Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

E-ID – Ausblick Vertrauensinfrastruktur
E-ID – Perspectives de l'infrastructure de confiance

Partizipationsmeeting // Zollikofen, 05.12.2022

Wer wir sind

Andreas Frey Sang

- Human Centered Designer
- Produkt Manager Vertrauensinfrastruktur

Carsten Plum

- Agile Coach
- Vorhabensverantwortlicher Vertrauensinfrastruktur

Agenda

Einleitung | Introduction

Erarbeitung des Ökosystems
Où en sommes-nous dans l'écosystème productif?

Public Ledger/Sandbox

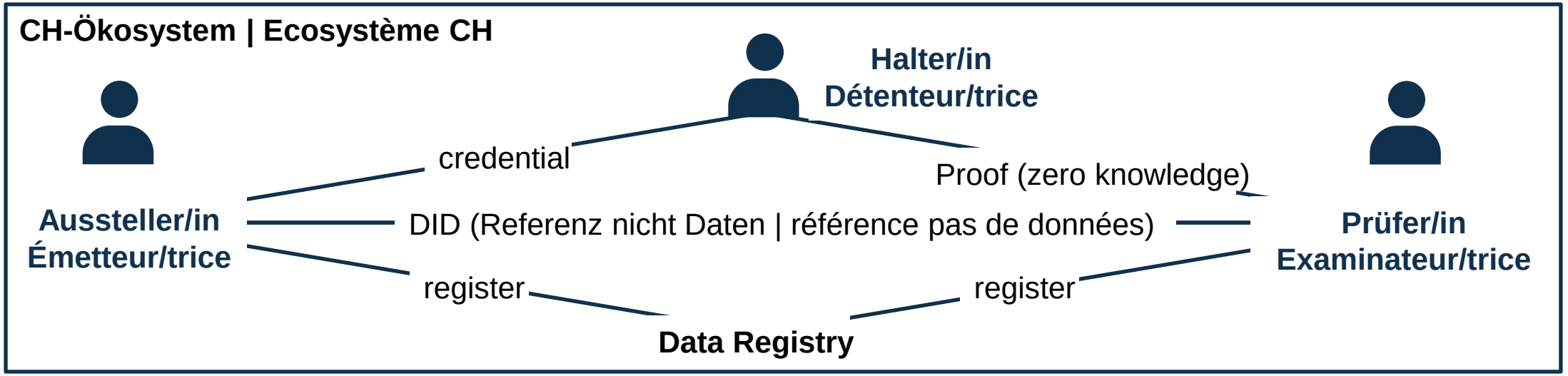
Einleitung | Introduction

Die E-ID kann nur mit möglichst vielen alltäglichen Anwendungsmöglichkeiten ihre Wirkung erzielen.

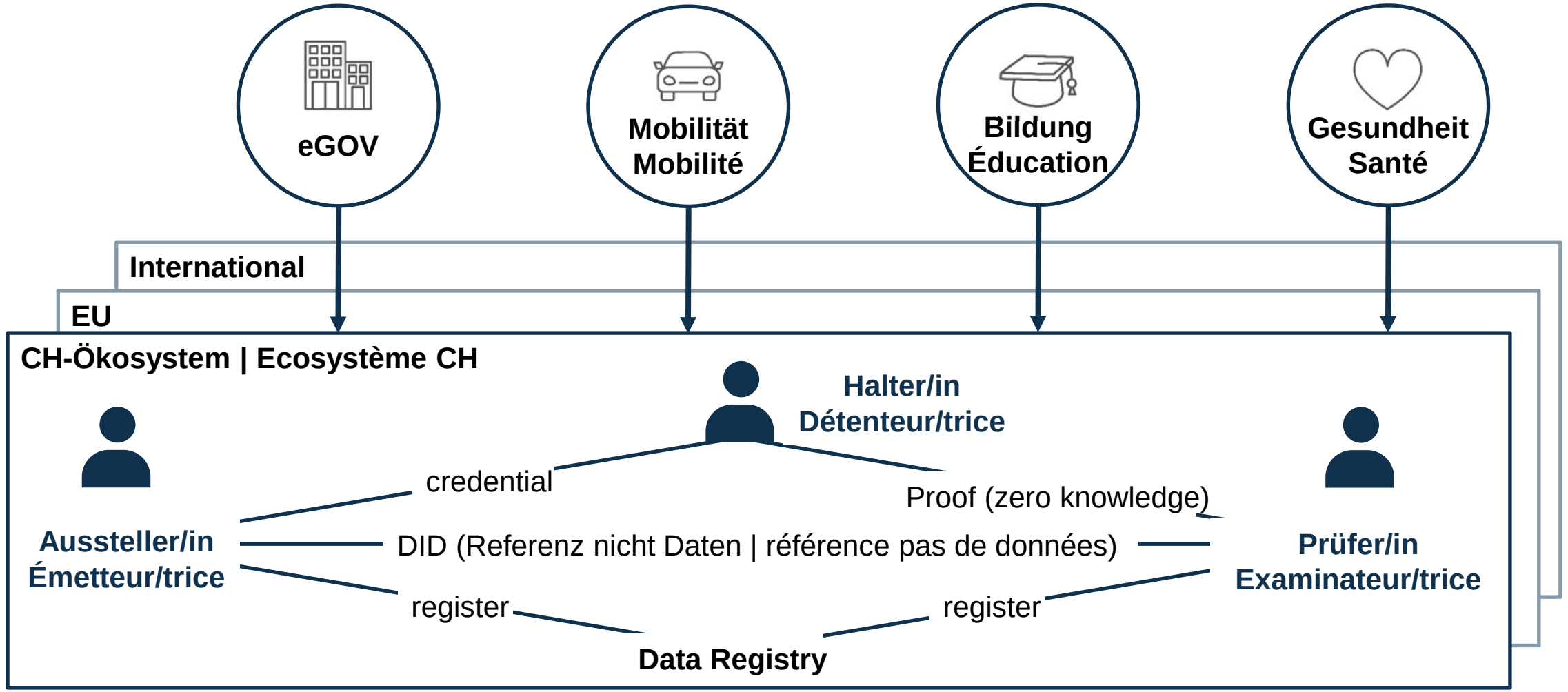
L'E-ID ne peut avoir un impact qu'avec le plus grand nombre d'applications possibles quotidiennes.

