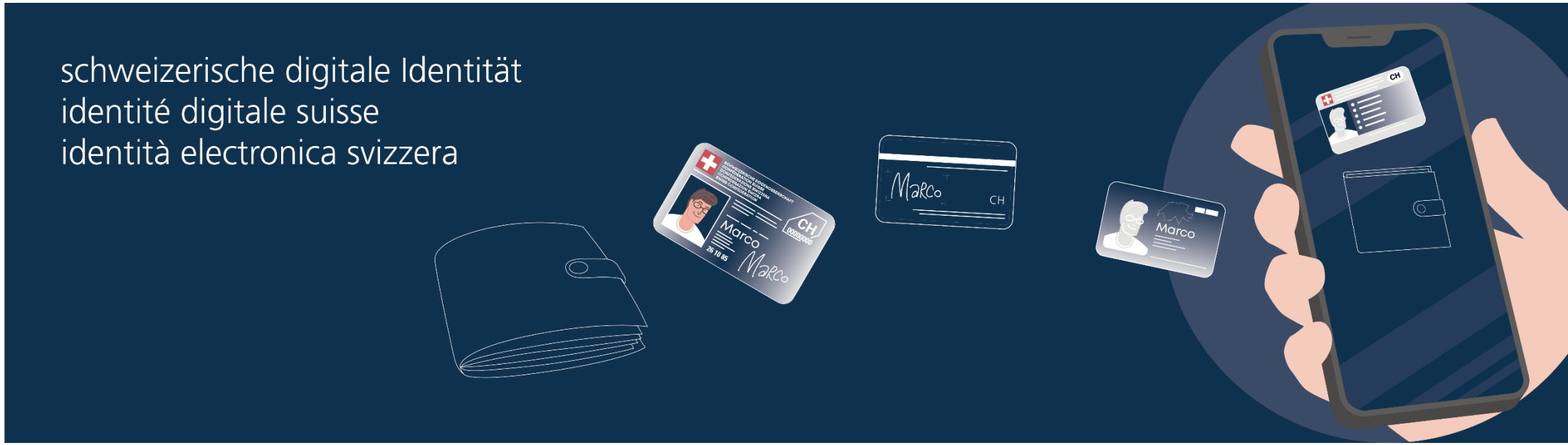
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra



Tech-Entscheid & Roadmap

Partizipationsmeeting 04.07.2024

Agenda

1. Technologie-Entscheid
2. Technologie-Roadmap
3. Bindung an die Inhaberin

Technologie-Entscheid

Technologie-Entscheid

- **Medienmitteilung** zum Technologie-Entscheid wurde am 14.06.2024 publiziert
- Die Ergebnisse der informellen **Konsultation** wurden berücksichtigt: Forderung nach möglichst **hohem Schutz der Privatsphäre** und **internationale Interoperabilität**
- Derzeit ist dem Bund keine Technologie bekannt, welche beide Anforderungen gleichzeitig abdeckt
- Das EJPD evaluiert für die Vertrauensinfrastruktur eine Strategie, welche **mehrere Technologien parallel** unterstützt
- Dazu sind **weitere Abklärungen** – insbesondere finanzielle – **erforderlich**
- Das EJPD wird dem Bundesrat **voraussichtlich vor Jahresende** einen konkreten Vorschlag unterbreiten: initiale Format(e) und Kryptographie für die E-ID werden dort festgelegt

E-ID: weitere Abklärungen zur technischen Umsetzung

Bern, 14.06.2024 - Das EJPD hat den Bundesrat am 14. Juni 2024 über die Ergebnisse der informellen Konsultation zur technischen Umsetzung der neuen elektronischen Identität des Bundes (E-ID) informiert. Die eingegangenen Stellungnahmen zeigen deutlich: die E-ID soll sowohl einen hohen Schutz der Privatsphäre garantieren als auch international verwendet werden können. Um beide Anforderungen zu erfüllen, muss die für die E-ID notwendige Vertrauensinfrastruktur parallel verschiedene Technologien unterstützen. Dazu sind weitere Abklärungen erforderlich. Das EJPD wird dem Bundesrat voraussichtlich vor Jahresende einen konkreten Vorschlag unterbreiten.

