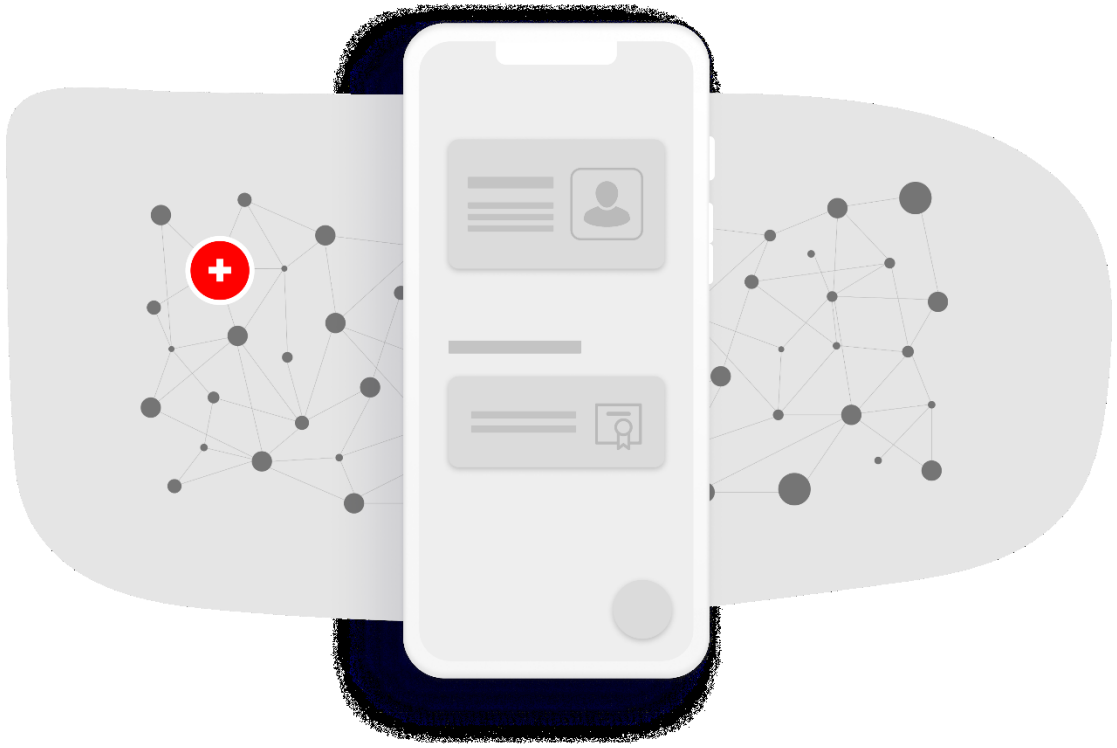
Fachhochschule Nordwestschweiz
Hochschule für Technik

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung,
Bevölkerungsschutz und Sport



Digitalisierung der Armee: Anwendung Blockchain-basierter Self-Sovereign Identity

Luca Dietiker, Ralf Winkelmann

FHNW – 12.9.2022

Ausgangslage

Ausbildungsgutschrift

Wer sich für eine Laufbahn als Unteroffizier, höherer Unteroffizier oder Offizier bis Stufe Stäbe der Truppenkörper bei der Armee entscheidet, erhält pro erreichte Gradstufe einen Betrag, den er/sie für eine zivile Aus- oder Weiterbildung verwenden kann. Der Antrag erfolgt manuell.

Ausgangslage

Problemstellung und Ziel

IST Situation

- Der Prozess ist für die Antragsteller aufwändig, analog und nicht mehr zeitgemäss
- Der interne Verwaltungsaufwand ist hoch und bedingt oft Rücksprachen
- Der Prozess ist für alle Beteiligten Stellen manuell, sequentiell nicht automatisiert

SOLL Situation

- Der Prozess ist für die Antragsteller einfach, effizient und digital
- Der interne Verwaltungsaufwand ist auf ein Minimum reduziert und automatisiert
- Der Prozess ist automatisiert, sicher, basiert auf der e-ID und dem SSI-Prinzip

Einleitung

Fragestellung und Methodik

- Eignet sich die Blockchain-Technologie als Basis für ein Register der E-ID, die vom VBS verwendet wird?