NZZ – 19.10.2022

Einleitung | Introduction



Einleitung | Introduction

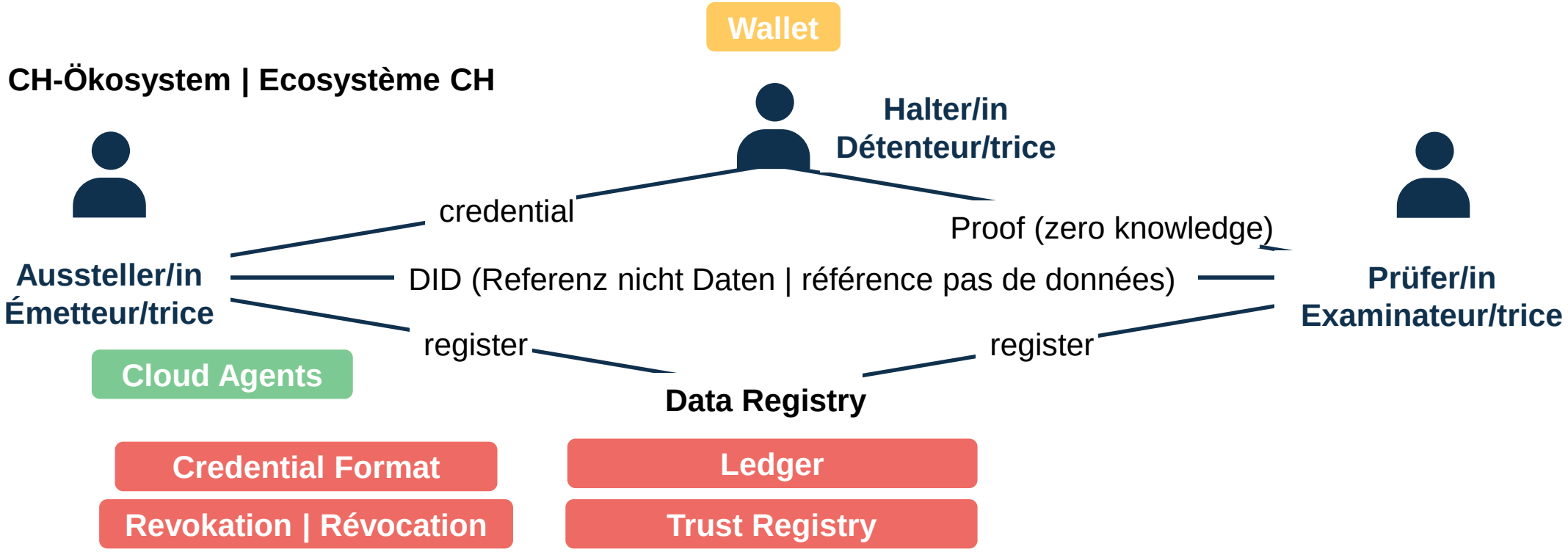


Erarbeitung des Ökosystems
Où en sommes-nous dans l'écosystème productif?

**“Release early. Release often.
And listen to your customers.”**

So here we are: 😅

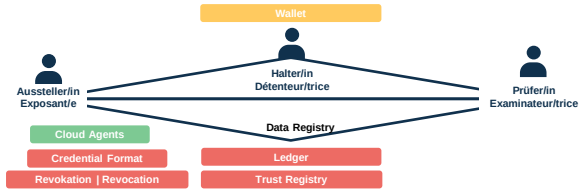
Erkenntnisse bezüglich der eingesetzten Technologie
Connaissances relatives à la technologie utilisée



Erkenntnisse bezüglich der eingesetzten Technologie
Connaissances relatives à la technologie utilisée

Revokation

Vertrauensinfrastruktur



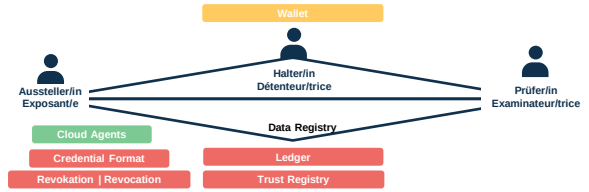
Indy Tails-Server

Wir antizipieren, dass die aktuelle Implementation der Lösung zur Revokation welche im Einsatz ist (Indy **Tails-Server**), in den Punkten **«Performance»** und **«Scalability»** für den Einsatz als zentrale nationale Lösung (vgl. Gesetz) derzeit nicht geeignet ist.

Die Delegation des gesamten Themenfelds «Revokation» an die Aussteller*in ist aus einer dezentralisierten Perspektive spannend und würde die oben genannten punkte mildern.
Aus unserer Sicht wird jedoch dadurch für Teilnehmer*innen die Hürde erhöht am Ökosystem teilzunehmen.
Aus einer «Bundesperspektive» als zukünftige Betreiber*in der Vertrauensinfrastruktur, wird durch die Dezentralität die Komplexität an Anforderungen wie «Zero Downtime» erhöht. Zusätzlich ergeben sich in der «Governance» neue Themenfelder welche bearbeitet werden müssen.

