Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz

Öffentliche Konsultation zum «Zielbild E-ID»

14. Oktober 2021

Programm

09.30 – 09.45	Begrüssung und Einführung
09.45 – 10.45	**Welchen Umfang soll ein E-ID-Ökosystem haben?**
10.45 – 11.15	*Kaffeepause*
11.15 – 12.15	**E-ID-Use-Cases aus der Praxis von Kantonen und Wirtschaft**
12.15 – 13.30	*Mittagspause*
13.30 – 14.30	**Wie soll eine E-ID umgesetzt werden?**
14.30 – 15.30	**Allgemeine Stellungnahmen zum E-ID-Zielbild** Nutzen und Definition der E-ID; Hervorhebung der wichtigen Fragen
15.30 – 16.00	*Kaffeepause*
16.00 – 17.00	**Moderierte offene Diskussionsrunde** mit Fragen aus dem Publikum und via Chat

Programme

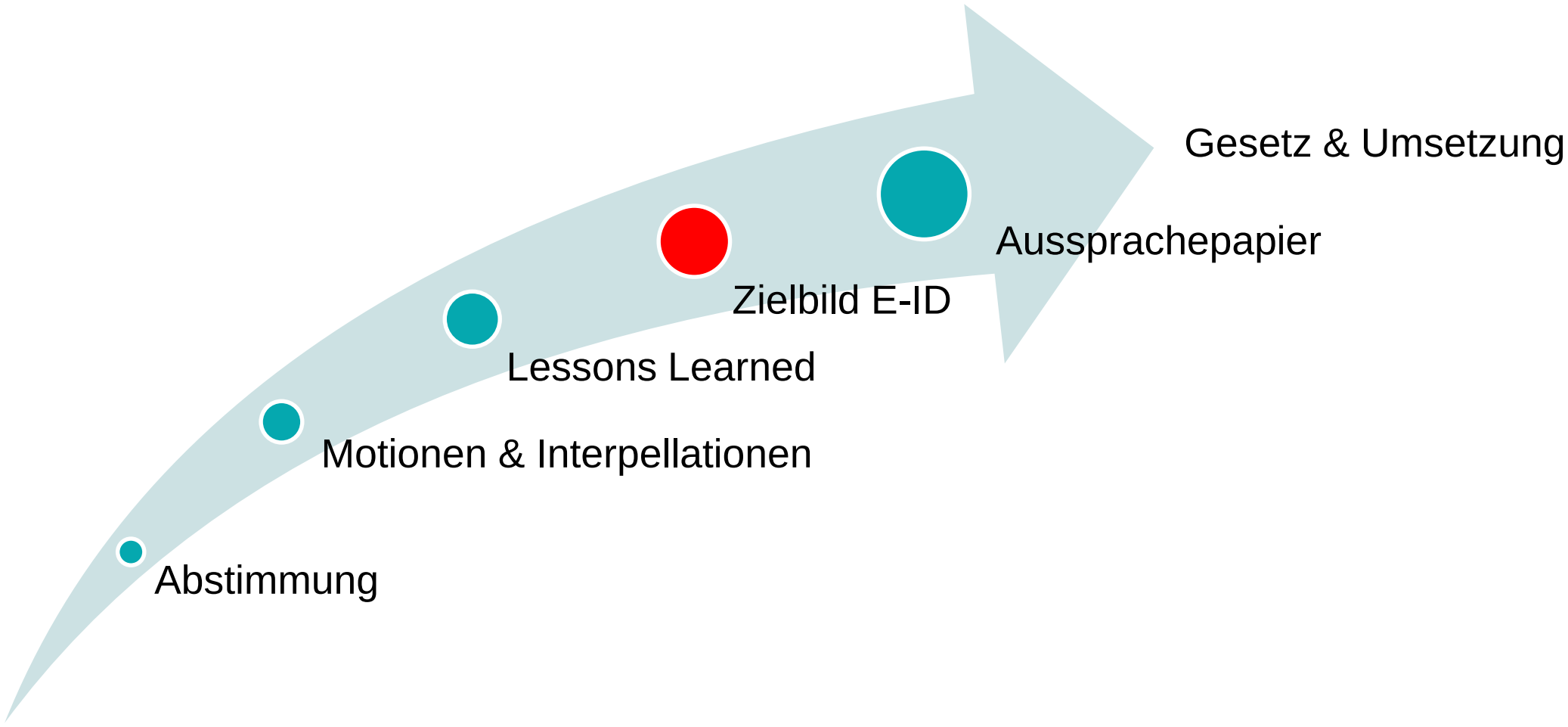
09.30 – 09.45	Acceuil et remarques introductives
09.45 – 10.45	**Quelle devrait être la portée d'un écosystème e-ID ?**
10.45 – 11.15	*Pause*
11.15 – 12.15	**Application de l'e-ID dans la pratique des cantons et des entreprises**
12.15 – 13.30	*Pause de midi*
13.30 – 14.30	**Comment mettre en œuvre une e-ID ?**
14.30 – 15.30	**Positions générales sur l'objectif de l'e-ID** Avantages et définition de l'e-ID ; mise en évidence des questions importantes
15.30 – 16.00	*Pause*
16.00 – 17.00	**Discussion et questions** avec un modérateur, hors ligne et en ligne

Einführung

Michael Schöll

Direktor Bundesamt für Justiz

Weg zur E-ID


Gesetz & Umsetzung
Aussprachepapier
Zielbild E-ID
Lessons Learned
Motionen & Interpellationen
Abstimmung

Lessons Learned
VOX-Analyse März 2021

- **Kein Votum** gegen Digitalisierung oder gegen staatliche E-ID
- **Hoheit** über die Herausgabe der E-ID muss beim Staat bleiben
- **Privacy by design**: Protokollierung oder Überwachung von Verwendungsarten und -orten durch zentrale Stelle muss technisch ausgeschlossen sein
- **Datenhoheit beim Nutzer**
- Daten**schutz** – Daten**sparsamkeit** – **Dezentralität**

Parlamentarische Vorstösse

- Am 10. März 2021 wurden **sechs gleichlautende Motionen «Vertrauenswürdige, staatliche E-ID» aus allen Fraktionen** eingereicht (vgl. 21.3124, 21.3125, 21.3126, 21.3127, 21.3128 und 21.3129).
- Am 18. März 2021 wurde die **Interpellation** 21.3310 **Andrey «Identitätskarte als Teil einer zukünftigen E-ID-Lösung»** eingereicht.
- Der **Bundesrat hat diese** parlamentarische Vorstösse **am 26. Mai 2021 beant-wortet** und das weitere Vorgehen festgelegt: E-ID: Bundesrat will vorwärts machen.
- Am 15. Juni 2021 wurde die **Interpellation** 21.3718 **Graf-Litscher «Selbstbe-stimmte elektronische Identitäten»** eingereicht.

Was verlangen die Motionen

- Die E-ID soll **vergleichbar mit der Identitätskarte** oder dem Pass sein.
- Es sollen die **Grundsätze** «privacy by design», Datensparsamkeit und dezentrale Datenspeicherung eingehalten werden.
- Die E-ID darf auf **privatwirtschaftlich entwickelten Produkten und Diensten** beruhen.
- Der Ausstellungsprozess und der Gesamtbetrieb der Lösung muss **aber in der Verantwortung staatlicher, spezialisierter Behörden** erfolgen.

Neue Projektorganisation E-ID

- Bundesrat hat das **Eidgenössische Justiz- und Polizeidepartement (EJPD) beauftragt**, bis Ende Jahr in Zusammenarbeit mit dem Eidgenössischen Finanzdepartement (EFD) und der Bundeskanzlei (BK) sowie **unter Einbezug der Wissenschaft und der Kantone** ein Grobkonzept zu erarbeiten.
- **Projektausschuss unter Leitung des Bundesamtes für Justiz (BJ)** und Mitglieder aus dem Bundesamt für Polizei (fedpol), der Digitalen Verwaltung Schweiz (DVS), dem Bundesamt für Informatik und Telekommunikation (BIT) und dem Bereich Digitale Transformation und IKT-Lenkung der Bundeskanzlei (DTI)
- **Projektteam unter Leitung des BJ**
  (mit Mitarbeitenden von BJ sowie fedpol und mit Einbezug der Kantone)

Ziele des Diskussionspapiers

- **Enthält keinen Lösungsvorschlag!**
- **2. September 2021:** Beiratstreffen E-ID (Medienmitteilung) und Eröffnung einer breiten, öffentlichen Diskussionen über:
  1. Vision und Definition der E-ID
  2. Umfang Ökosystem (Ambitions-Niveau)
  3. Technologie-Ansatz
- Gesamtverständnis fördern
- Stakeholder abholen und einbinden
- **14. Oktober 2021:** Konferenzielle Bereinigung
- Ergebnis der Diskussion bildet die Grundlage für den Richtungsentscheid durch den Bundesrat (Ende 2021)

Diskussionsthemen
E-ID und Ökosystem

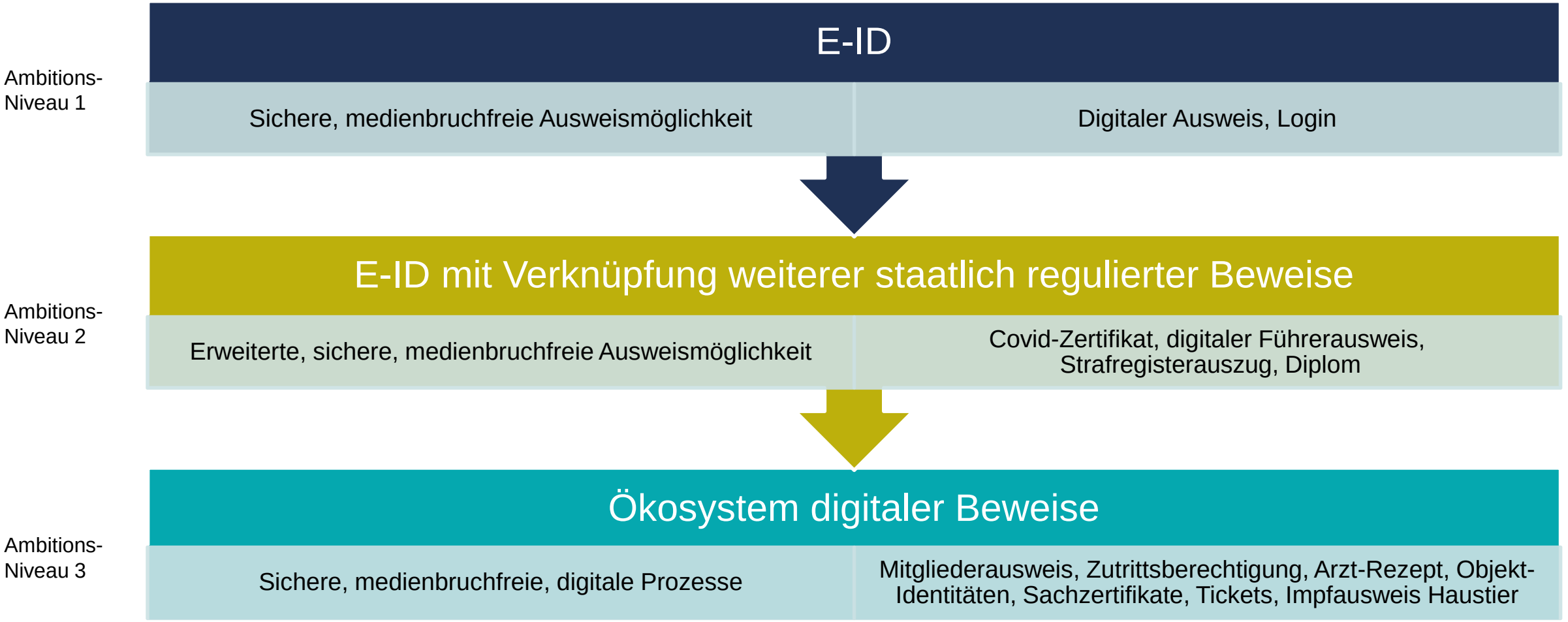
- Mögliche Definition der E-ID:

  «Eine E-ID ist ein vom Staat ausgestellter digitaler Ausweis, um die eigene Identität nachweisen zu können.»

- Vision einer breit genutzten Infrastruktur der Schweiz:

  «Die Schweiz hat eine staatlich betriebene digitale Vertrauensinfrastruktur, welche sichere, medienbruchfreie Prozesse ermöglicht und fördert.»

Diskussionsthemen
Ökosystem und Ambitionsniveaus



Diskussionsthemen
Beispiel-Anwendungsfälle E-ID

- Altersüberprüfung (analoge Welt, digitale Welt)
- Bankkonto-Eröffnung
- Betreibungsregisterauszug
- Staatliches Login
- Elektronische Signatur

Diskussionsthemen
Lösungsansätze

SSI – Self-Sovereign Identity

PKI – Public Key Infrastructure

IdP – staatlicher Identitätsprovider

Aktuelle Schritte

Aussprachepapier für Richtungsentscheid

Welchen Umfang soll ein E-ID-Ökosystem haben?

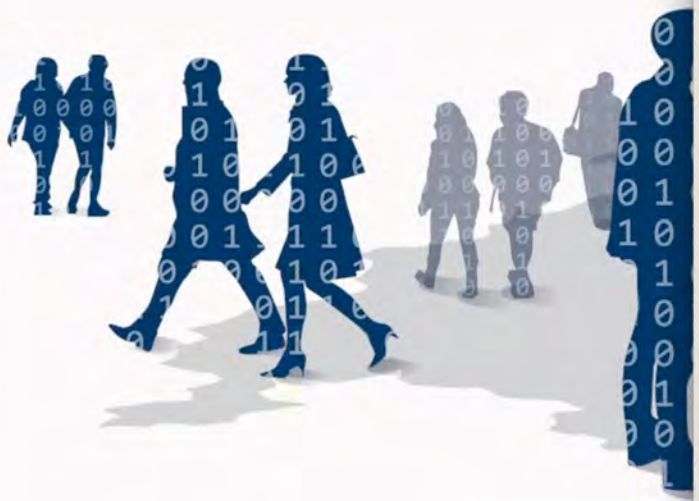
Abraham Bernstein

Universität Zürich, Digital Society Initiative

Die E-ID – Einführende Gedanken zum Diskussionspapier «Zielbild E-ID»

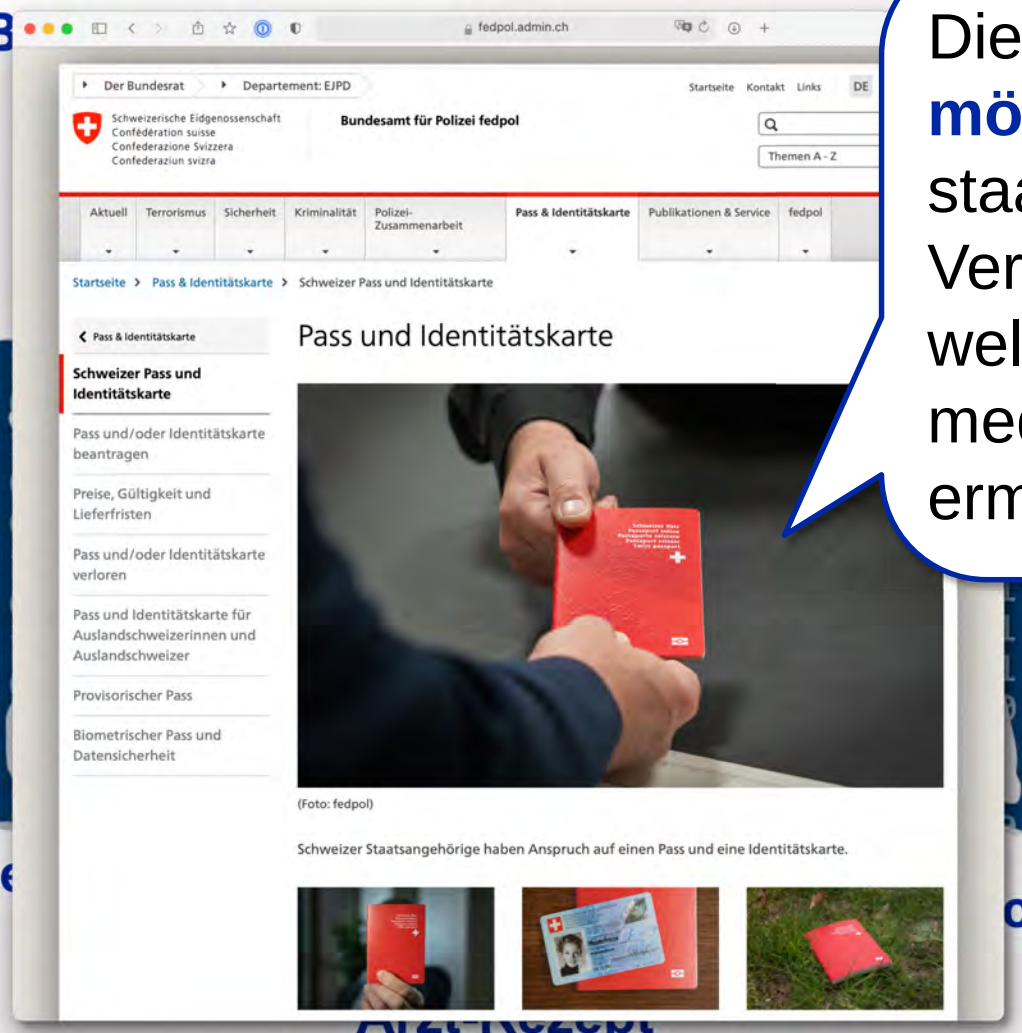
Prof. Abraham Bernstein, Ph.D.

online Einkaufen

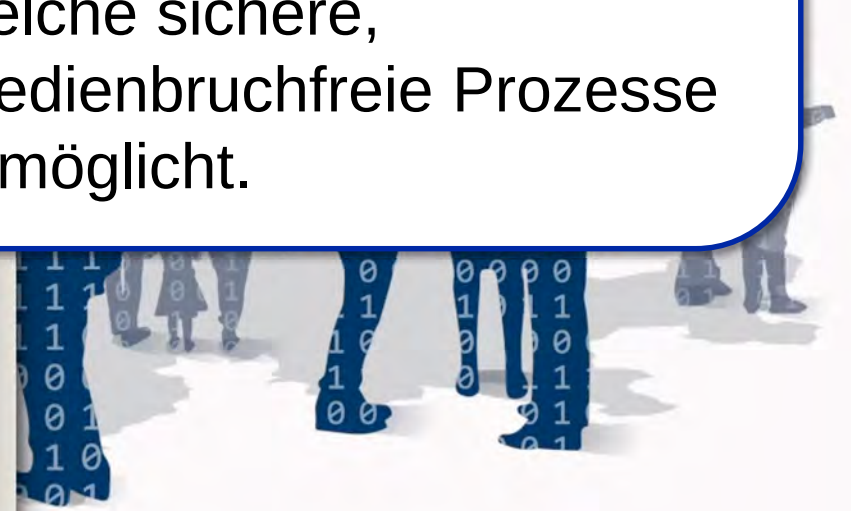


Mitgliede

Gesuche



Die Schweiz **benötigt möglichst bald** eine staatlich betriebene digitale Vertrauensinfrastruktur, welche sichere, medienbruchfreie Prozesse ermöglicht.



che Tickets

Identitätsnachweis

E-ID als einer der Hauptpfeiler der Digitalisierung

E-ID Ökosystem	**Sichere, medienbruchfreie, digitale Prozesse**	Mitgliederausweise, Arzt-Rezept, Zutrittsberechtigung, Identitäten, Tickets, Haustier-Impfausweis
E-ID + staatlich regulierte Beweise	**Erweiterte, sichere, medienbruchfreie Ausweismöglichkeit**	Diplom, digitaler Führerausweis, Strafregisterauszug, Covid-Zertifikat
E-ID	**Sichere, medienbruchfreie, Ausweismöglichkeit**	Digitaler Ausweis, Login

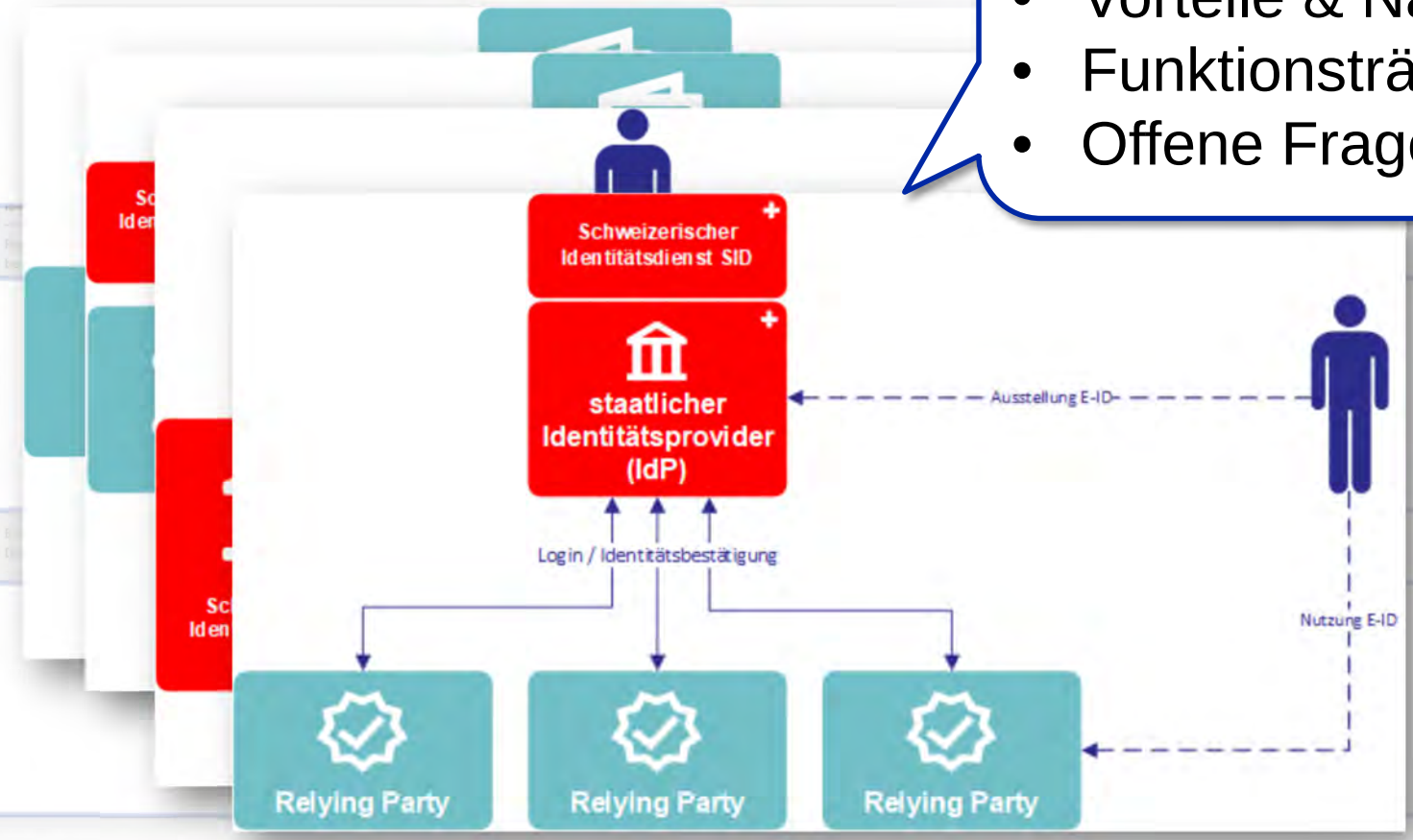
E-ID als einer der Hauptpfeiler der Digitalisierung

- Funktionsweise
- Vorteile & Nachteile
- Funktionsträger
- Offene Fragen

E-ID Ökosystem

E-ID + staatlich regulierte Beweise

E-ID

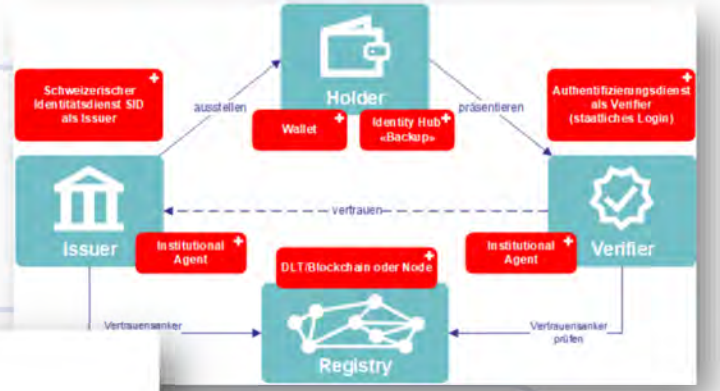


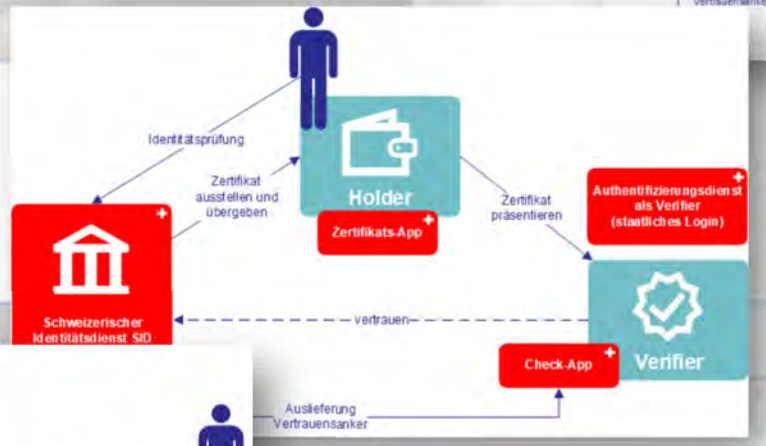
E-ID als einer der Hauptpfeiler der Digitalisierung

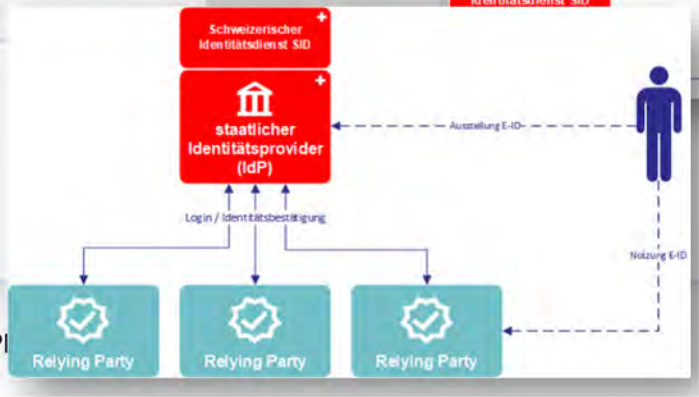
E-ID Ökosystem

E-ID + staatlich regulierte Beweise

E-ID







E-ID als einer der Hauptpfeiler der Digitalisierung

E-ID Ökosystem

E-ID + staatlich regulierte Beweise

E-ID

Bürger:innen
Inkl. Zivilgesellschaft

- vertrauenswürdig
  - sicher
  - Datenschutz
  - transparent & verständlich
- Einfach für alle
- nützlich, möglichst überall einsetzbar
- kostenlos
- kompatibel
- Alternativen
- ...

