

Réunion de participation

Identité électronique et
infrastructure de confiance

08.05.2025

La version allemande
est disponible sur
GitHub.

La version anglaise
est disponible sur
GitHub.

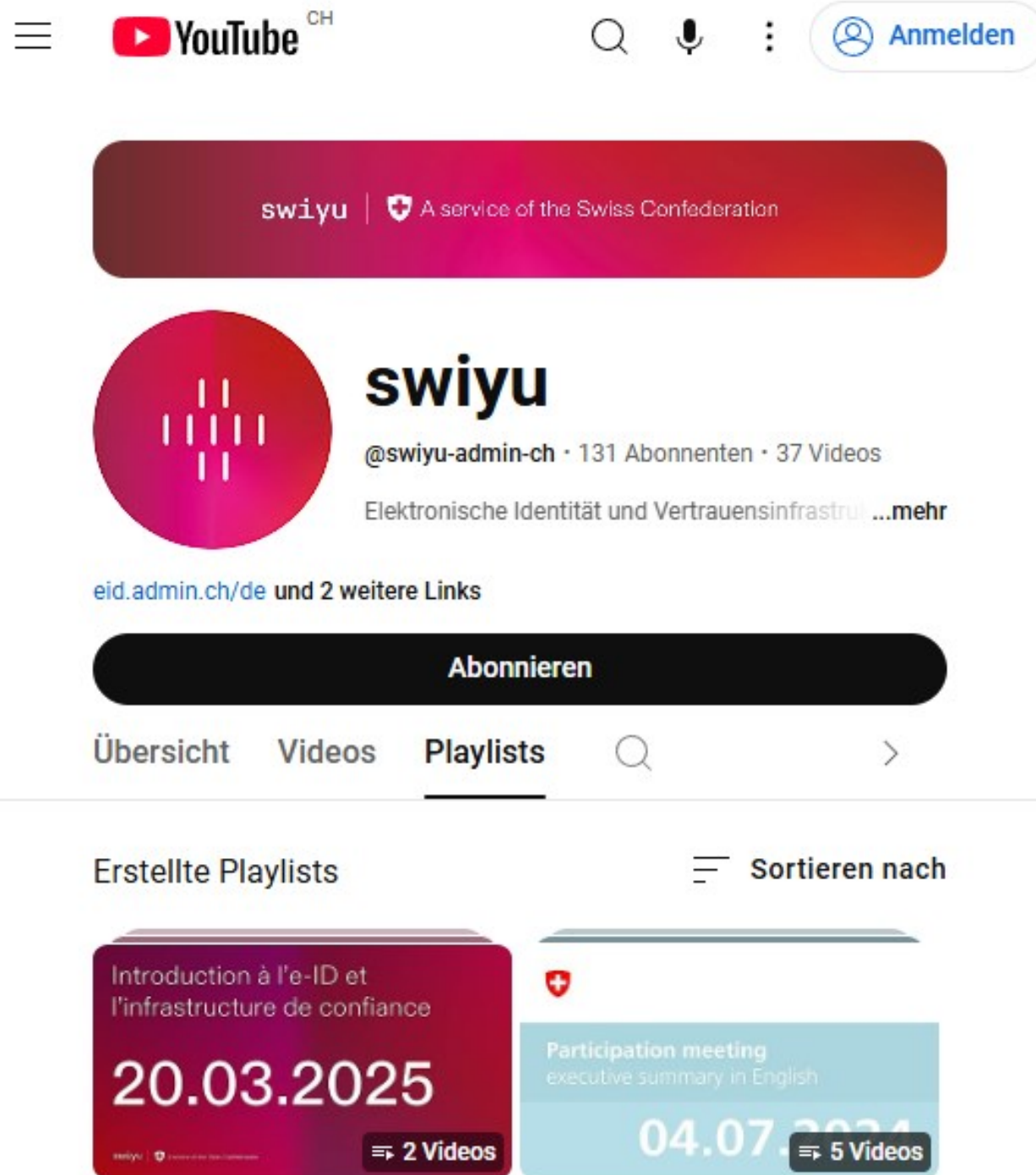


Contenu

- Accueil
- Postes vacants
- Global Collaboration on Wallets and Credentials
- Législation – Situation actuelle et perspectives
- Public Beta
 - Situation actuelle et perspectives
 - Premières réactions du secteur privé
 - Tests utilisateurs
- Non-traçabilité : Émission par lots et concept de clé de renouvellement
- Questions du public
- Résumé en anglais (18 h)


Enregistrement


La réunion participative est enregistrée et publiée sur YouTube.