Révocation

Infrastructure de confiance



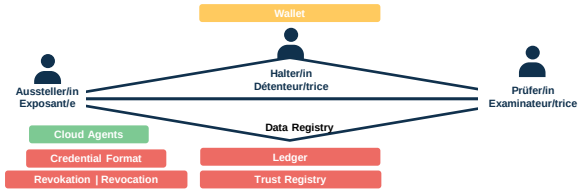
Indy Tails-Server

Nous anticipons que l'implémentation actuelle de la solution de révocation utilisée (serveur Indy Tails) ne convient pas en termes de **«performance»** et de **«scalabilité»** pour une utilisation en tant que solution centrale nationale (cf. loi).

La délégation de l'ensemble du domaine thématique «Revocation» à l' émetteur·rice est intéressante d'une perspective décentralisée et atténuerait les points mentionnés ci-dessus.
Cependant, de notre point de vue, cela augmente les obstacles à la participation des participant·e·s à l'écosystème.
D'un point de vue «fédéral», en tant que futur exploitant de l'infrastructure de confiance, la décentralisation augmente la complexité des exigences telles que le «temps d'arrêt zéro». De plus, de nouveaux champs thématiques apparaissent dans la «gouvernance» et doivent être traités.

Credential Format

Vertrauensinfrastruktur



Anoncreds

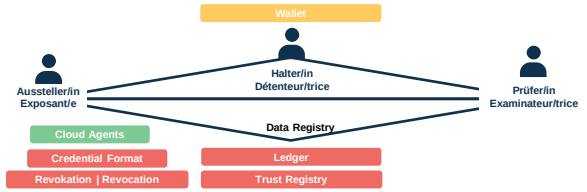
Die Handlungsfelder bezüglich Verbesserungen bei Anoncreds sind von der Community weitgehend identifiziert und anerkannt. Spezifisch für die Anwendung im Schweizer Ökosystem (resp. Einführung als technischer Standard) präferieren wir eine Lösung, welche **«rich schemas»** unterstützt. Es ist für die Interoperabilität des Ökosystems aus unserer Perspektive von grossem Nutzen, wenn **«Multi-Language»**, sowie **«Attribute Types»** direkt im Credential enthalten, resp. aus einem Credential verlinkt sind. Wir möchten zum jetzigen Zeitpunkt davon absehen für die technische Umsetzung unserer **Landessprachen** auf «kreative» Lösungen ausweichen zu müssen (Bsp. Hardcoding/Delegation der Übersetzungen an Ökosystem-Teilnehmer*innen).

Weiter sehen wir, ausgenommen von **OCA**s**,** wenig Initiative bezüglich der **standardisierten Darstellung** von Credentials. Es ist zu diskutieren, ob wir für die Schweiz ein eigenes MVP anstreben. Bsp: Hex-Code (Farbe) und SVG (Icon) im Credential enthalten, resp. aus dem Credential verlinkt.

Beim Experimentieren mit der Signierung von «Dummy» E-ID Credentials, welche Bilder enthalten (wie vom Gesetz vorgesehen), haben wir am eigenen Leib die mittelmässige **«Signatur Performance»** erlebt. Die Signierung einer hohen Anzahl digitaler Nachweise, welche grössere Datensätze enthalten, könnten aufwändiger sein, als initial angenommen.

Credential Format

Infrastructure de confiance



Anoncreds

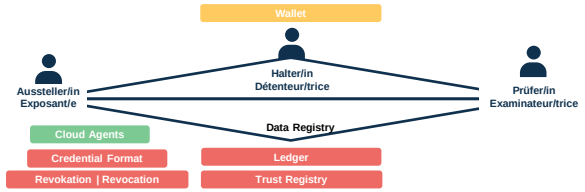
Les champs d'action concernant les améliorations d'Anoncreds sont largement identifiés et reconnus par la communauté. En ce qui concerne l'application dans l'écosystème suisse (ou l'introduction en tant que norme technique), nous préférons une solution qui supporte les «schémas riches». De notre point de vue, il est très utile pour l'interopérabilité de l'écosystème que les «Multi-Language» et les «Attribute Types» soient contenus directement dans le Credential ou reliés à partir d'un Credential. Pour l'instant, nous ne souhaitons pas recourir à des solutions «créatives» pour la mise en œuvre technique de nos langues nationales (par ex. hardcoding / délégation des traductions aux participant·e·s de l'écosystème).

En outre, nous voyons peu d'initiatives, à l'exception des **OCA**, concernant la **représentation standardisée** des credentials. Il convient de discuter de l'opportunité de créer un MVP spécifique pour la Suisse. Ex : Code hexadécimal (couleur) et SVG (icône) contenus dans le Credential, respectivement liés à partir du Credential.

En expérimentant la signature d'E-ID Credentials «factices» contenant des images (comme le prévoit la loi), nous avons pu constater par nous-mêmes la médiocrité de la «**performance de signature**». La signature d'un grand nombre de preuves numériques contenant de grands ensembles de données pourrait s'avérer plus complexe qu'on ne le pensait initialement.

Mobile Wallet

Holder



Aries Bifold Wallet

Die Aries Bifold Wallet (basierend auf React Native) war als Basis für die PoC's von grossem Nutzen.
Für einen Einsatz auf nationaler Ebene, wird eine Lösung bevorzugt, welche auf nativer Technologie basiert.
Der Ausstellungsprozess der E-ID wird in der Bundeswallet integriert:

Mit hoher Wahrscheinlichkeit bedingt das eine Härtung der Wallet, welche durch Nähe zum OS vereinfacht wird.

