Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

schweizerische digitale Identität
identité digitale suisse
identità electronica svizzera

# Tech decision & roadmap

Participation meeting 04.07.2024

# Agenda

1 **Technology decision**

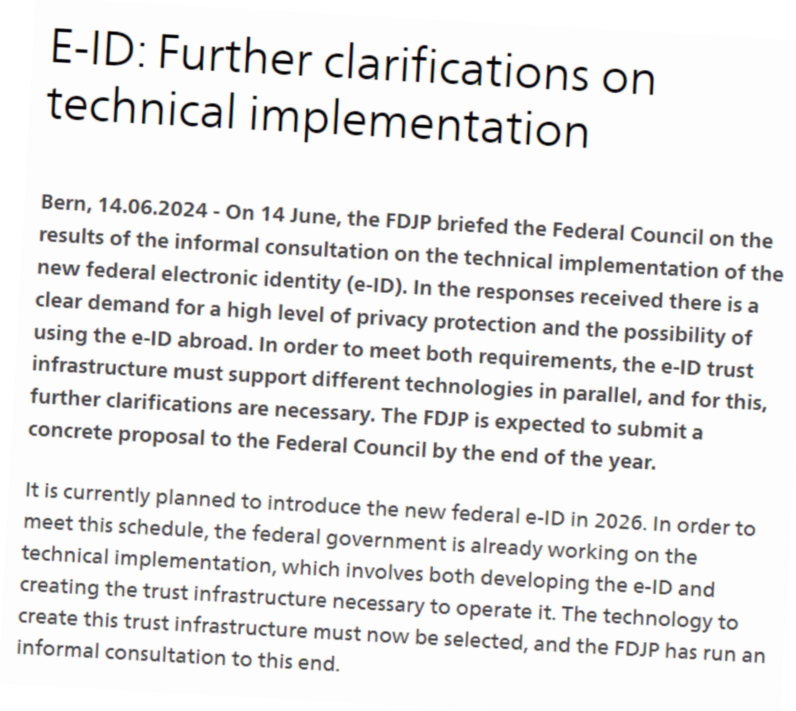
2 **Technology roadmap**

3 **Holder binding**

# Technology decision

# Technology decision

- **Media release** on the technology decision was published on 14.06.2024
- The results of the informal **consultation** were considered: Demand for the **highest** possible **level of privacy protection** and **international interoperability**
- At present, the federal government is not aware of any technology that fulfils both requirements simultaneously
- The FDJP is evaluating a strategy for the trust infrastructure that supports **multiple technologies in parallel**
- This requires **further clarification** - especially regarding the financial impacts
- The FDJP expects to submit a concrete proposal to the Federal Council **before the end of the year**: initial format(s) and cryptography for the e-ID will be defined there



## E-ID: Further clarifications on technical implementation

**Bern, 14.06.2024 - On 14 June, the FDJP briefed the Federal Council on the results of the informal consultation on the technical implementation of the new federal electronic identity (e-ID). In the responses received there is a clear demand for a high level of privacy protection and the possibility of using the e-ID abroad. In order to meet both requirements, the e-ID trust infrastructure must support different technologies in parallel, and for this, further clarifications are necessary. The FDJP is expected to submit a concrete proposal to the Federal Council by the end of the year.**

It is currently planned to introduce the new federal e-ID in 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. The technology to create this trust infrastructure must now be selected, and the FDJP has run an informal consultation to this end.

