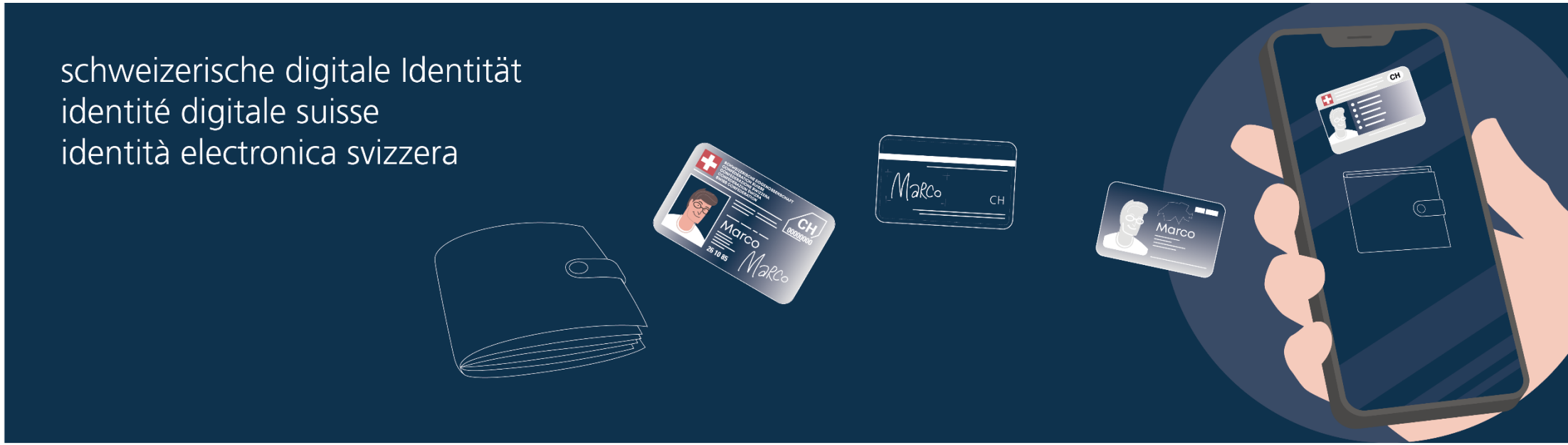
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra



