

Eine sicherere Methode als die Unterschrift, ist das wirklich möglich?

• Be Respectful

• Be Responsible

Totals 6 5 6 6

Parent Signature MOM

SEEMS LEGIT

Parent Signature MOMMY

Any questions or comments:

♥ ♥ ♥

Wenn meine Eltern etwas unterschreiben:

Wenn ich etwas unterschreibe:



Self-Sovereign Identity Initiative

Erfolgreiche Vorbereitung auf die E-ID

Syrian Hadad, CTO Informatik Aargau

Ziel & Teilnehmer

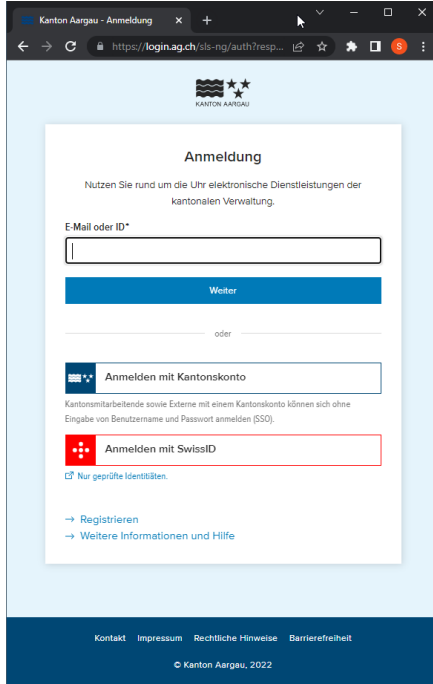
Ziel:

Prüfung von Self-Sovereign Identity
auf **Mehrwert, Akzeptanz** und
technische Machbarkeit durch die
Implementierung
von repräsentativen Use Cases

Teilnehmer:



Ausgangslage Kanton Aargau



Kanton Aargau – Anmeldung

Nutzen Sie rund um die Uhr elektronische Dienstleistungen der kantonalen Verwaltung.

E-Mail oder ID*

Weiter

oder

Anmelden mit Kantonskonto

Kantonsmitarbeitende sowie Externe mit einem Kantonskonto können sich ohne Eingabe von Benutzername und Passwort anmelden (SSO).

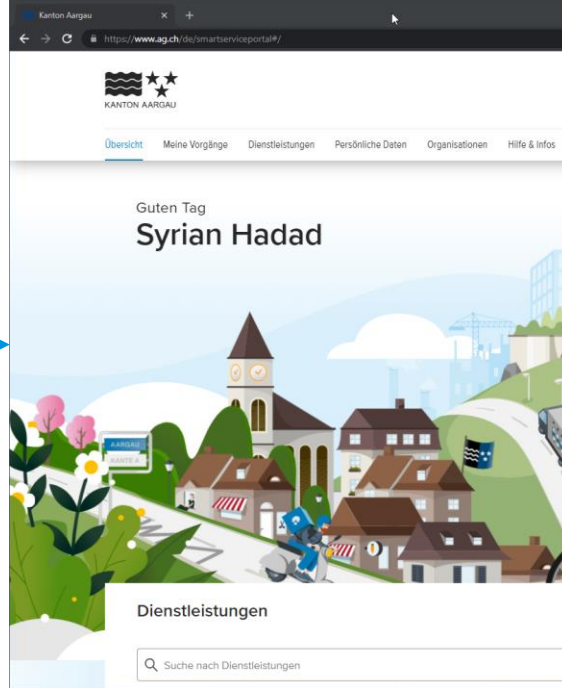
Anmelden mit SwissID

Kur geprüfte Identitäten.