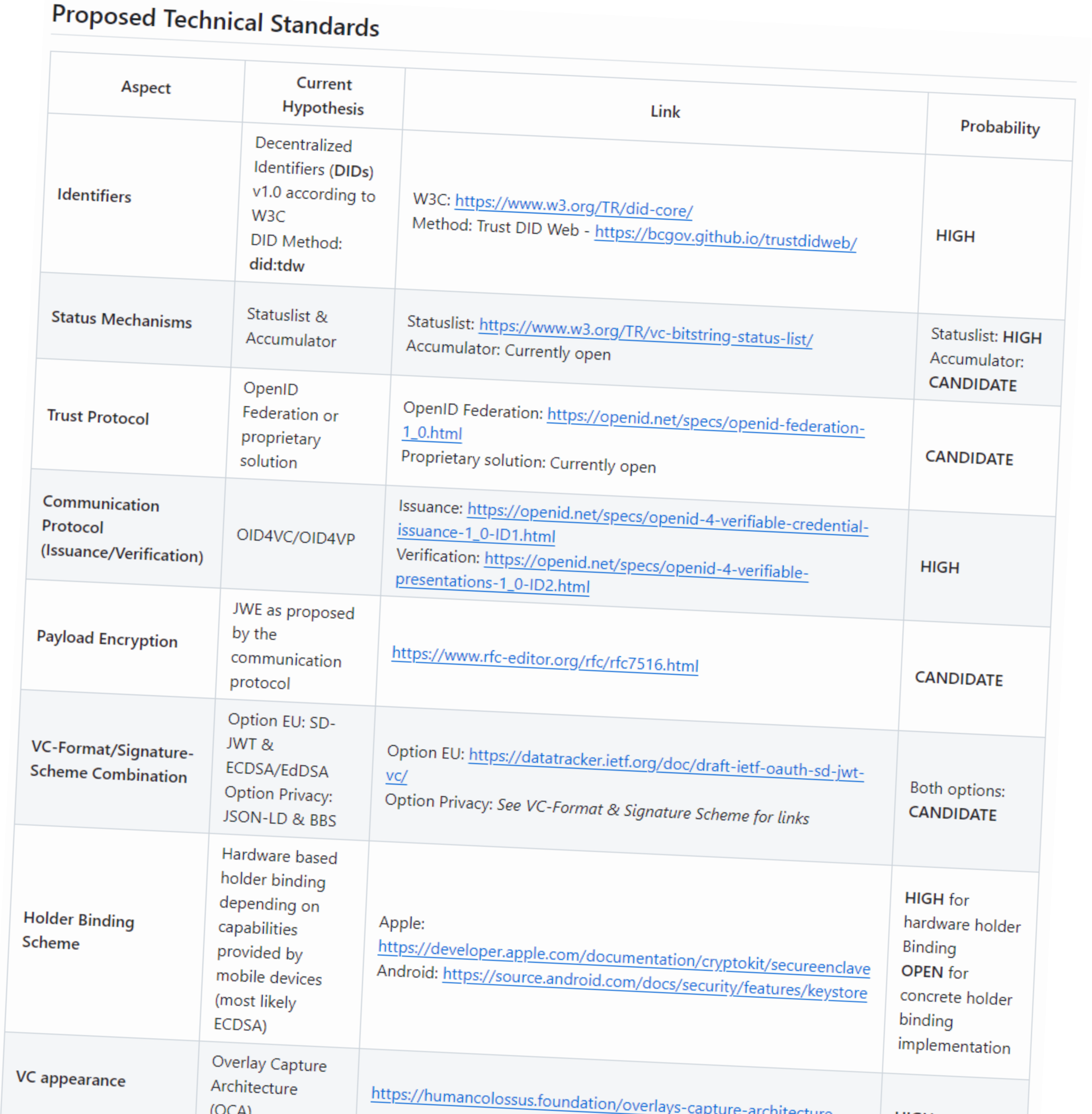
https://www.ejpd.admin.ch/ejpd/en/home/latest-news/mm.msg-id-101414.html

# Tech roadmap

# Tech roadmap

- In the interests of transparency, an **initial tech roadmap** has been published on **GitHub**
- It shows the current **hypothesis (work in progress)** regarding technical **standards** and **formats**
- In case of **new developments,** the document will be **updated**

[https://github.com/admin-ch-ssi/technical-publications-int/blob/main/tech-roadmap.md](https://github.com/admin-ch-ssi/technical-publications-int/blob/main/tech-roadmap.md)