- Welche Blockchain-Ausprägung eignet sich hinsichtlich unterschiedlicher Faktoren (z.B. Nachhaltigkeit, Performance, etc.) am besten?

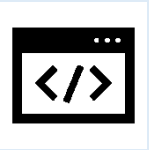
- Wie könnte eine mögliche Umsetzung des Use-Case «Ausbildungsgutschrift» in einem SSI-Ökosystem aussehen?

Einleitung

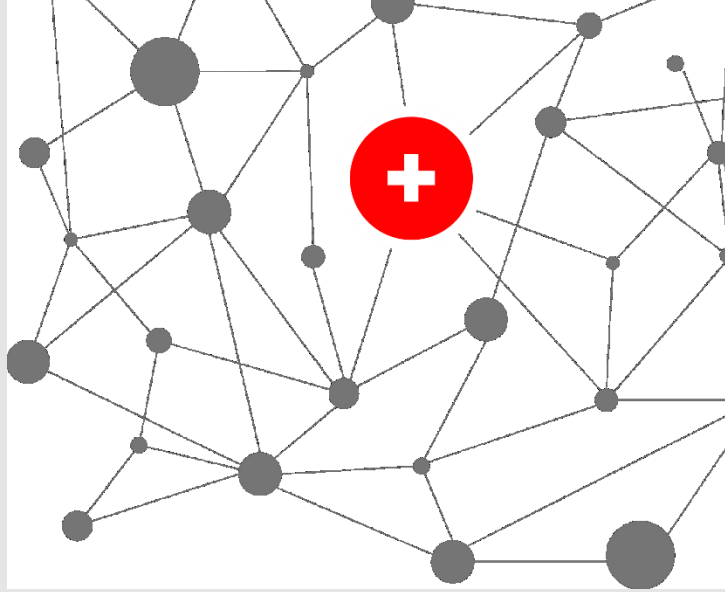
Fragestellung und Methodik

- Eignet sich die Blockchain-Technologie als Basis für ein Register der E-ID, die vom VBS verwendet wird?
- Welche Blockchain-Ausprägung eignet sich hinsichtlich unterschiedlicher Faktoren (z.B. Nachhaltigkeit, Performance, etc.) am besten?
- Wie könnte eine mögliche Umsetzung des Use-Case «Ausbildungsgutschrift» in einem SSI-Ökosystem aussehen?

Literaturarbeit



Implementierung PoC



Blockchain als VDR

Ergebnisse Evaluation

Evaluation VDR-Technologie

Herangehensweise

Anwendungen

→ Viele produktive SSI Anwendungen

→ Südamerika & Europa führend

→ Blockchain dominiert

Szenarien

→ Nationale Risikoanalyse des BABS

→ Austausch mit VBS

- Umweltkatastrophen
- DDoS-Attacken
- Krieg
- etc…

Kriterien

→ Kriterien VBS
z.B. «Nachhaltigkeit»

→ Kriterien aus Szenarien
z.B. «Transnationalität»

→ Kriterien aus SSI-Prinzipien
z.B. «Dezentralität»

Evaluation VDR-Technologie

Erkenntnisse

Zentrale und **Verteilte Systeme eignen sich nicht** als VDR.

- Die Kontrolle über die Daten liegt bei einer zentralen Instanz
- Anfälligkeit für Angriffe auf zentrale Instanz

Nicht erfüllbare Kriterien

- Dezentralität
- Persistenz
- Unstoppbarkeit
- Zensurresisten
- …

Evaluation VDR-Technologie

Erkenntnisse

Private Blockchains eigenen sich nicht als VDR.