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'.



YouTube^{CH}


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**

Questions et réponses

- Veuillez utiliser notre offre d'information !
 - www.eid.admin.ch
 - <https://www.youtube.com/@swiyu-admin-ch>
 - <https://github.com/swiyu-admin-ch>
- Veuillez poser vos questions spécifiques via le chat - vous recevrez une réponse via le chat.
- Veuillez poser les questions qui intéressent tout le monde via le microphone.
- Nous n'avons pas de discussions politiques ici.

Postes vacants

Le sous-domaine e-ID recherche du nouveau personnel

- Consultant TIC spécialisé en marketing de l'écosystème e-ID
- Consultant TIC en intégration de l'écosystème e-ID
- Consultant TIC en veille technologique et interopérabilité

[Pour plus d'informations et pour postuler, rendez-vous sur \[www.stelle.admin.ch\]\(http://www.stelle.admin.ch\)](http://www.stelle.admin.ch)

Global 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

Informations sur la conférence

Programme

- 1^{er} juillet : aperçu géographique et sectoriel en plénière
- 2 juillet : analyses approfondies en parallèle dans 15 salles différentes
- La langue de la conférence est l'anglais.

Participation

- La participation est gratuite
- Inscription sur www.lu.ma/gc25 via DIDAS ou Digital Society

Législation

Situation actuelle et perspectives

Loi sur l'e-ID: référendum a abouti

- Dans le délai référendaire, 55 683 signatures ont été déposées contre la loi fédérale du 20 décembre 2024 sur l'identité électronique et d'autres moyens de preuves électroniques (loi sur l'e-ID, LeID). La Chancellerie fédérale a constaté, après vérification, que 55 344 des signatures déposées sont valables.
- Le référendum a donc formellement abouti.
- Le Conseil fédéral doit déterminer les objets soumis à votation au moins quatre mois avant la date du scrutin.
- Les prochaines dates de votation sont le 28 septembre et le 30 novembre 2025.