## Proposed Technical Standards

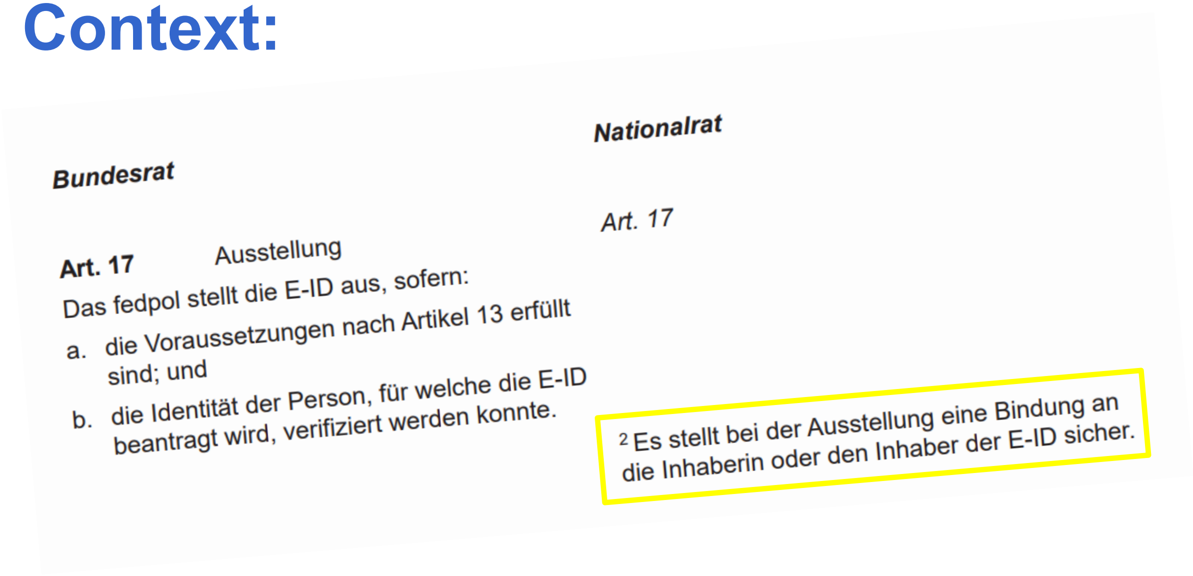
| Aspect | Current Hypothesis | Link | Probability |
|---|---|---|---|
| **Identifiers** | Decentralized Identifiers (**DIDs**) v1.0 according to W3C<br>DID Method: **did:tdw** | W3C: https://www.w3.org/TR/did-core/<br>Method: Trust DID Web - https://bcgov.github.io/trustdidweb/ | HIGH |
| **Status Mechanisms** | Statuslist & Accumulator | Statuslist: https://www.w3.org/TR/vc-bitstring-status-list/<br>Accumulator: Currently open | Statuslist: **HIGH**<br>Accumulator: **CANDIDATE** |
| **Trust Protocol** | OpenID Federation or proprietary solution | OpenID Federation: https://openid.net/specs/openid-federation-1_0.html<br>Proprietary solution: Currently open | **CANDIDATE** |
| **Communication Protocol (Issuance/Verification)** | OID4VC/OID4VP | Issuance: https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0-ID1.html<br>Verification: https://openid.net/specs/openid-4-verifiable-presentations-1_0-ID2.html | **HIGH** |
| **Payload Encryption** | JWE as proposed by the communication protocol | https://www.rfc-editor.org/rfc/rfc7516.html | **CANDIDATE** |
| **VC-Format/Signature-Scheme Combination** | Option EU: SD-JWT & ECDSA/EdDSA<br>Option Privacy: JSON-LD & BBS | Option EU: https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/<br>Option Privacy: *See VC-Format & Signature Scheme for links* | Both options: **CANDIDATE** |
| **Holder Binding Scheme** | Hardware based holder binding depending on capabilities provided by mobile devices (most likely ECDSA) | Apple: https://developer.apple.com/documentation/cryptokit/secureenclave<br>Android: https://source.android.com/docs/security/features/keystore | **HIGH** for hardware holder Binding<br>**OPEN** for concrete holder binding implementation |
| **VC appearance** | Overlay Capture Architecture (OCA) | https://humancolossus.foundation/overlays-capture-architecture | **HIGH** |

Swiss Confederation
**E-ID programme**

# Holder Binding

# Holder Binding

## Context:



| *Bundesrat* | *Nationalrat* |
|---|---|
| **Art. 17** Ausstellung<br>Das fedpol stellt die E-ID aus, sofern:<br>a. die Voraussetzungen nach Artikel 13 erfüllt sind; und<br>b. die Identität der Person, für welche die E-ID beantragt wird, verifiziert werden konnte. | *Art. 17*<br><br>[2] Es stellt bei der Ausstellung eine Bindung an die Inhaberin oder den Inhaber der E-ID sicher. |