- Geschlossene Architektur steht im Widerspruch zu SSI Prinzipien

Nicht erfüllbare Kriterien

- Unstoppbarkeit
- Dezentralität
- Zugänglichkeit, Portabilität und Interoperabilität

Evaluation VDR-Technologie

Erkenntnisse

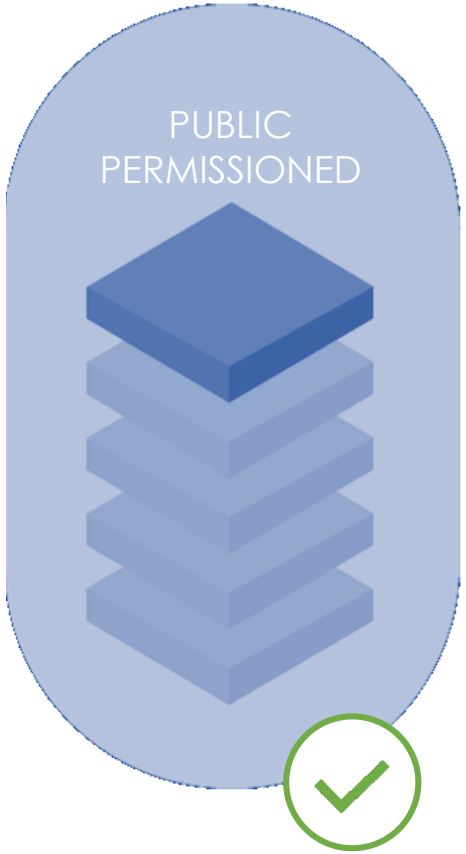
Public Blockchains eigenen sich als VDR.

- Offene Architektur
- Für jede/n einsehbar
- Unterschiedliche Erfüllbarkeit je nach Ausprägung
- Regulationskonformität & Datenschutz: Permissioned schneidet besser ab

Alle Kriterien erfüllbar

Evaluation VDR-Technologie

Fazit

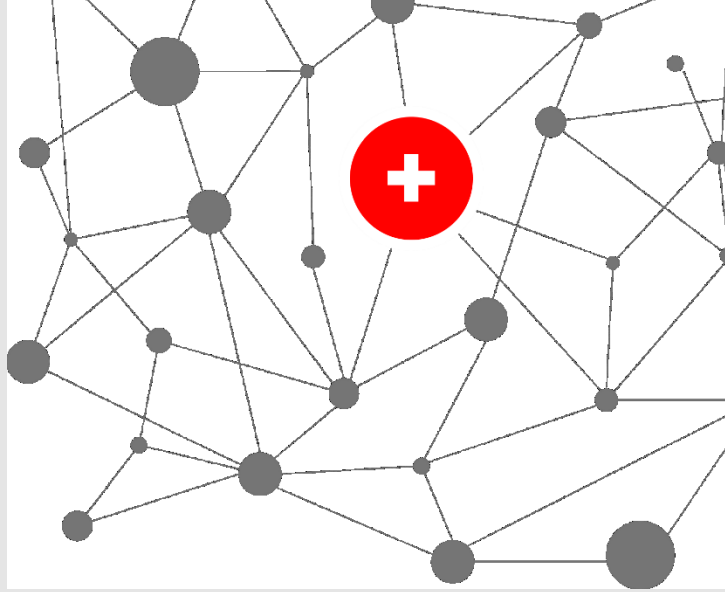


Fazit

→ Dezentraler Ansatz geeignet

→ Public Blockchains eignen sich als VDR

→ Public Permissioned Blockchain erfüllt Kriterien am besten – vor allem Regulationskonformität & Datenschutz.