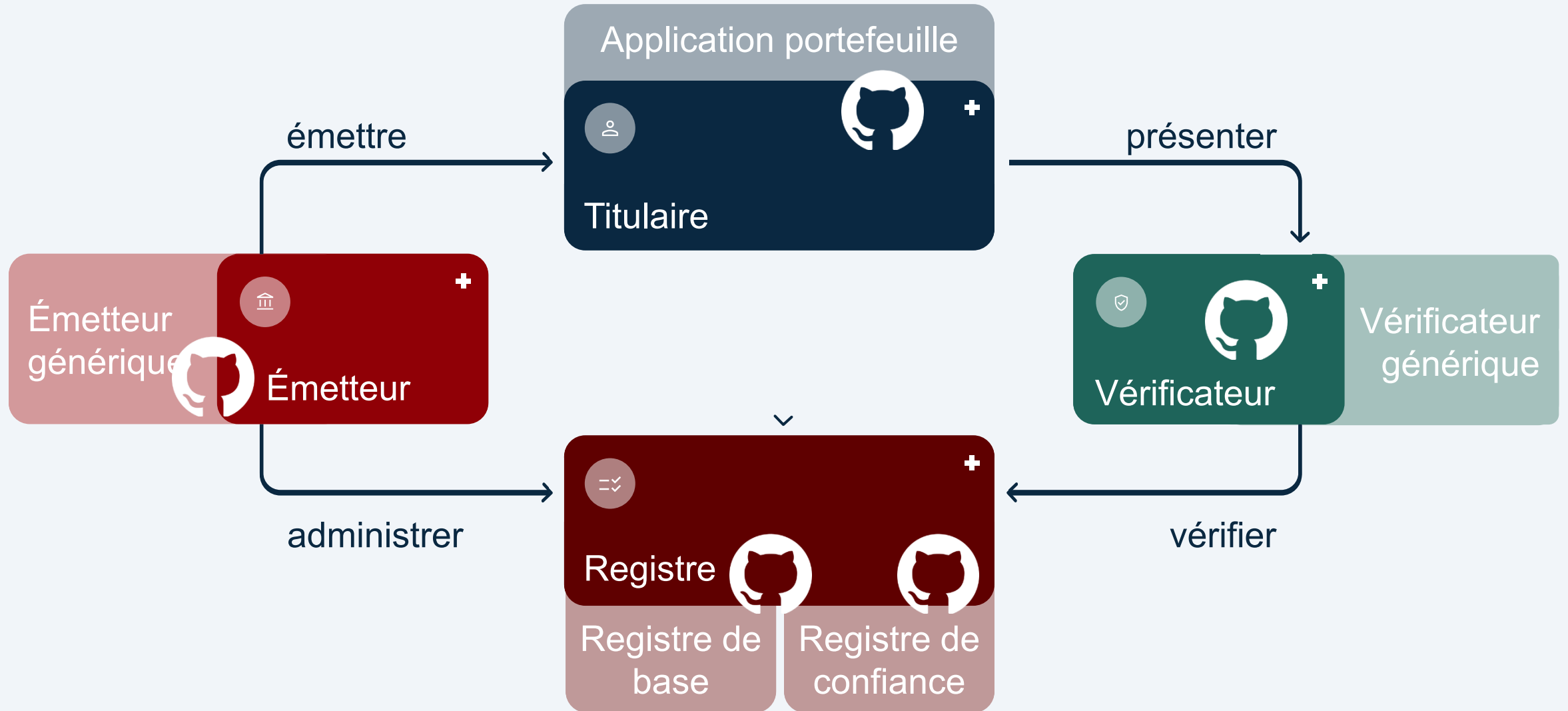
Consultation relative à l'ordonnance

- Les travaux relatifs à l'ordonnance avancent comme prévu.
- La consultation relative à l'ordonnance devrait être ouverte avant la pause estivale.

Public Beta

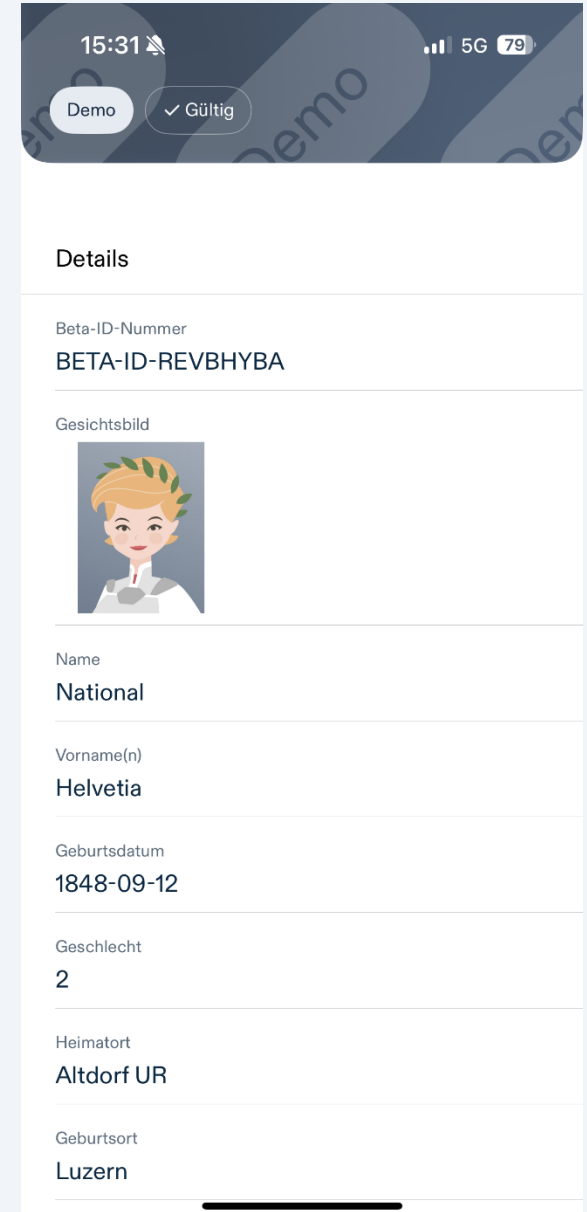
Situation actuelle et perspectives

Composants de la Public Beta



Beta-ID

- Les champs de données sont identiques aux champs de données de l'e-ID :
 - Prénom(s), nom de famille, date de naissance, plus de 16/18/65 ans, nationalité, numéro AVS, etc.
 - De même que les autres données telles que : Numéro de document, Type de processus de vérification, Valable jusqu'au, etc.
- Le format de la Beta-ID est un SD-JWT, selon la définition dans le swiss-profile (GitHub)
- Le verrouillage du titulaire est possible (au matériel, ou sinon par logiciel)
- Les utilisateurs peuvent définir eux-mêmes le contenu.