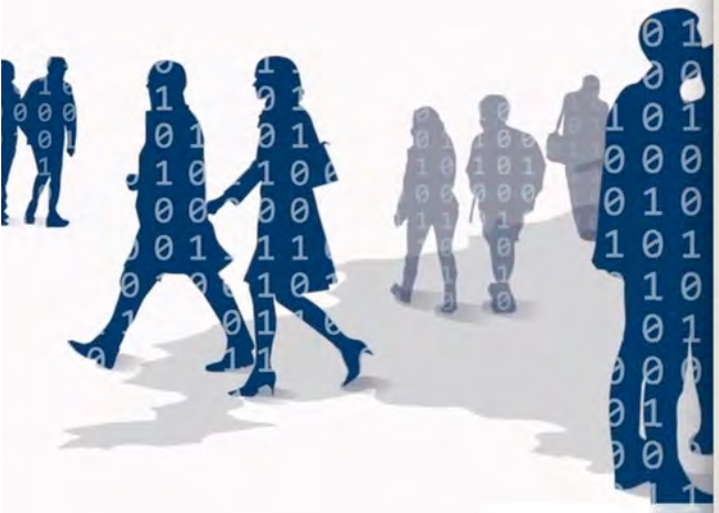
Anbieter
Behörden, Wirtschaft, ...

Diejenigen der Bürger:innen sowie

- Rechtssicherheit
- einfach einzubinden
- günstig
- Verfügbarkeit
- ...

Regulatoren
Bund, Kantone, ...

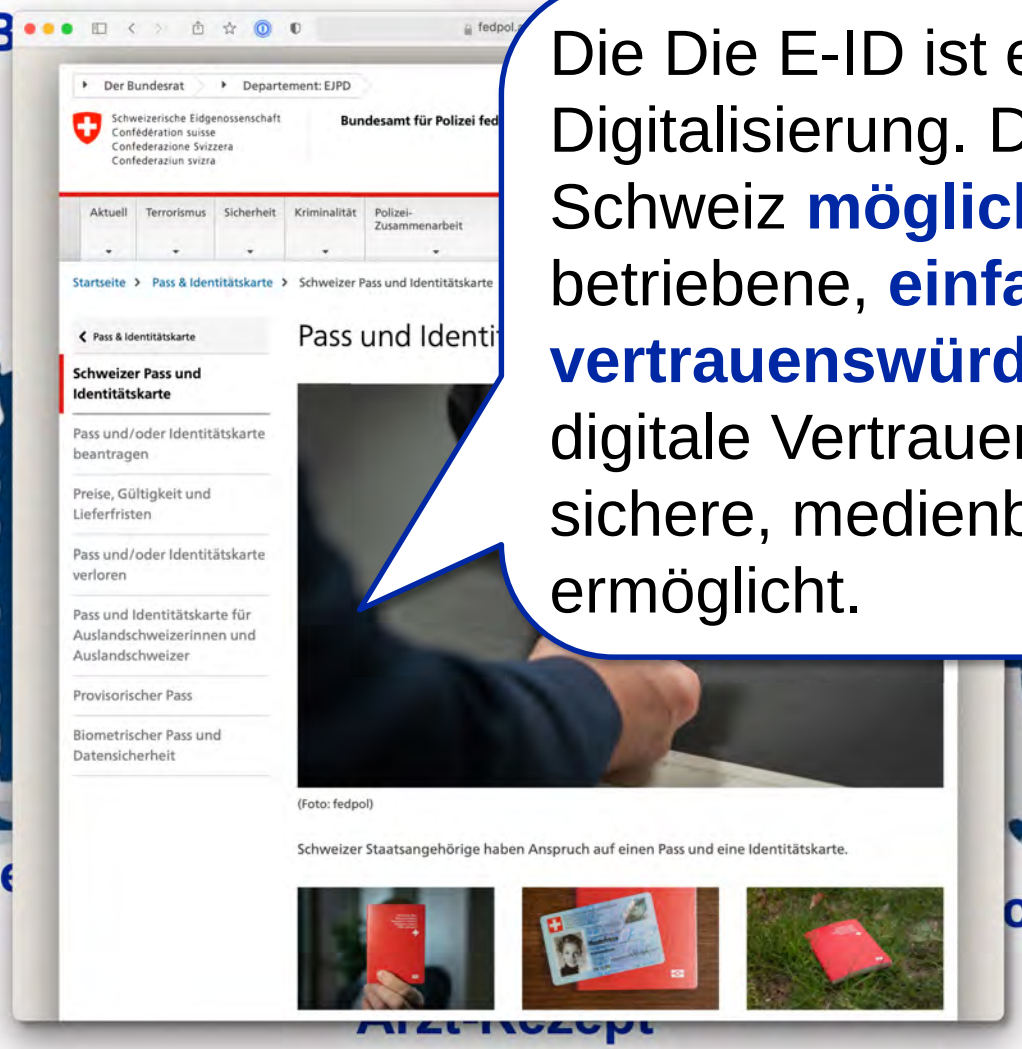
- gesellschaftlichen Anforderungen entsprechen
- klare regulatorische Prozesse
- Kosten
- unterstützbar
- Verfügbarkeit
- ...



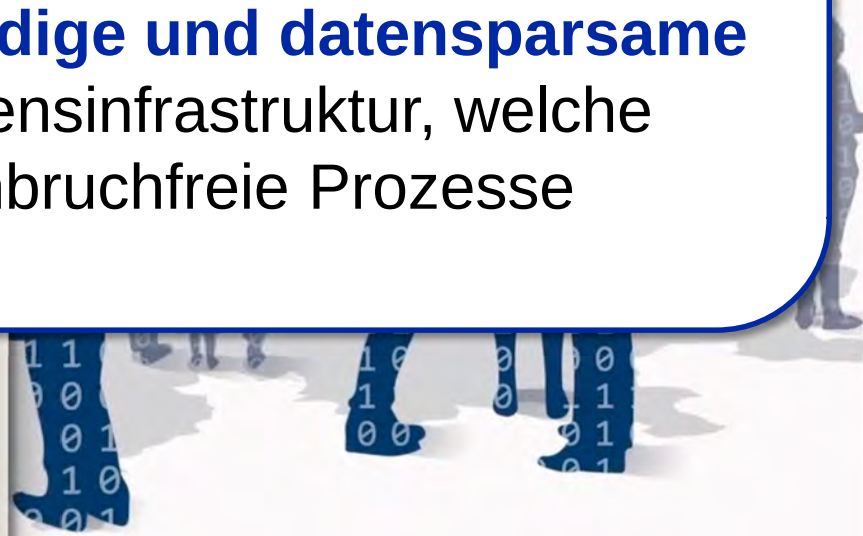
online Einkaufen

Mitgliede

Gesuche



Die Die E-ID ist eine der Grundpfeiler der Digitalisierung. Deshalb **benötigt** die Schweiz **möglichst bald** eine staatlich betriebene, **einfach zu benutzende, vertrauenswürdige und datensparsame** digitale Vertrauensinfrastruktur, welche sichere, medienbruchfreie Prozesse ermöglicht.



che Tickets

Identitätsnachweis

Welchen Umfang soll ein E-ID-Ökosystem haben?

Gerhard Andrey

Nationalrat Grüne

Welchen Umfang soll ein E-ID-Ökosystem haben?

Min Li Marti

Nationalrätin SP

Welchen Umfang soll ein E-ID-Ökosystem haben?

Jörg Mäder

Nationalrat GLP

Welchen Umfang soll ein E-ID-Ökosystem haben?

Simon Stadler

Nationalrat Die Mitte

Welchen Umfang soll ein E-ID-Ökosystem haben?

Christian Wasserfallen

Nationalrat FDP


PAUSE

E-ID-Use-Cases aus der Praxis

Vitus Ammann

SBB

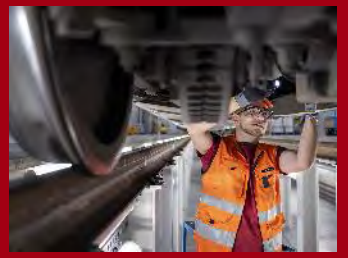
Use Cases SBB

Vitus Ammann, SBB
Konferenzielle Diskussion E-ID
Bern, 14. Oktober 2021

2 Anwendungsbereiche im Vordergrund

Mobilitäts-Ökosystem

Prozess-Integration



Infrastruktur für Digitale Nachweise

Kund*innen werden einfacher Zugang zu verschiedenen Mobiltätsangeboten haben

Mobilitäts-Ökosystem



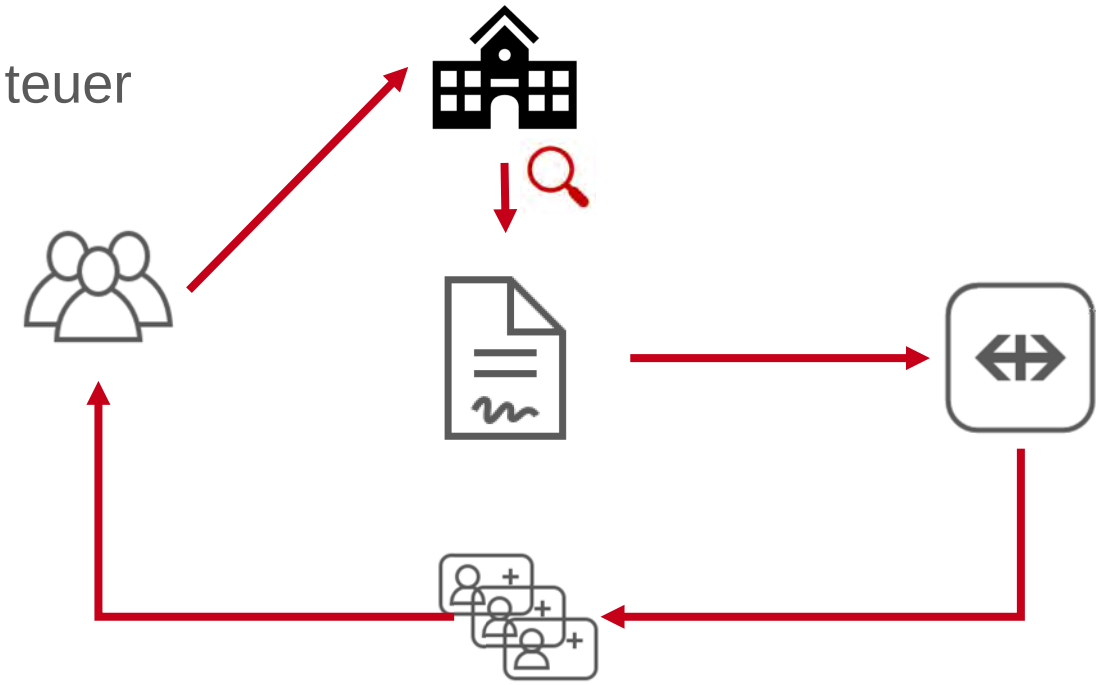
- Identifikation
- Zugangsschlüssel
- Internationale Berechtigungen
- Führer- und Fahrzeugausweise
- Versicherungsnachweise
- Nachweise für Vergünstigungen

Infrastruktur für Digitale Nachweise

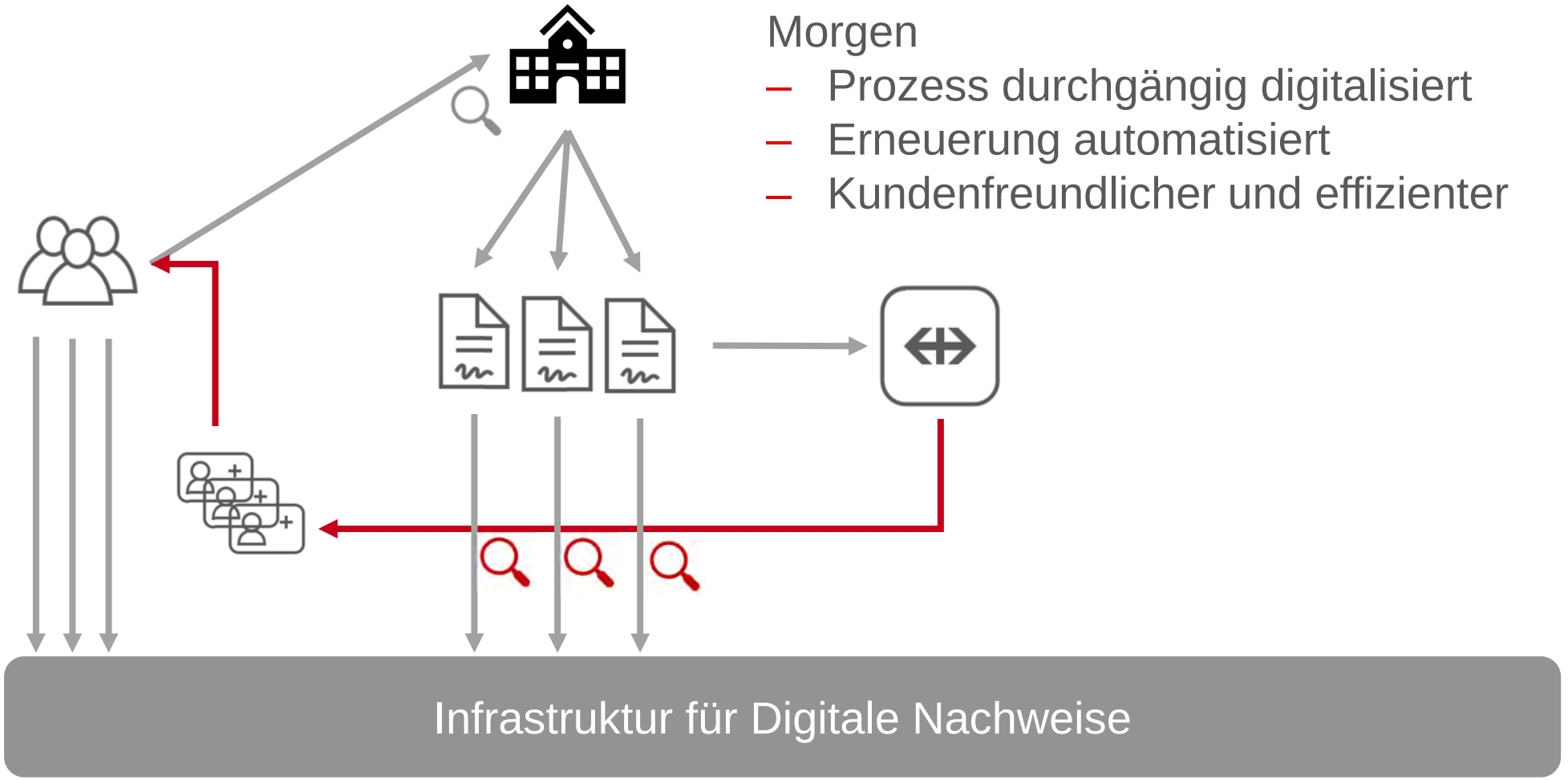
Aktuelles Beispiel: Wohnsitzbestätigung für Partner- und Familien-GA

Heute

- Prozess mit Medienbrüchen
- Wiederholt sich jährlich z.T. mehrfach
- Hohe Nachbearbeitungsrate
- Wenig kundenfreundlich und teuer



Aktuelles Beispiel: Digitale Wohnsitzbestätigung für Partner- und Familien-GA (proof of value/concept)



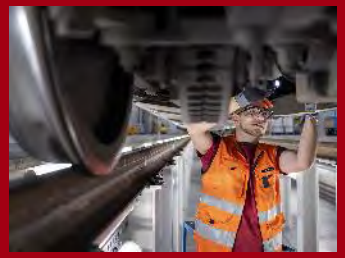
Morgen

- Prozess durchgängig digitalisiert
- Erneuerung automatisiert
- Kundenfreundlicher und effizienter

Prozesse über Unternehmens- und Landesgrenzen hinweg durchgängig digitalisieren

- Identifikation von Menschen und Dingen (IoT)
- Zugangsschlüssel
- Ausbildungs- und Gesundheitsnachweise
- Digitale Signaturen
- Herkunfts- und Wartungsnachweise

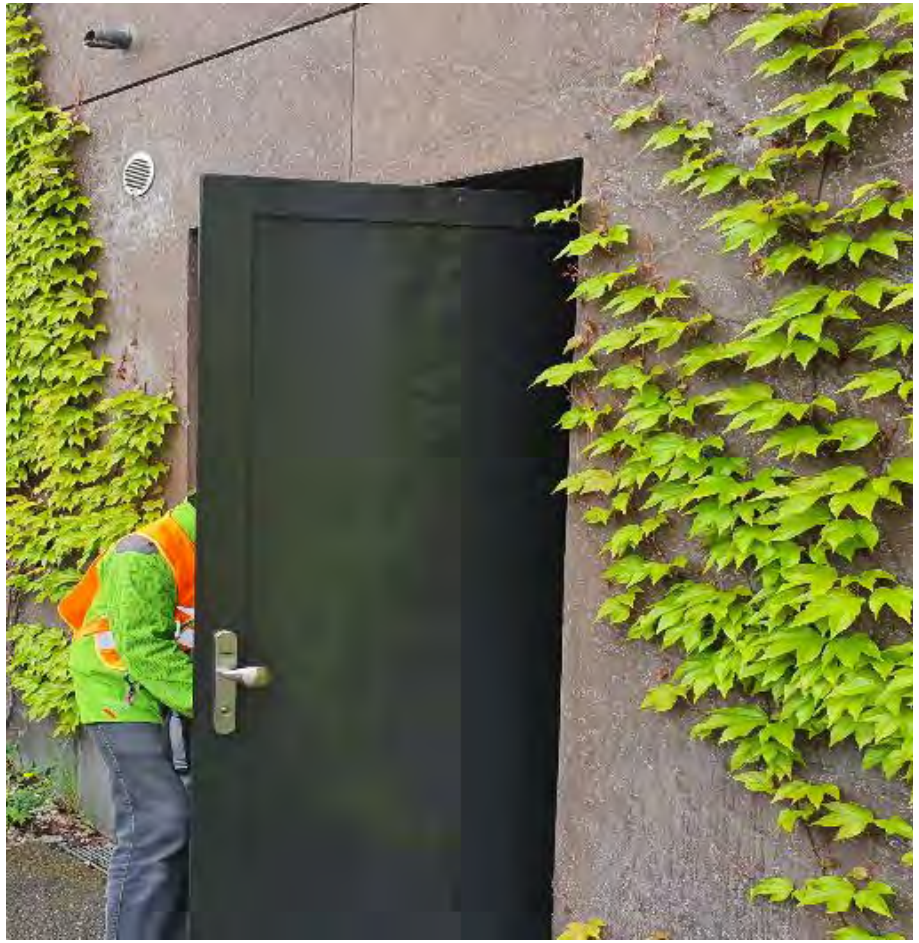
Prozess-Integration

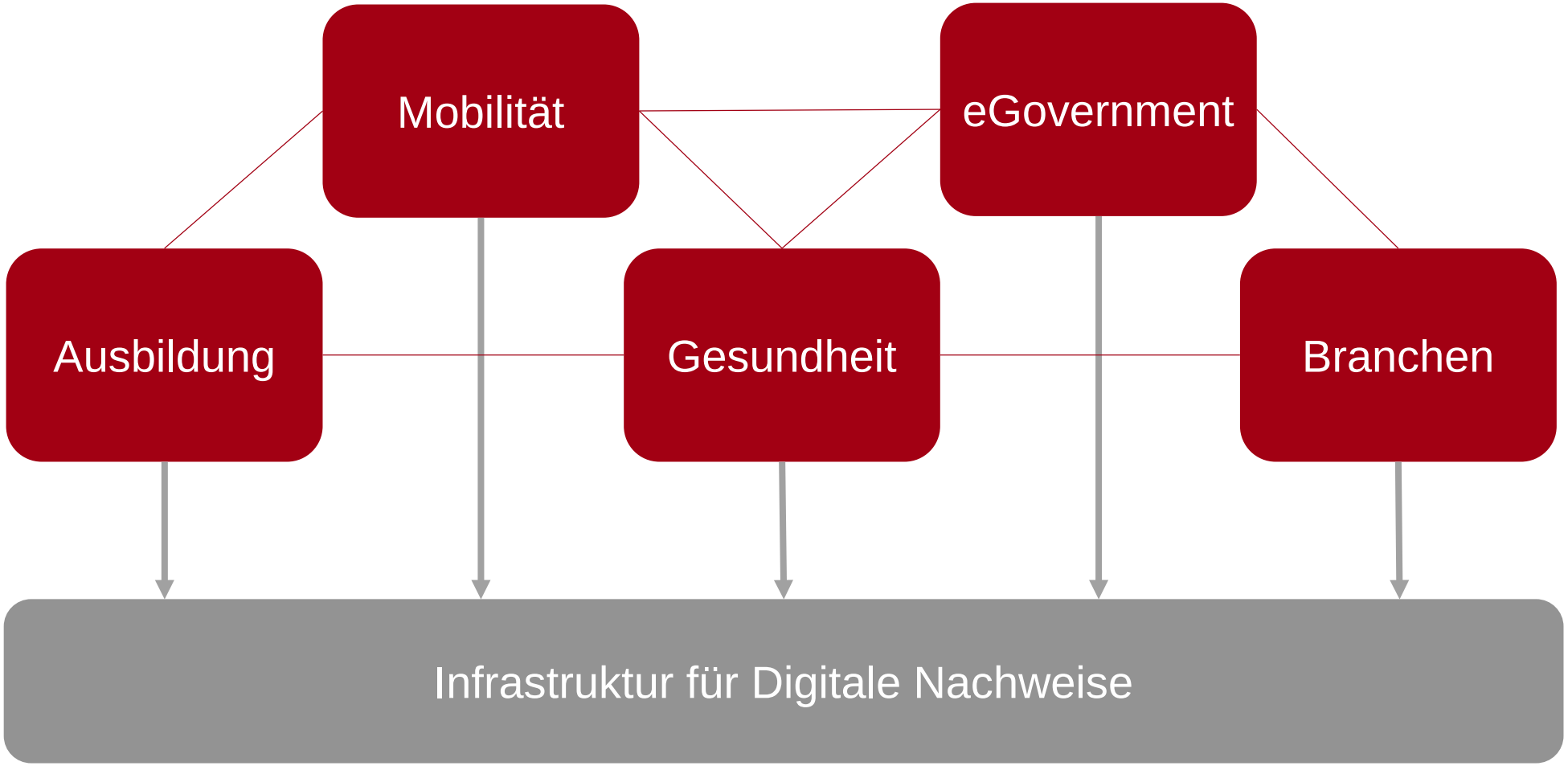
Infrastruktur für Digitale Nachweise

Aktueller Pilot: Zugang zu Bahntechnikgebäude im Bahnhof Solothurn auf Basis von Qualifikationen

- 5 Türen
- 16 digitale Nachweise
- 60 interne und externe Testpersonen aus den Bereichen Sicherheitsanlagen, Telecom, HLK, Immobilien



Auf Basis einer gemeinsamen Infrastruktur können Ökosysteme ihre digitalen Nachweise entwickeln




SBB CFF FFS
Danke, merci
& grazie.