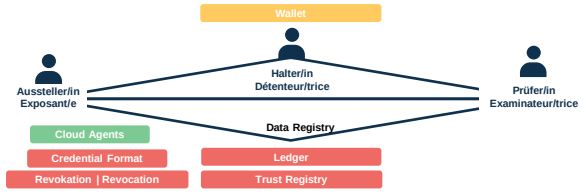
Weiter ist derzeit wenig **«Abstraktion»** in der Bifold Wallet umgesetzt. Für die Bundeswallet möchten wir eine Architektur, welche stärker vom Indy Stack losgelöst ist und dadurch potenziell weitere **zukünftige Implementationen** unterstützt.

Connection Reuse ist derzeit in der Wallet nicht umgesetzt (Update AIP 2.0 ist nötig).
Aus Nutzer*innen Perspektive ist das aktuelle Verwalten von Verbindungen nur schwer verständlich und nicht «massentauglich».

Wir erwarten **einfacheres Debugging** von nativen Libraries (Entwicklerperspektive), weil der React Native Layer obsolet wird.

Mobile Wallet

Holder



Aries Bifold Wallet

Le Aries Bifold Wallet (basé sur React Native) a été d'une grande utilité comme base pour les PoC. Pour une utilisation au niveau national, la préférence est donnée à une solution basée sur une technologie native. Le processus d'émission de l'E-ID est intégré dans le portefeuille fédéral :

Il est fort probable que cela implique un renforcement du wallet, qui est facilité par la proximité de l'OS.

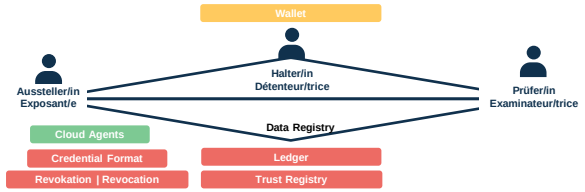
De plus, il y a actuellement peu d'«**abstraction**» dans le portefeuille bifold. Pour le wallet fédéral, nous souhaitons une architecture qui soit plus détachée de le stack Indy et qui puisse ainsi supporter d'autres **implémentations futures**.

La **réutilisation des connexions** n'est actuellement pas mise en œuvre dans le wallet (la mise à jour AIP 2.0 est nécessaire). Du point de vue des utilisateur·rices, la gestion actuelle des connexions est difficile à comprendre et n'est pas «adaptée aux masses».

Nous nous attendons à un **débogage plus facile** des librairies natives (perspective du développeur), car la couche React Native devient obsolète.

Cloud Agent

Businesscase



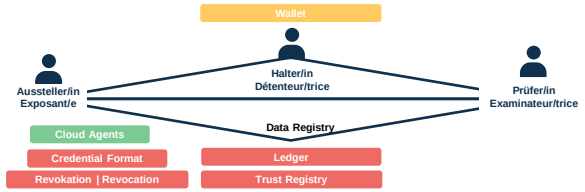
Aries Cloud Agents (AcaPy)

Bisher waren wir zufrieden mit der
Funktionalität, welche durch den AcaPy zur Verfügung gestellt wird, sowie der
Aktivität der Community.

Aus der Perspektive des öffentlichen Sektors, wäre es gut, wenn beim Zustand der **Dokumentation** nachgebessert werden könnte.
Uns ist zu Ohren gekommen, dass es aktuelle Entwicklung gibt, um eine **HSM-Erweiterung** zu implementieren und damit das «on premise» Schlüsselmanagement zu ermöglichen.
Wir begrüssen dies und denken, dass dies eine **Vorbedingung** für den **produktiven Betrieb** darstellt.

Cloud Agent

Businesscase



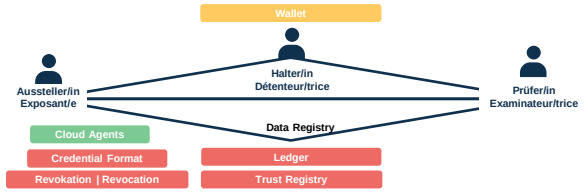
Aries Cloud Agents (AcaPy)

Jusqu'à présent, nous avons été satisfaits des fonctionnalités mises à disposition par l'AcaPy et de l'activité de la communauté.

Du point de vue du secteur public, il serait bon d'améliorer l'état de la **documentation**.
Nous avons appris que des développements sont en cours pour mettre en œuvre une **extension HSM** et permettre ainsi une gestion des clés "on premise".
Nous nous en félicitons et pensons qu'il s'agit d'une **condition préalable** à **l'exploitation productive**.

Ledger

Vertrauensinfrastruktur



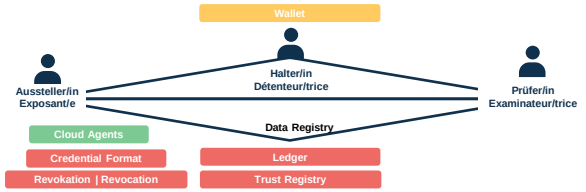
Hyperledger Indy

Tombstoning Support für den Ledger sollte implementiert werden.
Als zukünftige Betreiber innerhalb der Verwaltung:
Wir benötigen Handlungsspielraum (juristisch und technisch), um im Falle von Missbrauch im Ökosystems Massnahmen einleiten zu können. Ein unveränderbarer Ledger, mit keinen Möglichkeiten um missbräuchliche Handlungen von «Bad Actors» zu adressieren, könnte zu einer kompromittierenden Situation für das gesamte Vertrauensökosystem führen.

Entwicklungs-Timeline der Hyperledger Community ist von einer «Aussenperspektive» nur schwer fassbar.