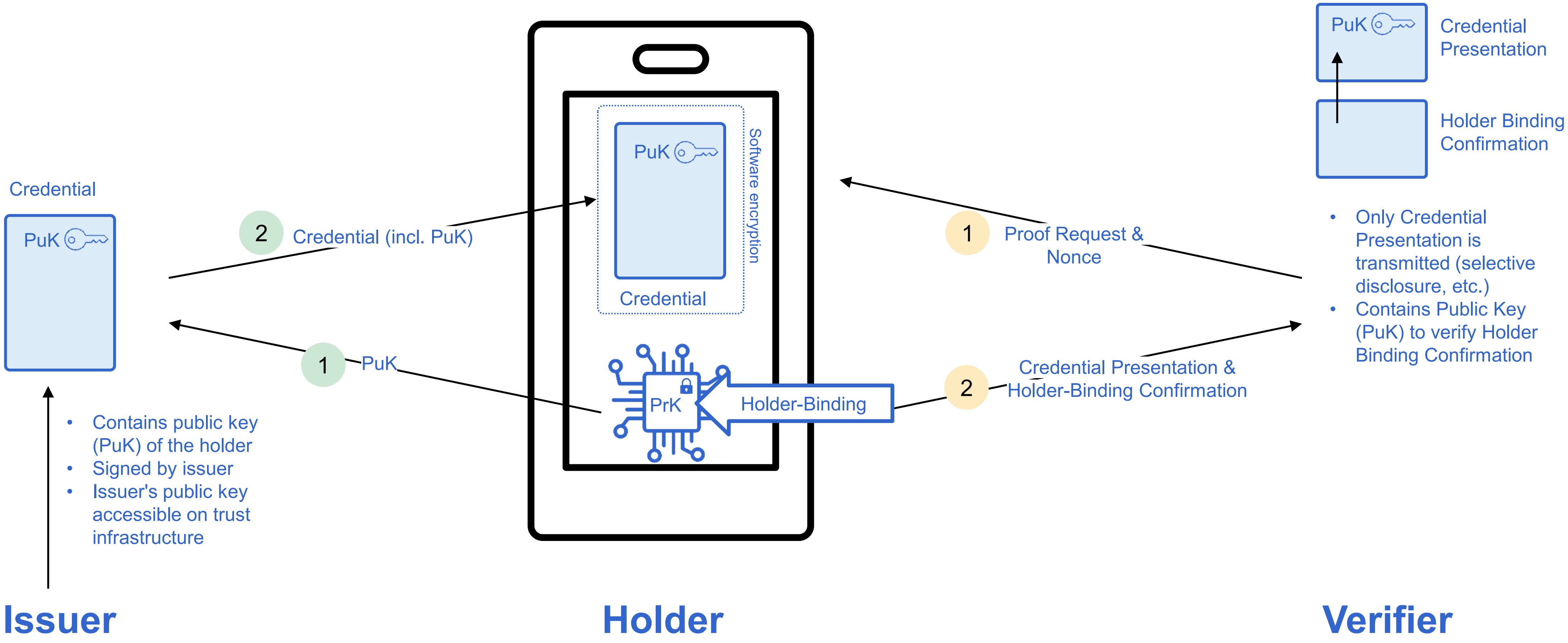
The National Council proposes that binding to the holder must be ensured during e-ID issuance.

https://www.parlament.ch/centers/eparl/curia/2023/20230073/N11%20D.pdf

At the DICE, Federal Councillor Beat Jans addressed the Holder Binding in his welcoming address:

https://www.eid.admin.ch/de/grussbotschaft-von-bundesrat-beat-jans-zur-der-digital-identity-unconference-europe-dice

# Holder Binding



- Contains public key (PuK) of the holder
- Signed by issuer
- Issuer's public key accessible on trust infrastructure

- Only Credential Presentation is transmitted (selective disclosure, etc.)
- Contains Public Key (PuK) to verify Holder Binding Confirmation

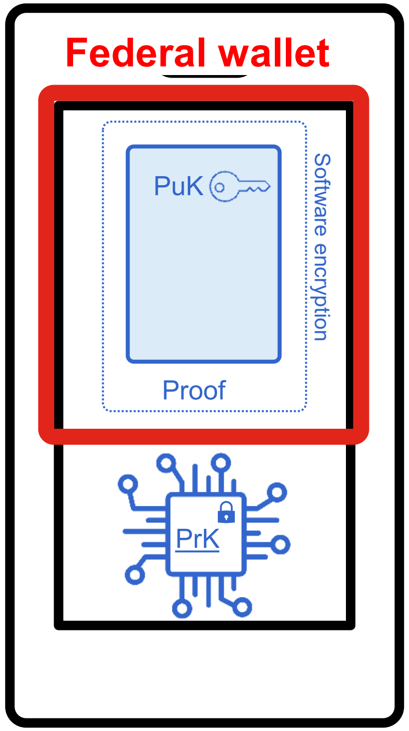
# Holder Binding Implementation

- Widespread distribution of holder binding can most realistically be reached by use of existing **hardware crypto processors on mobile devices (smartphones).** By the generation of hardware backed key pairs before e-ID issuance, the credential can be bound to the mobile device.