→ Registrieren
→ Weitere Informationen und Hilfe

Kontakt Impressum Rechtliche Hinweise Barrierefreiheit
© Kanton Aargau, 2022

Zentrales Identitäts- und Rollenmanagement



Kanton Aargau

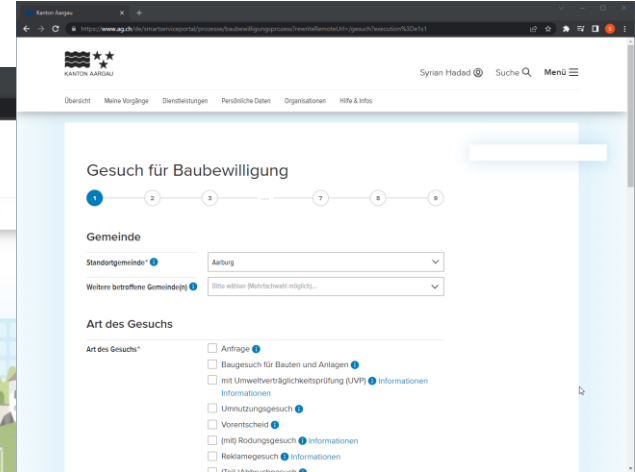
Übersicht Meine Vorgänge Dienstleistungen Persönliche Daten Organisationen Hilfe & Info

Guten Tag
Syrian Hadad

Dienstleistungen

Suche nach Dienstleistungen

Portal für kantonale und kommunale E-Services



Kanton Aargau

Syrian Hadad Suche Menü

Übersicht Meine Vorgänge Dienstleistungen Persönliche Daten Organisationen Hilfe & Info

Gesuch für Baubewilligung

1 2 3 4 5 6

Gemeinde

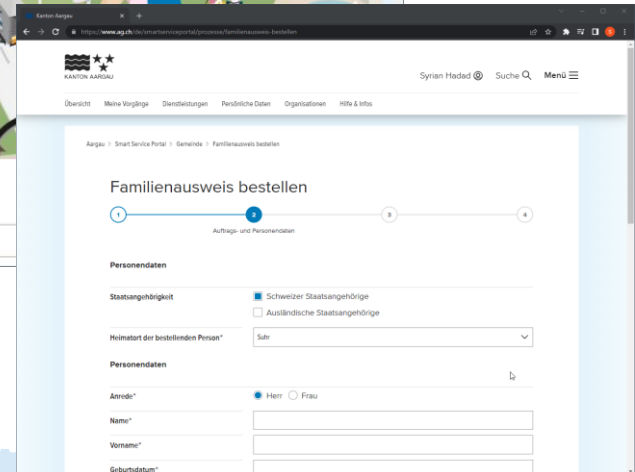
Standortgemeinde* Aargau

Weitere betroffene Gemeinde* (Bitte wählen (Mehrfachwahl möglich))

Art des Gesuchs

Art des Gesuchs*

- ☐ Anfrage
- ☐ Baugesuch für Bauen und Anlagen
- ☐ mit Umweltverträglichkeitsprüfung (UVP)
- ☐ Umnutzungsgesuch
- ☐ Vorentscheid
- ☐ (mit) Rodungsgesuch
- ☐ Reklamesuch



Kanton Aargau

Syrian Hadad Suche Menü

Übersicht Meine Vorgänge Dienstleistungen Persönliche Daten Organisationen Hilfe & Info