Ledger

Infrastructure de confiance



Hyperledger Indy

Le support du tombstoning pour le ledger devrait être mis en œuvre.
En tant que futurs opérateurs au sein du gouvernement :
Nous avons besoin d'une marge de manœuvre (juridique et technique) pour pouvoir prendre des mesures en cas d'abus dans l'écosystème. Un ledger immuable, sans possibilité de s'attaquer aux actions abusives des «mauvais acteurs», pourrait conduire à une situation compromettante pour l'ensemble de l'écosystème de confiance.

La timeline de développement de la communauté Hyperledger est difficile à saisir d'un «point de vue extérieur».

Erkenntnisse bezüglich Ökosystem und dessen Nutzung
Connaissance de l'écosystème et de son utilisation

Ökosystem Design & Betrieb

Unklare Evolution der technischen Stacks

Aus unserer Perspektive gibt es derzeit wenig Klarheit, in welche Richtung sich SSI bezüglich der Standardisierung, sowie Durchdringung von technischen Stacks entwickelt. Unterschiedliche Implementation haben jeweils ihre eigenen Vor- und Nachteile.
Bisher: «no solution to rule them all»

OIDC / DIDcomm / …

Anoncreds / Json LD & BBS+ / ISO mDL

W3C / DIF / ToIP

Um dieser «Unklarheit» zu begegnen, gedenken wir im Moment architektonische Abstraktion in die Bundeslösungen (Ausstellung, Wallet) zu implementieren.

Écosystème Conception et fonctionnement

Une évolution peu claire des stacks techniques

De notre point de vue, il y a actuellement peu de clarté sur la direction que prend la SSI en termes de standardisation et de pénétration des stacks techniques. Les différentes implémentations ont chacune leurs propres avantages et inconvénients.
Jusqu'à présent : «no solution to rule them all»

OIDC / DIDcomm / …

Anoncreds / Json LD & BBS+ / ISO mDL

W3C / DIF / ToIP

Pour remédier à cette «ambiguïté», nous envisageons pour le moment d'implémenter l'abstraction architecturale dans les solutions fédérales (émission, portefeuille).

Nutzung durch die «Bevölkerung»

User Experience

- Bezüglich User Experience stellen wir fest, dass eine stark divergierende Maturität der Lösungen vorhanden ist.
- Gespräche mit bestehenden Akteuren im SSI-Bereich, haben uns aufgezeigt, dass viele Massnahmen um die User Experience zu verbessern, proprietär umgesetzt wurden.
- Unser Wunsch wäre gewesen, dass bereits mehr Standardisierung und «Best-Practices» bezüglich UX vorhanden sind.

Konfrontiert mit einem Rollout an die Öffentlichkeit:

- Zum jetzigen Zeitpunkt: Wir werden viel in UX investieren müssen, um die aktuelle Implementation, für alle Anspruchsberechtigten, verständlich und einfach nutzbar zu machen.
- Mehrere bestehende Implementation zeichnen sich durch hohe User Experience aus – die Machbarkeit ist gegeben.

Utilisation par la «population»

User Experience

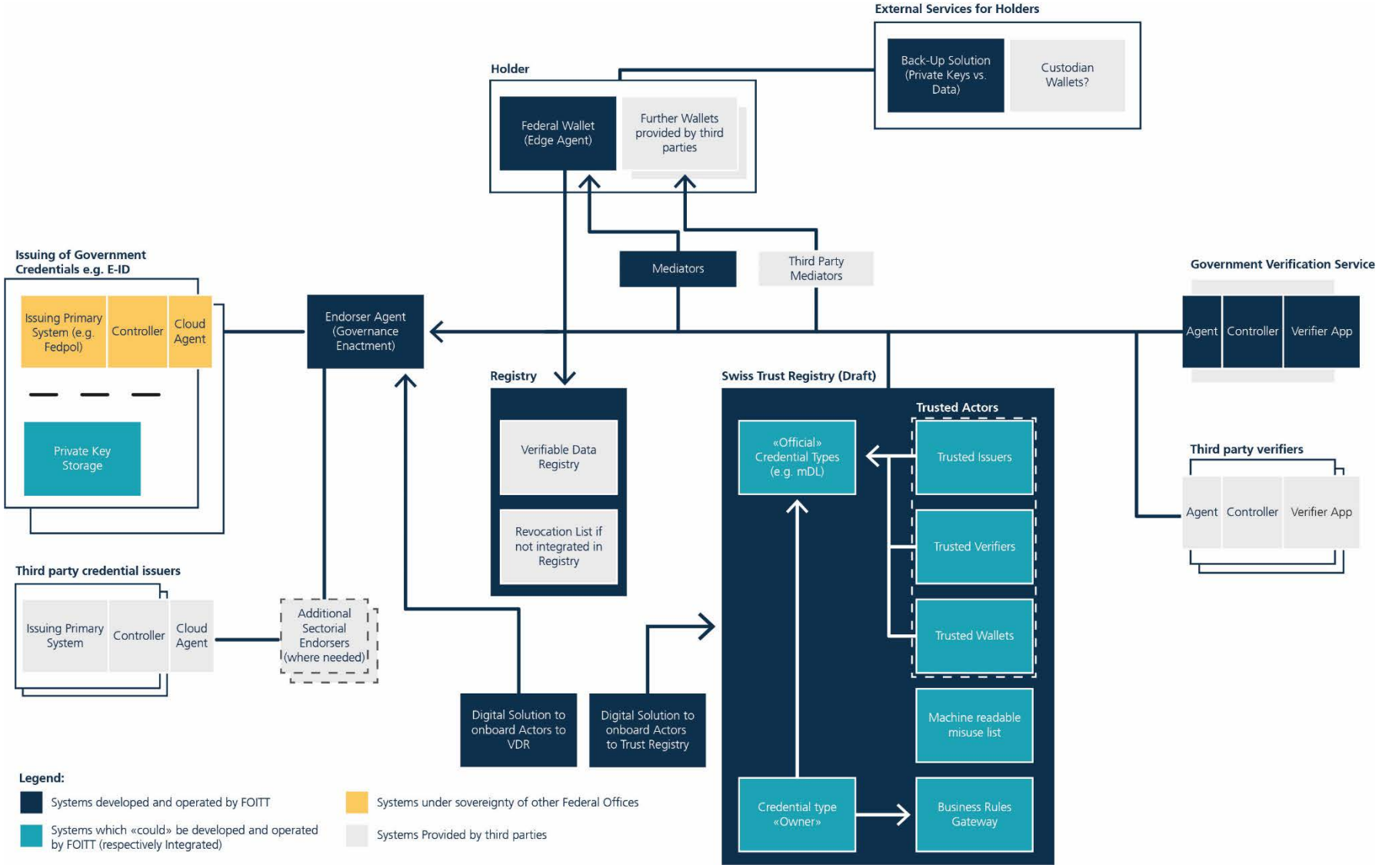
- En ce qui concerne l'expérience utilisateur, nous constatons qu'il existe une forte divergence de maturité entre les solutions.
- Des échanges précieux avec des acteurs existants dans le domaine de la SSI nous ont montré que de nombreuses mesures visant à améliorer l'expérience utilisateur ont été mises en œuvre de manière propriétaire.
- Nous aurions souhaité qu'il y ait déjà plus de standardisation et de "bonnes pratiques" en matière d'UX.