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 der E-ID notwendigen Vertrauensinfrastruktur. Hier ist nun zu entscheiden, mit welcher Technologie dieser Aufbau erfolgen soll. Dazu hat das EJPD eine informelle Konsultation durchgeführt.

https://www.ejpd.admin.ch/ejpd/de/home/aktuell/mm.msg-id-101414.html

Tech-Roadmap

Tech-Roadmap

- Im Sinne der Transparenz wurde auf **GitHub** die **initiale Tech-Roadmap** veröffentlicht
- Darin wird die aktuelle **Arbeitshypothese** bezüglich technischer **Standards** und **Formate** festgehalten
- **Neue Erkenntnisse** werden dokumentiert

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 DID Method: **did:tdw**	W3C: https://www.w3.org/TR/did-core/ Method: Trust DID Web - https://bcgov.github.io/trustdidweb/	**HIGH**
Status Mechanisms	Statuslist & Accumulator	Statuslist: https://www.w3.org/TR/vc-bitstring-status-list/ Accumulator: Currently open	Statuslist: **HIGH** Accumulator: **CANDIDATE**
Trust Protocol	OpenID Federation or proprietary solution	OpenID Federation: https://openid.net/specs/openid-federation-1_0.html 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 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 Option Privacy: JSON-LD & BBS	Option EU: https://datatracker.ietf.org/doc/draft-ietf-oauth-sd-jwt-vc/ 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 Android: https://source.android.com/docs/security/features/keystore	**HIGH** for hardware holder Binding **OPEN** for concrete holder binding implementation
VC appearance	Overlay Capture Architecture (OCA)	https://humancolossus.foundation/overlays-capture-architecture	

Bindung an die Inhaberin

Bindung an die Inhaberin (Holder Binding)

Kontext:

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

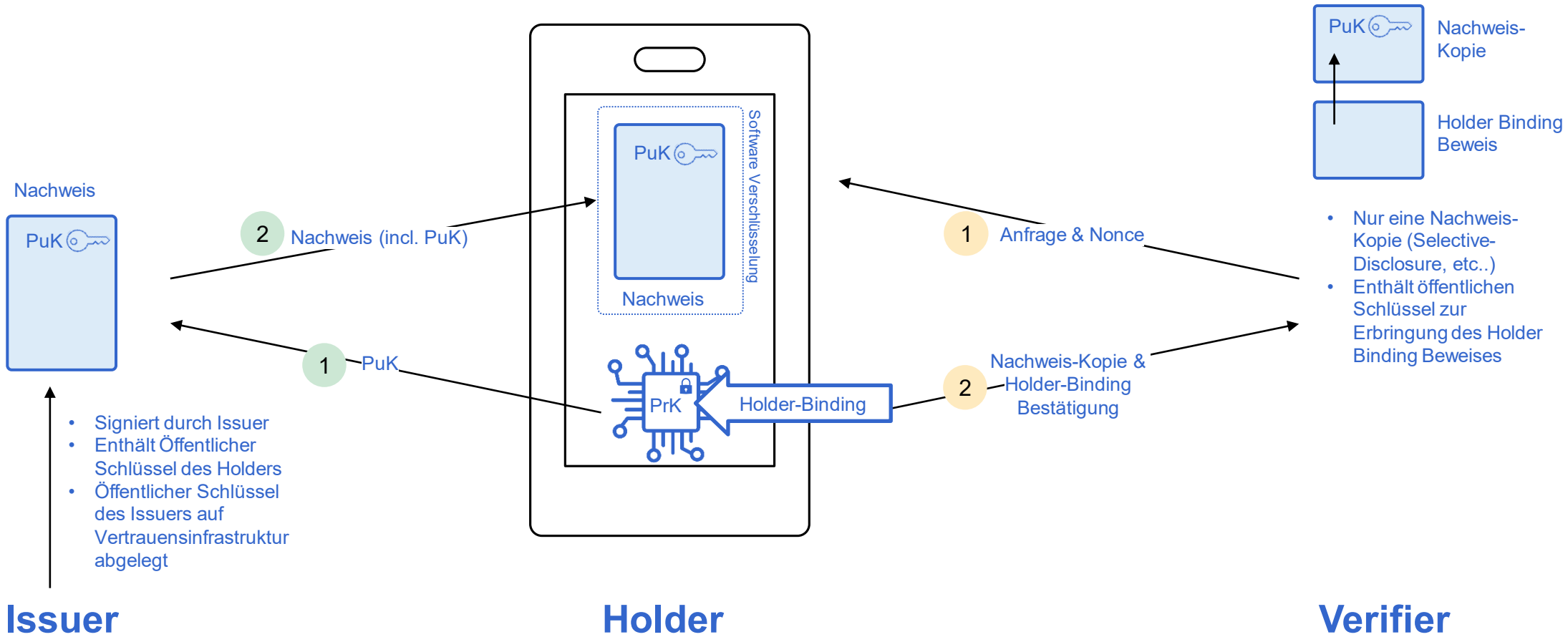
Der Nationalrat hat festgelegt, dass bei der Ausstellung der E-ID eine Bindung an die Inhaberin oder den Inhaber sichergestellt werden muss.