Aargau > Smart Service Portal > Gemeinde > Familienausweis bestellen

Familienausweis bestellen

1 2 3 4

Auftrag- und Personendaten

Personendaten

Staatsangehörigkeit

- ☒ Schweizer Staatsangehörige
- ☐ Ausländische Staatsangehörige

Heimatort der bestehenden Person* Suhr

Personendaten

Gender* Herr Frau

Nachname*

Vorname*

Geburtsdatum*

Vertrauensstufen nach E-ID / eIDAS



Hoch

Registrierung mit SwissID

Physische Überprüfung durch geschultes Personal

Substanziell

Registrierung mit SwissID

Identitätskarte + Selbstaufnahme

Niedrig

Selbstregistrierung auf **ag.ch**

Mobiltelefon für 2-Faktor Authentifizierung

-

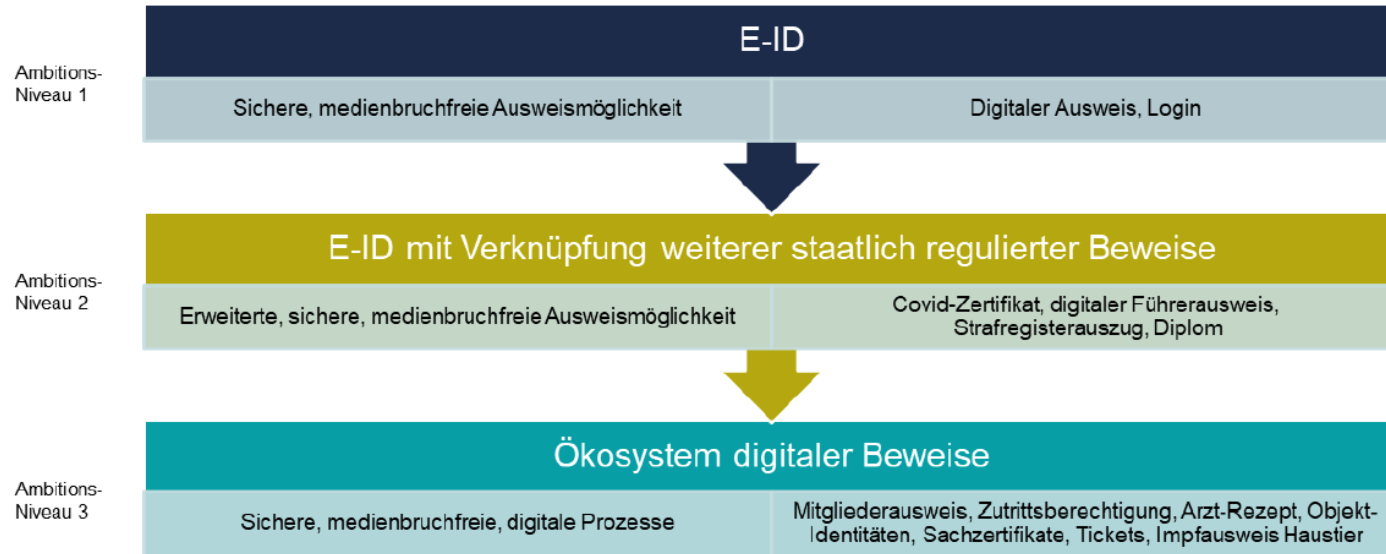
Selbstregistrierung auf **ag.ch**

Smart Service Portal



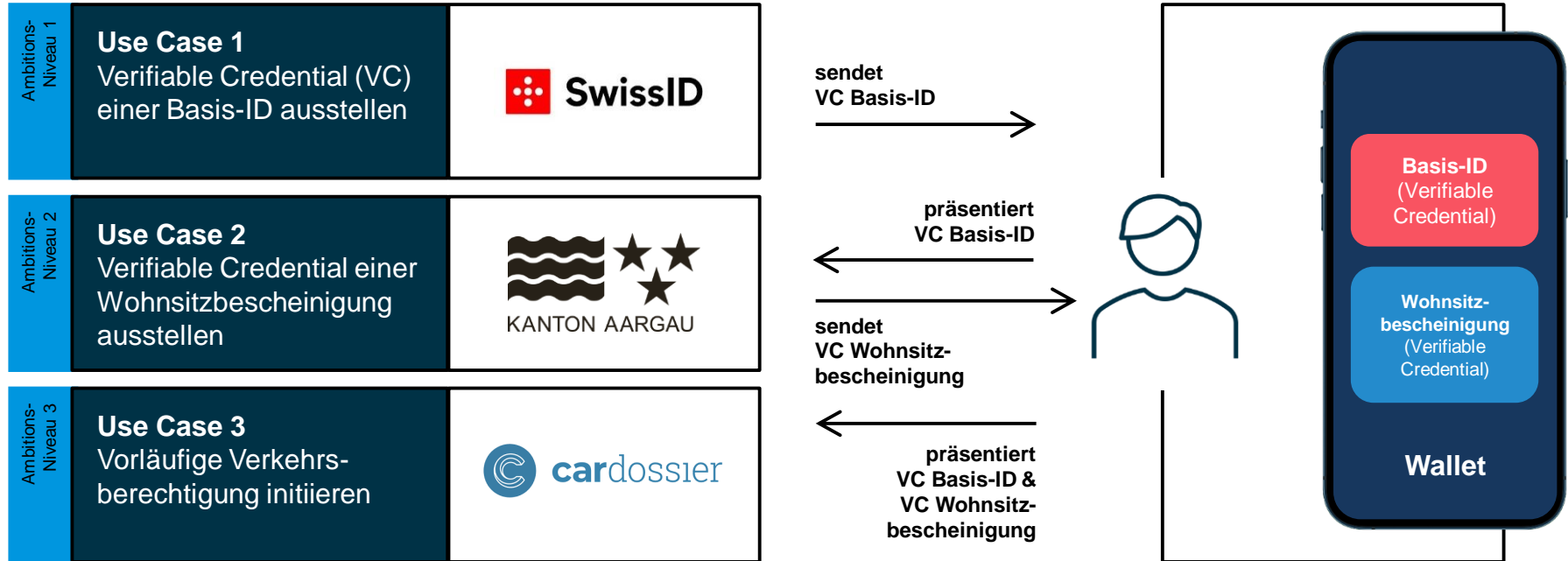
E-Service

Aufbau der Use Cases entlang der Ambitions-Niveaus



Quelle: Diskussionspapier zum «Zielbild E-ID»