15:31 5G 79%

Demo ✓ Gültig

Details

Beta-ID-Nummer
BETA-ID-REVBHYBA

Gesichtsbild


Name
National

Vorname(n)
Helvetia

Geburtsdatum
1848-09-12

Geschlecht
2

Heimatort
Altdorf UR

Geburtsort
Luzern

Premiers chiffres concernant la Public Beta

Utilisateurs

- Téléchargements swiyu : +11 000
- Délivrances de Beta ID : +9 000
- Liens pour une vérifications : +5 000
- Vérifications : +1 500
- Révocations : +350
- Business-Partner au e-Portal : +125
- Entrées dans le registre de confiance : 16

Infrastructure

- Utilisation du CPU : moins de 2 %

GitHub

- Vérificateur générique : +450 téléchargements des images Docker
- Émetteur générique : +600 téléchargements des images Docker
- Problèmes et demandes différents dans le forum de discussion : +30

Public Beta

Premières réactions du secteur privé

Public Beta

Test utilisateur

e-ID non-traçable

Émission par lots et concept de clé
de renouvellement

Situation initiale

Qu'est-ce que la non-traçabilité ?

- L'impossibilité d'établir un lien entre **différentes transactions** effectuées avec une e-ID.
- Il s'agit de déterminer s'il est possible **de savoir ce qu'une personne fait avec sa e-ID** (profilage).
- Cela peut se faire à l'aide des **contenus**, **les métadonnées** générées lors de l'établissement de la communication ou des **données cryptographiques**
- [Article de blog sur la non-traçabilité](#)




Possibilité de relier le contenu de l'e-ID

✓ Valide

Détails

Photo



Nom

Schweizer Sample

Prénom(s)

Helvetia

Date de naissance

01.08.1995

Lieu de naissance

Berne

Lieu d'origine

Berne

Nationalité

Suisse

Genre

Contenu transmis

- Schweizer Sample
- Helvetia
- 01.08.1995

Données techniques

(pertinent pour la non-traçabilité)

- Signature de l'émetteur du VC
- Disclosures (Salted/Hashed Claims)
- Clé publique du détenteur
- Informations sur la révocation


Verifier

Possibilité de relier les données techn. de l'e-ID

✓ Valide

Détails

Photo



Nom

Schweizer Sample

Prénom(s)

Helvetia

Date de naissance

01. 08.1995

Lieu de naissance

Berne

Lieu d'origine

Berne

Nationalité

Suisse

Genre

Contenu transmis

- plus de 18 ans

Données techniques

(pertinent pour la non-traçabilité)