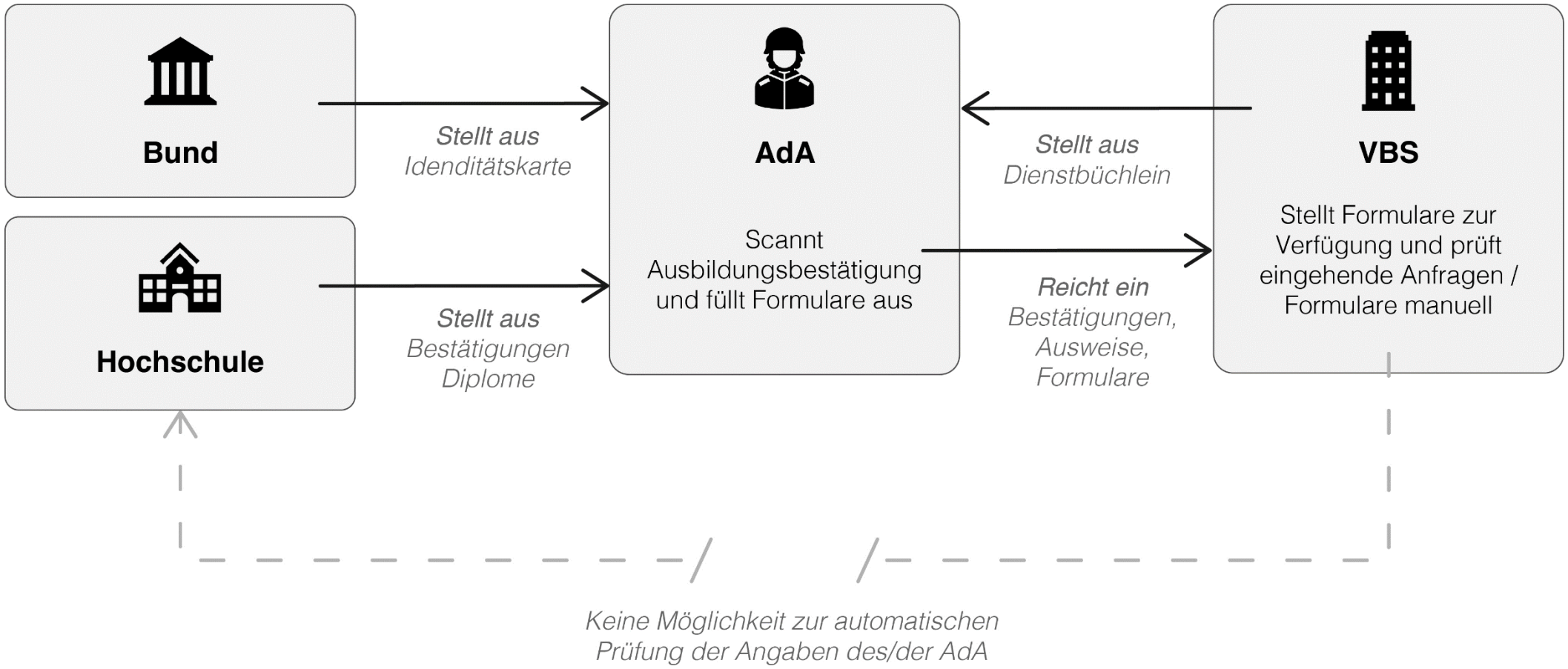


Proof of Concept

Umsetzung SSI-Ökosystem

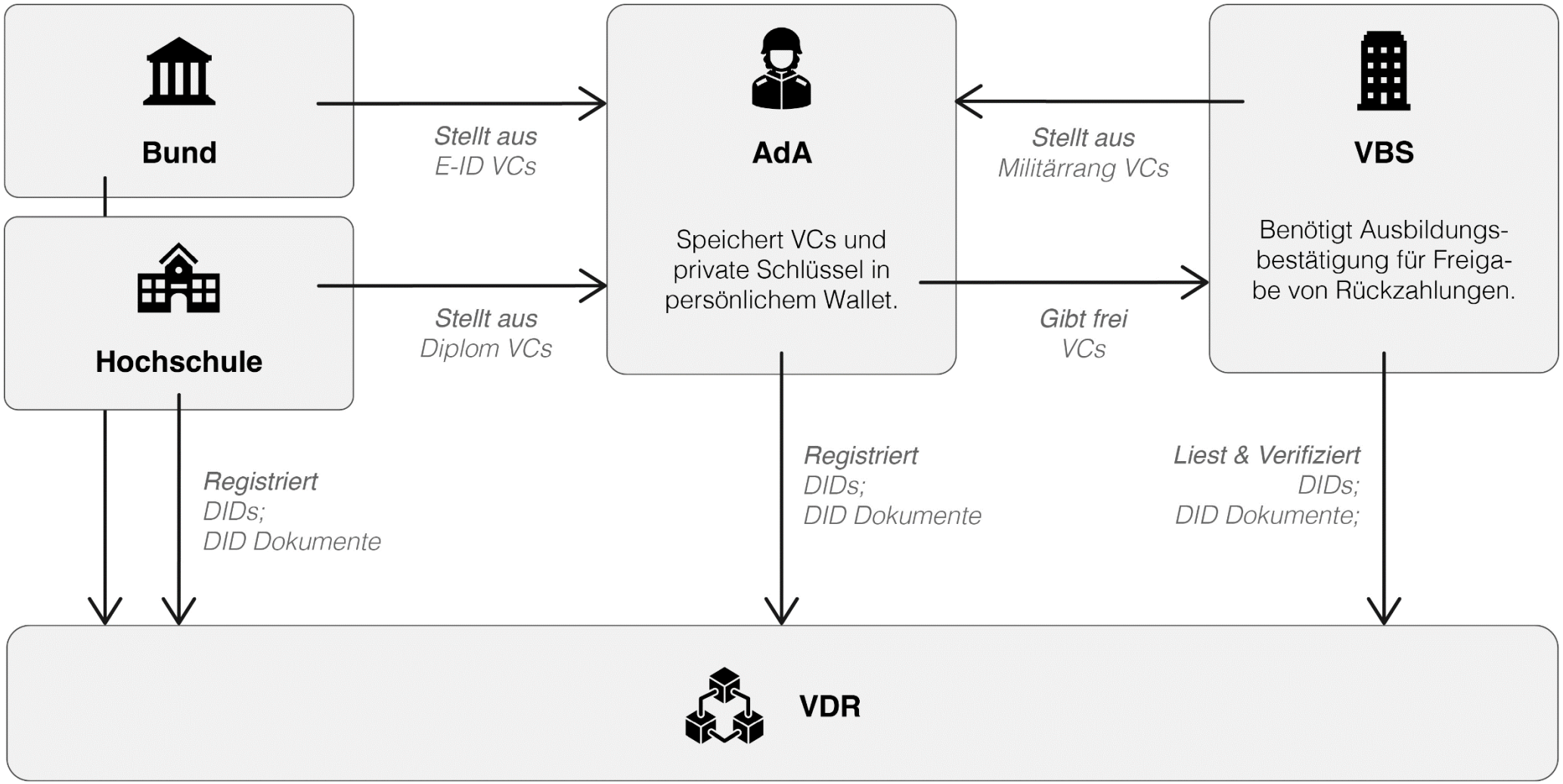
Proof of Concept

Use-Case Ausbildungsgutschrift — Bisher



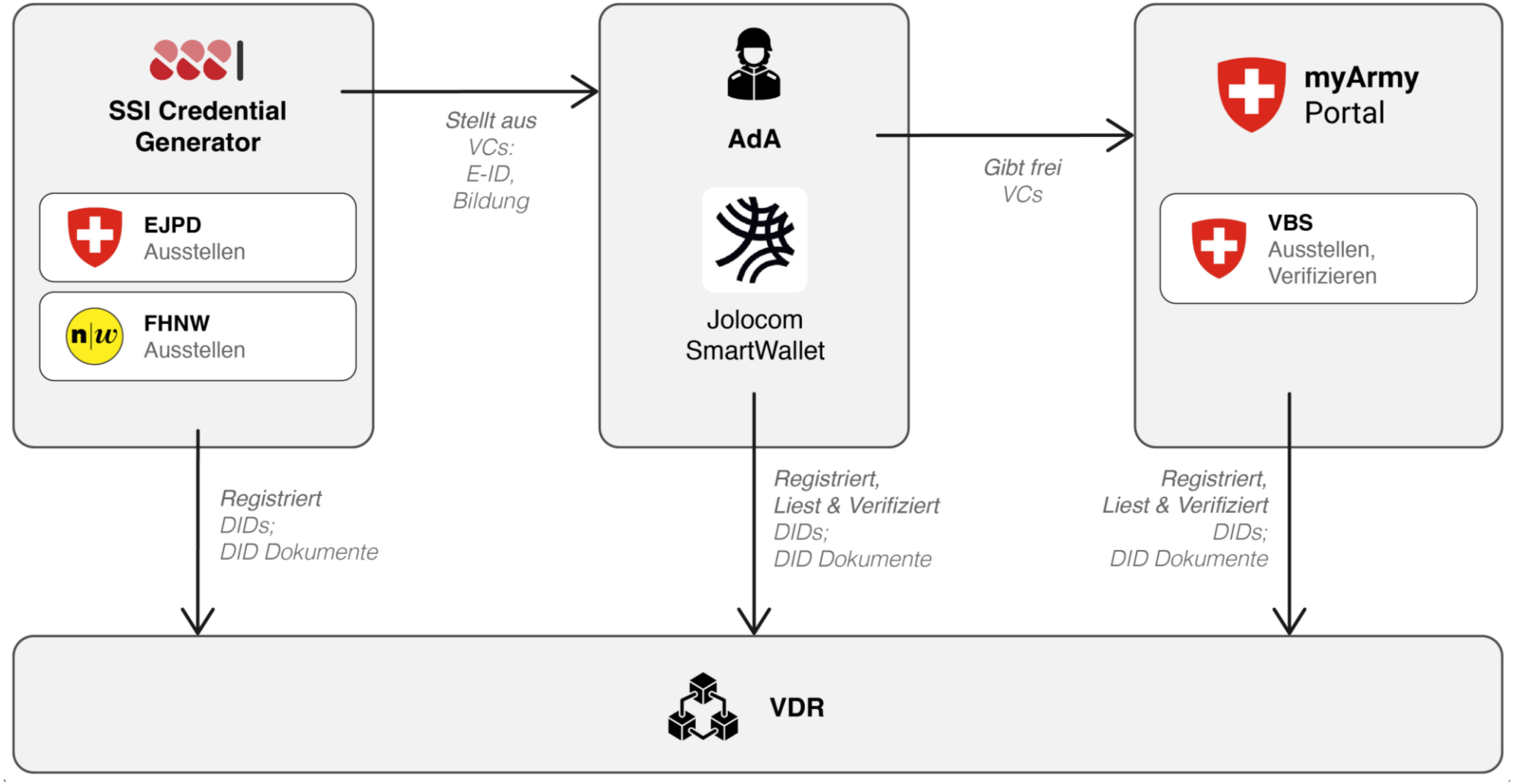
Proof of Concept

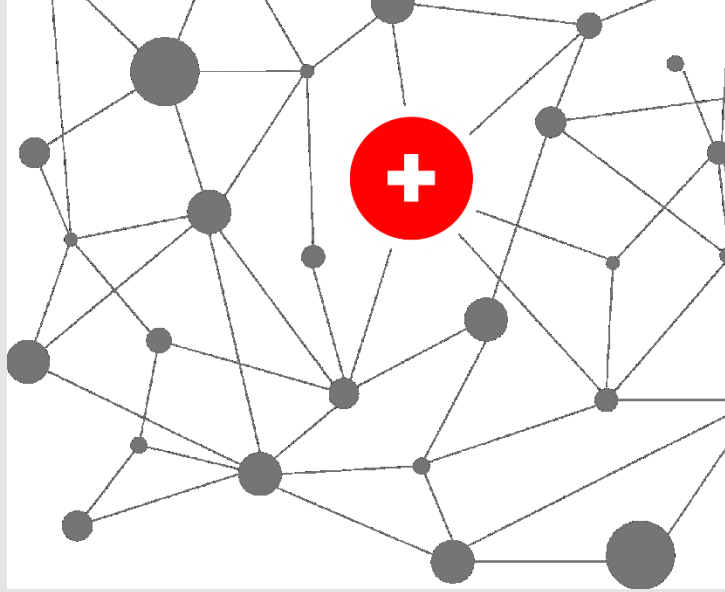