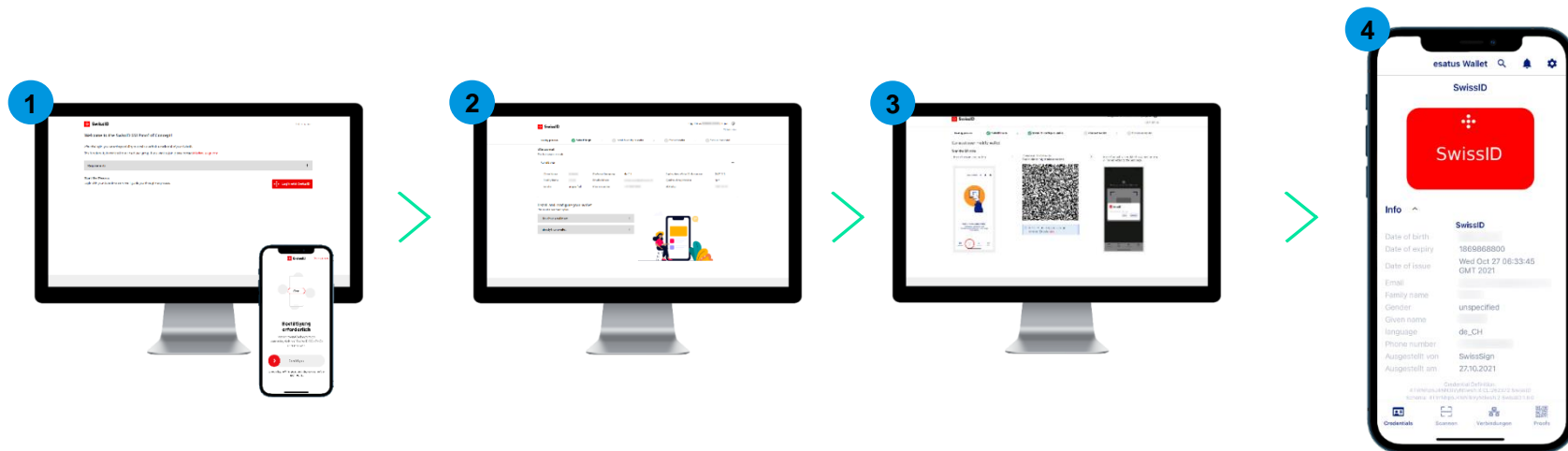
Self-Sovereign Identity-Initiative



Powered by



Use Case 1: Verifiable Credential basierend auf der SwissID ausstellen



Sicherer Login mit Zwei-Faktor-Authentifizierung

Anzeigen der SwissID Benutzerdaten