E-ID-Use-Cases aus der Praxis

Syrian Hadad

Kanton Aargau

KANTON AARGAU

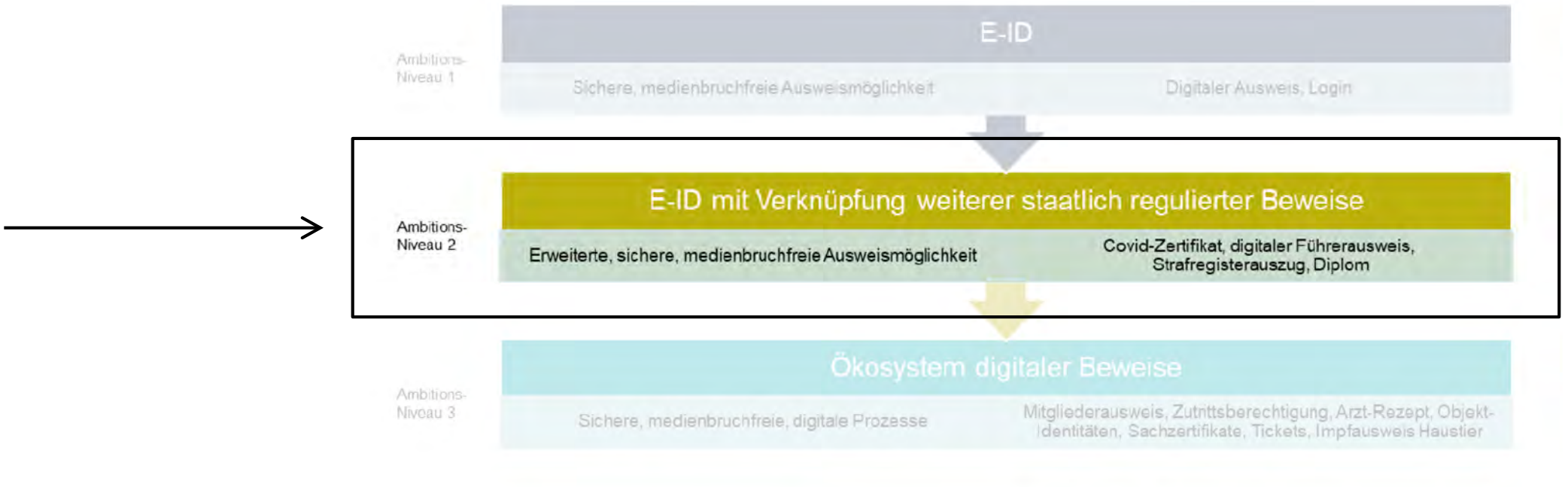
DEPARTEMENT
FINANZEN UND RESSOURCEN

Digitale Wohnsitzbescheinigung

Self-Sovereign Identity-Initiative

Syrian Hadad
14. Oktober 2021 @ E-ID Konferenz Bern

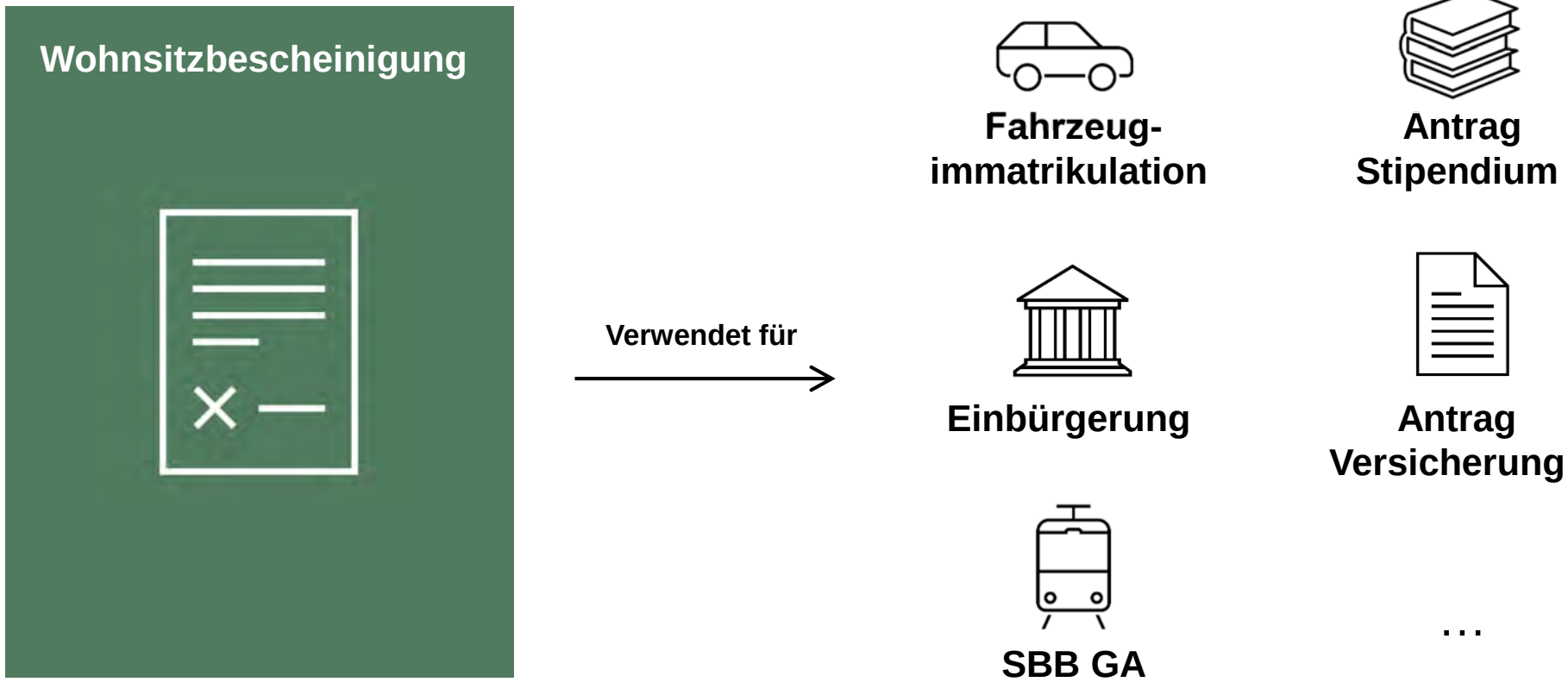
Fokus des Kantons Aargau im Kontext des E-ID-Ökosystems



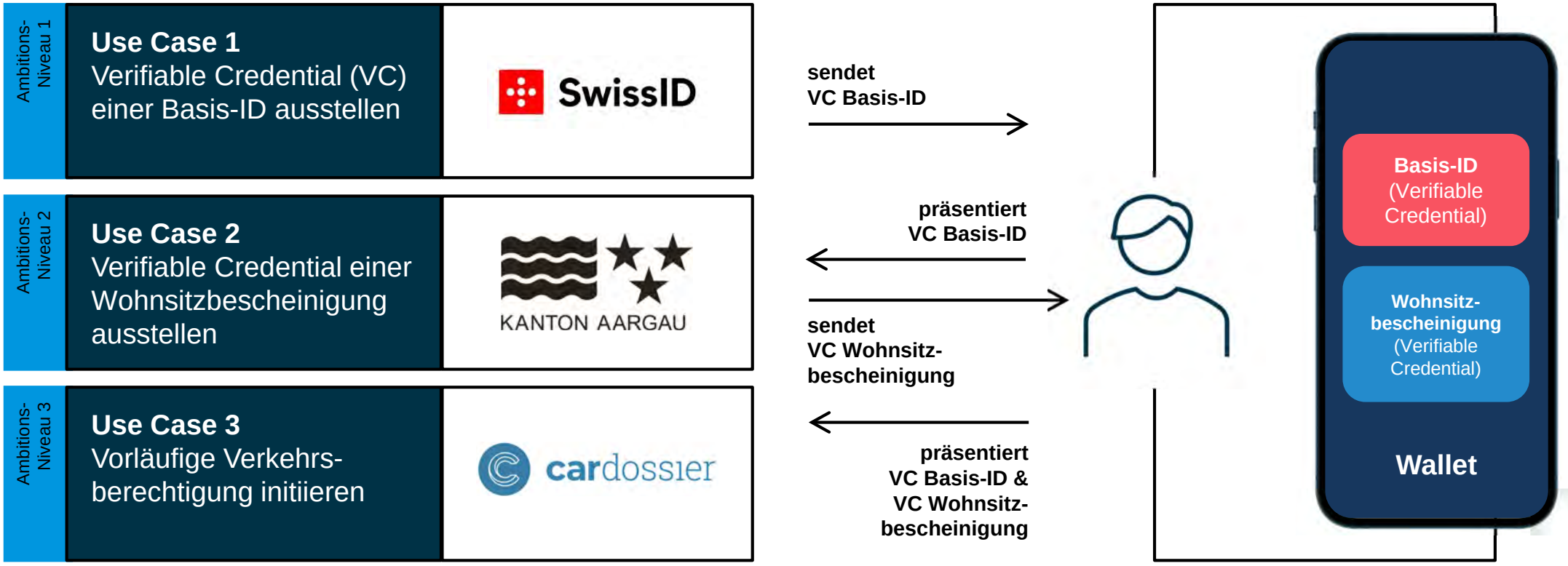
Quelle: Diskussionspapier zum «Zielbild E-ID»

Wohnsitzbescheinigung:

Beispielhafter Nachweis des Ambitionslevels 2



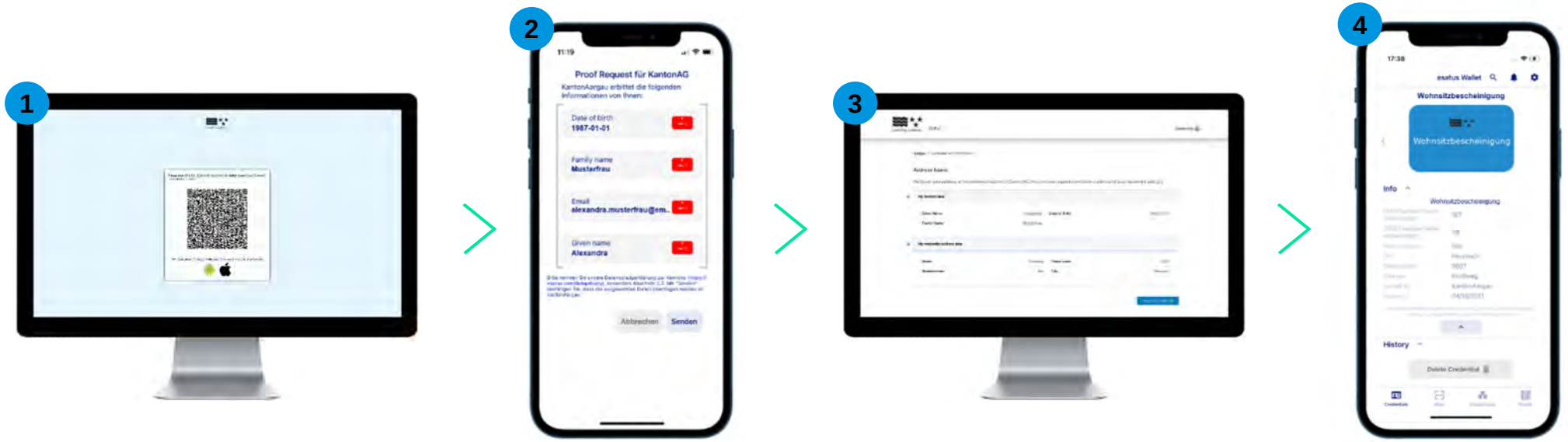
Self-Sovereign Identity-Initiative



Powered by adnovum

Use Case 2:

Verifiable Credential einer **Wohnsitzbescheinigung** ausstellen



Datenanfrage via QR Code	Datenversand der Basis ID aus dem Mobile Wallet	Anzeigen der Wohnsitz-adresse und Senden der Wohnsitzbescheinigung	Prüfung und Speicherung Wohnsitzbescheinigung als Verifiable Credential

Übermittlung selektiver Daten der Basis-ID → **Herausgabe der Wohnsitzbescheinigung** →

Fazit

- Als Verwaltung ist es unsere Verantwortung, nicht nur unsere eigenen eGov-Prozesse zu optimieren, sondern auch die **Digitalisierung** weiterer **öffentlicher** und **privater Geschäftsfälle** zu **fördern**

- Self-Sovereign Identity (SSI) ermöglicht eine effiziente Herausgabe, aber vor allem auch eine **flexible Nutzung** der ausgestellten Nachweise durch die anderen Beteiligten

- Somit und dank der kombinierten Verwendung von Verifiable Credentials unterstützt SSI den effizienten und flexiblen **Bau** des **gesamten Ökosystems** digitaler Nachweise (Ambitionslevel 2 und 3)

Vielen Dank für Ihre Aufmerksamkeit!

Bei Fragen zur Initiative

Syrian Hadad
CTO
Kanton Aargau
syrian.hadad@ag.ch

Tom Sprenger
CTO
SwissSign Group AG
tom.sprenger@swisssign.com

This Loepfe
CTO
Verein cardossier
matthias.loepfe@cardossier.ch

Stéphane Mingot
Head of AdNovum Incubator
Adnovum Informatik AG
stephane.mingot@adnovum.ch

KANTON AARGAU

SwissSign

cardossier

adnovum

E-ID-Use-Cases aus der Praxis

Nicolas Lemaitre

Stadt Zug

Stadt Zug

E-ID Konferenz, Use-Cases aus der Praxis

eZug – Smart City App der Stadt Zug, Nicolas Lemaitre

Einführungsvideo eZug

eZug – Smart City App der Stadt Zug

Das ist eZug

eZug – Smart City App der Stadt Zug
Elektronische Identität

Motion vom 10. März 2021:

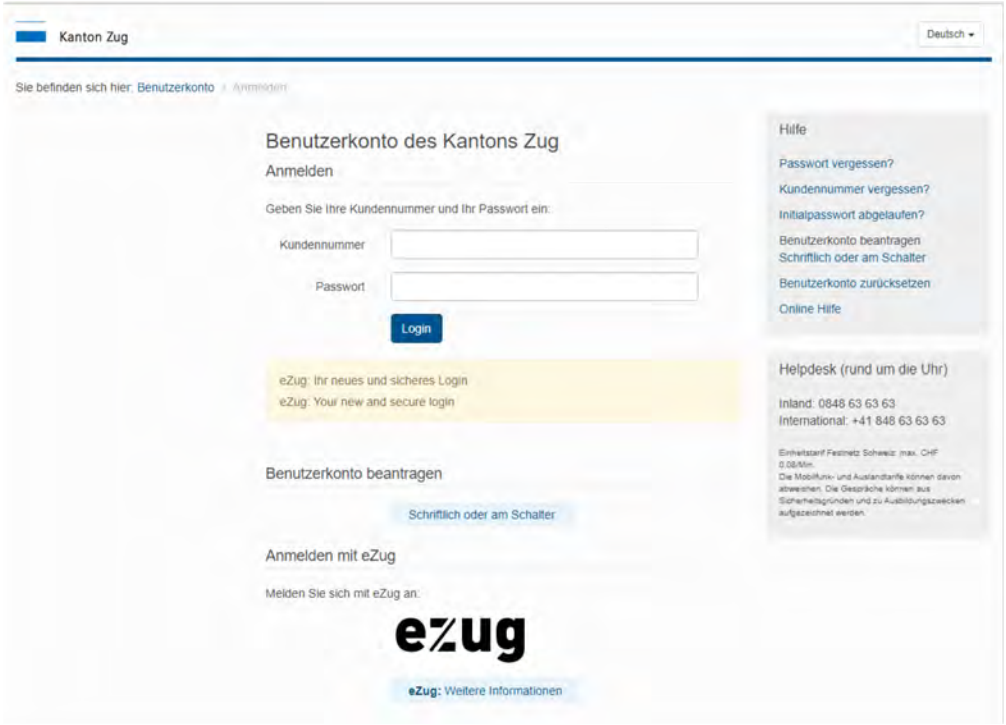
- ✓ Verantwortung für den Ausstellungsprozess und den Gesamtbetrieb bei staatlichen Behörden (Stadt Zug)
- ✓ Staatliches elektronisches Identifikationsmittel vergleichbar mit Pass (Zuglogin)
- ✓ Dezentrale Datenspeicherung (Smartphone)

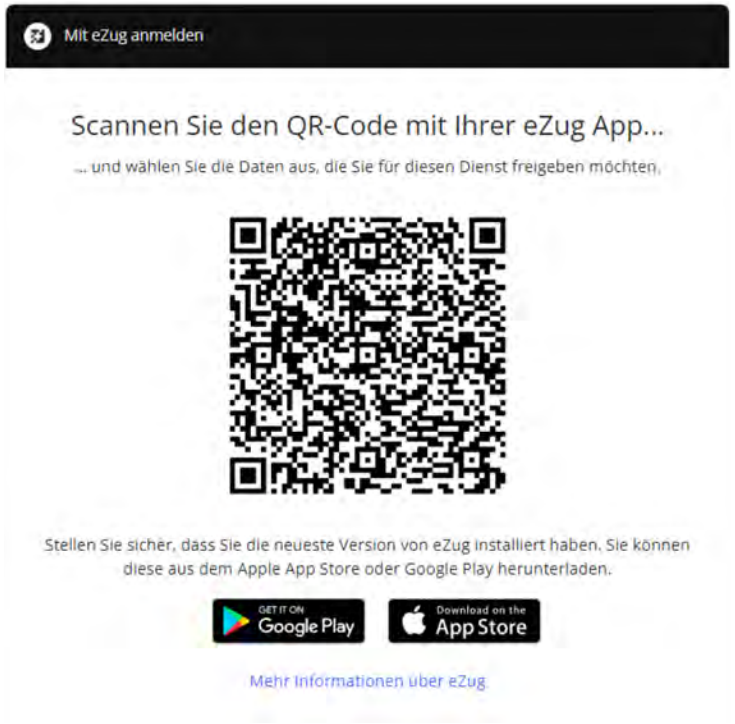
→ "Zielbild E-ID":
Ambitions-Niveau 1

eZug – Smart City App der Stadt Zug
Elektronische Identität

Motion vom 10. März 2021:

✓ Datensparsamkeit und «privacy by design» (Kontrolle beim User)





eZug – Smart City App der Stadt Zug
Nutzen

Eine E-ID hat keinen inhärenten Nutzen!

Aufgabe für Kantone und Gemeinden:
Baut das Haus (=Anwendungen), Schlüssel und Schloss (=E-ID) alleine bringt keinen Nutzen.

eZug – Smart City App der Stadt Zug
Anwendungen

Dienstleistungen der Einwohnerkontrolle:
- Handlungsfähigkeitszeugnis
- Heimatausweis
- Leumundszeugnis
- Wohnsitzbescheinigung

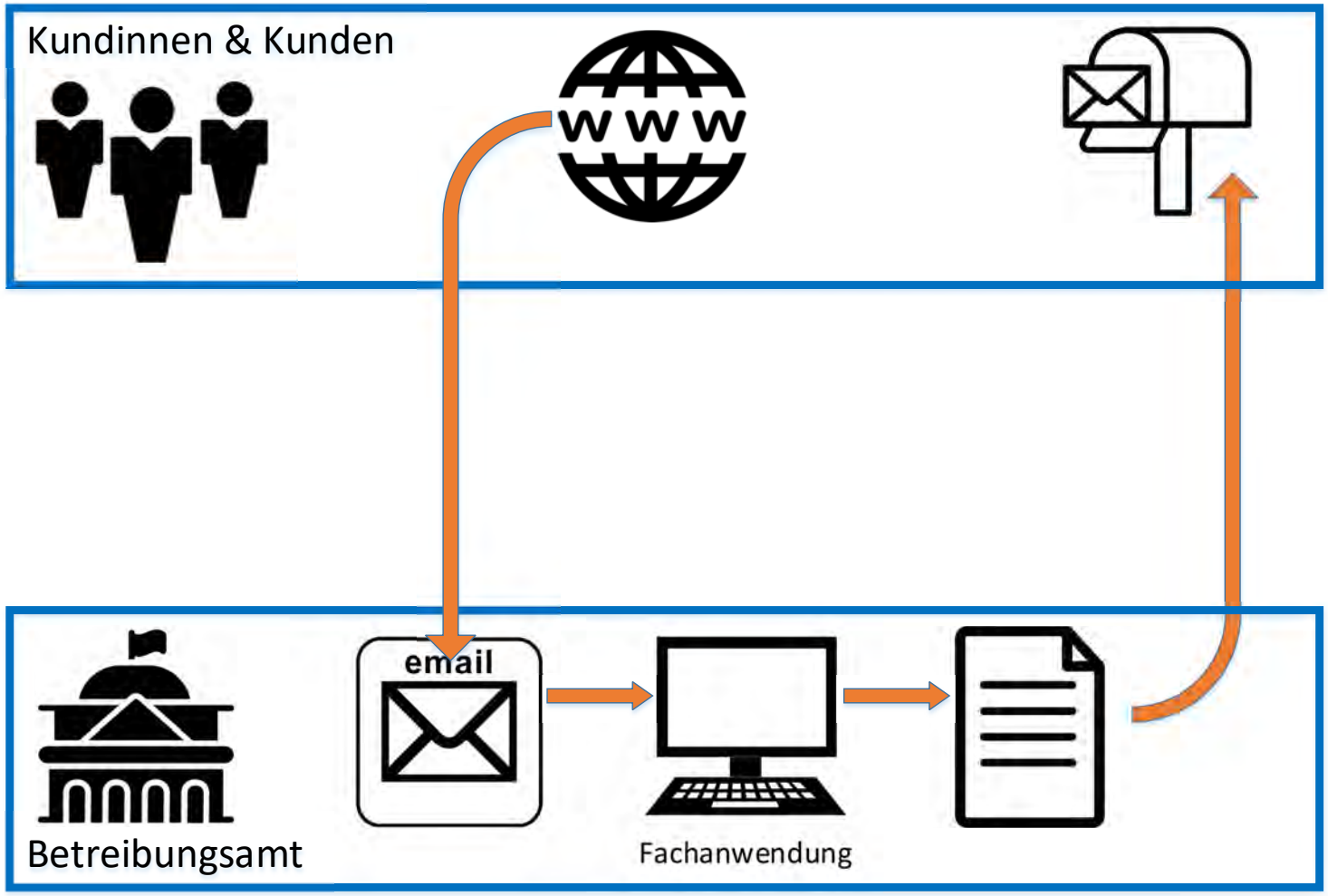
Dienstleistungen des Betreibungsamts:
- Betreibungsauszug (Selbstauskunft)
- Betreibungs- und Fortsetzungsbegehren

Elektronisches Siegel beweist Echtheit der Dokumente.

eZug – Smart City App der Stadt Zug

Anwendungen

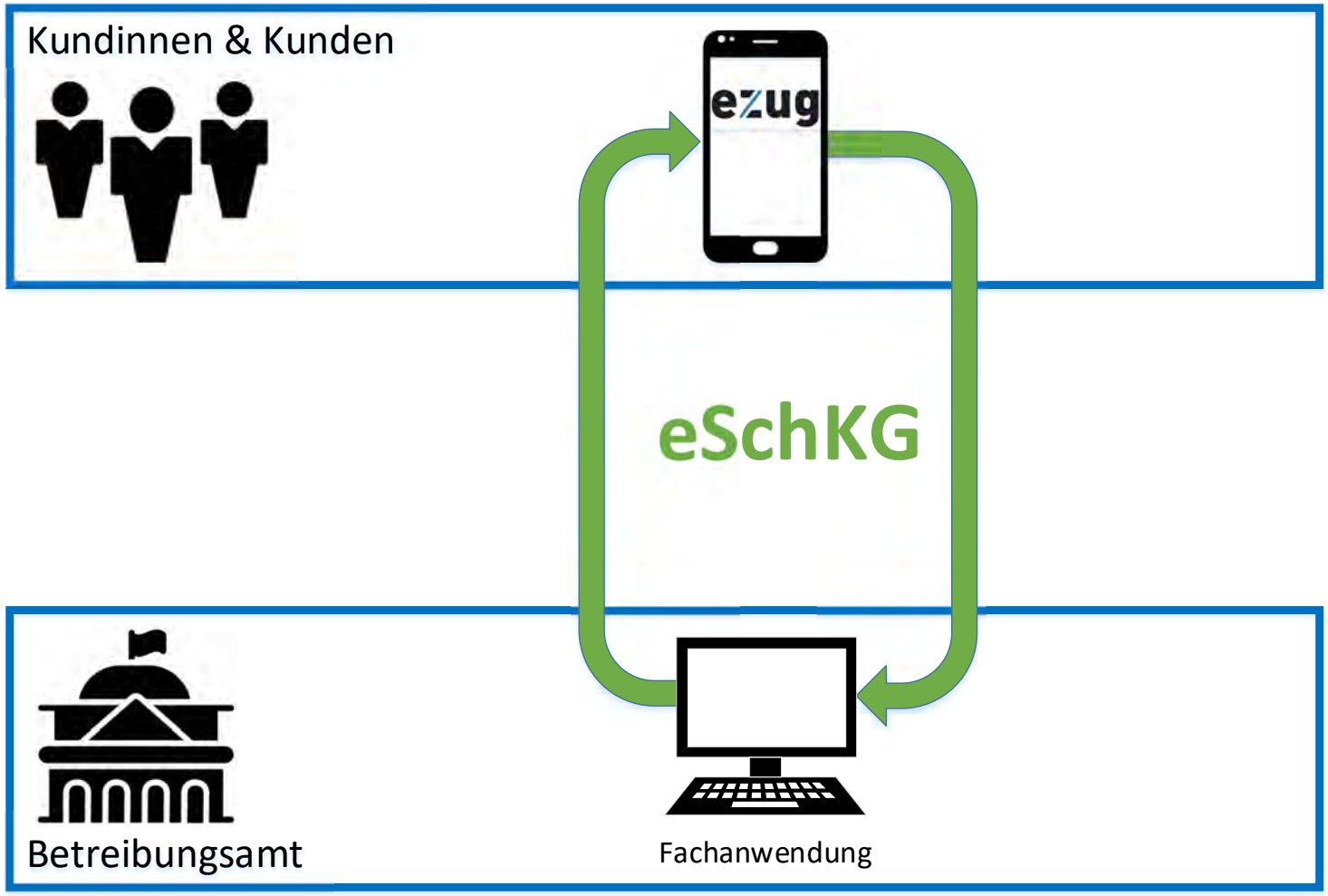
Betreibungsamt ohne eZug & eSchKG



eZug – Smart City App der Stadt Zug

Anwendungen

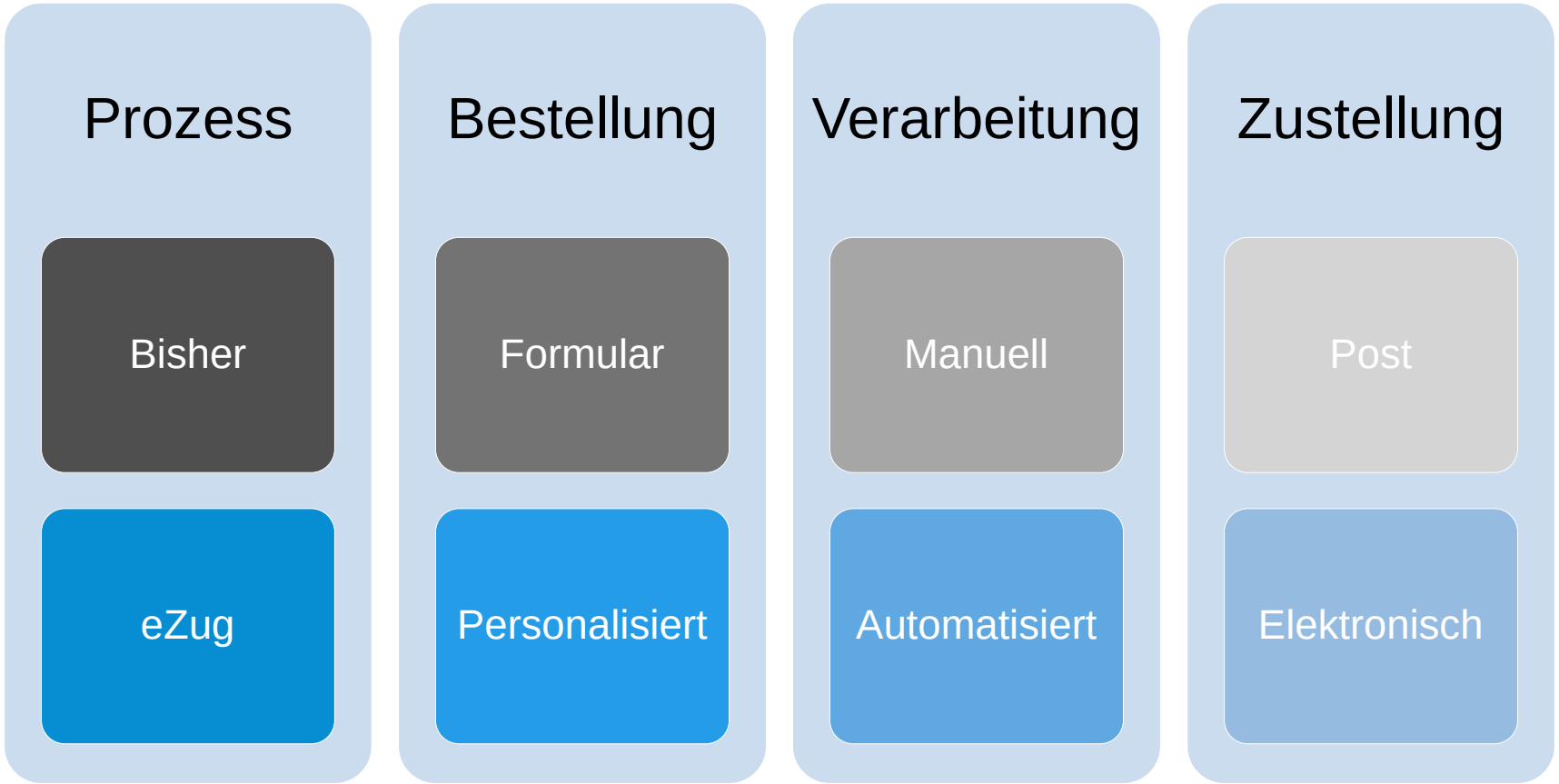
Betreibungsamt mit eZug & eSchKG



eZug – Smart City App der Stadt Zug

Anwendungen

Fazit



E-ID-Use-Cases aus der Praxis

Andreas Frey Sang

Bundesamt für Informatik und Telekommunikation

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Bundesamt für Informatik und Telekommunikation BIT