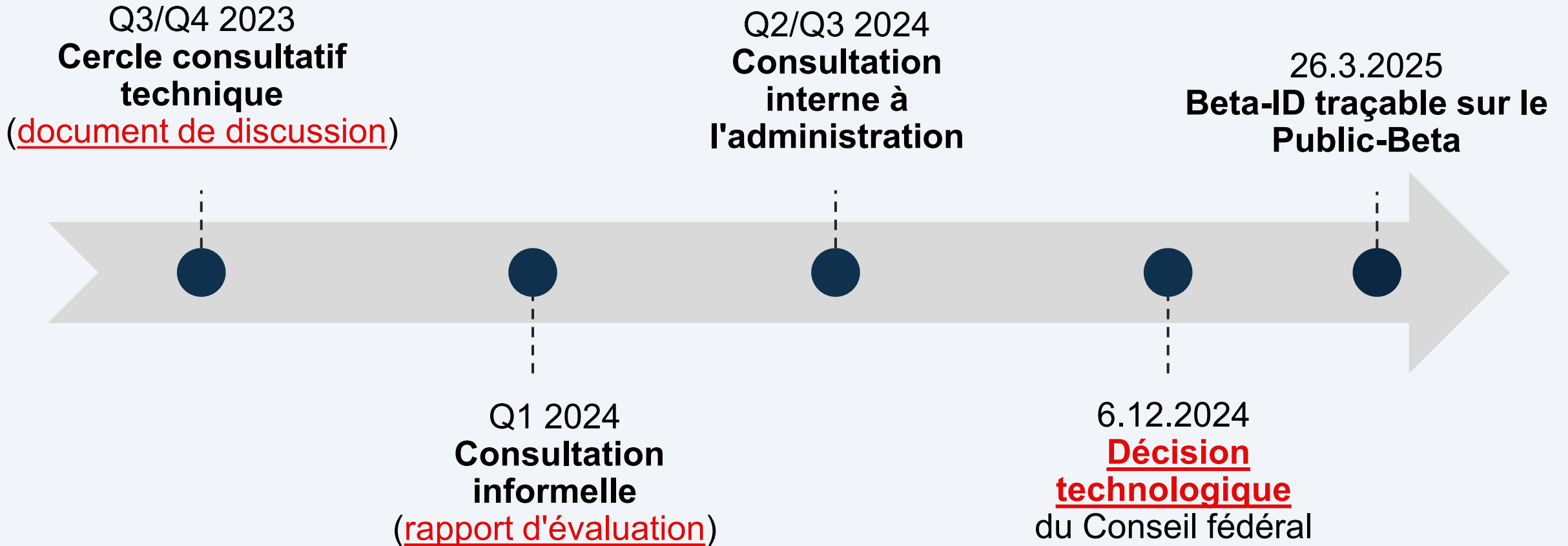
- Signature de l'émetteur du VC
- Disclosures (Salted/Hashed Claims)
- Clé publique du détenteur
- Informations sur la révocation

Même si les SD-JWT ne peuvent pas être reliés cryptographiquement, **les métadonnées** pourraient être utilisées abusivement pour établir des **liens**.

Les utilisateurs du portefeuille peuvent en outre éviter activement le fingerprinting et la corrélation IP.

Verifier

Rétrospective de la non-traçabilité dans le programme e-ID



Décision technologique décembre 2024

- **L'e-ID** doit être introduit le plus rapidement possible
- **L'e-ID** doit être le plus rapidement possible **non-traçable avec d'autres données**
- L'introduction de l'**e-ID** n'est **pas** liée à la **mise en œuvre** de la non-traçabilité
- **Des moyens dédiés et une équipe** sont engagés pour faire avancer le sujet.



The screenshot shows a news article from the 'News Service Bund' (Le portail du Gouvernement suisse). The article is dated 'Publié le 6 décembre 2024' and is titled 'E-ID : le Conseil fédéral prend une décision sur la technologie'. The text states that on December 6, 2024, the Federal Council decided on the technical principles for the implementation of the new electronic identity proof of the Confederation (e-ID). The implementation will be in two stages. The name of the confidence infrastructure to be implemented has also been fixed: the electronic wallet of the Confederation will be called SWIYU. A second paragraph mentions that the launch of e-ID is planned for 2026, and the Confederation is already in full technical preparation to ensure this timeline, with one part developing e-ID itself and another part setting up the necessary confidence infrastructure for its operation.

Toutes les autorités fédérales FR

News Service Bund
Le portail du Gouvernement suisse

Publié le 6 décembre 2024

E-ID : le Conseil fédéral prend une décision sur la technologie

Berne, 6.12.2024 - Lors de sa séance du 6 décembre 2024, le Conseil fédéral a arrêté les principes de la mise œuvre, sur le plan technique, de la nouvelle preuve d'identité électronique de la Confédération (l'e-ID). La réalisation se fera en deux étapes. Le nom de l'infrastructure de confiance a également été fixé : le portefeuille électronique de la Confédération s'appellera SWIYU.