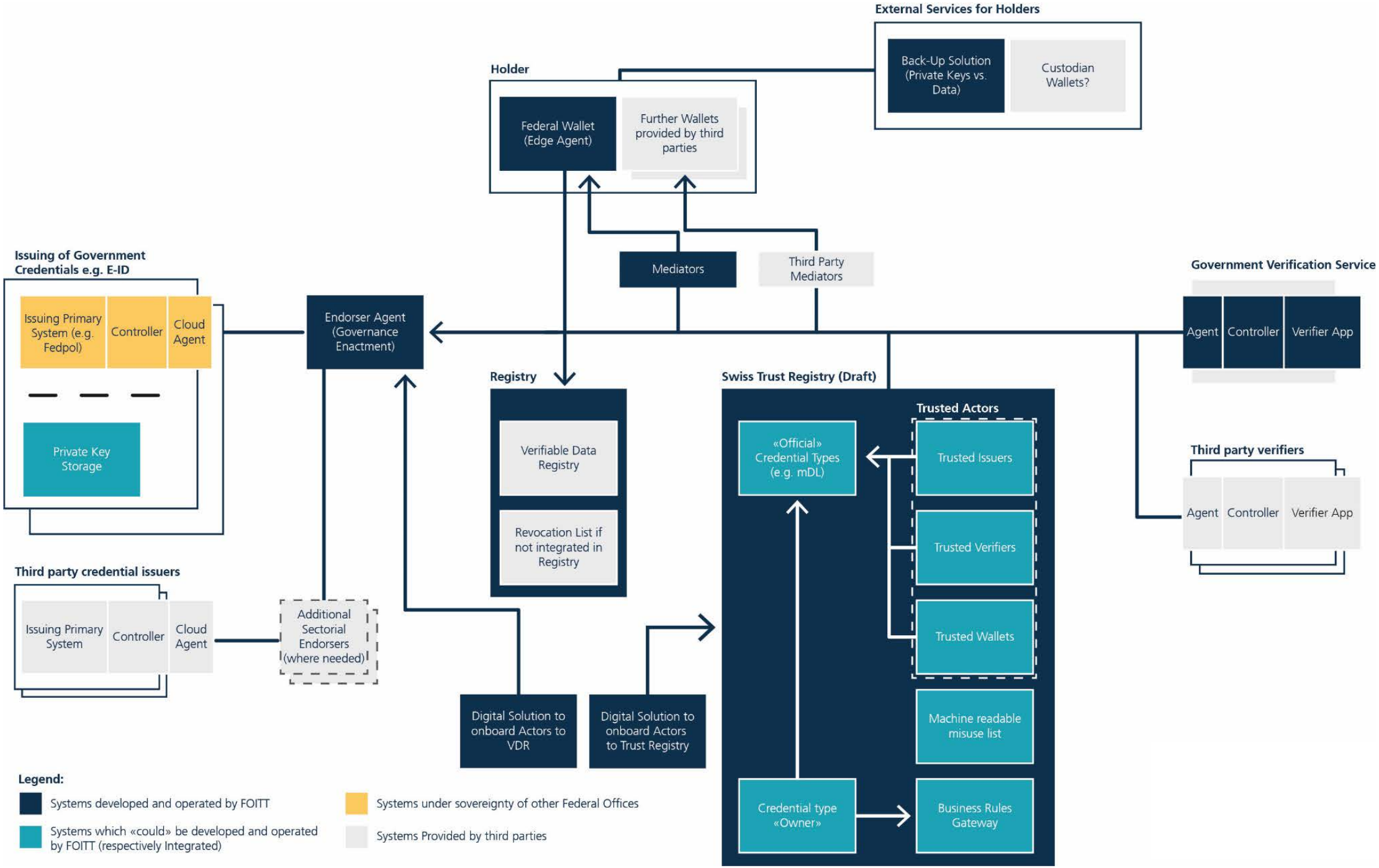
Confronté à un déploiement vers le grand public :

- A l'heure actuelle : nous devrons investir beaucoup dans l'UX afin de rendre l'implémentation actuelle compréhensible et facile à utiliser pour tous les ayants droit.
- Plusieurs implémentations existantes se distinguent par une expérience utilisateur élevée - la faisabilité est donnée.