Praxisbeispiel: Covid-Zertifikat

Öffentliche Konsultation zum «Zielbild E-ID» — 14.10.2021


E-ID


9:41
COVID-ZERTIFIKAT
Studer Martina
14.03.1964
Nur mit einem
Ausweisdokument gültig


Impftermin buchen
Ich werde geimpft
Mein Zertifikat wird ausgestellt
Ich erhalte mein Zertifikat
Ich weise das Zertifikat vor

Impftermin buchen

Geprüfte digitale Identität als Unterstützung um sich für einen Impftermin anzumelden:

- Erhöhte Nutzungsfreundlichkeit & Datenqualität
- Erster Vertrauensanker wird gesetzt
- Verbreitung/Einsatz eindeutiger Identifikatoren ist nicht gegeben

Ich werde geimpft

Erhöhtes Vertrauen in Gesamtprozess:

- Nachvollziehbarkeit: Person, welche vor mir steht, ist jene, welche sich angemeldet hat
- Verifikation von Personendaten vs. erneute Eingabe
- Verhinderung von nachträglicher Korrektur, weil Personalien nicht übereinstimmen

Impftermin buchen

Ich werde geimpft

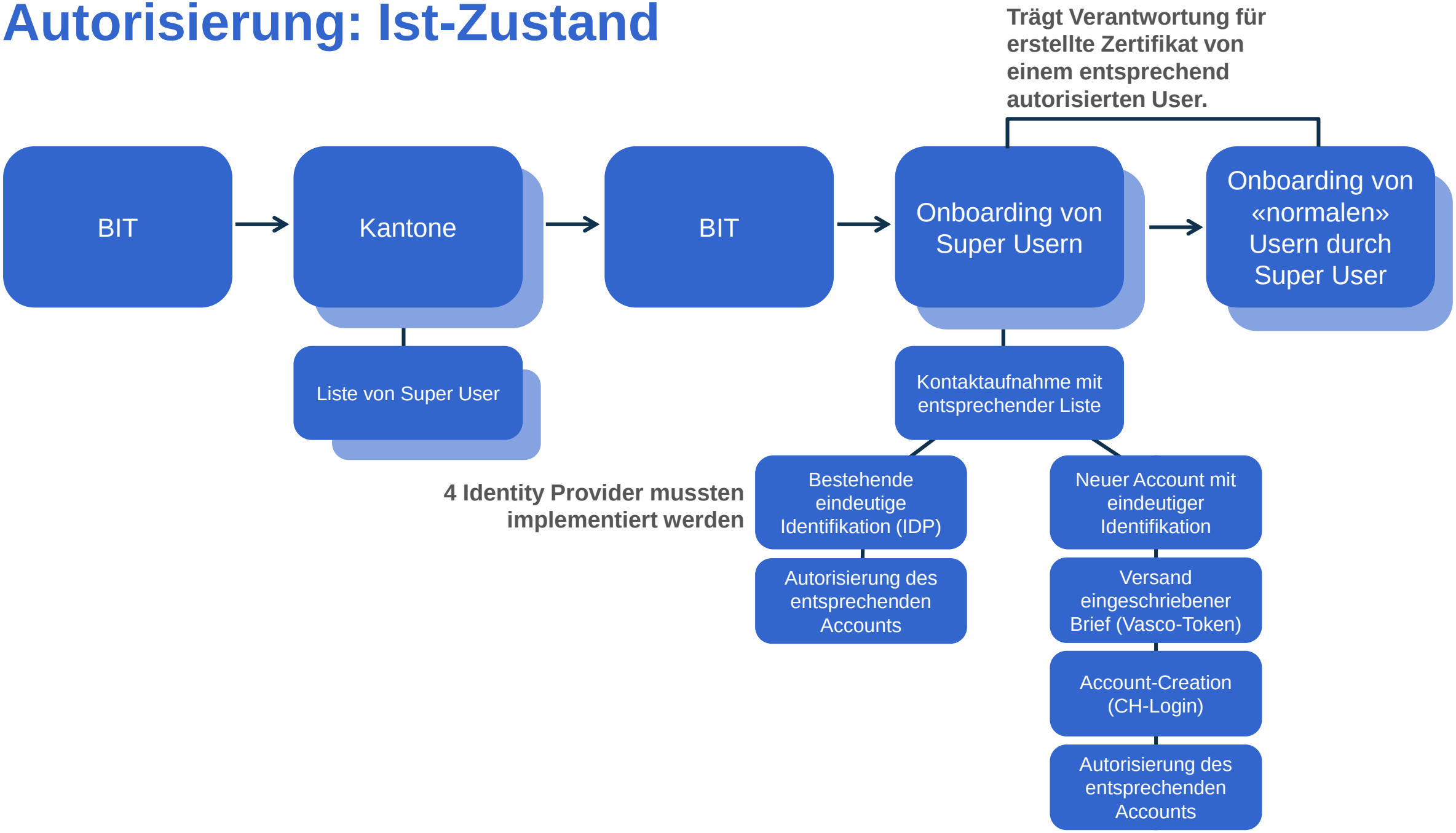
Mein Zertifikat wird ausgestellt

Ich erhalte mein Zertifikat

Ich weise das Zertifikat vor


Wer ist autorisiert Zertifikate auszustellen?

Autorisierung: Ist-Zustand



Autorisierung: Idealvorstellung

Login basierend auf E-ID mit entsprechendem Credential

Wer ist autorisiert Zertifikate auszustellen?

- Eindeutige Identifikation von Aussteller*innen
- Grosses Potenzial Geschäftsprozesse zwischen unterschiedlichen föderalen Akteuren (Bund, Kantone, Private, Wirtschaft) zu vereinfachen.
- Digitale Identität als einheitliches Login für die Interaktion mit dem Staat
- Missbrauchspotenzial «Account»-Weitergabe vs. «E-ID»-Weitergabe
  - Vereinfachtes Monitoring von Missbrauchsfällen
- Zertifikatssignatur basierend auf digitaler Identität des Ausstellers

Ich erhalte mein Zertifikat

- Inhalt des Zertifikates = Besonders schützenswerte Personendaten
- Zustellung soll auf sicherem Kanal erfolgen
- Postalischer Weg / Transfer Code / Delegation an Aussteller*innen

- Grosses Potenzial die E-ID als sicherer Identifikator für die Zustellung von vergleichbaren Dokumenten zu verwenden

Ich weise das Zertifikat vor

- Verknüpfung von Immunitätsnachweis und digitaler Identität
- Kombinierte Prüfung von Identität und Immunität
- Hinterlegung in Drittsystemen – Zugang mit remote Biometrie Überprüfung
- Light-Zertifikat zur Wahrung des Datenschutzes
  - SSI hätte dies wohl «hinfällig» gemacht
- Erhöhter Datenschutz je nach gewählter technologischen Variante
- Grosses Bedürfnis nach Kombination von Identität, Zugang/Mitgliedschaft und Immunitätsnachweis
  - Ambitionsniveau 3

Key Learnings

Generell:

- Ohne digitale Identität müssen «Umgehungslösungen» gebaut werden
- Gesetzesgrundlage, welche erlaubt, dass für staatliche «Geschäftsprozesse» Credentials «flexibel» vergeben werden können.
- Grosses Potenzial für Einsatz im Gesundheitswesen:
  - Datenschutz (Privacy by Design)

Key Learnings

In Bezug auf das Covid-Zertifikat:

- Erhöhte Nutzungsfreundlichkeit
  - Gerade im fragmentierten Gesundheitswesen
- Erhöhtes Vertrauen ins Gesamtsystem, wenn sämtliche Akteure anhand einer digitalen Identität identifizierbar sind
- Werkzeug/Basis für effizientere Pandemiebekämpfung
  - Ressourcen müssen nicht in Umgehungslösungen investiert werden


MITTAGSPAUSE

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz

Wie soll eine E-ID umgesetzt werden?

Daniel Markwalder

Bundeskanzlei, Bereich DTI

Technologie und Rechtsetzung

- Technologie soll nicht im Vordergrund stehen.
  Wichtiger ist
  - erstens, was man erreichen will (Nutzen) und
  - zweitens, welche Eigenschaften umgesetzt werden sollen (Datensparsamkeit, Privacy by Design, etc.)

- Technik muss sich danach ausrichten. Ausserdem: Technik und Gesetzgebung müssen stärker zusammenspielen
  (nicht nur, aber *auch* bei E-ID)

- Ziel: Bereits während Gesetzgebung Erfahrungen sammeln

Lösungsansätze im Diskussionspapier

SSI – Self-Sovereign Identity

PKI – Public Key Infrastructure

IdP – staatlicher Identitätsprovider

Lösungsansatz «IDP»

(Identity Provider)

- Bei der Person wird nur Zugang (Login) abgespeichert.
  Es braucht zentralen Speicher, der die Logins mit den Eigenschaften (Name, Vorname, Geburtsdatum, etc.) verknüpft ➔ Identity Provider
  Im Gegensatz zur gescheiterten E-ID: Staatlicher IDP
- *Metapher: «Beglaubigungsautomat»*

Lösungsansatz «IDP»

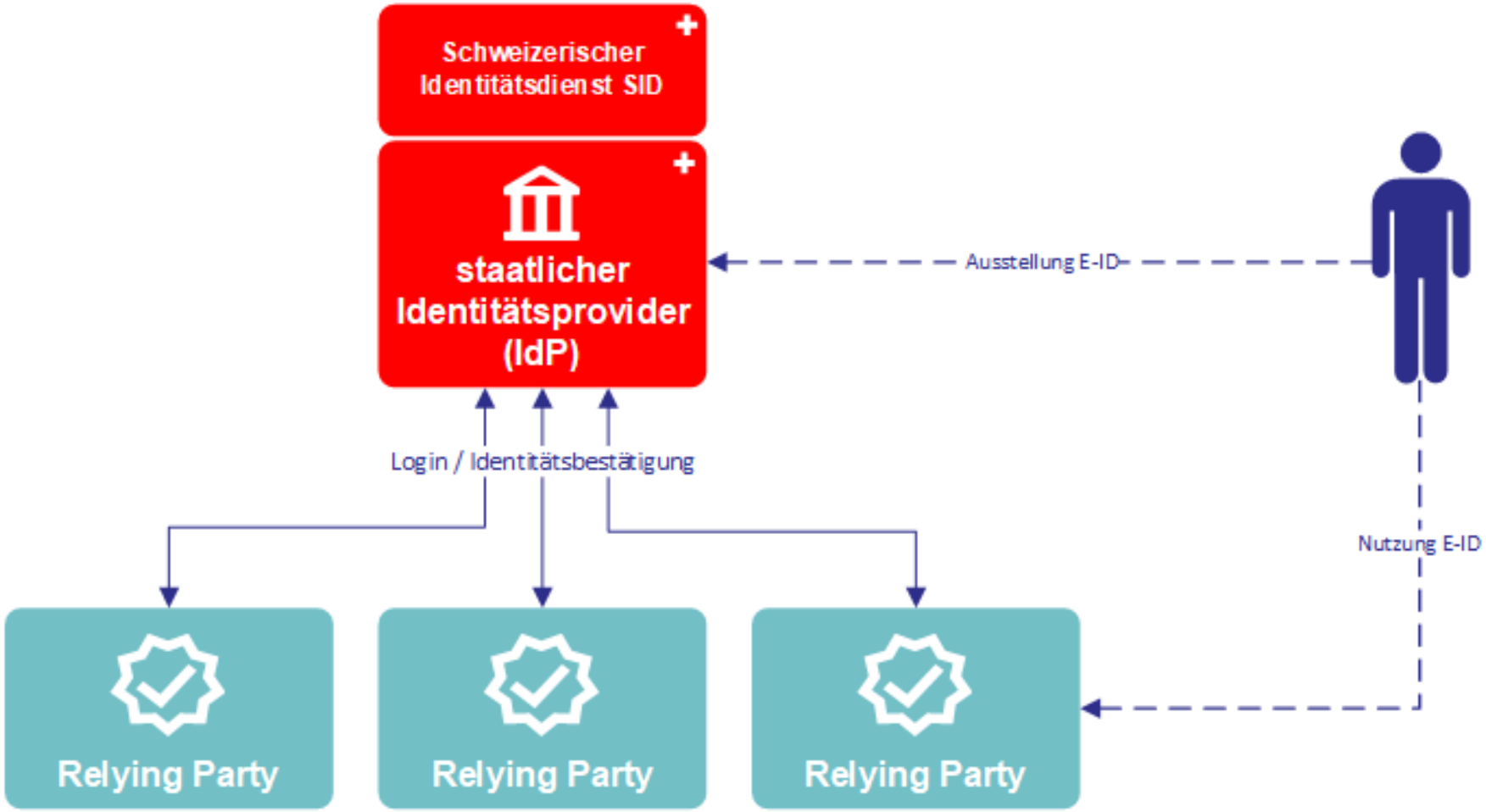
(Identity Provider)

- Bei der Person wird nur Zugang (Login) abgespeichert.
  Es braucht zentralen Speicher, der die Logins mit den Eigenschaften (Name, Vorname, Geburtsdatum, etc.) verknüpft ➔ Identity Provider
  Im Gegensatz zur gescheiterten E-ID: Staatlicher IDP
- *Metapher: «Beglaubigungsautomat»*

- Einige Vor- und Nachteile:

+ Breit genutzte Technologien und Protokolle (insb. Anwendungsseite) **+** Einfache Architektur	**-** Keine Trennung Ausstellung und Nutzung. Beim IDP fallen viele Daten an (auch bei der Verwendung) **-** Systemabhängigkeit vom IDP; breite Nutzung erschwert

Infrastruktur IdP-Lösungsansatz



Lösungsansatz «PKI» (only)

(Public Key Infrastructure)

- Bei der Person wird Identität abgespeichert in Form eines starren Ausweises, der vom Staat ausgestellt wird.
  Es handelt sich um ein Set von Angaben. Mit einem «privaten Schlüssel» beweist die Inhaberin, dass sie die zu diesen Angaben passende Person ist
- *Metapher: «Grosser Siegelring»*

Lösungsansatz «PKI» (only)

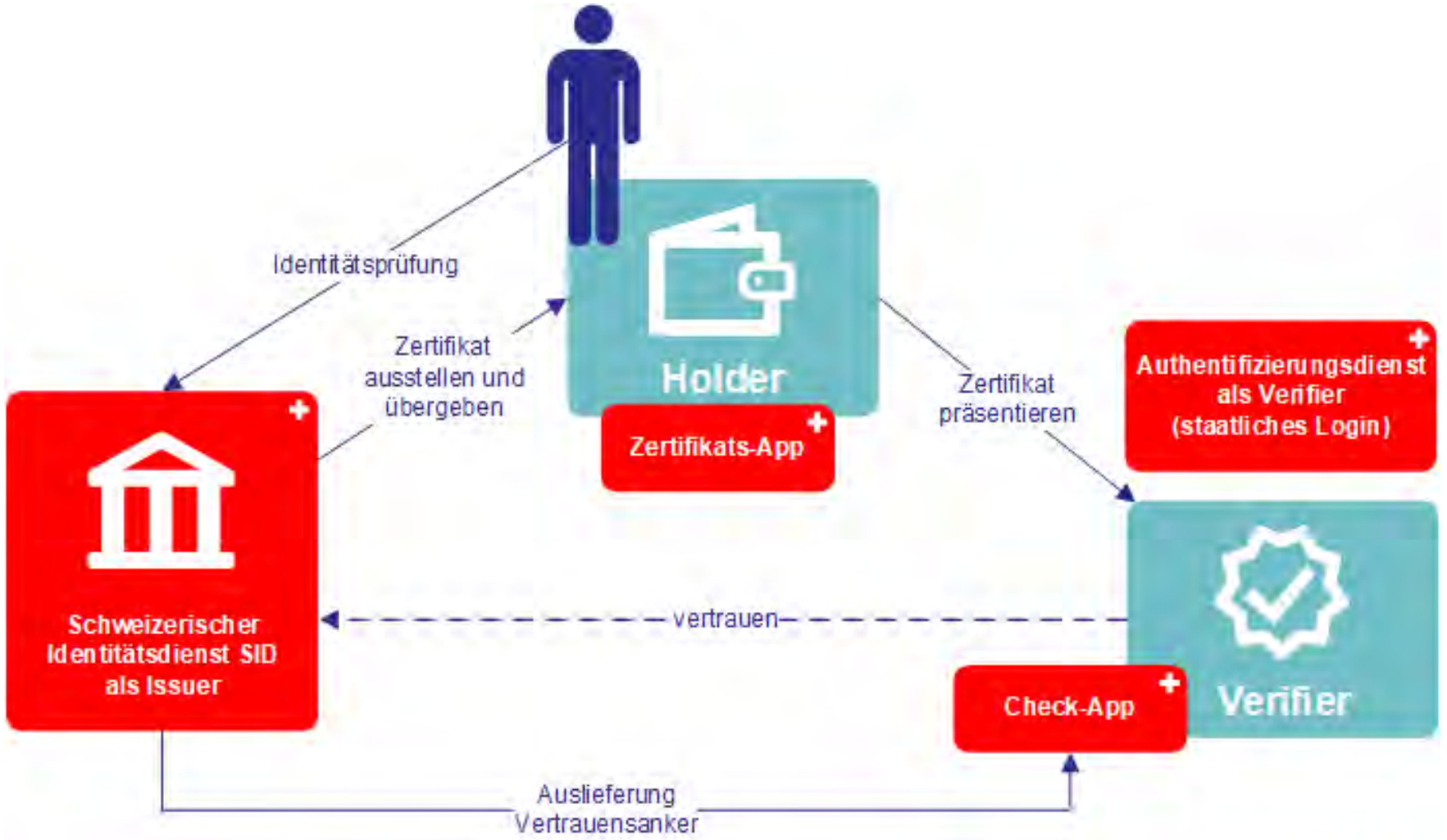
(Public Key Infrastructure)

- Bei der Person wird Identität abgespeichert in Form eines starren Ausweises, der vom Staat ausgestellt wird.
  Es handelt sich um ein Set von Angaben. Mit einem «privaten Schlüssel» beweist die Inhaberin, dass sie die zu diesen Angaben passende Person ist
- *Metapher: «Grosser Siegelring»*

- Einige Vor- und Nachteile:

+ Etablierte Technologie **+** Keine Randdaten bei der Nutzung, kein IDP nötig (aber möglich für zusätzliche Eigenschaften und/oder als Broker für Anwendungen)	**-** Starres Konstrukt: Man gibt immer alle Daten im "Ausweis" ab und kann diese nicht erweitern.

Infrastruktur PKI-Lösungsansatz



Lösungsansatz «SSI»

(Self-Sovereign Identity)

- Bei der Person wird Identität in einer Wallet abgespeichert in Form eines flexiblen Ausweises. Wallets sind auch zur Speicherung anderer digitalen Nachweise nutzbar. Basistechnologie ist wie bei PKI die asymmetrische Kryptografie
- *Metapher: «Brieftasche»*

Lösungsansatz «SSI»

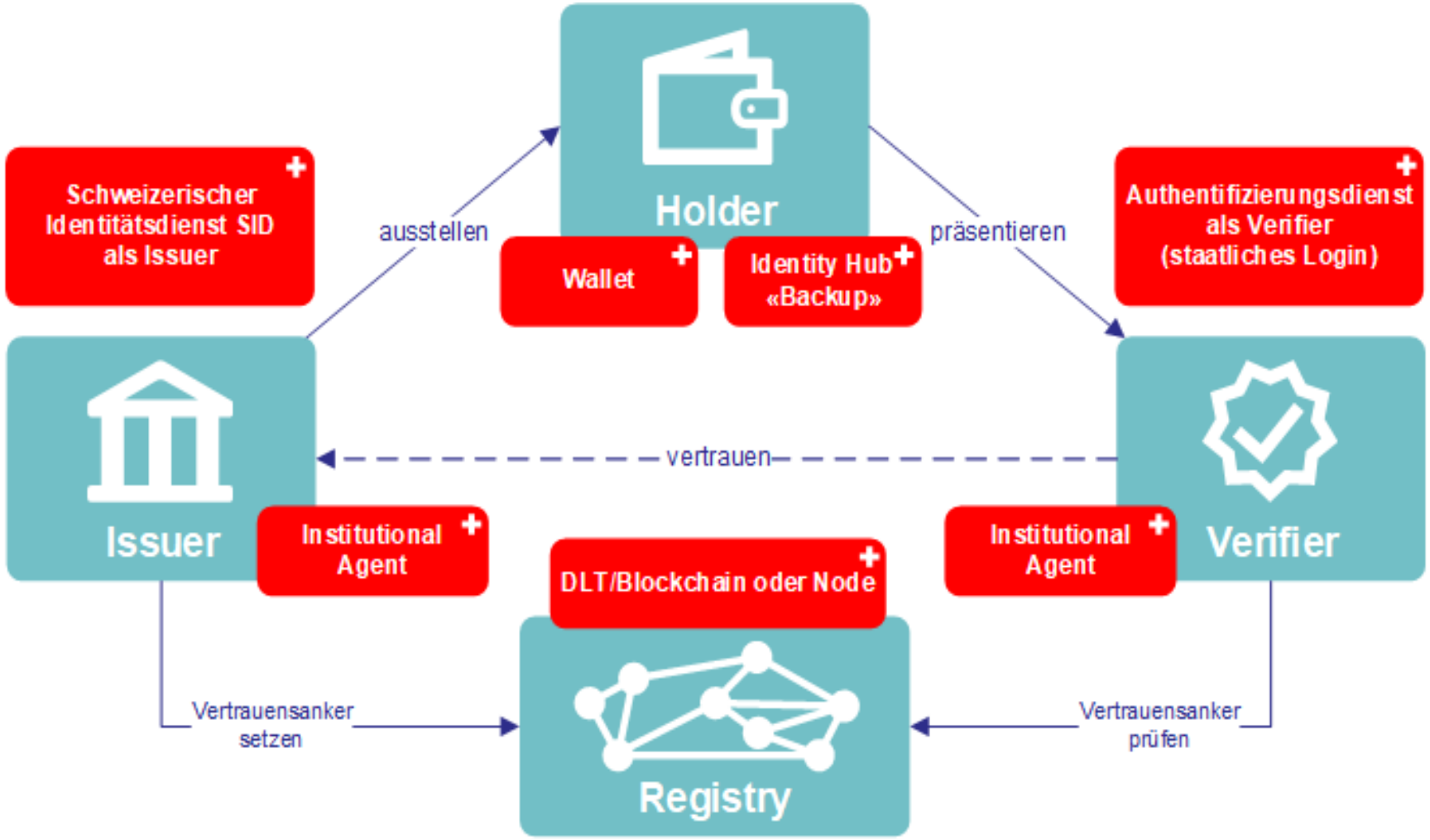
(Self-Sovereign Identity)

- Bei der Person wird Identität in einer Wallet abgespeichert in Form eines flexiblen Ausweises. Wallets sind auch zur Speicherung anderer digitalen Nachweise nutzbar. Basistechnologie ist wie bei PKI die asymmetrische Kryptografie
- *Metapher: «Brieftasche»*

- Einige Vor- und Nachteile:

+ auf Datenschutz, Daten-sparsamkeit und «privacy by design» ausgerichtet **+** Anbindung Drittsysteme mit direktem Kommunikationskanal **+** Internationale Entwicklung geht in diese Richtung	**-** Junge Technologie (noch in Entwicklung)

Infrastruktur SSI-Lösungsansatz



Self-Sovereign Identity Anwendung

Fazit: Technische Aspekte

- Offenheit von SSI ist Risiko und Chance
- Es sind keine strikte «Entweder-Oder» Ansätze: SSI und PKI beruhen auf gleicher Technologie und ergänzen sich

Fazit: Technische Aspekte

- Offenheit von SSI ist Risiko und Chance
- Es sind keine strikte «Entweder-Oder» Ansätze: SSI und PKI beruhen auf gleicher Technologie und ergänzen sich
- Herausforderung bei allen Varianten. Z.B. wie «Geheimnis» gesichert wird: Nur im Telefon oder auf Hardware?
- Vermittler (IDP) kann in jeder Variante sinnvoll sein, um (bestehende) Anwendungen zu entlasten (Alternative/Ergänzung: offene SDK)

Fazit: Technische Aspekte

- Offenheit von SSI ist Risiko und Chance
- Es sind keine strikte «Entweder-Oder» Ansätze: SSI und PKI beruhen auf gleicher Technologie und ergänzen sich
- Herausforderung bei allen Varianten. Z.B. wie «Geheimnis» gesichert wird: Nur im Telefon oder auf Hardware?
- Vermittler (IDP) kann in jeder Variante sinnvoll sein, um (bestehende) Anwendungen zu entlasten (Alternative/Ergänzung: offene SDK)
- Paradigmenwechsel zur vorherigen E-ID:
  - Ausweis und nicht nur Login
  - Vision einer breit nutzbaren Infrastruktur der Schweiz
- Es ist wichtig, sich nicht zu früh auf eine Option einzuschiessen => Ausprobieren! Varianten

Wie soll eine E-ID umgesetzt werden?

