Schalter) ein wichtiges Element um die Bindung an die richtige Inhaberin sicherzustellen.
- Das Abholen neuer e-ID VCs mit weiterhin sicherer Bindung an die Inhaberin wird mit dem **Renewal-Key-Konzept** adressiert

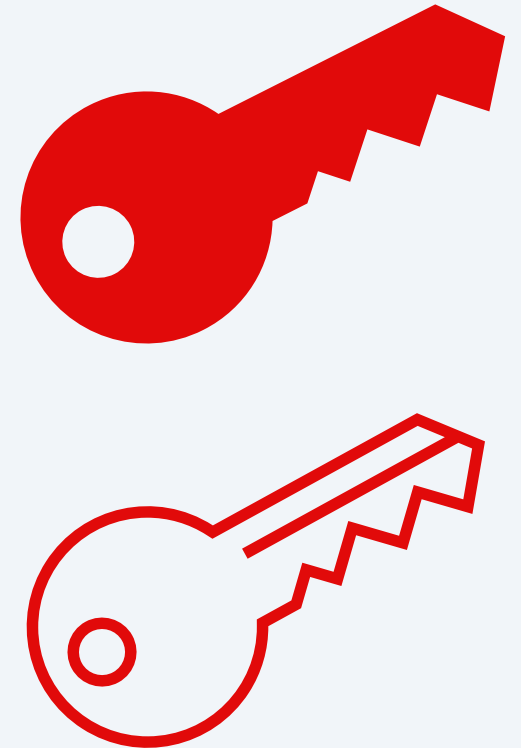
Renewal Key

- **An die Inhaberin gebundenes Schlüsselpaar** (hardware bound) zur Authentifizierung
- **Ausschliesslich zum Bezug zusätzlicher e-ID-VCs.**
- Der **öffentliche Schlüssel** wird bei der ersten e-ID Ausstellung von fedpol erfasst
- Das Schlüsselpaar ist **kein Teil der e-ID-VCs**



Wieso Renewal Key?

- **Ermöglicht Bezug eines neuen Batches mit sicherer Bindung an die bestehende Inhaberin**
- Wird während initialer Ausstellung durch Wallet erzeugt und von Ausstellerin geprüft
- Keine Degradation durch Vorweisen an andere Verifikator*innen
- Möglichkeit zur Trennung der Gültigkeitsdauer zwischen Erneuerungszyklus und VC-Gültigkeit







Verwendung des Renewal Keys

Erstausstellung

Binding keys  

Renewal key 


Issuer key 





e-ID	
Name: Alice	e-ID
Geburtsdatum: 01.01.1975	Name: Alice
Über 18: Ja	Geburtsdatum: 01.01.1975
Nationalität: Schweiz	Über 18: Ja
Binding Public Key: 	Nationalität: Schweiz
Ausstellersignatur: Fedpol 	Binding Public Key: 
Signatur der Challenge	Ausstellersignatur: Fedpol 
	Signatur der Challenge


Erneuerung

Binding keys  

Renewal key 

Issuer key 

e-ID	
Name: Alice	e-ID
Geburtsdatum: 01.01.1975	Name: Alice
Über 18: Ja	Geburtsdatum: 01.01.1975
Nationalität: Schweiz	Über 18: Ja
Binding Public Key: 	Nationalität: Schweiz
Ausstellersignatur: Fedpol 	Binding Public Key: 
Signatur der Challenge	Ausstellersignatur: Fedpol 
	Signatur der Challenge





 Batch Erneuerung

Neuausstellung


Binding keys  

Renewal key 

Issuer key 

e-ID	
Name: Alice	e-ID
Geburtsdatum: 01.01.1975	Name: Alice
Über 18: Ja	Geburtsdatum: 01.01.1975
Nationalität: Schweiz	Über 18: Ja
Binding Public Key: 	Nationalität: Schweiz
Ausstellersignatur: Fedpol 	Binding Public Key: 
Signatur der Challenge	Ausstellersignatur: Fedpol 
	Signatur der Challenge

Ablauf
Renewal Key

 Batch Erneuerung

Verwendetes kryptografisches Material

INHABER

AUSSTELLER

Bindung eines Nachweises i				
Secret Key	Public Key	Key Type	Key Attestation*	Signature (of issuer)
sk_i	pk_i	ECDSA (NIST p-256)	ka_i	sig_i

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

Nachweis Signatur		
Secret Key (HSM)	Public Key	Key Type
sk_{Bund}	pk_{Bund}	EdDSA (Ed448)

*Key Attestations werden von iOS nicht unterstützt. Stattdessen wird eine App Attestation verwendet werden, hierfür muss die App vom Bund zertifiziert werden.

Ablauf der Erstaussstellung einer e-ID

- 1) Wallet generiert Schlüssel zur Bindung (sk_i/pk_i) und Erneuerung (sk_{renew}/pk_{renew}). Schlüssel werden in der Secure Enclave generiert und sind dadurch an das Endgerät gebunden
- 2) Wallet übermittelt «Proofs of Possession» (für sk_i und sk_{renew}) und «Key Attestations» (ka_i für pk_i und ka_{renew} für pk_{renew}) und ein JWT_{renew} an die Ausstellerin, um die Schlüsselbindung an die Hardware zu beweisen
- 3) Identifikation der Inhaberin durch Identitätsprüfung (online, am Schalter)
- 4) Ausstellerin verifiziert «Proofs of Possession» und «Key Attestations» und definiert die Attribute (Bspw. Gültigkeit). Sie signiert das JWT_{renew} und übermittelt dies der Inhaberin
- 5) Ausstellerin generiert e-ID-VCs (salted-hash Verfahren) und bindet diese an die Wallet (pk_i als Attribut im VC)

Ablauf eines Batch Bezugs

- 1) Wallet generiert **neue(s)** «Binding» Key Pair(s) (sk_{i+1}/pk_{i+1})
- 2) Wallet übermittelt «Proofs of Possession» (für sk_{i+1} und sk_{renew}), «Key Attestations» (ka_{i+1} und ka_{renew}) und JWT_{renew} an Ausstellerin, um Wallet zu authentifizieren und Bindung der Schlüssel an die Hardware zu beweisen
- 3) Ausstellerin verifiziert, JWT_{renew} , «Proofs of Possessions» und «Key Attestations»
- 4) Ausstellerin generiert e-ID-VCs (salted-hash Verfahren) und bindet diese an die Wallet (pk_{i+1} als Attribut im VC)

Weitere Details werden auf GitHub veröffentlicht

e-ID

Analysis of the Key Management related to the Verifiable Credentials

1 Introduction

This document describes the cryptographic 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 hold-ership. 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

Q & A

Fragen aus dem Publikum

Executive summary in English

6 pm

Nächstes Partizipationsmeeting

Donnerstag, 05.06.2025 16 Uhr

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

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

Links

Allgemeine Informationen zur e-ID
www.eid.admin.ch

Informationen zur e-ID-Gesetzgebung
www.bj.admin.ch
www.parlament.ch

Diskussionsplattform zur e-ID
www.github.com

Anmeldung zum e-ID-Newsletter
www.eid.admin.ch