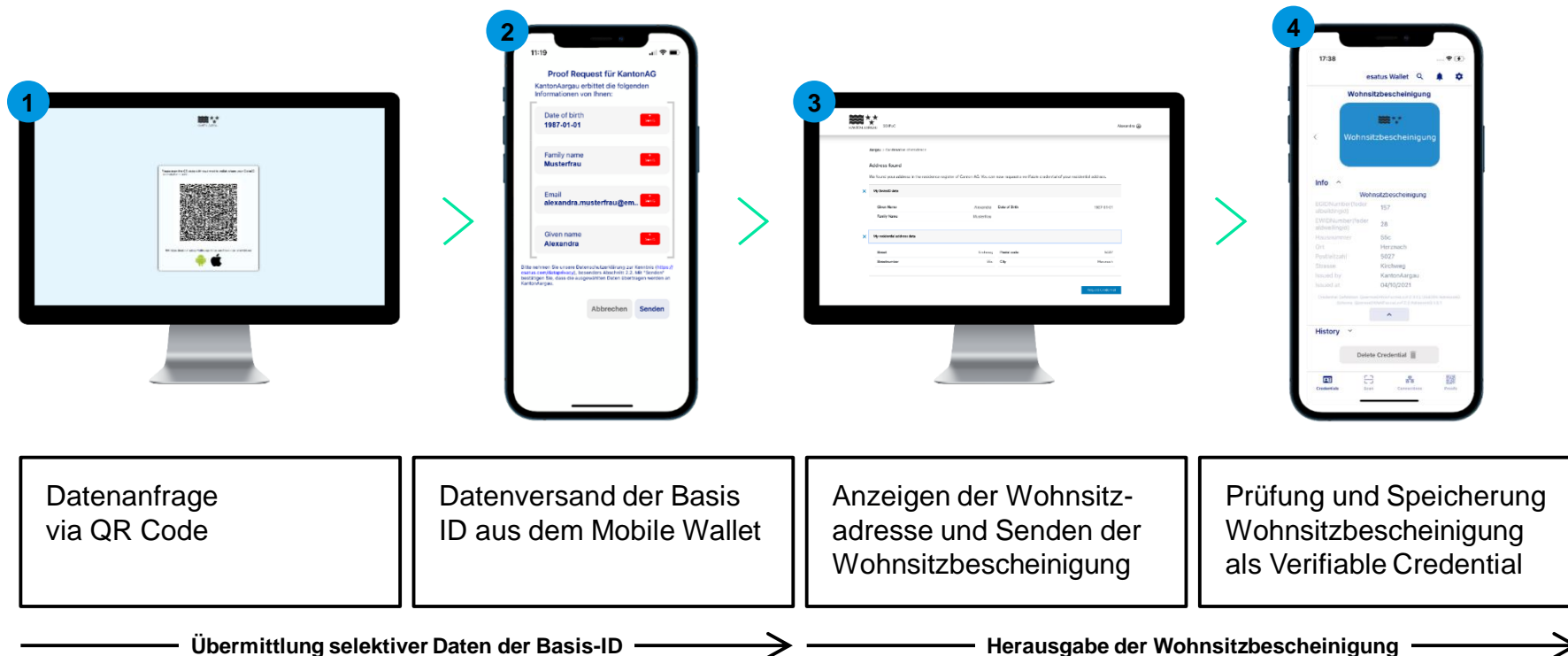
Senden der Identitätsbescheinigung

Speicherung der Identitätsbescheinigung als Verifiable Credential

Sichere Anmeldung im Issuer Portal

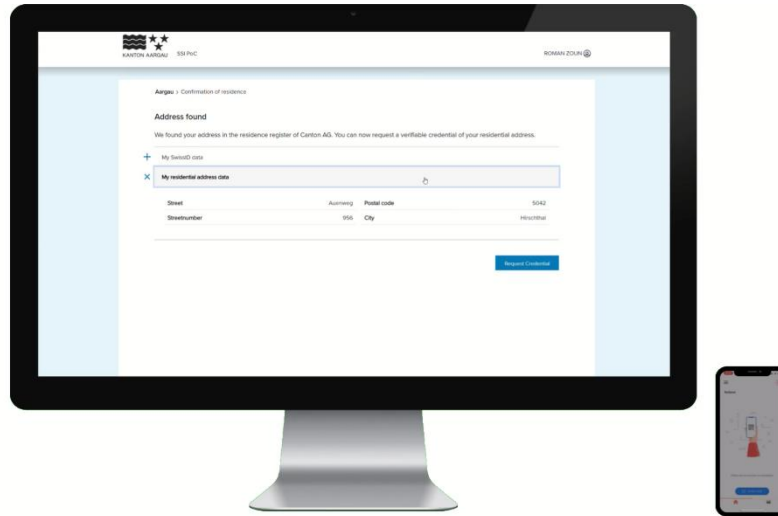
Herausgabe der Identitätsbescheinigung als Verifiable Credential