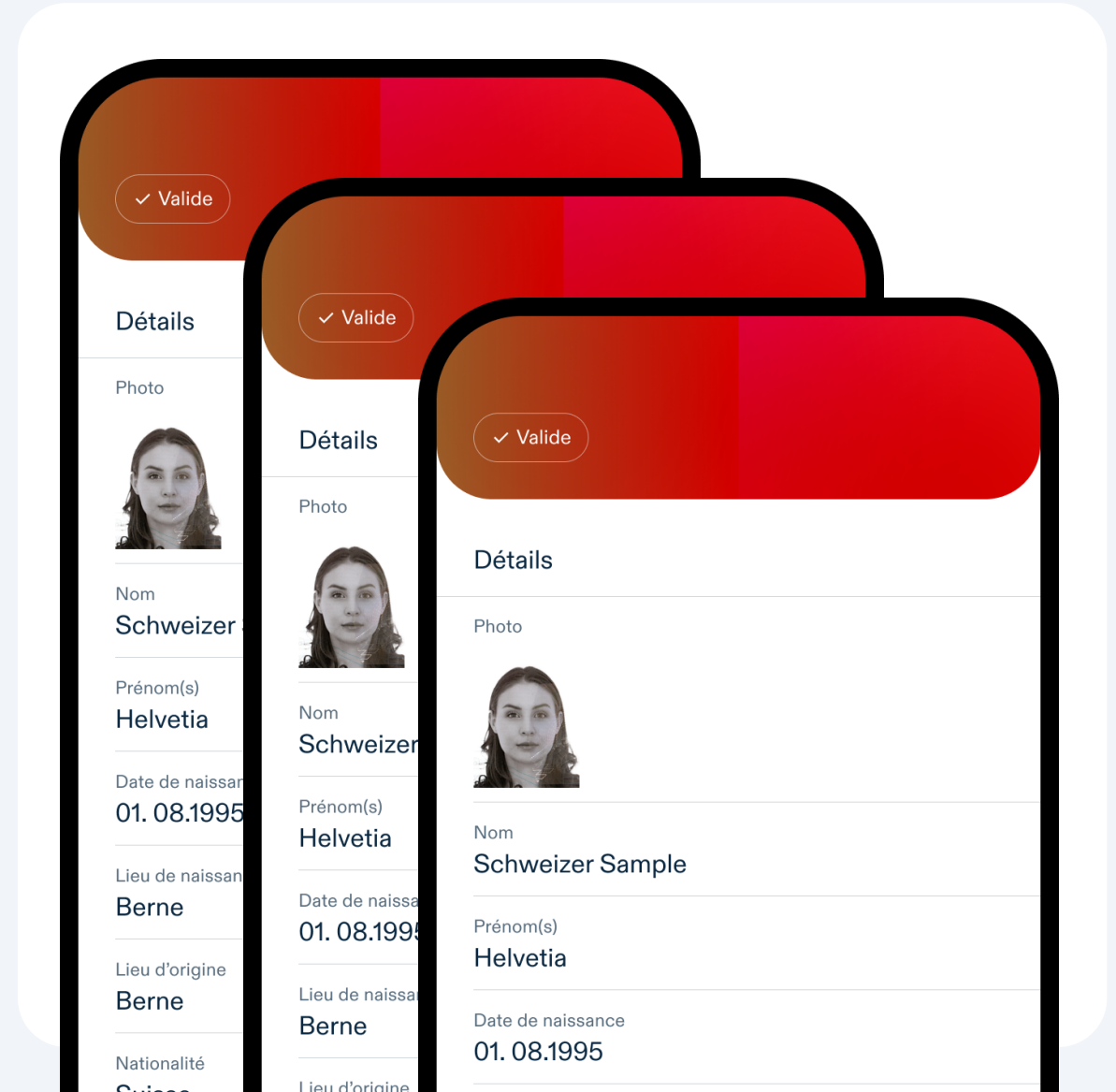
Le lancement de l'e-ID est prévu pour 2026. La Confédération est déjà en pleins préparatifs de sa réalisation technique, afin de pouvoir tenir ce calendrier. Il s'agit d'une part de développer l'e-ID elle-même, d'autre part de mettre sur pied l'infrastructure de confiance nécessaire à son exploitation. Lors de sa séance du 6 décembre 2024, le Conseil fédéral a arrêté les principes de la mise en œuvre sur le plan technique.

Go-Live e-ID 2026

Dès le lancement : e-ID non-traçable grâce à l'émission par lots

L'émission de plusieurs VC d'apparence identique (Batch-Issuance) permet l'impossibilité de liaison cryptographique **dès l'introduction** de l'e-ID.

! Il n'est pas possible d'empêcher la mise en relation sur la base d'attributs présentés ou de métadonnées produites.