Décision tech & roadmap

Réunion participative 04.07.2024

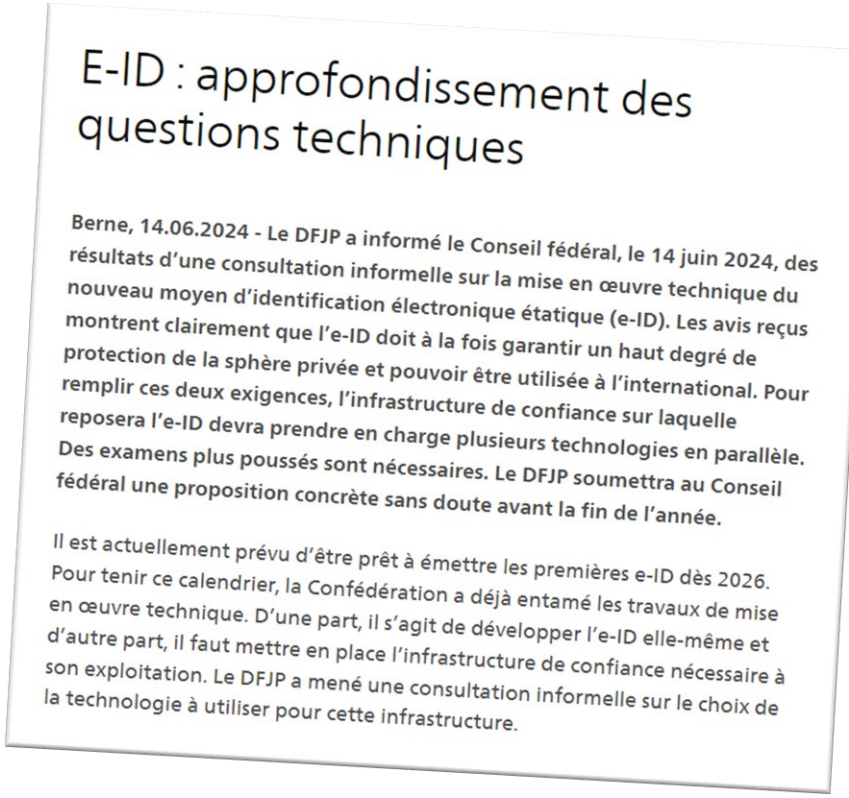
Agenda

1. Décision sur la technologie
2. Roadmap de la technologie
3. Liaison avec la ou le titulaire (holder binding)

Décision technologique

Décision technologique

- **Communiqué de presse** sur la décision technologique a été publié le 14.06.2024
- Il a été précédé d'une **consultation** informelle : **Une protection** maximale **de la vie privée** et l'**interopérabilité internationale** restent des exigences fortes.
- Actuellement, la Confédération ne connaît aucune technologie qui couvre les deux exigences en même temps.
- Le DFJP évalue une stratégie pour l'infrastructure de confiance qui doit soutenir **plusieurs technologies en parallèle**.
- Pour mieux comprendre les conséquences possibles, il est nécessaire de **procéder à des clarifications supplémentaires** (en particulier financières).
- Le DFJP soumettra probablement une proposition concrète au Conseil fédéral avant la fin de l'année: le(s) format(s) initial(aux) et la cryptographie de l'**e-ID** y seront définis



E-ID : approfondissement des questions techniques

Berne, 14.06.2024 - Le DFJP a informé le Conseil fédéral, le 14 juin 2024, des résultats d'une consultation informelle sur la mise en œuvre technique du nouveau moyen d'identification électronique étatique (e-ID). Les avis reçus montrent clairement que l'e-ID doit à la fois garantir un haut degré de protection de la sphère privée et pouvoir être utilisée à l'international. Pour remplir ces deux exigences, l'infrastructure de confiance sur laquelle reposera l'e-ID devra prendre en charge plusieurs technologies en parallèle. Des examens plus poussés sont nécessaires. Le DFJP soumettra au Conseil fédéral une proposition concrète sans doute avant la fin de l'année.

Il est actuellement prévu d'être prêt à émettre les premières e-ID dès 2026. Pour tenir ce calendrier, la Confédération a déjà entamé les travaux de mise en œuvre technique. D'une part, il s'agit de développer l'e-ID elle-même et d'autre part, il faut mettre en place l'infrastructure de confiance nécessaire à son exploitation. Le DFJP a mené une consultation informelle sur le choix de la technologie à utiliser pour cette infrastructure.

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

Roadmap de la technologie

Roadmap

- Dans un souci de transparence, une **feuille de route préliminaire de la technologie** a été publiée sur **GitHub.**
- **Les hypothèses de travail** actuelles concernant les **normes** techniques et **les formats** y sont consignées.
- Les **nouvelles constatations** seront documentées

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	

Lien entre la titulaire et l’e-ID (Holder Binding)

Lien entre la titulaire et l’e-ID (Holder Binding)

Contexte :

Conseil fédéral	Conseil national
	Art. 17
Art. 17 Émission	
fedpol émet l’e-ID si:	
a. les conditions visées à l’art. 13 sont remplies, et que	
b. l’identité de la personne pour qui l’e-ID est demandée a pu être vérifiée.	
	2 Lors de l’émission, il établit un lien entre l’e-ID et son titulaire.