Use-Case Ausbildungsgutschrift — Neu



Proof of Concept

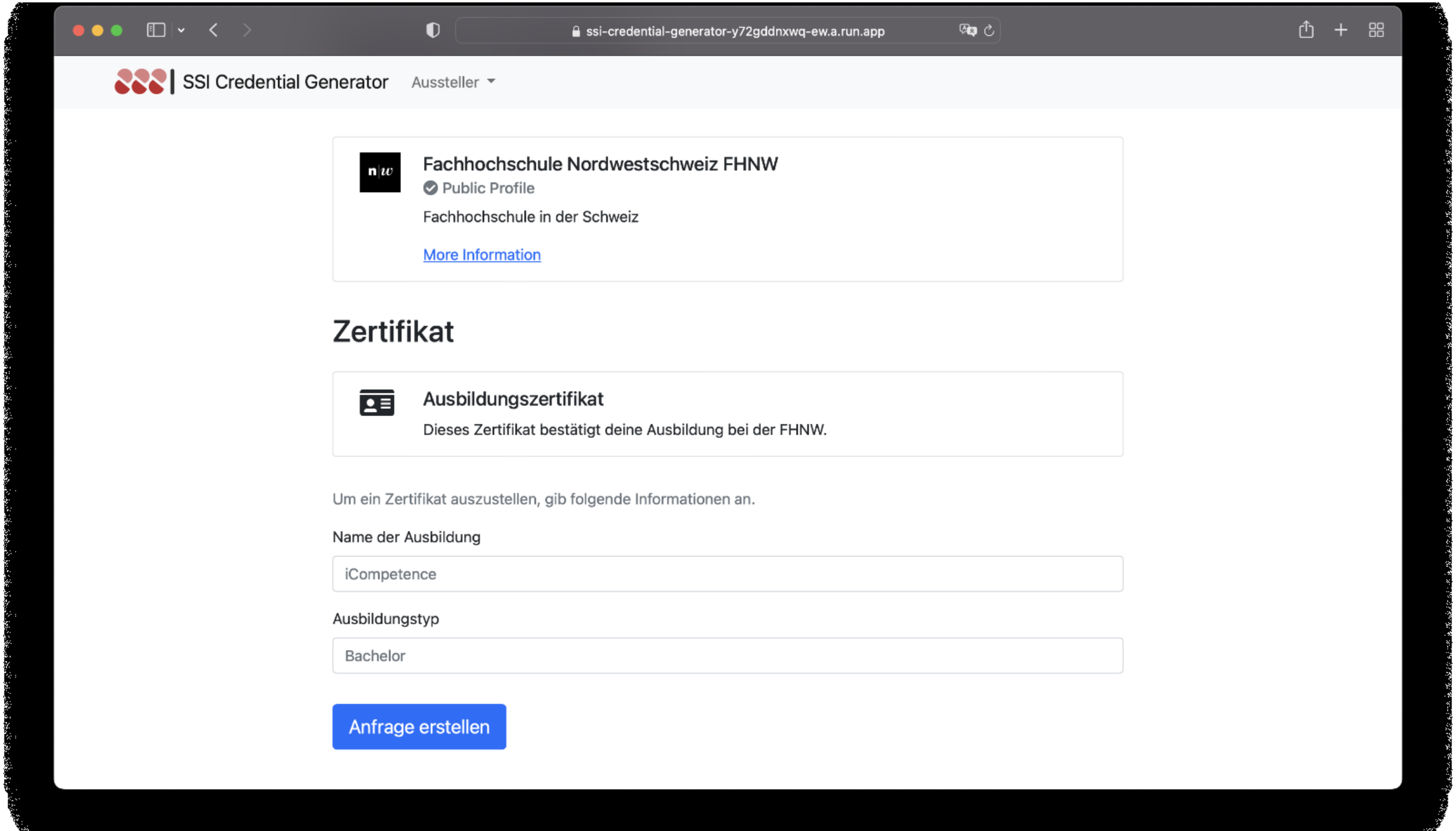
Umgesetztes Ökosystem





Proof of Concept

Live Demo


ssi-credential-generator-y72gddnxwq-ew.a.run.app
SSI Credential Generator
Aussteller
Fachhochschule Nordwestschweiz FHNW
Public Profile