- It is apparent that a high level of trustworthiness is required by relevant use cases (EPD, QES etc.) as documented in eCH-0170 (VS 3) - this also postulates binding to hardware.

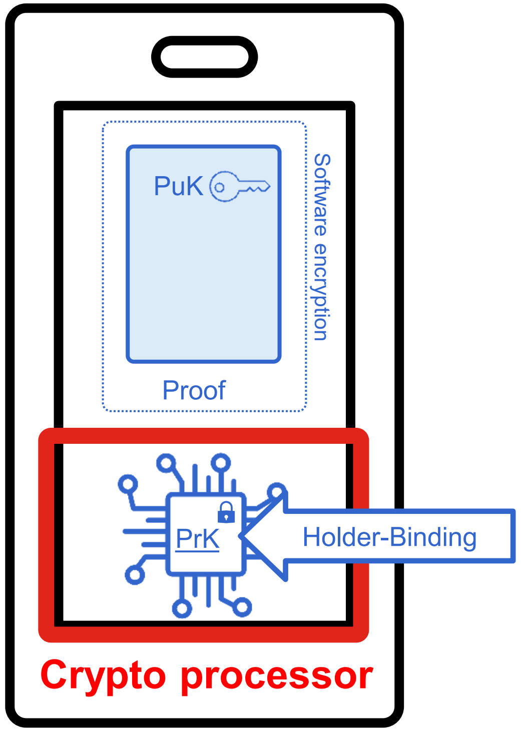
# Holder Binding Implementation: Wallet

- This means that certain measures must be taken when issuing the e-ID with regard to usable mobile devices and applications for obtaining and storing the e-ID:
  - The Legal Affairs Committee of the Council of States proposes that initially **only the Confederation**'s **electronic wallet should be** able to receive and store the e-ID.
  - An opening for certified electronic **wallets from third parties** could follow after the introduction of the system by the Federal Council.



# Holder Binding Implementation : Device

- This means that certain measures must be taken when issuing the e-ID with regard to usable mobile devices and applications for obtaining and storing the e-ID:
  - **Issuing** the e-ID **exclusively** to mobile devices with a built-in **cryptographic processor (Secure Enclave / Trusted Execution Environment)**



# Holder Binding vs. Unlinkability

- The Confederation is aware that there may be a contradiction between **the hardware-based binding of credentials** to mobile devices and the requirement to **ensure the highest possible level of privacy** (unlinkability).

- This is primarily due to the **limited cryptographic functions** that today's mobile devices support on their cryptographic processors (ECDSA: P-256).

- The federal government is evaluating **multiple approaches** to counteract this problem. These are described in more detail under the following link:

  https://github.com/admin-ch-ssi/technical-publications-int/blob/main/tech-roadmap.md#privacy-preserving-holder-binding

# Holder Binding and Digital Inclusion

- From the perspective of digital inclusion, restricting eligible devices is not ideal. It is to be expected that certain devices will have to be excluded. This is the **price of a trustworthy E-ID**.

- Naturally, the aim is to **minimize** this **exclusion as much as possible**. We will evaluate which devices can be accepted in due time.

- Initial discussions have taken place with **telecom providers, OS providers and mobile device manufacturers.** Anyone who has relevant information in this context is invited to contact us.

Photo by Girl with red hat on Unsplash

# Open Wallet Foundation

- As a long-term measure, the Confederation is committed to collaborating on tackling these issues **at an international level.**

- The Confederation is a member of the Governmental Advisory Circle of the **OpenWallet Foundation** (a sub-foundation of the Linux Foundation).

- This body is to be transferred to a multilateral forum unter the roof of the **International Telecommunication Union** (a specialized UN agency).

- One of the aims of this initiative is to promote the distribution of **crypto processors** on mobile devices and their provision as open hardware.