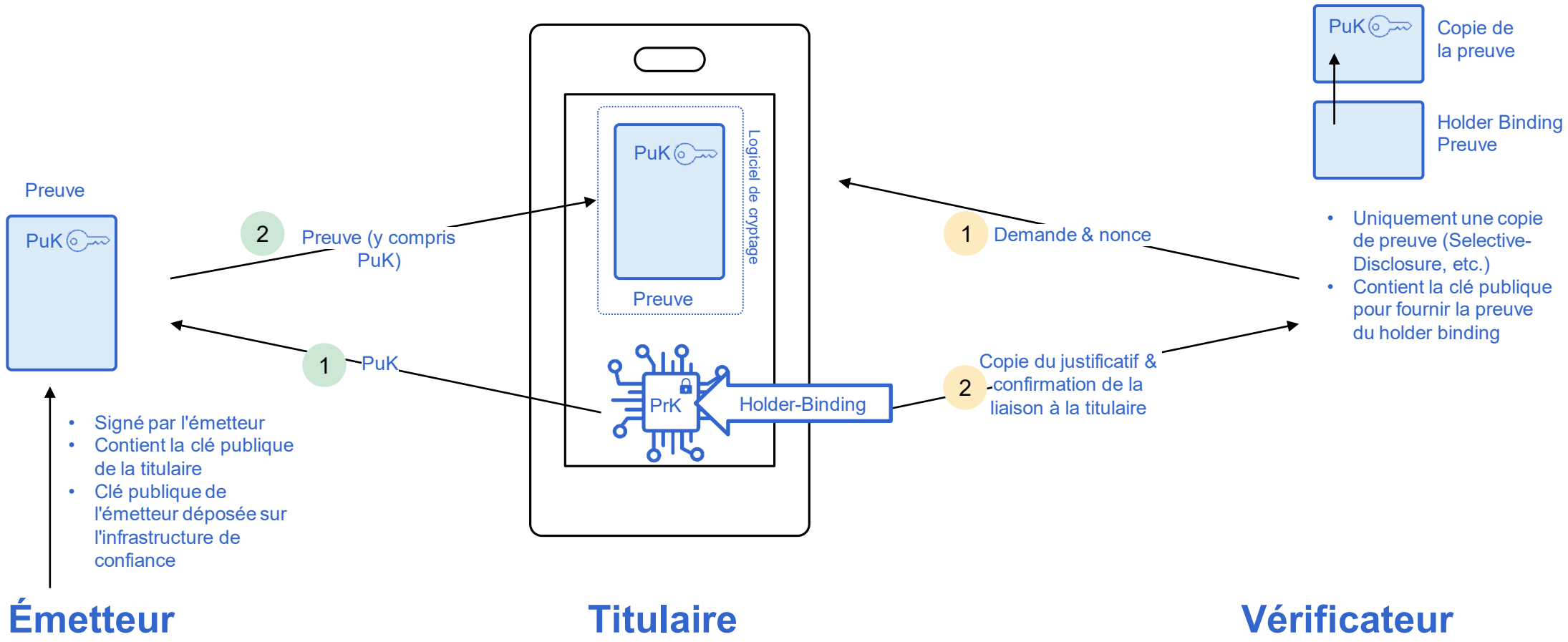
Le Conseil national a établi qu'il fallait garantir un lien avec le titulaire lors de la délivrance de l’e-ID.

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

Lors de la DICE, le conseiller fédéral Beat Jans a expliqué les conséquences dans son discours de bienvenue :

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

Lien entre la titulaire et l'e-ID (Holder Binding)



Mise en œuvre du Holder Binding

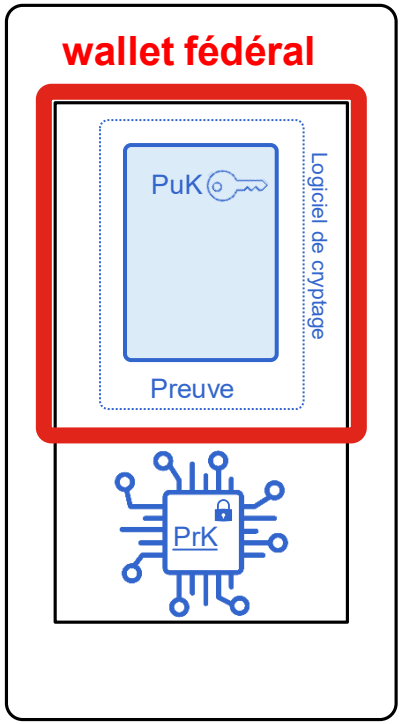
- Une mise en œuvre à grande échelle est plus réaliste si l'on génère des paires de clés au moyen de **processeurs cryptographiques de hardwares**. Dans ce cas, l'e-ID est liée à un terminal mobile, soit à un téléphone portable.

- Il apparaît que pour les cas d'application qui nécessitent une confiance de haute qualité (AGOV aq500, dossier médical du patient, etc...), le VS 3 (eCH-0170) doit être atteint - celui-ci propose également une liaison au hardware.