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

Bundesrat Beat Jans ist an der DICE in seinem Grusswort auch auf das Holder Binding eingegangen:

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

Bindung an die Inhaberin (Holder Binding)



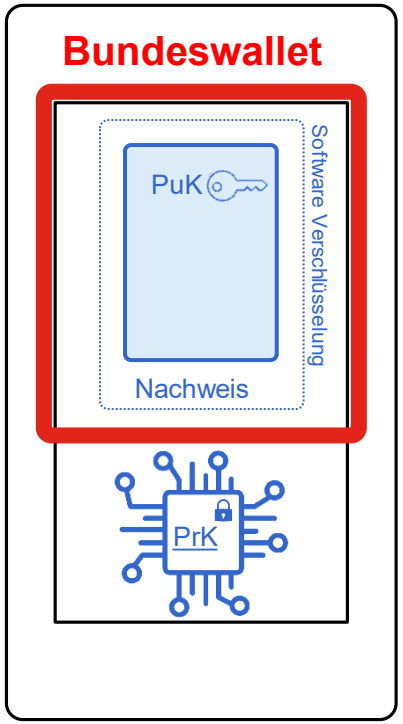
Umsetzung Holder Binding

- Die Umsetzung des Holder Bindings ist anhand der Generierung von Schlüsselpaaren mittels **Hardware Krypto-Prozessoren** am realistischsten. Dabei wird die E-ID an das mobile Endgerät (Smartphone) gebunden.

- Es zeichnet sich ab, dass für Anwendungsfälle, welche hohes Vertrauen benötigen (EPD, QES etc.) VS 3 (eCH-0170) erreicht werden muss – auch dieses postuliert eine Hardware-Bindung.