Ausblick | Perspectives

Moving forward: Swiss Trust Ecosystem




External Services for Holders
Back-Up Solution (Private Keys vs. Data)
Custodian Wallets?
Holder
Federal Wallet (Edge Agent)
Further Wallets provided by third parties
Mediators
Third Party Mediators
Issuing of Government Credentials e.g. E-ID
Issuing Primary System (e.g. Fedpol)
Controller
Cloud Agent
Private Key Storage
Endorser Agent (Governance Enactment)
Government Verification Service
Agent
Controller
Verifier App
Registry
Verifiable Data Registry
Revocation List if not integrated in Registry
Swiss Trust Registry (Draft)
Trusted Actors
«Official» Credential Types (e.g. mDL)
Trusted Issuers
Trusted Verifiers
Trusted Wallets
Machine readable misuse list
Credential type «Owner»
Business Rules Gateway
Third party verifiers
Agent
Controller
Verifier App
Third party credential issuers
Issuing Primary System
Controller
Cloud Agent
Additional Sectorial Endorsers (where needed)
Digital Solution to onboard Actors to VDR
Digital Solution to onboard Actors to Trust Registry
Legend:
Systems developed and operated by FOITT
Systems which «could» be developed and operated by FOITT (respectively Integrated)
Systems under sovereignty of other Federal Offices
Systems Provided by third parties

Moving forward: Trust Registry

Basisregister

Verifiable Data Registry ← Identifikator

Öffentlicher Schlüssel

Revocation (Lists) if not held decentraly ← Revokationsinformation

Vertrauensregister (Abb. gesetzliche Grundlage)

Trusted Actors

Staatliches Gütesiegel Identifikator n:
Is «who they claim to be»

Erweitertes Vertrauensregister?

Nachweis entspricht «offiziellem» Schema/Typ e.g. eFührerausweis

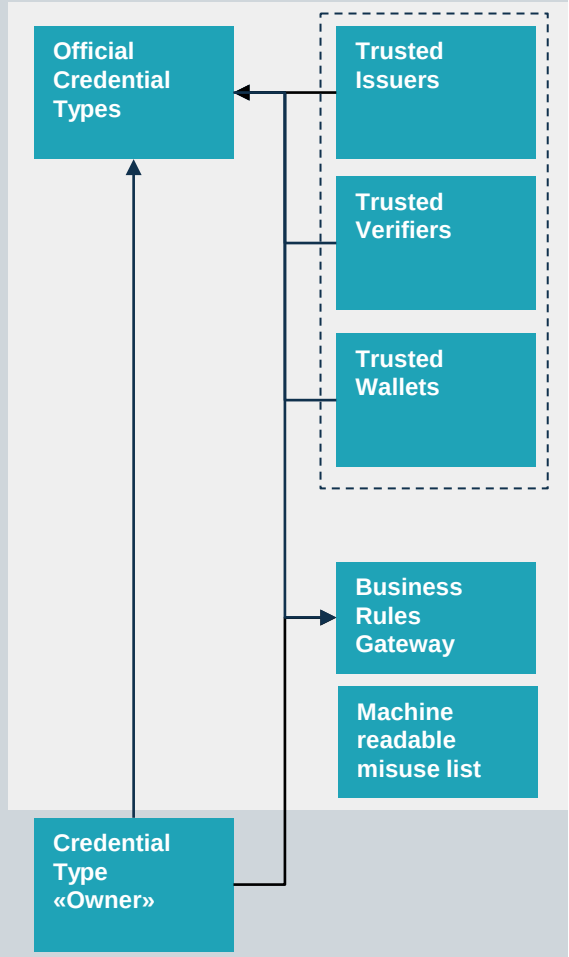
Aussteller*in ist vertrauenswürdig Nachweise gemäss Typ auszustellen

Verifikator*in ist vertrauenswürdig um Credentials gemäss Typ zu verifizieren

Wallet ist «vertrauenswürdig» um Nachweise gemäss Typ zu halten.

Nachweise gemäss Typ sollen gegen folgenden Regelsatz geprüft werden

Liste von Identifikatoren, welche als missbräuchliche Teilnehmer*innen gemeldet sind.