Daniel Saeuberli

DIDAS

DIDAS

Der Weg zu einer vertrauenswürdigen Schweizer eID

Daniel Säuberli - daniel.saeuberli@didas.swiss

Bern, 14. Oktober 2021

Was ist DIDAS?

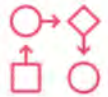
Digital Identity and Data Sovereignty Association

Wir sind eine Schweizer Non-Profit-Organisation, die sich für die Realisierung von selbstbestimmten digitalen Identitäten (SSI) in der Schweiz einsetzt.

Entmystifizierung von SSI für Menschen und Entscheidungsträger

Best Practices sammeln und weiterentwickeln

Experten Gemeinschaften verbinden und ausbauen

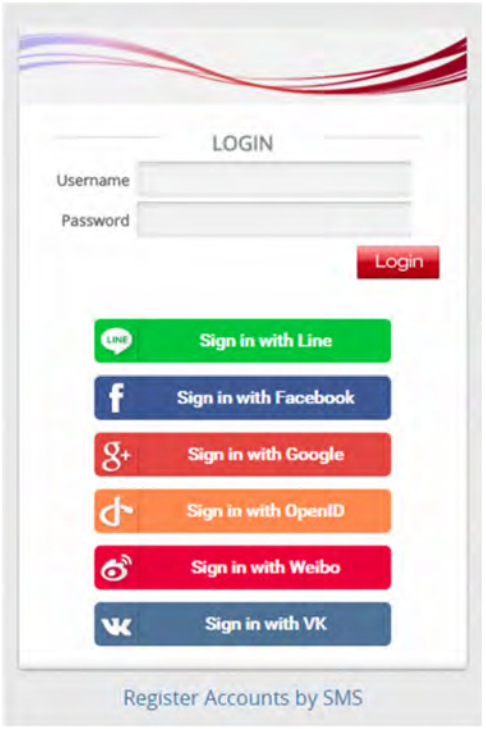


Anwendungsfälle identifizieren und fördern

Gedankenführung zu gesetzgeberischen und anderen Aspekten

Was sind…?

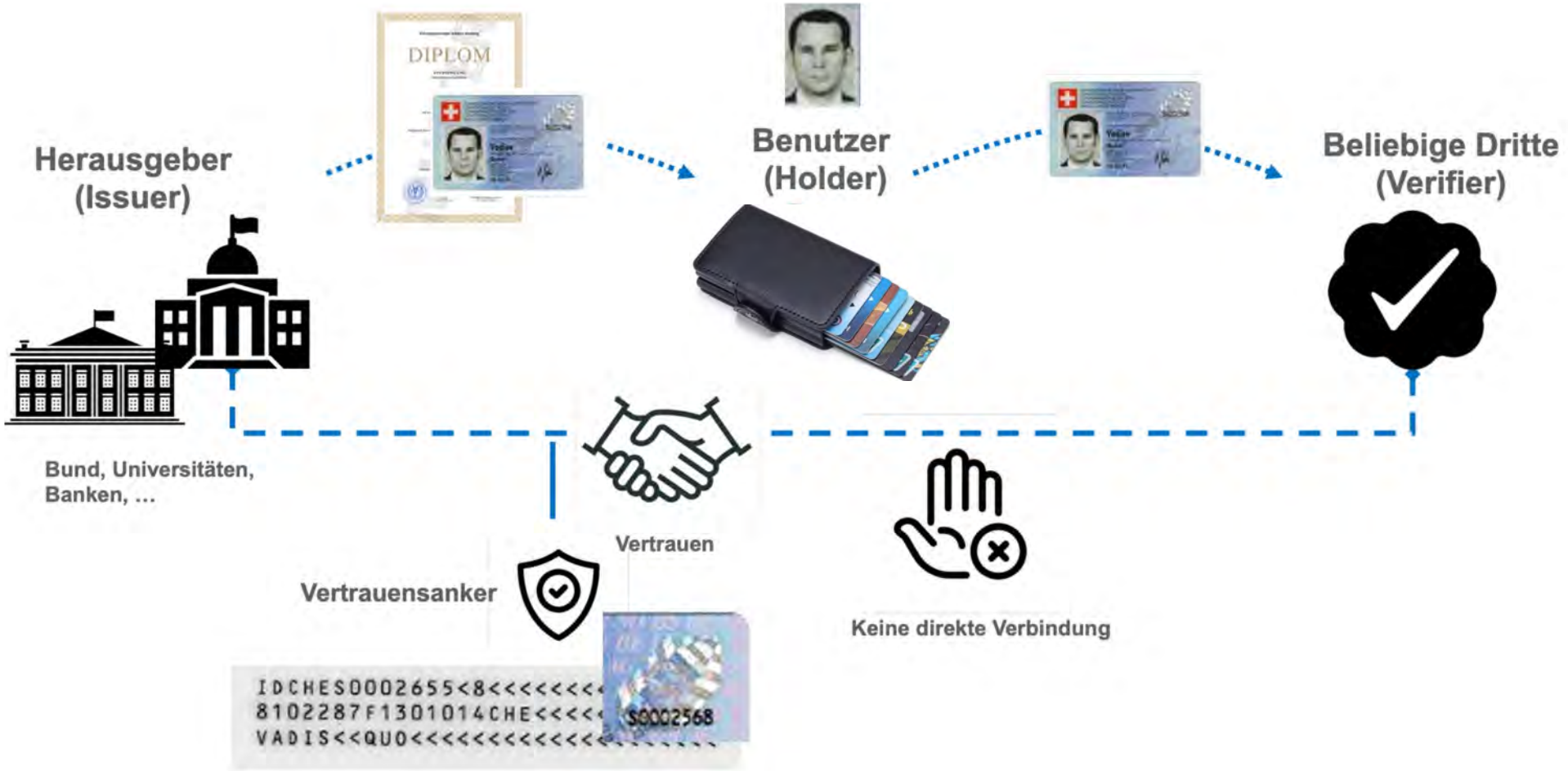
Physische (Identitäts-)Nachweise



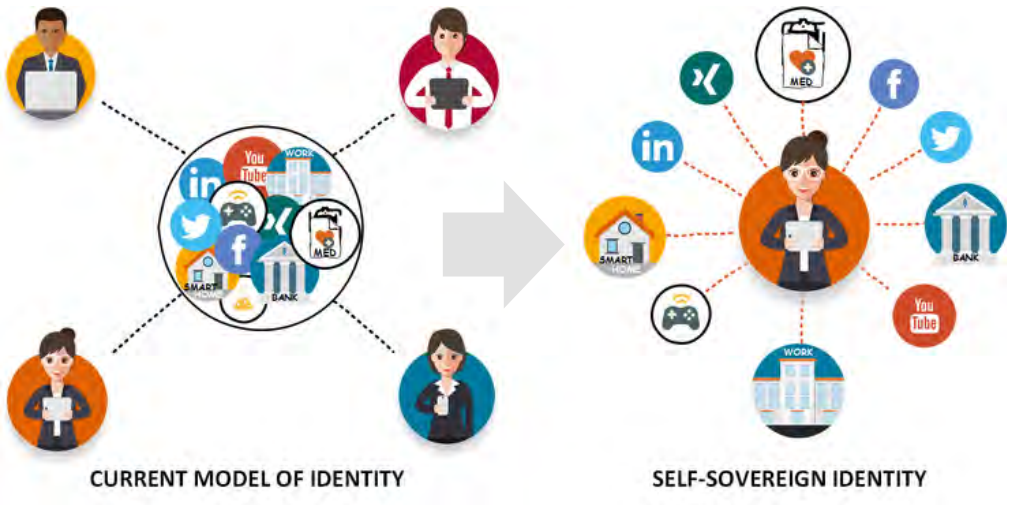
Digitale Silos und mächtige Intermediäre

Self-Sovereign Identity In einem Ökosystem

Digital soll sein wie normal - mit mehr Privatsphäre und Möglichkeiten



Warum «Self-Sovereign Identity»?



- Die selbstbestimmte Identität **oder Self-Sovereign Identity (SSI)** bringt die Identität wieder zurück zum Benutzer.
- Sie funktioniert ähnlich wie die physische Identität. **Der Benutzer hält die Identitätsdaten** bei sich (analog zur ID im Portemonnaie). Die Daten werden durch die herausgebende Partei kryptographisch bestätigt (analog einer Beglaubigung). Die prüfende Partei vertraut der herausgebenden Partei.
- Mit SSI wird die fehlende Identitätsfunktionalität des Internets oder allgemein digitaler Medien gelöst.
- Gleichzeitig wird eine Unabhängigkeit von einer zentralen herausgebenden und verwaltenden Einheit gewährleistet.
- Die Daten bleiben beim Benutzer (wichtig für Datenschutz).
- Blockchain kann als Speicher für die Beglaubigungen genutzt werden, **muss aber nicht eingesetzt werden**.
- Sie ermöglicht das einsetzen neuer Verfahren zur Datensparsamkeit (z.B. ZKP)

Bildquelle: https://hpi.de/meinel/lehre/master-projects/self-sovereign-identity-with-blockchain-technology.html

Datenschutz und Datensicherheit sind zentral

Personenbezogene Daten müssen geschützt sein

- Privacy – by - design
- Benutzer muss die Daten-hohheit besitzen
- Minimale Datenoffenlegung & Maximale Datensparsamkeit → Nutzung von Zero-Knowledge-Proof (ZKP) «Niemand muss das Geburtsdatum für eine Altersprüfung kennen»

Maximal mögliche Datensicherheit

- Keinen «Single-Point of Failure» → Dezentralisierte Lösung
- Flexibilität für Anpassungen bei der Datensicherheit

E-ID muss zukunftsfähig sein

Rolle des Bundes

Rolle der Technologie

«Human Trust»

- Legitimierter Vertrauensrahmen
- Gemeinsame definierte und gelebte Spielregeln
- Akzeptierte Qualitätsanforderungen
- Zertifizierte Prozesse und Technologien

«Digital Trust»

- Kryptographische Verfahren
- Dezentrale, konsensbasierte Systemtechnologien
- Bidirektionale, multi-device fähige Protokolle
- **Open Source** und international anerkannte Spezifikationen

Die wichtigsten Take-Aways

- **Self-Sovereign Identity (SSI) deckt die Anforderung der vershiedenen Stakeholder, der Politik und unserer föderalistischen Werte zur E-ID ab.**
- **SSI** ermöglicht, den Pass/ID als wichtigen **Baustein in ein bereits heute wachsendes, digitales Ökosystem** zu bringen.
- **SSI ist unabhängig** von einer herausgebenden Partei und kann für unterschiedliche Identitätsnachweise genutzt werden (z.B. Personendaten, Zeugnisse, Zutrittsberechtigung, Versicherungsnachweis,).
- **SSI ist mehr als eine Technologie** und umfasst viele andere Themen (z.B. rechtliche Grundlagen, Governance, Datenschutz).
- Blockchain kann als Trust Anchor genutzt werden, muss aber nicht. Eine **dezentrale und vertrauenswürdige Infrastruktur** ist jedoch wichtig.
- **Internationale Kompatibilität zu anderen Ländern** kann durch Einhaltung von Standards (z.B. W3C – DID) sichergestellt werden.
- ID mit Chip plus SSI Wallet = **Komplementär**

BACKUP

Die wichtigsten Vorteile des SSI Konzepts[1)]

Bottom Line Growth

Einsparungen

Zusatzgeschäfte

Betrugsbekämpfung

Compliance

Datenschutz und -sicherheit

Privatsphäre

Daten-Portabilität

Business Effizienz

Workflow Automation

Vereinfachte Delegation (Rollen)

Time-to-Market

Reputations-management

Privater Kanal

Relationship Management

Permanente Verbindung

Auto-Autorisierung

Vereinfachtes Onboarding

Auto-Authentifizierung

UX und Convenience

1) In Anlehnung an Drummond Reed / Alex Preukschat, Self-Sovereign Identity MEAP V10, 2021

Die 12 Kernprinzipien der Self Sovereign Identity[1)]

Repräsentation

Ein SSI-Ökosystem stellt die Mittel zur Verfügung, damit jede Entität - menschlich, juristisch, natürlich, physisch oder digital - durch eine beliebige Anzahl digitaler Identitäten repräsentiert werden kann.

Interoperabilität

Ein SSI-Ökosystem ermöglicht die Darstellung, den Austausch, die Sicherung, den Schutz und die Verifizierung digitaler Identitätsdaten für eine Entität auf interoperable Weise unter Verwendung offener, öffentlicher und gebührenfreier Standards.

Dezentralisierung

Ein SSI-Ökosystem darf nicht von einem zentralisierten System abhängen, um digitale Identitätsdaten einer Entität darzustellen, zu kontrollieren oder zu verifizieren.

1) Die Grundsätze von SSI, Sovrin Fundation, Principles of SSI - Sovrin.

Die 12 Kernprinzipien der Self Sovereign Identity[1)]

Kontrolle & Vermittlung

Ein SSI-Ökosystem soll Entitäten, die natürliche, menschliche oder juristische Rechte bezogen auf ihre Identität besitzen, befähigen, die Nutzung ihrer digitalen Identitätsdaten zu kontrollieren und diese Kontrolle durch das Verwenden und/oder die Delegierung von/zu Agenten und Vertretern ihrer Wahl, einschließlich Personen, Orgai-sationen, Geräte und Software, auszuüben.

Beteiligung

Ein SSI-Ökosystem darf die Teilnahme eines Inhabers von Identitätsrechten nicht vorschreiben.

Gleichheit & Eingliederung

Ein SSI-Ökosystem darf einen Inhaber von Identitätsrechten innerhalb seines Geltungsbereichs nicht ausschließen oder diskriminieren.

1) Die Grundsätze von SSI, Sovrin Fundation, Principles of SSI - Sovrin.

Die 12 Kernprinzipien der Self Sovereign Identity[1)]

Benutzerfreundlichkeit, Zugänglichkeit & Konsistenz

Ein SSI-Ökosystem soll die Benutzerfreundlichkeit und Zugänglichkeit von Agenten und anderen SSI-Komponenten für Inhaber von Identitätsrechten maximieren. Dies gilt auch für eine konsistente Nutzererfahrung.

Portabilität

Ein SSI-Ökosystem darf die Fähigkeit eines Inhabers von Identitätsrechten, seine Identitätsdaten zu einem anderen Agenten oder System seiner Wahl zu transferieren oder zu kopieren, nicht beschränken.

Sicherheit

Ein SSI-Ökosystem soll Inhaber von Identitätsrechten befähigen, die Speicherung und Übertragung ihrer digitalen Identitätsdaten zu sichern, ihre eigenen Identifikatoren und kryptographische Schlüssel zu kontrollieren und eine Ende-zu-Ende-Verschlüsselung für alle Interaktionen anzuwenden.

DIDAS

1) Die Grundsätze von SSI, Sovrin Fundation, Principles of SSI - Sovrin.

Die 12 Kernprinzipien der Self Sovereign Identity[1)]

Überprüfbarkeit & Authentizität

Ein SSI-Ökosystem soll Inhaber von Identitätsrechten befähigen, die Authentizität ihrer digitalen Identitätsdaten überprüfbar nachzuweisen.

Datenschutz & minimale Offenlegung

Ein SSI-Ökosystem soll Inhaber von Identitätsrechten befähigen, die Privatsphäre ihrer digitalen Identitätsdaten zu schützen und in jeder Interaktion nur die dafür zwingend erforderlichen Daten auszutauschen.

Transparenz

Ein SSI-Ökosystem soll Inhabern von Identitätsrechten und allen anderen Beteiligten die Möglichkeit geben, notwendige Informationen leicht einzusehen und zu verifizieren, um die Anreize, Regeln, Richtlinien und Algorithmen zu verstehen, unter denen Agenten und andere Komponenten von SSI-Ökosystemen arbeiten.

DIDAS

1) Die Grundsätze von SSI, Sovrin Fundation, Principles of SSI - Sovrin.

Wie soll eine E-ID umgesetzt werden?

Srdjan Capkun

ETHZ

(Federated) IDP vs PKI vs Self-Sovereign ID?

Srdjan Čapkun
ETH Zurich

Oct 2021

(Federated) IDP vs PKI vs Self-Sovereign ID?

(Federated) IDP vs PKI vs Self-Sovereign ID?

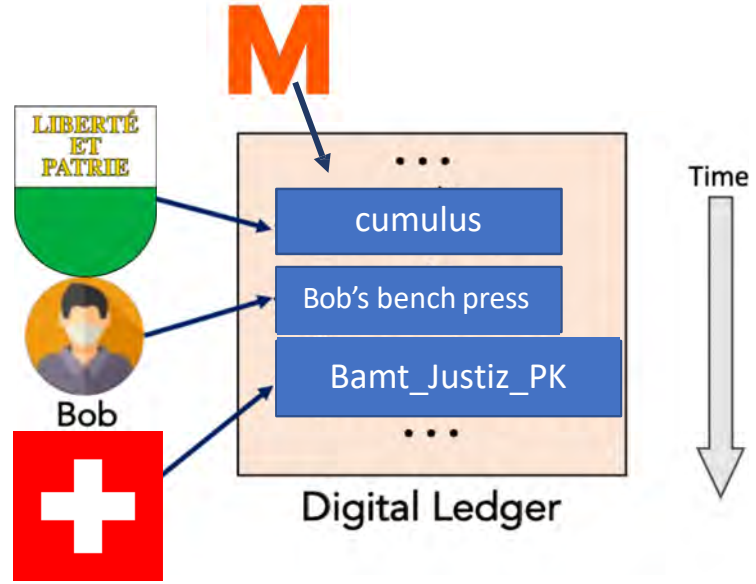
but SSI can be many things and
the devil is in the details

SSI: Key Aspects*

- Ledger Infrastructure
- Account and Identity Management
- Digital Wallets / Custody
- Balancing Privacy and Transparency

Other aspects:

- Need for Smart Contracts?
- Reliance on Secure Hardware?



Ledger type:
Centralized?
Centralized but verifiable?
Semi-centralized (Cantons)?
Public?

Immutable / reversible?

** These aspects are also common to CBDCs:*

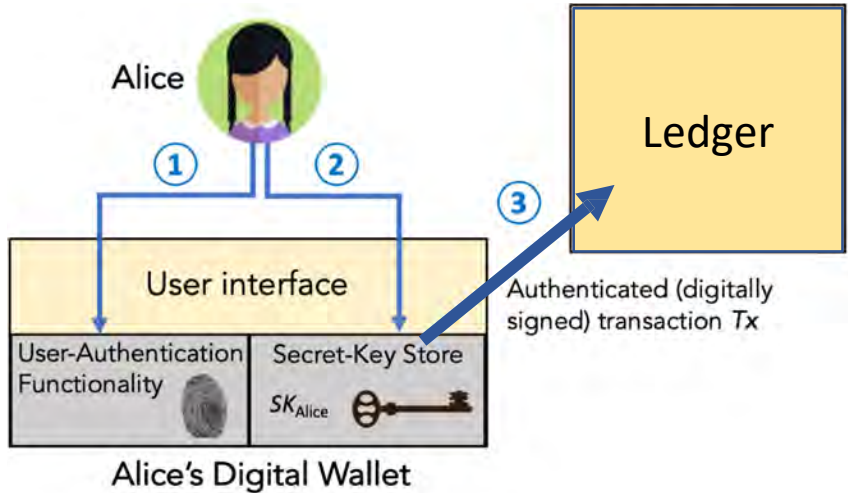
https://www.brookings.edu/research/design-choices-for-central-bank-digital-currency-policy-and-technical-considerations/

SSI: Key Aspects

- Ledger Infrastructure
- Account and Identity Management
- Digital Wallets / Custody
- Balancing Privacy and Transparency

Other aspects:

- Need for Smart Contracts?
- Reliance on Secure Hardware?



Identity Verification:
In-person?
Online?
Social networks?
Biometric?

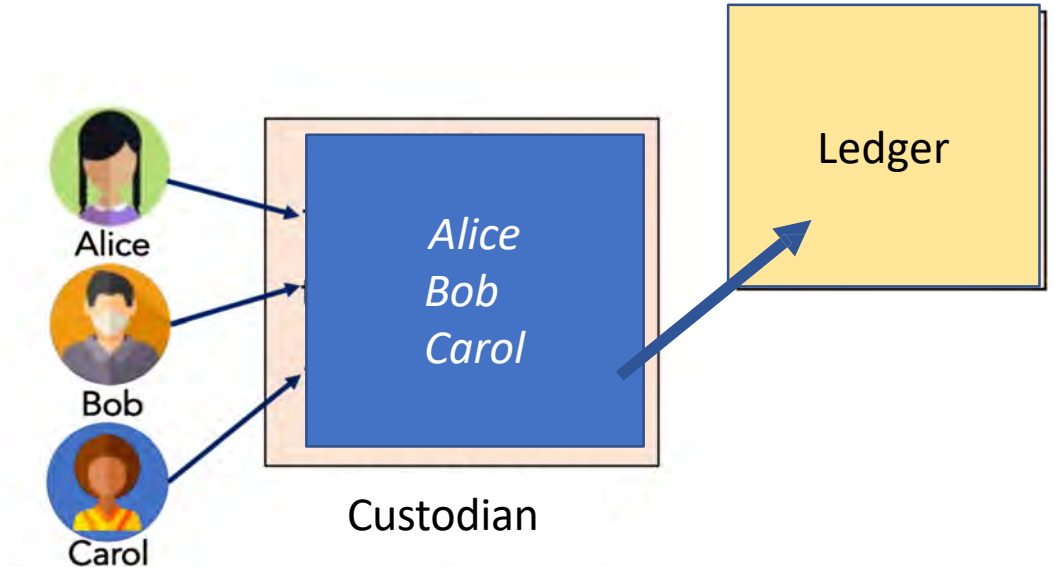
Account Management?
Light vs Full Clients?

SSI: Key Aspects

- Ledger Infrastructure
- Account and Identity Management
- Digital Wallets / Custody
- Balancing Privacy and Transparency

Other aspects:

- Need for Smart Contracts?
- Reliance on Secure Hardware?



Custody might be crucial for wide adoption, but introduces risks

Who will (be allowed to) offer such services?

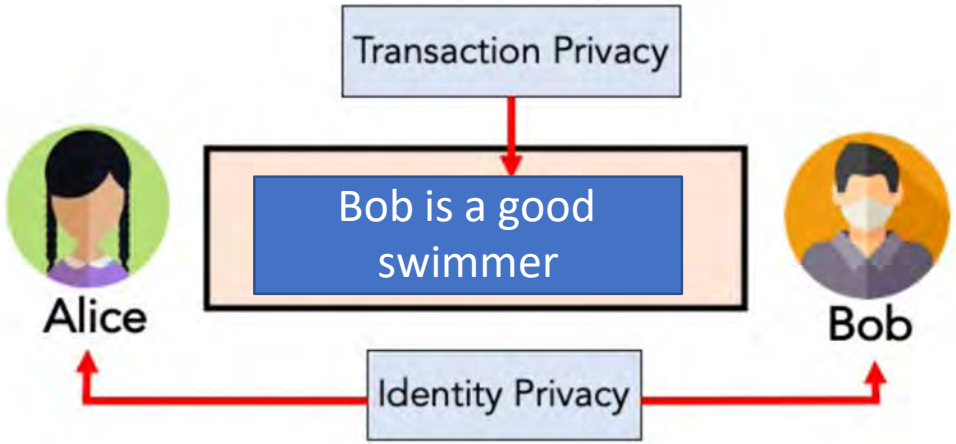
'Trustless' Custody Services?

SSI: Key Aspects

- Ledger Infrastructure
- Account and Identity Management
- Digital Wallets / Custody
- Balancing Privacy and Transparency

Other aspects:

- Need for Smart Contracts?
- Reliance on Secure Hardware?



e.g., revocation requires some level of transparency

Users expect privacy:
Which credentials or certificates does a user hold or held (revoked)?
Which services did the citizen use with the credentials or certificates?