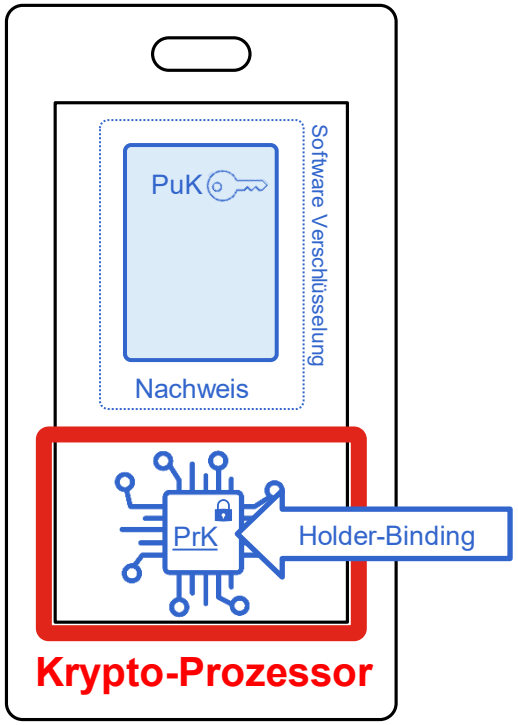
Umsetzung Holder Binding: Wallet

- Das bedeutet, dass bei der Ausstellung gewisse Massnahmen bezüglich nutzbarer mobiler Endgeräte und Applikationen für den Erhalt und die Speicherung der E-ID ergriffen werden müssen:
  - Die Rechtskommission des Ständerrates schlägt vor, dass initial **nur die elektronische Brieftasche** des **Bundes** den Erhalt und die Speicherung der E-ID ermöglicht.
  - Eine Öffnung für zertifizierte elektronische **Brieftaschen von Dritten** könnte nach der Einführung des Systems durch den Bundesrat erfolgen.



Umsetzung Holder Binding: Gerät

- Das bedeutet, dass bei der Ausstellung gewisse Massnahmen bezüglich nutzbarer mobiler Endgeräte und Applikationen für den Erhalt und die Speicherung der E-ID ergriffen werden müssen:
  - **Ausstellung** der E-ID **ausschliesslich** auf mobilen Endgeräte mit eingebautem **Krypto-Prozessor (Secure Enclave / Trusted Execution Environment)**



Holder Binding vs. Unlinkability

- Der Bund ist sich bewusst, dass ein Widerspruch zwischen **Hardware-basierter Bindung** eines Nachweises an ein mobiles Endgerät und der **Wahrung einer möglichst hohen Privatsphäre** (Unlinkability) bestehen kann.

- Dies entsteht primär durch die **limitierten kryptographischen Funktionen**, welche die heutigen mobilen Endgeräte auf ihren Krypto-Prozessoren unterstützen (ECDSA: P256).

- Der Bund evaluiert im Rahmen der E-ID-Umsetzung **unterschiedliche Ansätze**, um dieser Problemstellung entgegenzuwirken. Diese sind unter folgendem Link im Detail beschrieben:

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

Holder Binding und Digitale Inklusion

- Aus Perspektive der digitalen Inklusion ist Einschränkung der Gerätewahl nicht optimal. Es ist zu erwarten, dass Personen ohne entsprechendes Endgerät ausgeschlossen werden müssen. Dies ist der **Preis einer vertrauenswürdigen E-ID**.

- Selbstverständlich wird angestrebt, diesen **Ausschluss so minimal wie möglich** zu halten. Es wird bis zur Inbetriebnahme evaluiert, welche Endgeräte akzeptiert werden können.

- Erste Gespräche mit einigen **Telekommunikations-Providern, OS-Provider und Endgeräte-Herstellern** haben stattgefunden. Wer in diesem Zusammenhang über relevante Informationen verfügt, ist gebeten, mit uns in Kontakt zu treten.

Photo by Girl with red hat on Unsplash

Open Wallet Foundation

- Als langfristige Massnahme engagiert sich der Bund auf **internationaler Ebene**, um diese Themen vorwärtszutreiben.
- Der Bund ist Mitglied des Governmental Advisory Circle der der **OpenWallet Foundation** (Unterstiftung der Linux Foundation).
- Dieses Gefäss soll unter der Schirmherrschaft der **Internationale Fernmeldeunion** (Sonderorganisation der UNO) in ein multilaterales Forum übertragen werden.
- Unter anderem soll in diesem Rahmen die Verbreitung von **Krypto-Prozessoren** auf mobilen Endgeräten und deren Bereitstellung als offene Hardware gefördert werden.