Points clés des VC e-ID en émission par lots



Validité de l'e-ID-VC : Validité du document d'identité sous-jacent ou 5 ans maximum



Taille du lot : 25 e-ID-VC par lot



Utilisation de VC par lots :

- Utilisation unique, obtention automatisée d'e-ID-VCs supplémentaires après consentement
- Utilisation aléatoire, en cas de refus de consentement ou d'échec du renouvellement



Obtention d'un nouveaux lots :

S'il reste 2 justificatifs non utilisés dans le portefeuille



Révocation :

L'obtention d'un nouveau lot n'entraîne pas la révocation → seule une nouvelle demande d'e-ID réussie entraîne la révocation de tous les e-ID-VCs. Si possible, révoquer les e-ID de plusieurs personnes de manière groupée (révocation par troupeau)

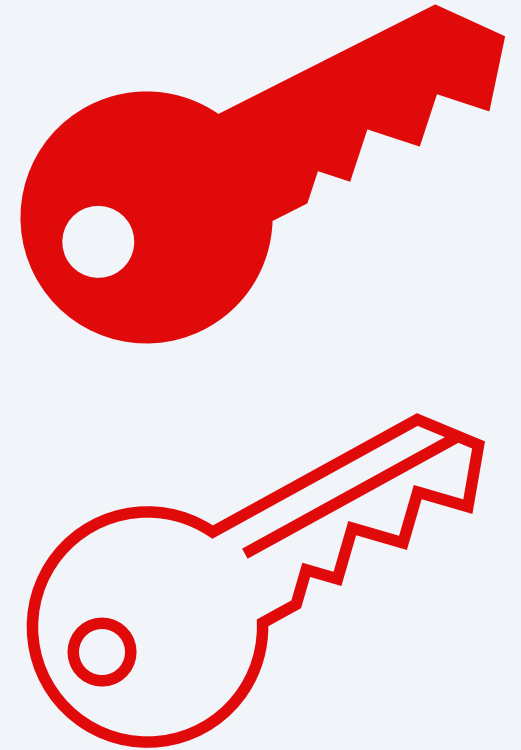
Concept de clé de renouvellement

Liaison avec le titulaire

- Lorsque les e-ID-VCs sont "consommés", le titulaire ou le portefeuille doit pouvoir **obtenir un nouveau lot**.
- Cela signifie qu'il faut à nouveau **établir** une **connexion sécurisée** entre le portefeuille et l'émetteur de l'e-ID (fedpol).
- Lors de la première délivrance de l'e-ID, l'**identification de la personne** (en ligne ou au guichet) est un élément important pour garantir la liaison avec le bon titulaire.
- Le **concept de clé de renouvellement** permet de récupérer de nouveaux e-ID VC tout en conservant un lien sécurisé avec le titulaire.

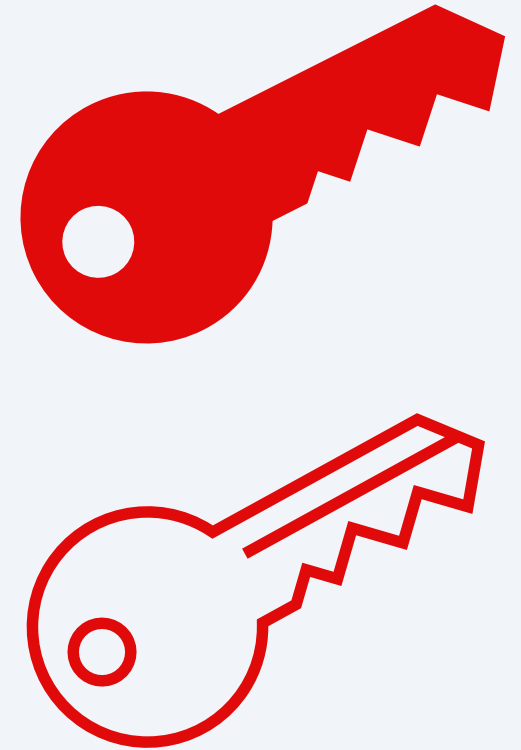
Clé de renouvellement

- **Paire de clés liées au titulaire** (hardware bound) pour l'authentification
- **Exclusivement pour obtenir des e-ID-VCs supplémentaires.**
- La **clé publique** est **saisie par fedpol** lors de la première émission de l'e-ID.
- La paire de clés ne **fait pas partie des e-ID-VCs**



Pourquoi une clé de renouvellement ?