Ledger access patterns might leak.

SSI: Final Note

- ‘Users in control’ sounds good but users are vulnerable to manipulation.
- Users might hand over their certificates ‘for fun and profit’.
- Large corporations (BigTech and SmallTech) will see SSI as an opportunity to learn more about users and to ‘mine’ their identities.

- SSI increases those risks compared to eg IDP.
- We need to make sure that such abuses do not happen.
  Mandating government apps for government certificates?
  Vetting entities who can receive government issued certificates?

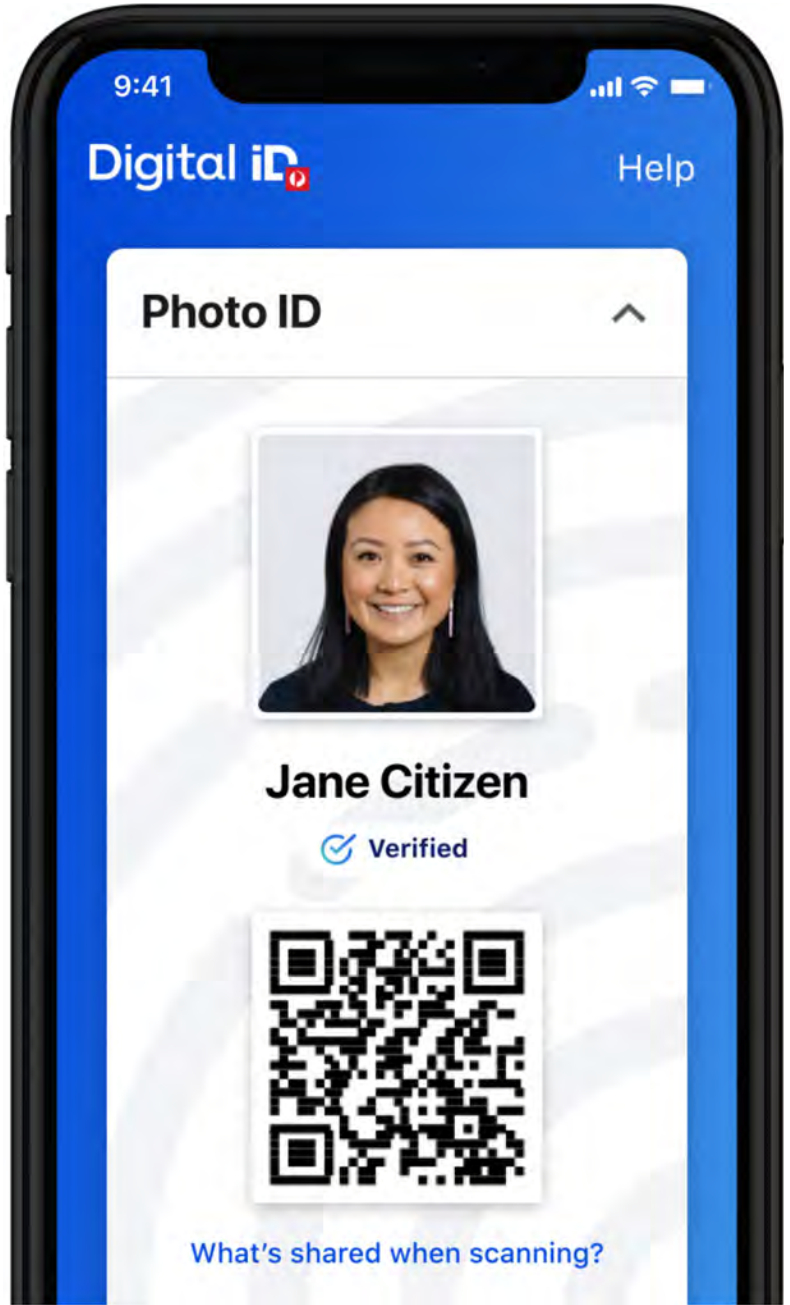
Have a good meeting …

Figures repurposed/based on:
https://www.brookings.edu/research/design-choices-for-central-bank-digital-currency-policy-and-technical-considerations/

Comment mettre en œuvre une e-ID?

Edouard Bugnion

EPFL



Swiss E-ID
Privacy aspects

I. Aad, C4DT - EPFL
E. Bugnion, DCSL - EPFL

+ contribution by
P. Schaller, ZISC - ETHZ

Outline

- This presentation is [not] about...
- Privacy comparison of the 3 approaches of the public consultation
- Proposed Methodology for Privacy in use-cases
- Domain-Specific IDs
- NIST SP 800-63-3
- Compatibility with the EU e-ID
- Conclusions

What this presentation is [not] about...

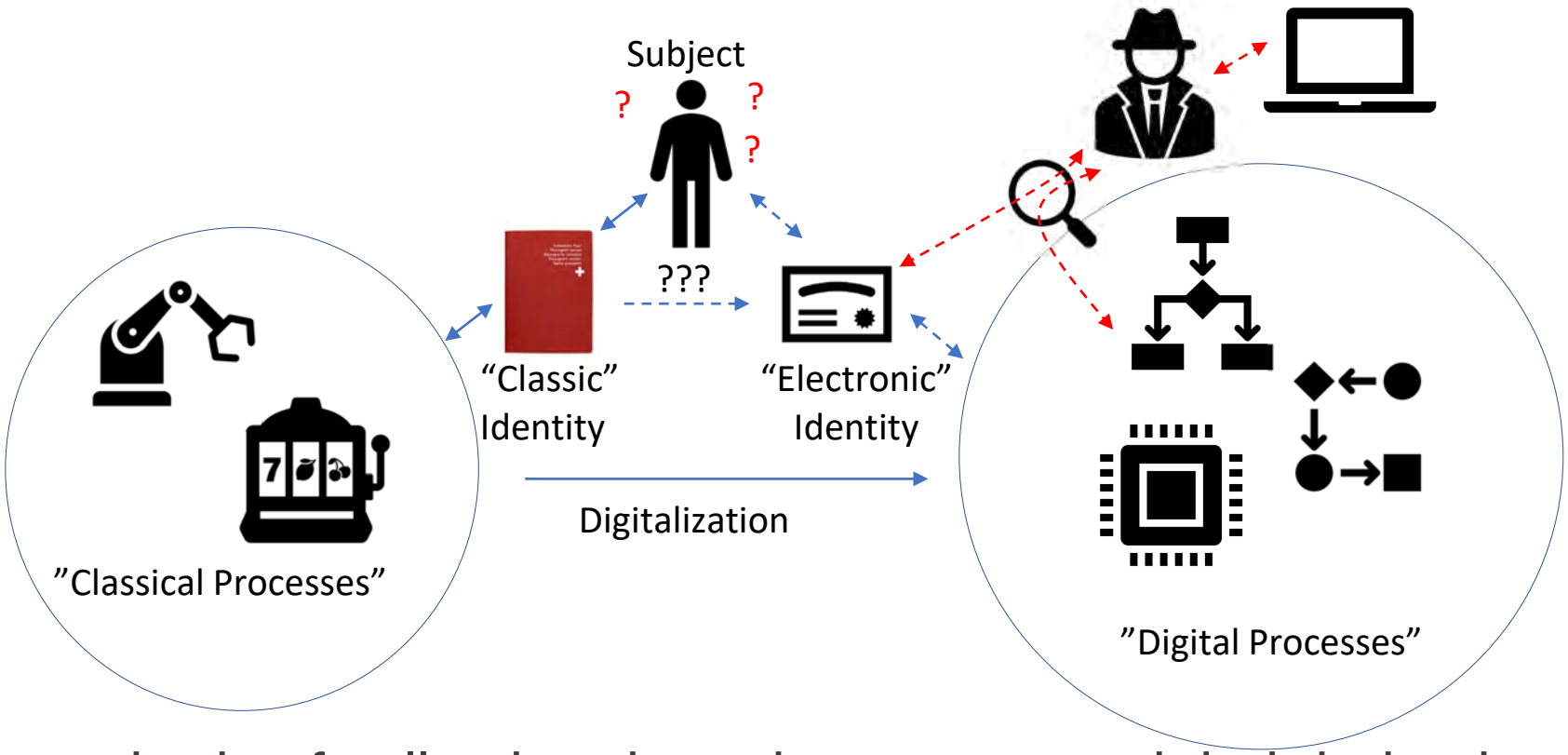
Not about...

- QR Code / smart card / login / App
- User Friendliness
- Legal Aspects
- Security aspects

About...

- Privacy by default/design, minimization in...
  - The 3 approaches
  - The use cases

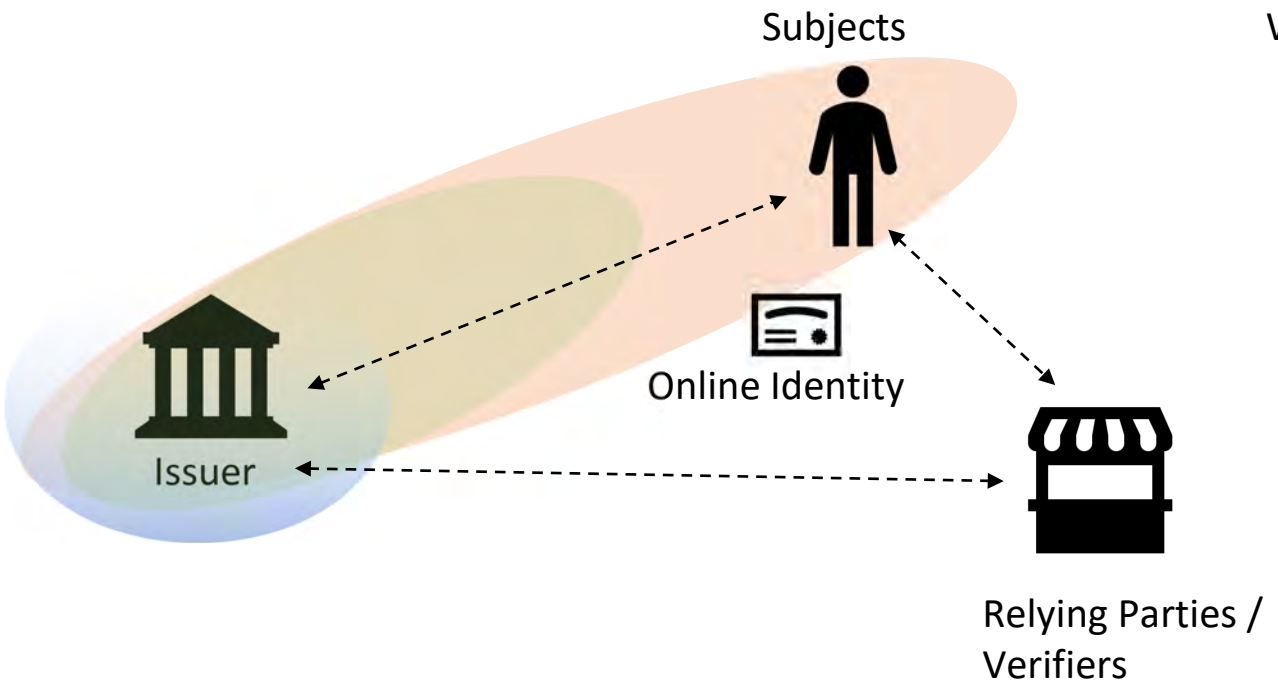
Privacy Challenges



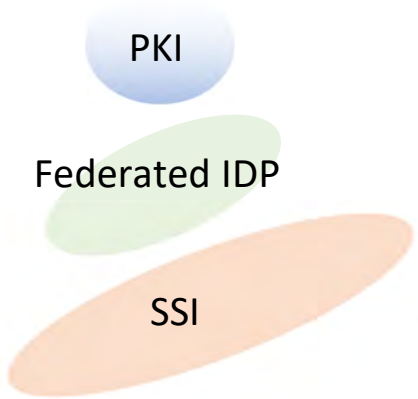
- new methods of collecting data about users and their behavior
- users are typically not aware of data collection options and thus miss the natural intuition of when their privacy is at risk.

(Fed.) IDP vs PKI vs Self-Sovereign ID

- What do all the three solutions have in common on an abstract level?



Who "controls" the identity and its attributes?



Privacy comparison of the 3 approaches of the public consultation

	Self-Sovereign ID	PKI (Public Key Infra.)	IdP (ID Provider)
Privacy leakage to ID provider / authorities	Care must be taken for details not specified in SSI (e.g. revocation) 		Countermeasures possible, but not supported by current standards
Privacy leakage to service provider		Limited flexibility	Tbd
...			

- With respect to the user's freedom, selfdetermination and liberty: the choice is Self-Sovereign ID (SSI)
- **BUT:**
  - SSI is not well-defined and can be implemented in different ways.
  - There are no strict separating lines between the three options (a federated IDP may include a PKI, SSI may rely on federation protocols).
  - As we have learned from the past: "*The devil hides in the details!*"

Choosing Privacy Elements for use-cases

- Various use-cases can be found in the e-ID documentations...

Rent a car

Pay online (e-ID+wallet)

Phone subscription

Open bank account

Driving license

Health insurance

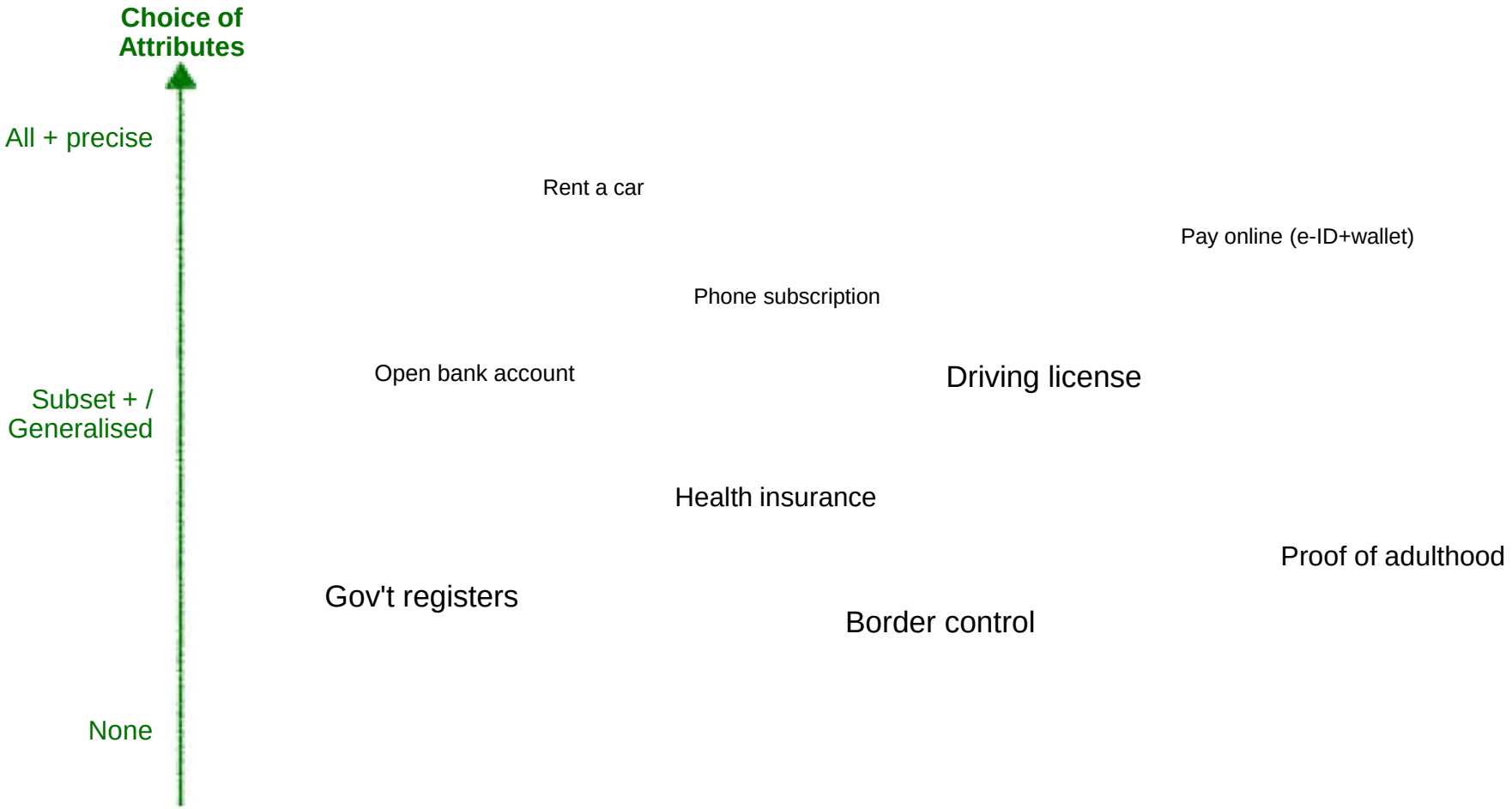
Proof of adulthood

Gov't registers

Border control

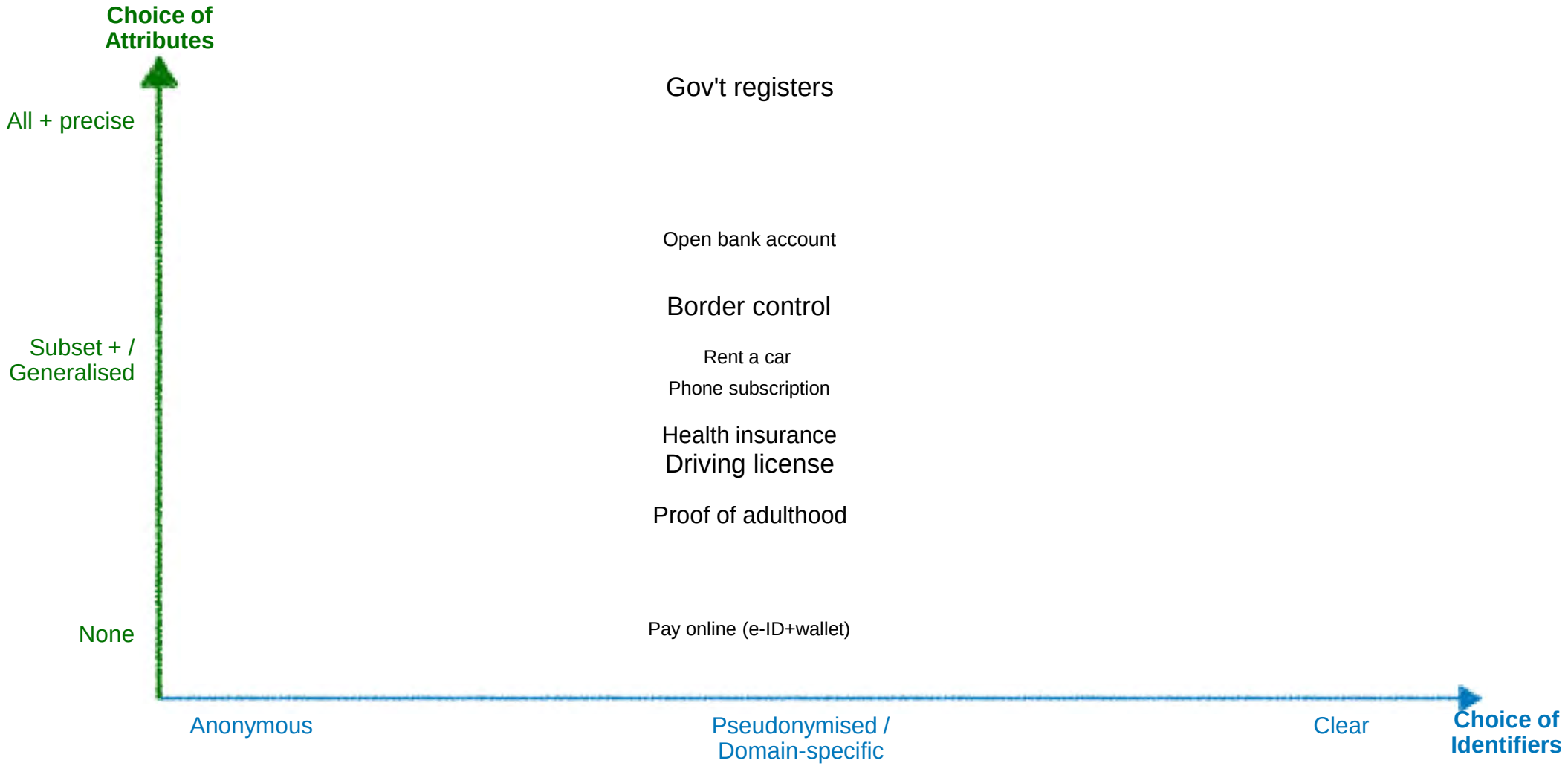
(Same observations when reading EU e-ID documentations)

... with the description of some privacy methods



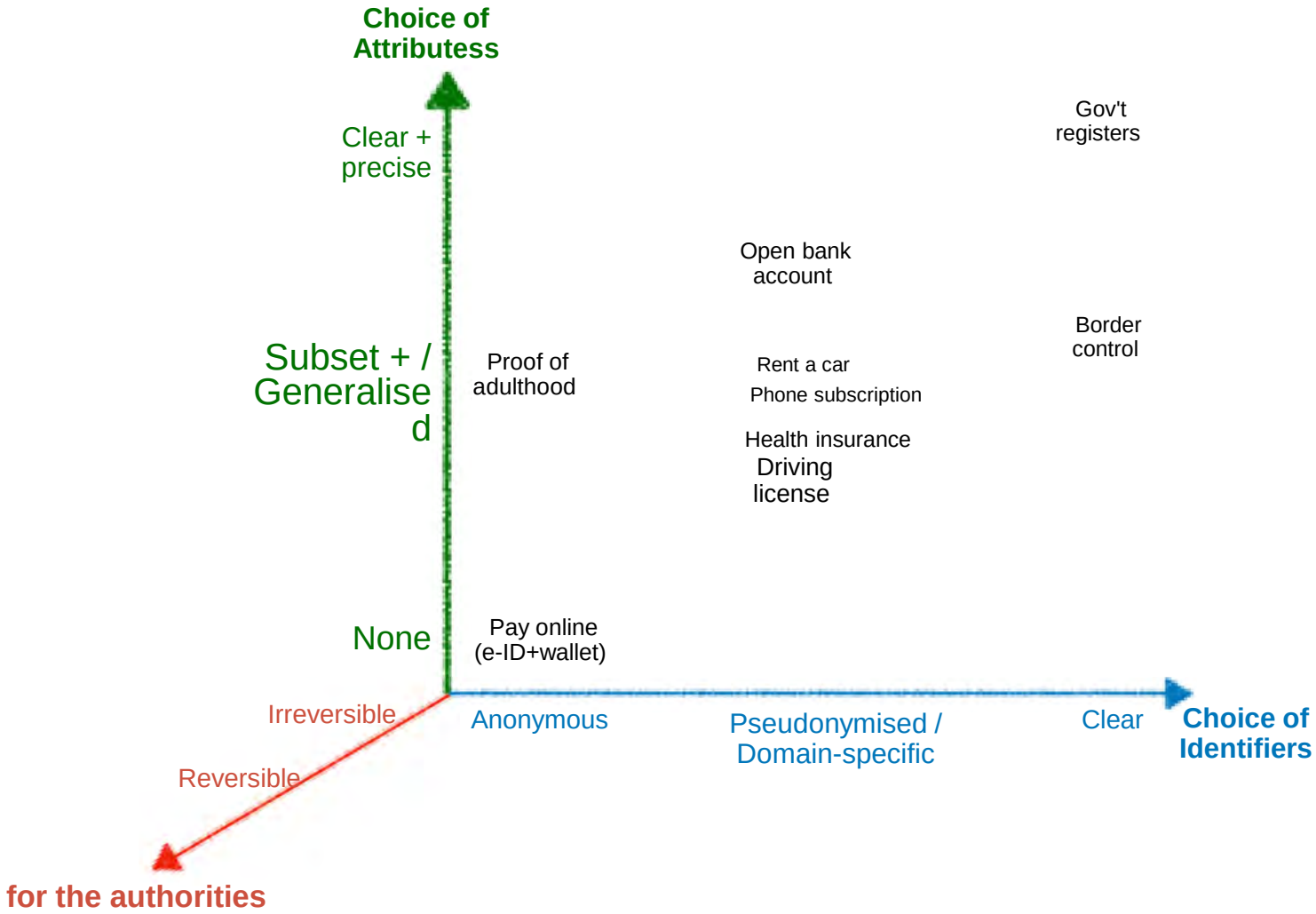
(Same observations when reading EU e-ID documentations)

However, privacy is more than just "which attributes are shared"



Privacy is about identifiers too. This dimension/aspect should not be overlooked.