Use Case 2: Verifiable Credential einer Wohnsitzbescheinigung ausstellen



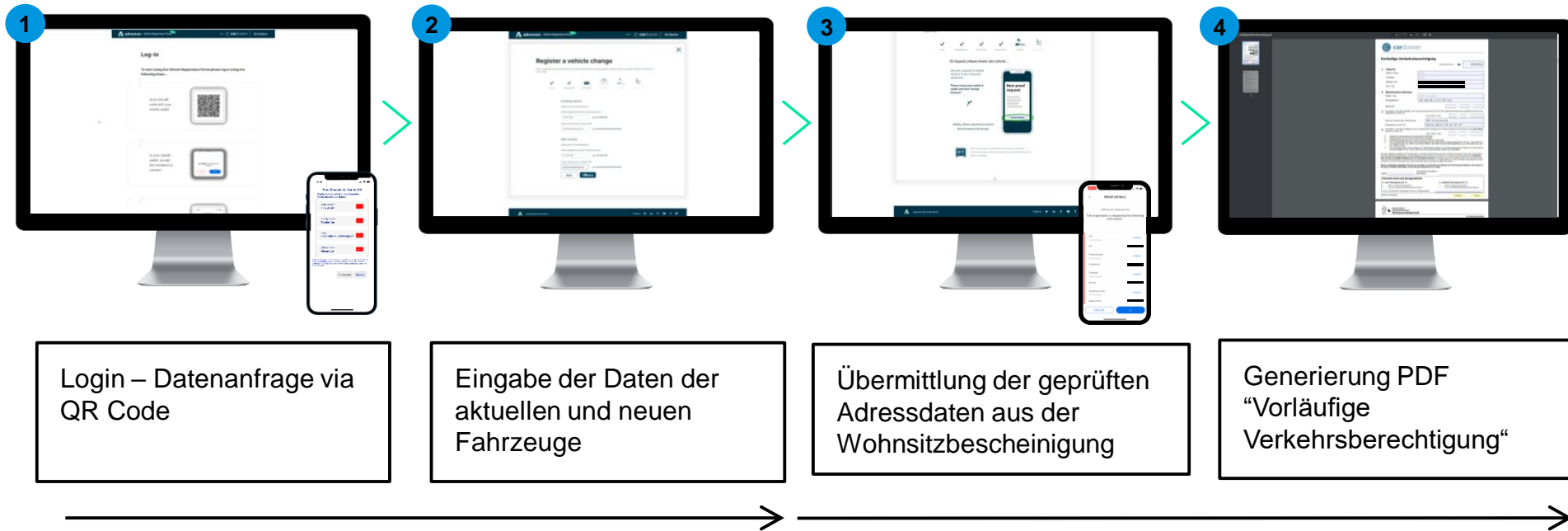
Video

Use Cases 1 & 2

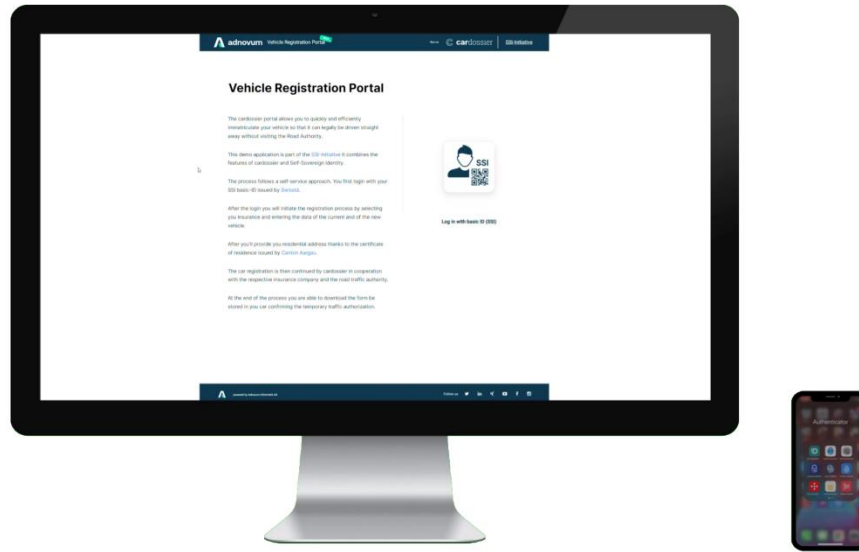


<https://www.youtube.com/watch?v=kBUD3kS6rj0>

Use Case 3: Vorläufige Verkehrsberechtigung initiieren



Video Use Case 3



https://www.youtube.com/watch?v=r4HJH_mgMLs

Hauptkenntnisse

Business-Value



SSI ermöglicht eine effiziente Herausgabe, aber vor allem auch eine flexible Nutzung der ausgestellten digitaler Nachweise durch die anderen Beteiligten