- **Permet d'obtenir un nouveau lot avec un lien sûr avec le titulaire actuel**
- Créé par le portefeuille lors de l'émission initiale et vérifié par l'émetteur.
- Pas de dégradation lors de la présentation à d'autres vérificateurs*.
- Possibilité de séparer la durée de validité entre le cycle de renouvellement et la validité du VC







Utilisation de la clé de renouvellement

Première délivrance

Clés de liaison  

Clé de renouvellement 

Clé de l'émetteur 



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

Renouvellement

Clés de liaison  

Clé de renouvellement 

Clé de l'émetteur 





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

Réémission

Clés de liaison  


Clé de renouvellement 

Clé de l'émetteur 

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

 Renouvellement
par lots

Déroulement
Renewal Key

 Renouvellement
par lots

Matériel cryptographique utilisé

PROPRIÉTAIRE

EXPORTATEURS

Lier une preuve				
Clé secrète	Clé publique	Clé Type	Clé Attestation*	Signature (de l'émetteur)
sk_i	pk_i	ECDSA (NIST p-256)	ka_i	sig_i

Renouvellement			
Clé secrète	Clé publique	Clé Type	Clé Attestation*
sk_{renew}	pk_{renew}	ECDSA (NIST p-256)	ka_{renew}

Preuve de la signature		
Clé secrète (HSM)	Clé publique	Clé Type
sk_{Bund}	pk_{Bund}	EdDSA (Ed448)

*Les attestations de clés ne sont pas supportées par iOS. A la place, une App Attestation sera utilisée, pour cela l'App doit être certifiée par la Confédération.

Déroulement de la première émission d'une e-ID

- 1) Le portefeuille électronique génère des clés à lier Bindung (sk_i/pk_i) et à renouveler (sk_{renew}/pk_{renew}). Les clés sont générées dans la Secure Enclave et sont donc liées au terminal.
- 2) Le portefeuille électronique transmet des "Proofs of Possession" (pour sk_i et sk_{renew}) et des "Key Attestations" (ka_i pour pk_i et ka_{renew} pour pk_{renew}) et un JWT_{renew} à l'émetteur pour prouver le lien entre la clé et le matériel informatique
- 3) Identification du titulaire par contrôle d'identité (en ligne, au guichet)
- 4) L'émetteur vérifie les "Proofs of Possession" et les "Key Attestations" et définit les attributs (p. ex. validité). Elle signe le JWT_{renew} et le transmet au titulaire.
- 5) L'émetteur génère des VC e-ID (procédé salted-hash) et les lie au portefeuille électronique (pk_i comme attribut dans le VC)

Déroulement d'une émission par lots

- 1) Le portefeuille électronique génère **une (des) nouvelle(s)** paire(s) de clés "Binding" (sk_{i+1}/pk_{i+1})
- 2) Le portefeuille électronique transmet des "Proofs of Possession" (pour sk_{i+1} et sk_{renew}), des "Key Attestations" (ka_{i+1} et ka_{renew}) et JWT_{renew} à l'émetteur pour authentifier le portefeuille électronique et prouver le lien entre les clés et le matériel.
- 3) Vérification de l'émetteur, JWT_{renew} , "Proofs of Possessions" et "Key Attestations".
- 4) L'émetteur génère des e-ID-VCs (procédé salted-hash) et les lie au portefeuille électronique (pk_{i+1} comme attribut dans le VC)

Plus de détails seront publiés sur GitHub

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 & R

Questions du public

Résumé exécutif en anglais

18 heures

Prochaine réunion participative

Jeudi, 05.06.2025, 16 heures

Merci de votre attention !

Contact

Rolf Rauschenbach
Directeur adjoint du domaine
spécialisé e-ID
Chargé de l'information e-ID

Département fédéral de justice et
police DFJP
Office fédéral de la justice OFJ

Bundesrain 20, 3003 Berne
Téléphone +41 58 465 31 20
rolf.rauschenbach@bj.admin.ch

Liens

Informations générales sur l'e-ID
www.eid.admin.ch

Informations sur la législation e-ID
www.bj.admin.ch
www.parlament.ch

Plate-forme de discussion sur l'e-ID
www.github.com

Inscription à la lettre d'information e-ID
www.eid.admin.ch