Mise en œuvre du Holder Binding: Wallet

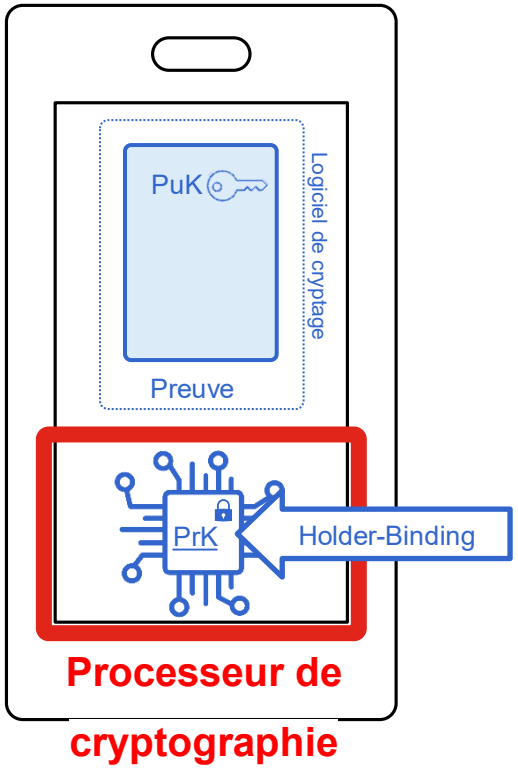
- Cela signifie que lors de l'émission, certaines mesures doivent être prises concernant les terminaux mobiles utilisables et les applications pour l'obtention et le stockage de l'e-ID :

  - La Commission juridique du Conseil des Etats propose que, initialement, seul le **portefeuille électronique de la Confédération** permette l'obtention et le enregistrement de l'E-ID.
  - Une ouverture aux **portefeuilles électroniques** certifiés **de tiers** pourrait avoir lieu après l'introduction du système par le Conseil fédéral.



Mise en œuvre du Holder Binding: Terminaux mobiles

- Cela signifie que lors de l'émission, certaines mesures doivent être prises concernant les terminaux mobiles utilisables et les applications pour l'obtention et le stockage de l'e-ID :
  - **L'émission** de l'e-ID se fera **exclusivement** aux terminaux mobiles avec **processeur cryptographique intégré (Secure Enclave / Trusted Execution Environment)**



Holder Binding vs. Unlinkability

- La Confédération est consciente qu'il peut y avoir une contradiction **entre un lien matériel (hardware) d'une preuve électronique** à un terminal mobile et la **préservation d'un maximum de sphère privée** (unlinkability).

- Cela est dû en premier lieu aux **fonctions cryptographiques limitées** que les terminaux mobiles actuels supportent sur leurs processeurs cryptographiques (ECDSA : P256).

- Dans le cadre de la mise en œuvre de l'e-ID, la Confédération met en **lumière différentes approches** pour contrer la problématique. Celles-ci sont présentées sous le lien suivant :

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

Holder Binding et inclusion numérique

- Du point de vue de l'inclusion numérique, cette évolution n'est pas optimale. Il n'est pas exclu que des personnes ne disposant pas d‘un téléphone portable adéquat soient exclues. En fin de compte, les mesures décrites visent à garantir **la fiabilité de l‘e-ID**.

- Il va de soi que l'on s'efforcera de **réduire au maximum cette exclusion**. Il sera évalué jusqu'à la mise en service quels terminaux seront acceptés.

- Les premiers entretiens avec certains fournisseurs de services de **télécommunication, fournisseurs d'OS et fabricants de téléphones portables** ont eu lieu. Si vous avez des informations pertinentes, n'hésitez pas à prendre contact avec nous.

Photo by Girl with red hat on Unsplash

Open Wallet Foundation

- Comme mesure à long terme, la Confédération s'engage au **niveau international** pour faire avancer ces thèmes.
- La Confédération est membre du Governmental Advisory Circle de l'**OpenWallet Foundation** (sous-fondation de la Linux Foundation).
- Ce forum doit être transformé en forum multilatéral sous l'égide de l'**Union internationale des télécommunications** (agence spécialisée de l'ONU).
- Il s'agit entre autres de promouvoir dans ce cadre la diffusion de **processeurs cryptographiques** sur les terminaux mobiles et leur mise à disposition en tant que hardware ouvert.