However, privacy is more than just "which attributes are shared"

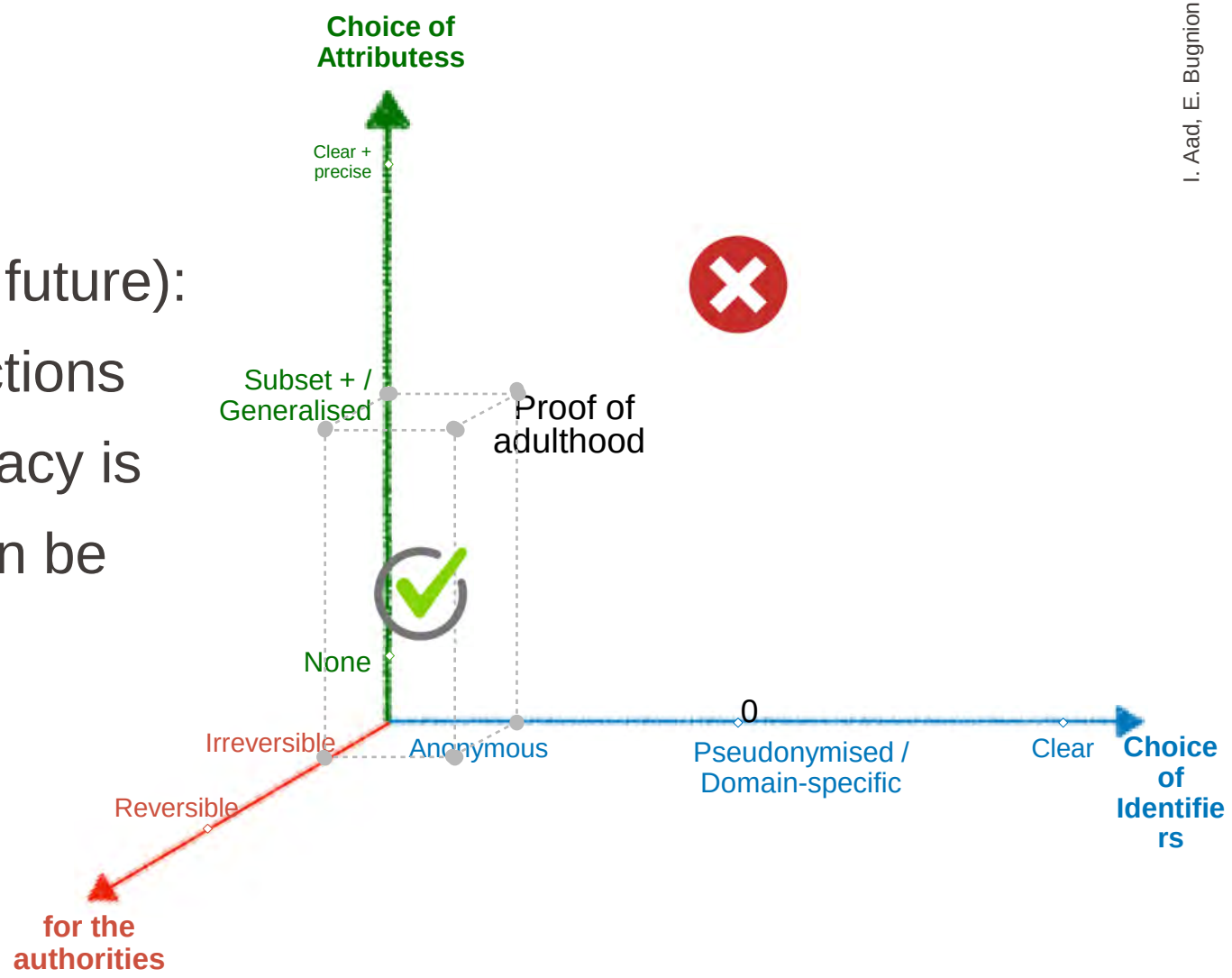


Privacy is about <u>re-identification</u>. This dimension/aspect should not be overlooked.

Privacy by design/default, and minimization…

I. Aad, E. Bugnion, P. Schaller

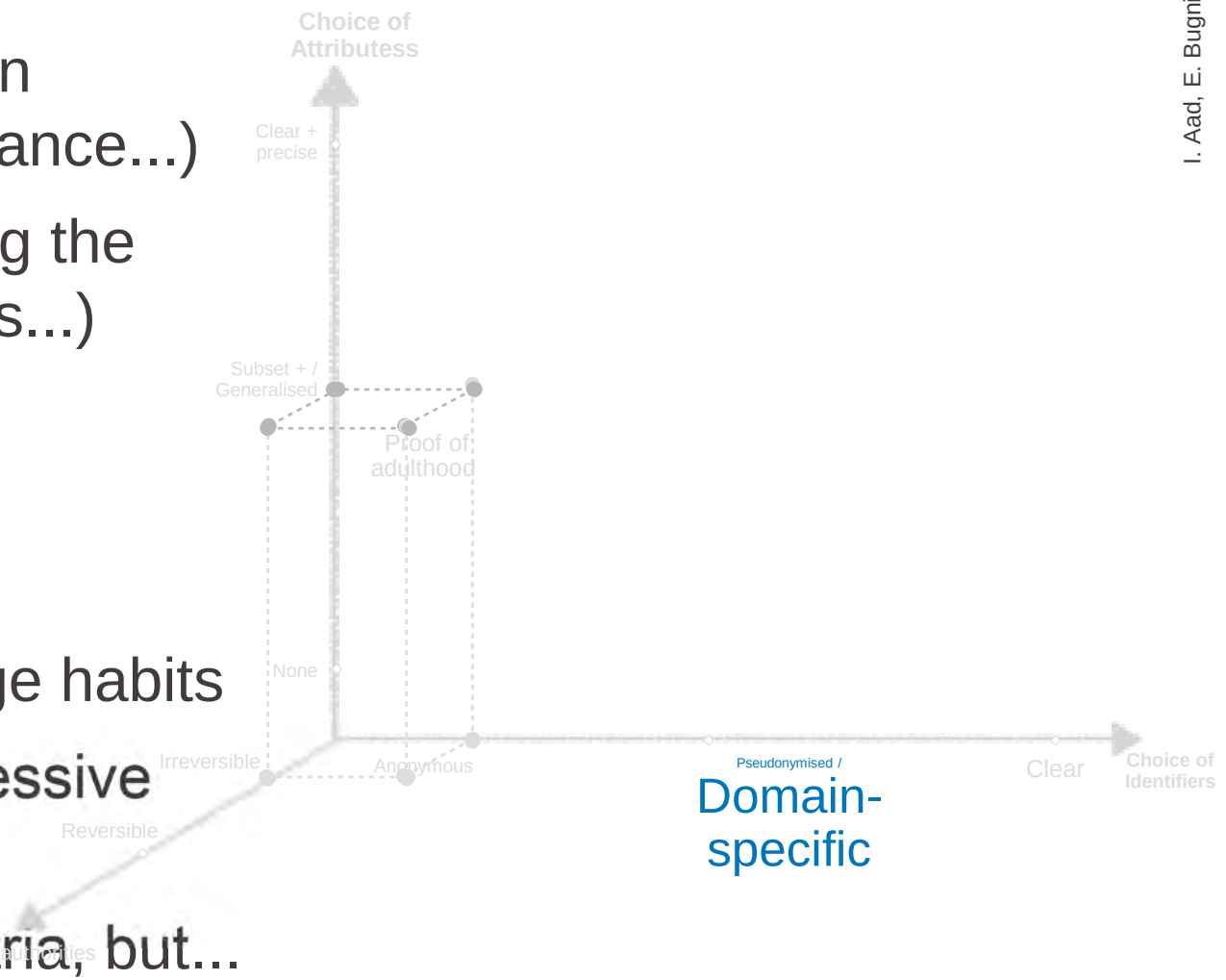
- For each use-case (current or future):
- Place it on each of the 3 directions
- The closer to 0 the better privacy is
- The technical components can be easily identified accordingly



I. Aad, E. Bugnion, P. Schaller

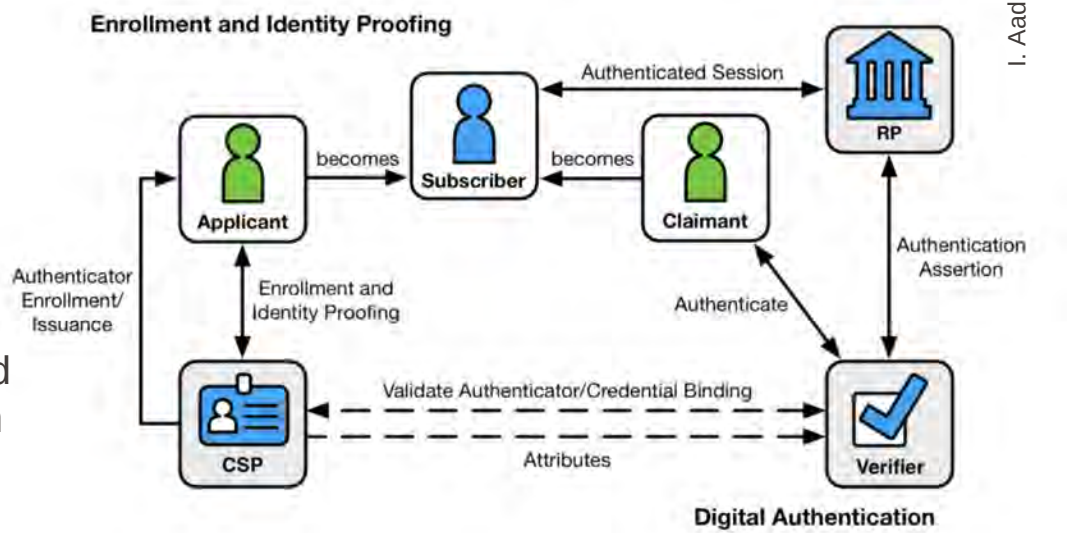
Domain-Specific IDs

- User has different (certified) IDs in different domains (e.g. health, finance...)
- No side-information compromising the "silos" is kept (e.g. name, address...)
- Possible inter-linkage by specific authorities for specific use-cases
- Requires very careful design
- Requires drastic changes in usage habits
- Can be prepared now with progressive adoption
- Partially used in France and Austria, but...



NIST SP 800-63-3

- Definitions of the elements involved in a digital identity system.
- Shows the necessary trust relations for the system to work.
- There are three assurance levels defined:
  - Identity Assurance Level (IAL)
    - IAL1: self-asserted
    - IAL2: remote or in person, verification of identifying attributes
    - IAL3: in-person, identifying attributes must be verified by an authorized representative through examination of physical documentation
  - Authentication Assurance Level (AAL)
  - Federation Assurance Level (FAL)



The Digital Identity Model defined in NIST SP 800-63-3

- The levels classify the “security / trust level” of the corresponding processes and/or security protocols.
- Shows nicely the unique feature of a federal e-ID, namely, the identity proofing process is given and can achieve IAL3 without any further effort.

Compatibility with the EU e-ID (privacy-wise)

- **For attributes**, privacy / data minimization must be properly aligned (ex. > 18y old vs. year of birth)
- **Domain-Specific IDs**, [partially] deployed in France and Austria, have similar compatibility challenges.
- **Pseudonymity, anonymity, and re-identification** would have to be "translated".

Conclusions

- Method for choices of Privacy by default / by design, data minimization, for current and future use-cases
- It may be the right time to adopt Domain-Specific IDs, for better privacy protection
- Adopt one of the well-defined frameworks (e.g. NIST SP 800-63-3)
- Compatibility with EU e-ID must be carefully designed

Comment mettre en œuvre une e-ID?

Stéphane Schnyder

Canton de Vaud

Mise en œuvre du MIE-VD

CYBERADMINISTRATION – CANTON DE VAUD – 14.10.2021

Direction générale du numérique et des systèmes d'information
Avenue de Longemalle 1, CH-1020 Renens
Tél: +41 21 316 26 00

Agenda

A. Qu’est-ce que le MIE-VD
B. Initialisation et conception
C. Réalisation
D. Déploiement
E. Constats et synthèse

A. Qu’est-ce que le MIE-VD?

Le Moyen d’Identification Électronique du canton de Vaud:

1. Est un identifiant électronique (eID) unique de la personne:
   - Basé sur le NAVS13, identificateur univoque des personnes
   - Un seul LoA (niveau substantiel, identification présentielle ou virtual-in-presence*).
2. Est un moyen pour accéder aux démarches administratives numériques:
   - Démarches qui nécessitent la preuve d’identité du demandeur, en nom propre
   - Démarches au nom d’une entité IDE (entreprises ou communes, après accréditation sur le portail sécurisé VD)
   - Permet de rendre une décision via le portail sécurisé**, en remplacement d’une lettre recommandée.
3. Est accessible au grand public depuis décembre 2020
4. Permet la fédération d’identités:
   - Permet l’accès à d’autres services sécurisés (portail Ville de Lausanne, communes, …)

** Projet ID-par-vidéo en phase d’initialisation*

*** Uniquement si la décision est accompagnée d’un cachet réglementé LSCSE / ZertES*

B. Mise en œuvre de la loi et principes de base

1. Développement des bases légales
   - 2012 – 2017: Adoption par le CE de la stratégie eVD
     - Pour développer la cyberadministration au bénéfice de la population, des entreprises et des communes
   - 2013 – 2022: Mise en œuvre de la stratégie (mandats de programme, organisation permanente)
     - Implication du porteur du projet (secrétariat général DIRH)
     - Implication des parties prenantes (juridique et opérationnelle) au travers de groupes de travail pour débattre de la notion de portail sécurisé, identité électronique et règles d'adhésion au portail sécurisé
     - Rédaction du projet de loi LCYBER et son règlement RLCYBER
     - Rédaction des mandats de programmes pour la mise en œuvre technique (les EMPDs Cyberadministration 2015 et 2018)
   - Décembre 2020: entrée en vigueur de la Loi Lcyber, déploiement du portail sécurisé et du MIE
2. Principes de base qui ont un impact sur les fonctionnalités
   - Protection des données personnelles
   - Gratuité du MIE
   - Simplifier la vie des usagers
   - Le MIE doit être délivré par l'État en tant que fournisseur d'identité public
   - Caractère facultatif de la cyberadministration pour l'usager, mais obligatoire pour les services (qui s'appuient sur une identification formelle)

C. Réalisation de la solution fonctionnelle

1. Définition des macro-processus fonctionnels:
   - Délivrance de l'identité numérique et identification
   - Gestion du cycle de vie de l'usager
   - Authentification donnant l'accès à un espace sécurisé
   - Gestion des autorisations (rattacher à un espace sécurisé IDE, autoriser l'accès à une prestation)
   - Fédération d'identités
2. Intégration dans l'écosystème de la cyberadministration
   - Gesdem – Intégrer le processus d'octroi de MIE dans le gestionnaire de demandes cyber
   - Coffre-fort numérique (pour garantir la durée de rétention et suppression des données selon la LCYBER)
   - Showdem – permettre aux e-prestation de fonctionner à la fois en mode sécurisé et public
3. Support L1:
   - Réaliser l'infrastructure du support level 1 (outil de ticketing + renfort RH)

D. Déploiement du dispositif

1. Déploiement du MIE
   - Désignation des LRA* (les autorités habilités, e.g. préfectures et le Service des automobiles et de la navigation)
   - Formation des LRA et mise en conformité des locaux d'identification
   - Opérations «Smart Bus» pour se rapprocher du citoyen et délivrer des MIEs
   - Communication du canton prévues
   - Mise en place d'un service de support (level 1) à la population
2. Permet d'accéder aux prestations sécurisée, en ligne:
   - Pour les communes: communication de l'arrêté d'imposition communal, …
   - Pour les citoyens: duplicata SAN, dossier fiscal à venir, …
   - Pour les entreprises: portail pour les mesures d'intégration social (MIS), …

** LRA: Local Registration Authority*

E. Constatations et synthèse

1. Paradoxe de l'œuf et de la poule:
   - Pas de prestations sécurisées → pas de nouvelles demandes de MIEs.
   - Pas de MIEs → pas de prestations sécurisées

1. Ce qui peut être amélioré:
   - Rebranding VaudID (plus parlant que « MIE »)
   - Décorréler le MIE et l'espace sécurisé dans la Loi LCYBER
   - Décorréler la preuve d'identité et le MIE (le « I » dans « IAM »)
   - Développer la base légale pour faciliter la fédération du MIE.

2. L'eID devrait être une carte d'identité numérique:
   - Il est une preuve d'identité mais c'est pas forcément un login
   - Il permet l'interopérabilité de l'écosystème
   - Il est garanti par la confédération
   - Le « self » dans « self-sovereign identity »

D Annexes

Processus de délivrance d’identité numérique

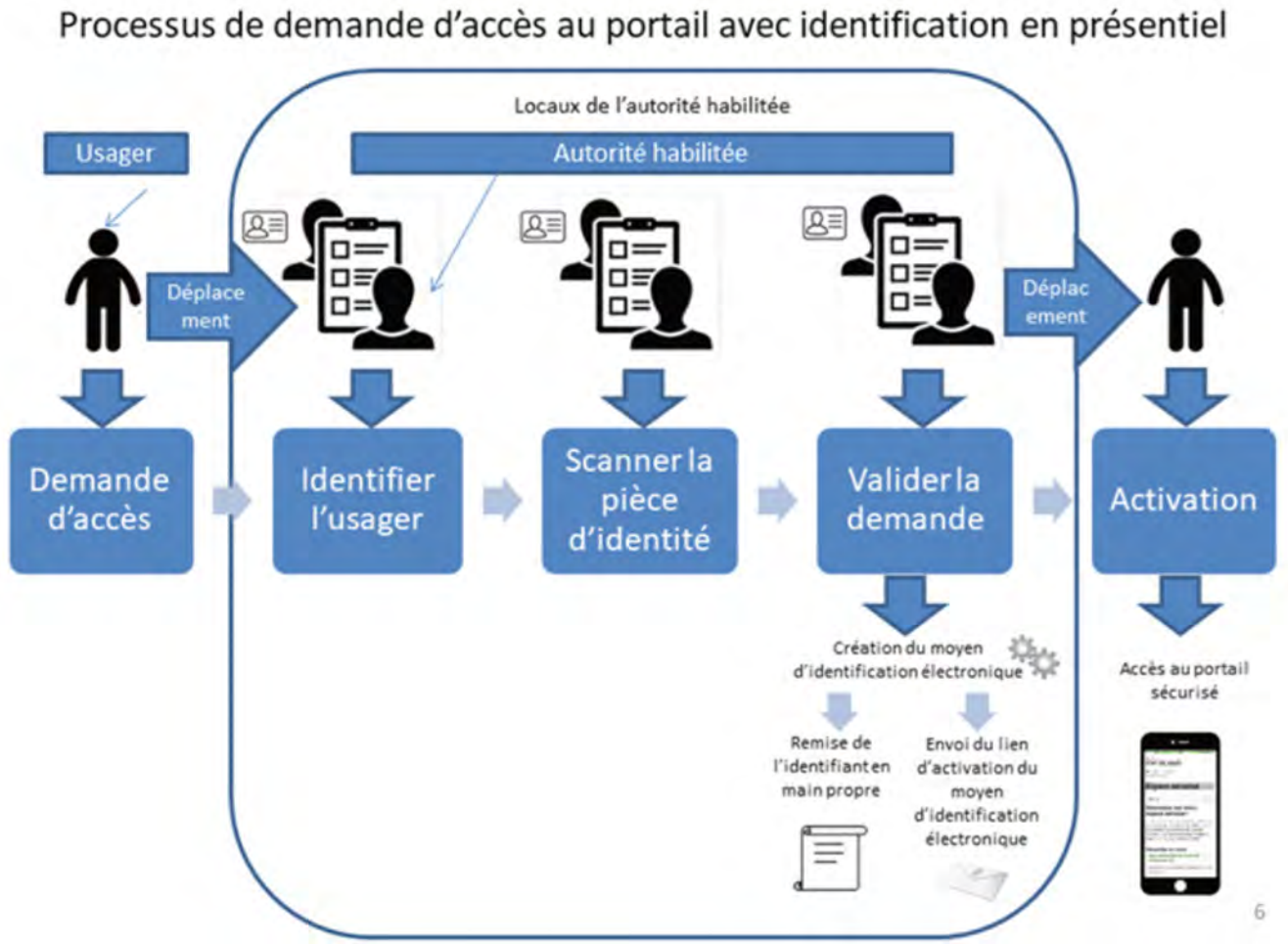
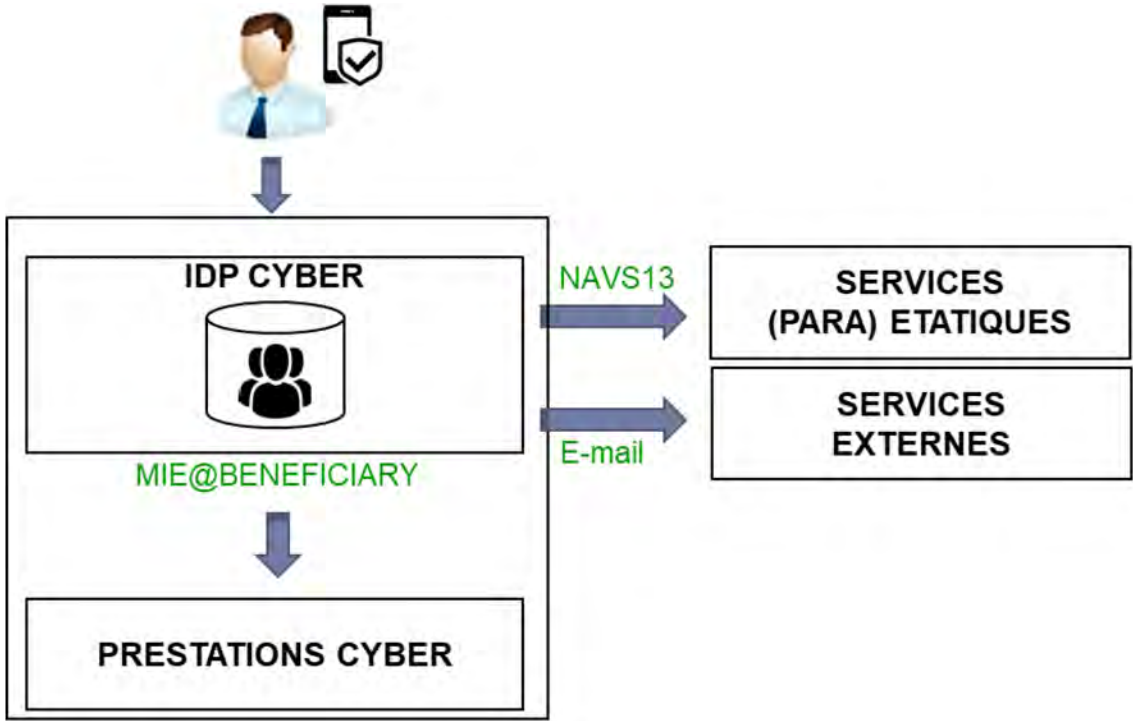


Schéma de fédération d'identité



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz

Allgemeine Stellungnahme

Adrian Lobsiger

Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter EDÖB

Allgemeine Stellungnahme

Lukas Federer

economiesuisse

Diskussion zur öffentlichen Konsultation zum „Zielbild E-ID“

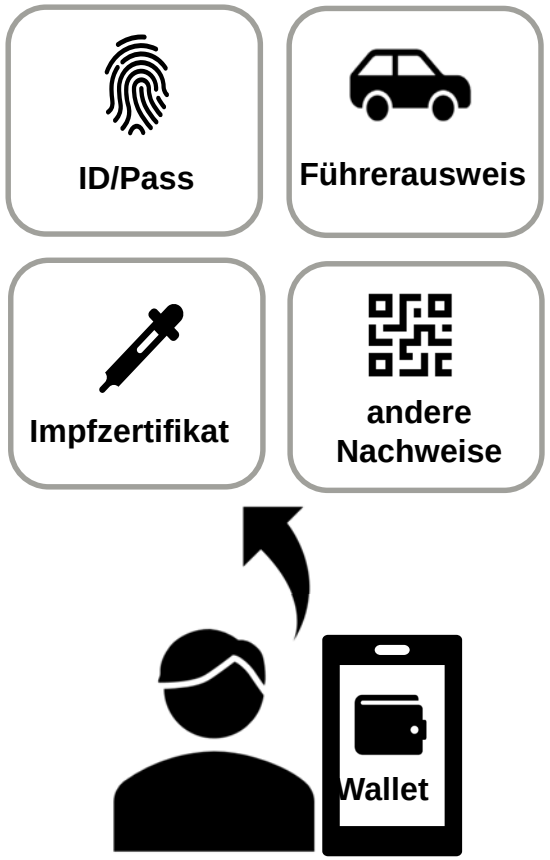
→ Stellungnahme der economiesuisse

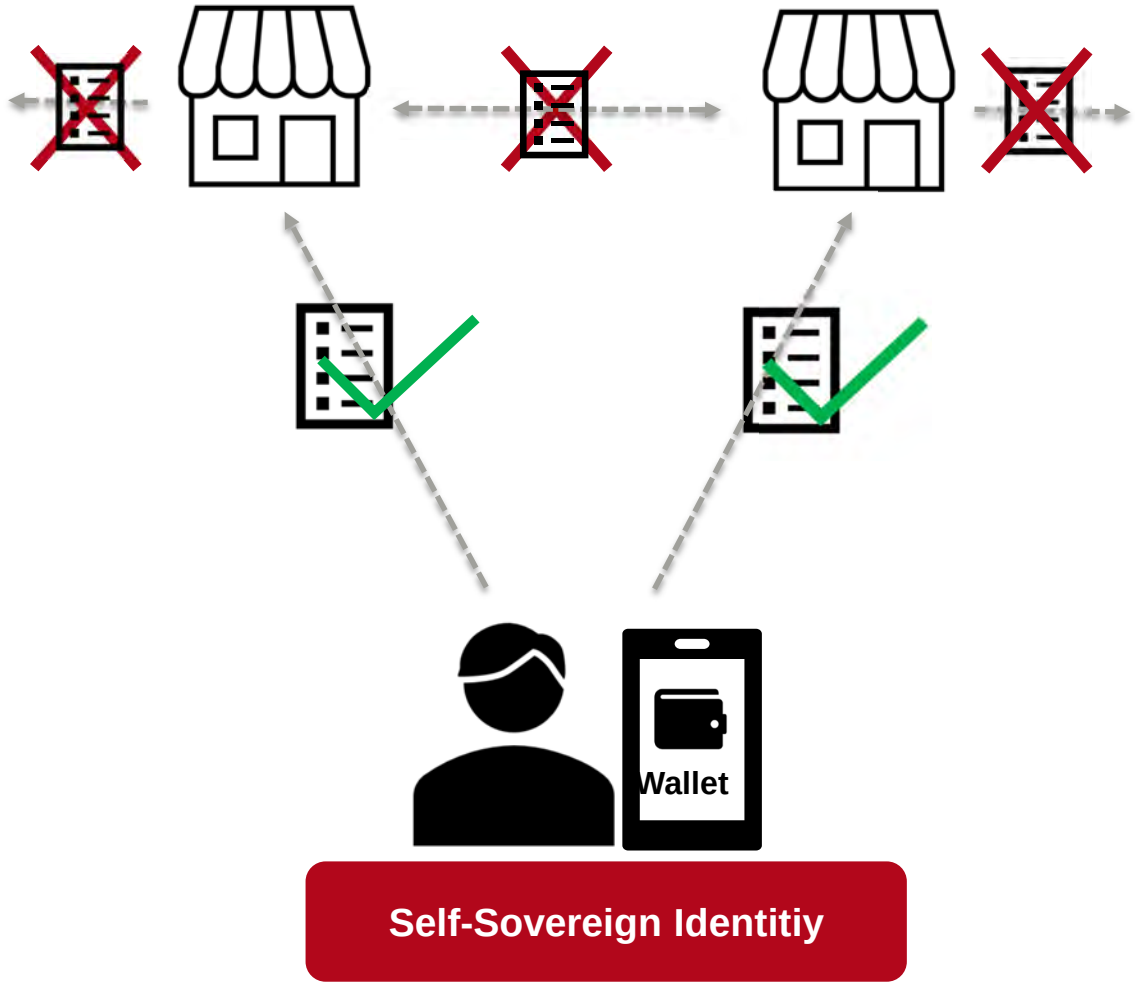
Lukas Federer
14. Oktober 2021

Agenda

- Einführung: Ein Ökosystem digitaler Nachweise
- Anforderungen, Anwendungsfälle und Nutzen
- Zusammenfassung der Stellungnahme economiesuisse

Ein Ökosystem digitaler Nachweise





Frage 1:

→ **Welches sind die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?**

Frage 1: Welches sind die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

Technische Anforderungen

- Benutzerfreundlichkeit und Transparenz
  - Transparenz ist notwendig für das Vertrauen
  - Anwendung soll benutzerfreundlich und sicher sein
- Datenschutz und Datenhoheit
  - „Privacy by Design“
  - Thematik Datenschutz und Datenhoheit im Zentrum des Publikums
- Datensparsamkeit
  - Herausgabe nur von notwendigen Datenpunkten der E-ID
- Dezentrale Architektur
  - Self-Sovereign Identity (SSI)
  - Klärung von Grundsatzfragen der Self-Sovereign Identity

Frage 1: Welches sind die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

Organisatorische Anforderungen

- Staatliche Kontrolle
  - Federführung vom Bund
- Pilotierung
  - Einbezug verschiedener Arbeitsgruppen aus Wirtschaft, Wissenschaft und Gesellschaft im Prozess zur Erstellung der E-ID

Frage 1: Welches sind die drei wichtigsten Anforderungen an eine staatliche E-ID als digitaler Ausweis?