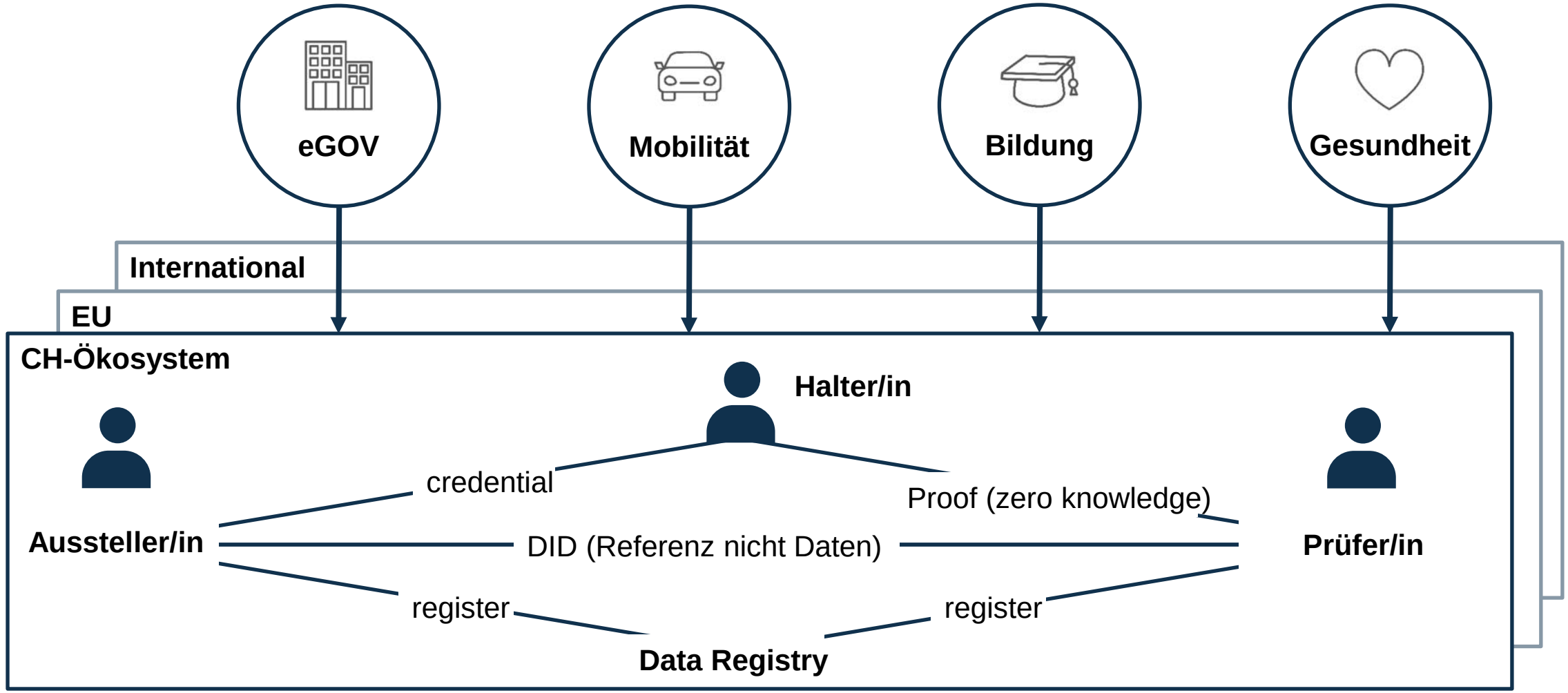


Public Ledger/Sandbox

Die Schweiz wagt einen zweiten Anlauf mit der E-ID, nachdem der erste an mangelnder Legitimität gescheitert ist. Mit der Bundeslösung ist die Legitimität gesichert, genügend Nutzungsvolumen kann aber nur die Wirtschaft bieten.

NZZ – 19.10.2022

Public Ledger/Sandbox



Public Ledger/Sandbox

Grundsätzlich wollen wir die Öffnung des Ökosystems frühzeitig im Sinne eines PoC ermöglichen und sehen darin u.a. verschiedene Chancen:

- generelle Erfahrungen im Betrieb des Ökosystens sammeln
- manuelles Onboarding von Ökosystem-Akteuren erproben
- Kompatibilität mit öffentlich verfügbaren Wallets sicherstellen
- weitere Schweizer SSI-Piloten ermöglichen und daraus Erkenntnisse für das Ökosystem gewinnen
- Exploration von Upgrade-Mechanismen
- Regulation des Ökosystems prüfen

Public Ledger/Sandbox

En principe, nous voulons permettre l'ouverture de l'écosystème à un stade précoce, dans l'esprit d'un PoC, et nous y voyons notamment plusieurs opportunités:

- acquérir une expérience générale dans le fonctionnement de l'écosystème
- tester l’onboarding manuel des acteurs de l'écosystème
- assurer la compatibilité avec les wallets disponibles publiquement
- permettre d'autres pilotes SSI suisses et en tirer des enseignements pour l'écosystème
- explorer les mécanismes des upgrades
- examiner la régulation de l'écosystème



Public Ledger/Sandbox

Grundsätzlich wollen wir die Öffnung des Ökosystems frühzeitig im Sinne eines PoC ermöglichen und sehen darin u.a. verschiedene Chancen
– ABER: wir werden «rules of play» haben (müssen):

- es werden in einer ersten Phase nur Schweizer Integratoren zugelassen.
- die Integration findet nach dem Model First Come First Served statt.
- die Anzahl der Integratoren wird in einer ersten Runde auf eine noch zu definierende Anzahl beschränkt.
- es dürfen keine "echten" Daten für die PoCs verwendet werden (ausschliesslich "Dummy" Daten) .
- Stabilität und Support wird für die Sandbox nach dem Model "Best-Effort" gewährt.

Diese Aufzählung ist hier beispielhaft und nicht abschliessend. Wir sind aktuell daran, sie zu schärfen und **für Q1.2023 verfügbar** zu machen.

Public Ledger/Sandbox

En principe, nous voulons permettre l'ouverture de l'écosystème à un stade précoce, dans l'esprit d'un PoC, et nous y voyons notamment plusieurs opportunités
- MAIS : nous devrons avoir des "règles du jeu" :

- seuls les intégrateurs suisses seront admis dans une première phase.
- l'intégration se fera selon le modèle "First Come First Served".
- le nombre d'intégrateurs sera limité dans un premier temps à un nombre qui reste à définir.
- aucune donnée "réelle" ne peut être utilisée pour les PoC (uniquement des données "factices") .
- la stabilité et le support sont assurés pour le Sandbox selon le modèle "Best-Effort".

Cette liste est donnée à titre d'exemple et n'est pas exhaustive. Nous sommes actuellement en train de l'affiner et de le rendre disponible pour le **1er trimestre 2023**.