Die Übergabe von strukturierten und verifizierten Daten in der Form von Verifiable Credentials erhöht signifikant die Datenqualität bei allen Beteiligten



Bei Prozessen übernimmt der Wallet die Rolle der „Integration-Zange“ und unterstützt firmenübergreifende Digitalisierungsprozesse



Der Mehrwert ist i.d.R. bescheiden, im Vergleich zu den initialen Gesamtaufwänden.

User Experience (UX)



Die Testnutzer empfanden es als sehr positiv, dass sie die Kontrolle über ihre eigenen Daten haben und begrüßten die Transparenz des Prozesses.



Wenn die Nutzung des VCs in den Prozess gut eingebettet ist, steigt der Benutzerkomfort



UX bleibt eine Herausforderung. SSI erfordert viele Interaktionen zwischen dem Browser und dem Smartphone und damit dem Benutzer.



Die Akzeptanz der User steigt mit der Anzahl der Anwendungsmöglichkeiten der Wallet – mit möglichst gleichem Vorgehen

Datenschutz und Compliance



DSGVO-Pflichten bezüglich Datensparsamkeit werden leichter erfüllt, da ein Service Provider Benutzerdaten nicht mehr speichern muss (z.B. mit Zero-Knowledge-Proof).



Etablierte Compliance-Prozesse wie Key Ceremony lassen sich ebenfalls im SSI-Kontext verwenden.



Die Vertrauensstufen bestehender digitaler Nachweise können auf neue Verifiable Credentials übertragen werden.



Die Identität des Issuers und Verifiers lässt sich noch nicht leicht verifizieren.

Technologie



Internationale Standardisierung von SSI durch W3C, Decentralized Identity Foundation und Hyperledger Foundation Cryptography ist weit verbreitet.



Die SSI-Technologie ist jedoch jung und steht im Wandel. Die Maturität für eine produktive Einführung oder ein Produkt wird innerhalb der nächsten 3 Jahre erreicht.



Interoperabilität basierend auf dem aktuellen Standard-Technologie Stack (Open Source, AIP 1.0) ist gesichert. Nachhaltige Pilotierung muss jedoch auf AIP 2.0 erfolgen.



Die Integration mit bestehenden IdP-Infrastrukturen via den bekannten Protokollen (wie OIDC oder SAML) ist problemlos möglich.



Die On-Premise Produktintegration war gleich aufwändig wie die Nutzung von Opensource- Komponenten

Fazit

Mein Fazit als CTO

- > SSI bringt sehr viele Vorteile im Bezug auf **Datenschutz** und **organisationsübergreifende Digitalisierung** über die drei Ambitionsniveaus.
- > Die notwendige Maturität für produktive Lösung wird innerhalb der nächsten 3 Jahre erreicht. Die aktuellen Implementierungen sind „Wegwerfprodukte“, mit den wir **viel lernen** können.
- > Dank starken Kryptosicherheit konnten wir mit **produktiven Daten** arbeiten und damit **repräsentative Anwendungen** ermöglichen.
- > Dank der Umsetzung von praktischen Use Cases konnten wir als Informatik im Kanton die **Auswirkungen** auf unsere Organisation und unsere Systemlandschaft evaluieren.
- > Potential einer starken **Vereinfachung** der **Lösungsentwicklung** für durchgehend digitale Prozesse.

Nützliche Informationen

- > Blog [“Mit repräsentativen Use Cases das Potenzial von Self-Sovereign Identity ausloten”](#)
- > Blog [”Self-Sovereign Identity – ein neues Zeitalter in Sachen Datenschutz”](#)
- > Website www.cardossier.ch
- > Website www.didas.ch
- > Blog [“Eine E-ID auf Basis SSI – welche regulatorischen Voraussetzungen müssen geschaffen werden?”](#)

Vielen Dank für Ihre Aufmerksamkeit!

Bei Fragen zur Initiative



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



Attila Fekete
Senior Digital Advisor
SwissSign Group AG
attila.fekete@swissign.com



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



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