Anforderungen an das Ökosystem

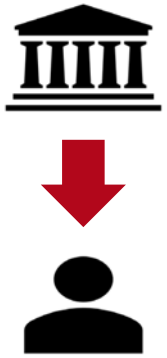
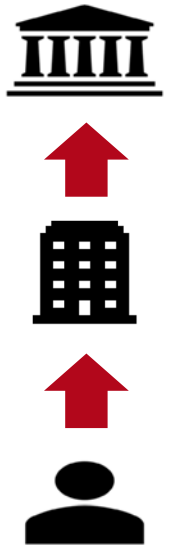
- Erweiterbarkeit
  - Offenes und inklusives Ökosystem
- Internationale Anschlussmöglichkeit
  - Orientierung an der Europäischer Union
  - Schweizer E-ID soll EUid entsprechen

economiesuisse

Frage 2:

→ **Welche Anwendungs-fälle der E-ID stehen im Vordergrund?**

Frage 2: Welche Anwendungsfälle der E-ID stehen im Vordergrund?

Anwendungsfall I	Anwendungsfall II	Anwendungsfall III
		

economiesuisse

Frage 3:

→ Welchen Nutzen bietet eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise auszustellen und überprüfen zu können?

Frage 3: Welchen Nutzen bietet eine nationale Infrastruktur, die es dem Staat und Privaten ermöglicht, digitale Beweise auszustellen und überprüfen zu können?

- Sicherheit
  - Erhöhte Sicherheit für Endnutzer mittels Ausstellung und Überprüfung digitaler Beweise
  - Digitale Beweise können unfälschbar ausgetauscht und überprüft werden
- Vertrauenswürdigkeit
  - Dezentrale Ausgestaltung führt zu Vertrauen und Akzeptanz der E-ID
- Erweiterung
  - Organisations- und grenzüberschreitende Anwendung

Zusammenfassung

→ Stellungnahme economiesuisse

Zusammenfassung

- economiesuisse unterstützt das Ambitions-Niveau 3 und somit die Schaffung eines Ökosystems digitaler Nachweise.

- E-ID ist erforderlich, um Digitalisierung in der Schweiz voranzubringen, wettbewerbsfähig zu bleiben und Innovationen zu fördern.

- Zeitnahe Einführung für die Attraktivität des Wirtschaftsstandortes Schweiz von enormer Bedeutung.

- Grundanforderungen sind die Benutzerfreundlichkeit, angemessener Datenschutz, dezentrale Architektur und staatliche Kontrolle. Entwicklungen in Europäischer Union sollen im Auge behalten werden.

Allgemeine Stellungnahme

Ulrich Brügger

Schweizerischer Verband für Seniorenfragen

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz

Allgemeine Stellungnahme

Ivette Djonova

SWICO

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD
Bundesamt für Justiz

Allgemeine Stellungnahme

Erik Schönenberger

Digitale Gesellschaft

DIGITALE | GESELLSCHAFT

POSITION DIGITALE GESELLSCHAFT

E-ID-Konferenz
14. Oktober 2021
Erik Schönenberger

DIGITALE GESELLSCHAFT

- Zivilgesellschaftliche Organisation
- Grund-, Menschen- und Konsumentenrechte
- Freie, offene und nachhaltige (digitale) Gesellschaft

E-ID-REFERENDUM

- Massgebliche Beteiligung
- Keine Verhinderung der E-ID
- Herausgeberschaft
- Datenschutz und Datensicherheit

ANFORDERUNGEN AN EINE E-ID

- «Privacy by Design» und «Privacy by Default»
- Nutzen für die Inhaber:innen
- Open-Source-Lizenz

ANWENDUNGSFÄLLE

- Digitaler Ausweis
- Gesichertes Login
- Elektronische Unterschrift

NATIONALE INFRASTRUKTUR

- Breiter Anwendungsbereich sorgt für grösseren Nutzen
  - Ambitionsniveau 3
- Beschränkung auf das technisch Notwendige
  - Keine Sammlung von Randdaten
  - Ausstellung von Beweisen
  - Beispielimplementierungen

LÖSUNGSANSÄTZE

- Self-Sovereign Identity: modern
- Public Key Infrastruktur: technisch ausgereift
- Zentraler Identitätsprovider: ungeeignet

Allgemeine Stellungnahme

André Kudra

Bundesverband IT-Sicherheit e.V. (TeleTrusT), Deutschland

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

Konsultation der Schweiz zum «Zielbild E-ID»

Bern, 14.10.2021

Self-Sovereign Identity (SSI): Einblicke Deutschland und europäische Ebene

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Dr. André Kudra

Agenda

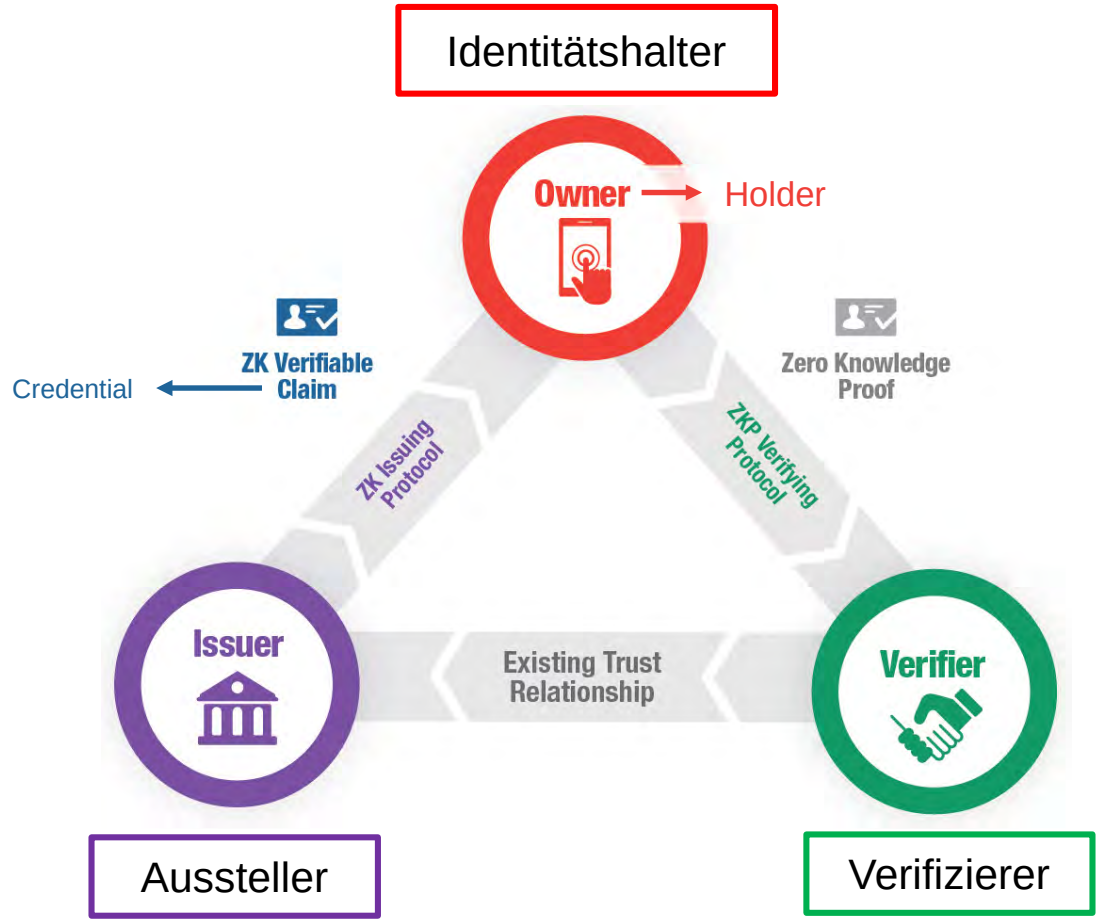
- **SSI in aller Kürze**
- **Schaufensterprojekte BMWi**
- **SSI-Pilotprojekte des Bundeskanzleramtes**
- **SSI-Entwicklungen auf europäischer Ebene**
- **TeleTrusT IT-Sicherheitsagenda 2029**

SSI als Grundlage eines europäischen Ökosystems

SSI ist eine Technologie, die den Nutzer in den Mittelpunkt stellt. Sie ermöglicht eine selbstbestimmte, selbst verwaltete digitale Identität für Alle.

Der Nutzer (Identitätshalter) hat die Kontrolle über seine persönlichen Daten und entscheidet, wem und zu welchen Zwecken er seine Identitätsdaten mittels digitaler Credentials zur Verfügung stellen möchte.

Grundlage dafür ist das Vertrauens-netzwerk.



Original Source: Sovrin™: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust – A White Paper from the Sovrin Foundation - Version 1.0 - January 2018

Schaufensterprojekte des Bundesministeriums für Wirtschaft und Energie (BMWi)

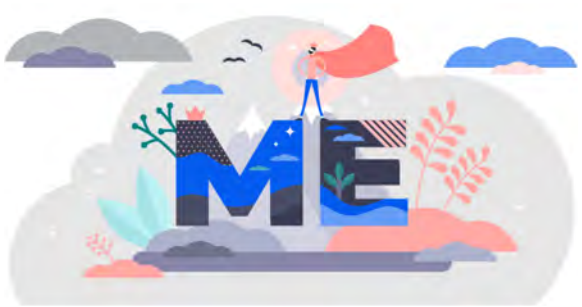
- Der **Innovationswettbewerb "Schaufenster Sichere Digitale Identitäten"** fördert herausragende Ansätze für neue ID-Ökosysteme, in denen sich Anwender und Anwenderinnen im Alltag mit ihrem Smartphone gegenüber Dienstleistern oder Behörden digital ausweisen können.
- Vier Schaufensterprojekte wurden vom BMWi ausgewählt:
  - ID-Ideal
  - SDIKA
  - ONCE
  - IDunion ← Fokus auf Self-Sovereign Identity

Quelle: https://www.digitale-technologien.de/DT/Navigation/DE/ProgrammeProjekte/AktuelleTechnologieprogramme/Sichere_Digitale_Identitaeten/Projekte_Umsetzungsphase/projekte_umsetzungsphase.html

IDunion:
Ein offenes Ökosystem für vertrauensvolle Identitäten

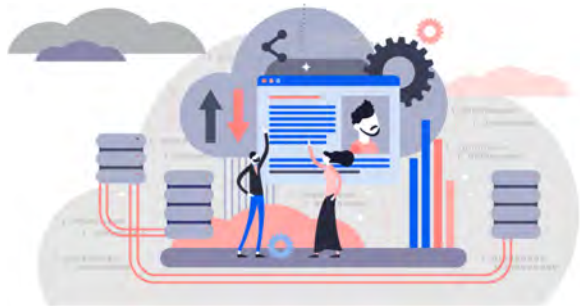
TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

➔ Aufbau eines offenen Ökosystems für die dezentrale Identitätsverwaltung, welches weltweit nutzbar ist und sich an europäischen Werten und Regularien orientiert.



Im Zentrum der Lösung für selbstbestimmte Identitäten – sog. Self-Sovereign Identities (SSI) – steht per Definition immer der Nutzer.

Über 45 Projektpartner sind beteiligt, 15 werden für die Umsetzung von 35+ Anwendungsfällen über drei Jahre Projektlaufzeit vom BMWi gefördert.



Zentrale Aspekte des Netzwerkbetriebs sind Sicherheit, Wirtschaftlichkeit, Nutzerfreundlichkeit und Datenschutzkonformität.

Quelle: https://idunion.org

SSI-Pilotprojekte des Bundeskanzleramtes

Alle relevanten verifizierbaren und personalisierten Nachweise sollten dem Nutzer digital zur Verfügung stehen, z.B. in einer Wallet

Die Bundesregierung

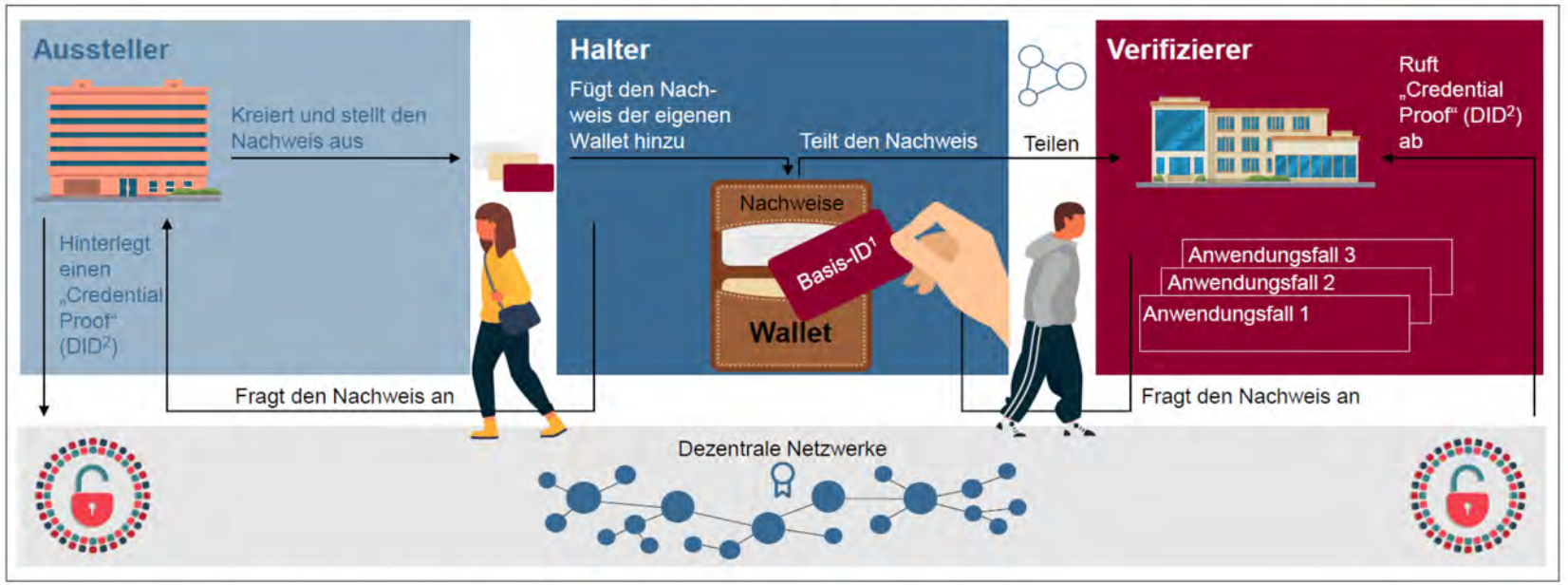
7

Quelle: https://www.bundesregierung.de/breg-de/suche/oekosystem-digitale-identitaet-1960124

SSI-Pilotprojekte des Bundeskanzleramtes

Grundlage für das Ökosystem ist der SSI-Ansatz – Nutzer im Zentrum mit voller Hoheit über seine eigenen Daten

Die Bundesregierung



Konkret bedeutet dies für die Anwendungsfälle, die im Rahmen des Projektes ausgewählt werden:

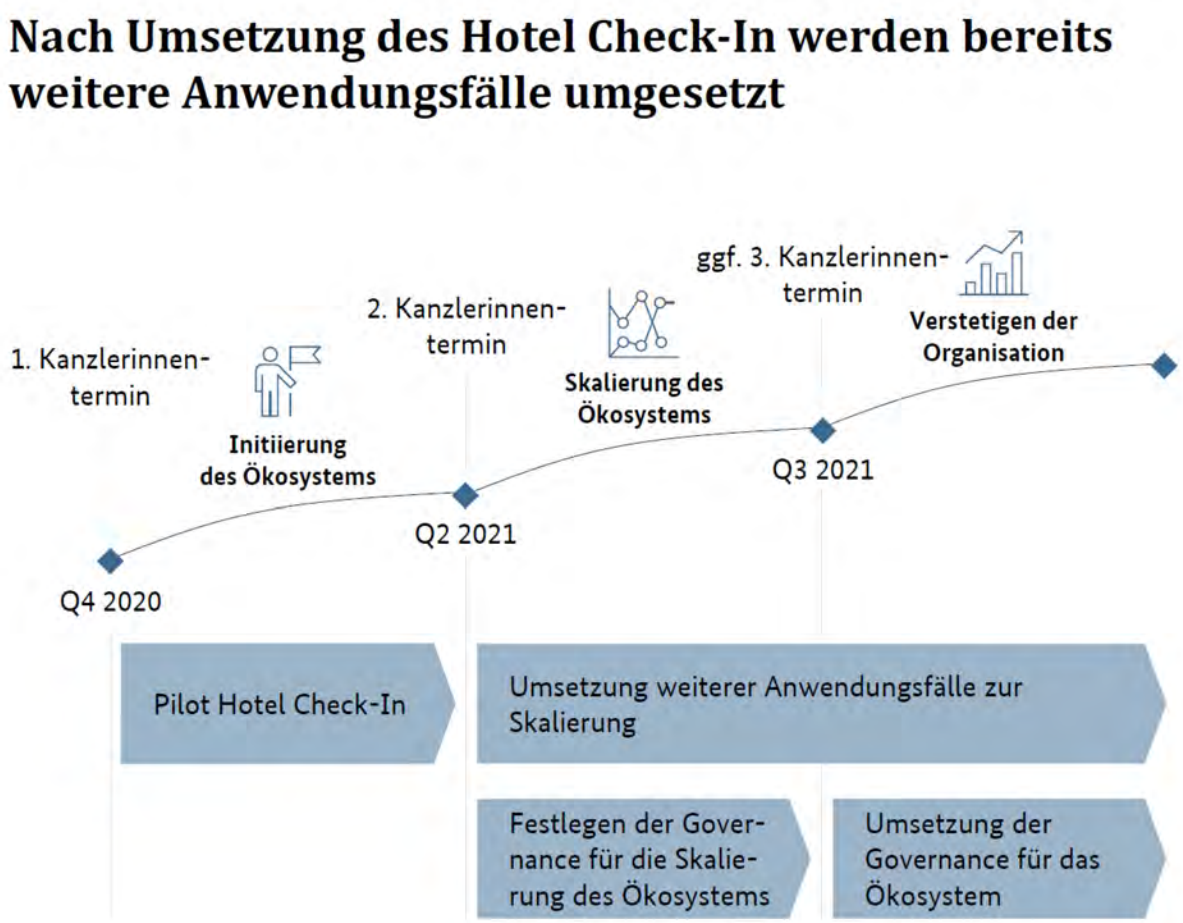
- Nachweise werden nach SSI-Standards ausgestellt
- Verifikation der Nachweise sollte für die Dauer des Projektes über das seitens des Projektes bereitgestellte SSI-basierte Netzwerk erfolgen ("blinde Verifizierung")
- Der Halter verfügt durch die Nutzung einer SSI-basierten Wallet über alle Nachweise

10

1. Entspricht dem Umfang des Personalausweises
2. Decentralized Identifier

Quelle: https://www.bundesregierung.de/breg-de/suche/oekosystem-digitale-identitaet-1960124

SSI-Pilotprojekte des Bundeskanzleramtes



Die Bundesregierung

Der **Pilot zum Hotel Check-in schafft einen ersten Anwendungsfall** in enger Zusammenarbeit von Bundesregierung und der Wirtschaft

Zur **weiteren Skalierung des Ökosystems werden aktuell Anwendungsfälle** aus den folgenden Bereichen umgesetzt:

- Betriebliches Zugangsmanagement für interne/ externe Mitarbeiter
- Führerscheinüberprüfung für Flottenmanagement
- Registrierung für Prepaid Verträge
- Kundenkonto Registrierung/ wiederkehrender Log-In für E-Commerce
- Online-Konto-/ Depoteröffnung bei Banken

11

Quelle: https://www.bundesregierung.de/breg-de/suche/oekosystem-digitale-identitaet-1960124

SSI-Pilotprojekte des Bundeskanzleramtes

EU-weiter Impuls für die digitale Identität - schnelle grenzüberschreitende Umsetzung in Vorbereitung

Press release | 3 June 2021 | Brussels

Commission proposes a trusted and secure Digital Identity for all Europeans

Der europäische Rahmen für digitale Identitäten

""Nach der neuen Verordnung werden die Mitgliedstaaten den Bürgern und Unternehmen digitale Wallets anbieten, mit denen sie ihre nationalen digitalen Identitäten mit dem Nachweis anderer persönlicher Merkmale (z. B. Führerschein, Diplome, Bankkonto) verknüpfen können. Diese Wallets können von öffentlichen Behörden oder privaten Einrichtungen bereitgestellt werden, sofern sie von einem Mitgliedstaat anerkannt werden."

Source: https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663

Die Bundesregierung

Die EU-Kommission hat die EU-Mitgliedstaaten öffentlich aufgefordert, bis September 2022 eine gemeinsame **Toolbox** zu erstellen, die unter anderem **folgende Elemente** enthält:

- **Technische Architektur**
- **Standards**
- **Leitlinien für bewährte Praktiken**

13

Quelle: https://www.bundesregierung.de/breg-de/suche/oekosystem-digitale-identitaet-1960124

SSI-Entwicklungen auf europäischer Ebene: TeleTrusT-Kommentierung zur eIDAS Neufassung

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

- TeleTrusT begrüßt den Vorschlag der Europäischen Kommission, durch eine novellierte eIDAS-Fassung vertrauenswürdige und sichere Digitale Identitäten für alle Europäer zu etablieren.
- Arbeitsgruppe "Blockchain" und Arbeitskreis "Forum elektronische Vertrauensdienste" haben die am 3. Juni 2021 publizierten Entwürfe analysiert und kommentiert:
  - **Self-Sovereign Identity (SSI) wird berücksichtigt und ermöglicht - ein Vertrauensmodell für SSI wird geschaffen**
  - Implementing Acts sind zu harmonisieren und möglichst viele sind zu implementieren, um ein "Level Playing Field" zu erreichen
  - Eine Umsetzungsförderung - auch der Kommunen - für Implementierung und Kommunikation sollte erfolgen
  - EU Trusted List ist der Vertrauensanker für die Datenautobahn - sie ist eine Stärke der eIDAS und sollte der zentrale Vertrauensanker bleiben
  - Die Verpflichtung, in Browsern Qualified Website Authentication Certificates (QWACs) anzuzeigen, wird unterstützt

Quelle: https://www.teletrust.de/publikationen/stellungnahmen

TeleTrusT IT-Sicherheitsagenda 2029 – IT-Sicherheit in der Digitalisierung

TeleTrusT Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-Forderungen

1. Klares Bekenntnis zu unbeschränkter IT-Sicherheit

2. Technologische Souveränität im Bereich IT-Sicherheit schaffen - für eine werteorientierte, sichere und vertrauenswürdige digitale Zukunft

3. **Auf- und Ausbau von IT-Sicherheitsinfrastrukturen für Bürger, Unternehmen und Verwaltung fordern und fördern**

4. Mehr IT-Sicherheitstechnologie "Made in Germany" in der Praxis

5. Verbot der Kompromittierung von IT-Sicherheit, keine Backdoors, Staatstrojaner oder geschwächte Verschlüsselung

6. Europäische IT-Sicherheitsgesetze für eine erhöhte Rechts- und Investitionssicherheit - klar, konsolidiert und agil

Quelle: https://www.teletrust.de/teletrust-it-sicherheitsagenda


PAUSE


DISCUSSION

Vielen Dank

für Ihr Interesse und Ihre Mitwirkung
zur zukünftigen E-ID!

Merci beaucoup

pour votre intérêt et votre participation
concernant l’e-ID future!