Fachhochschule in der Schweiz
More Information
Zertifikat
Ausbildungszertifikat
Dieses Zertifikat bestätigt deine Ausbildung bei der FHNW.
Um ein Zertifikat auszustellen, gib folgende Informationen an.
Name der Ausbildung
iCompetence
Ausbildungstyp
Bachelor
Anfrage erstellen

vbs-ssi-portal-y72gddnxwq-ew.a.run.app

myArmy Portal

Ausbildungsgutschrift Scannen

Du bist bereit – Wir sind bereit! Scanne den QR-Code rechts mit deinem SmartWallet um uns die benötigten Zertifikate freizugeben.

1 Auswählen — 2 Scannen — 3 Prüfen

Abbrechen

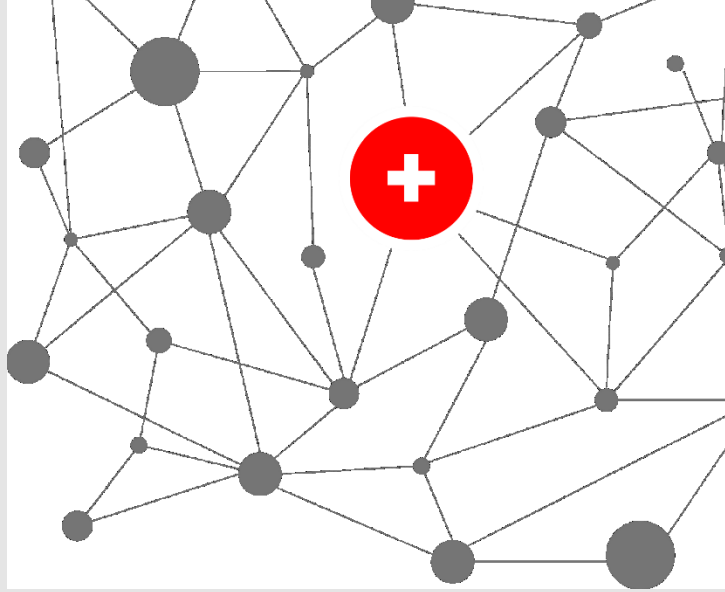
Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport (VBS)

Öffentliches Profil

Eines der sieben Departemente der Schweizer Landesregierung mit dem zentralen Anliegen, «Sicherheit und Bewegung» für die Schweiz und ihre Bevölkerung zu schaffen.

Weitere Informationen

Token Manuell eingeben

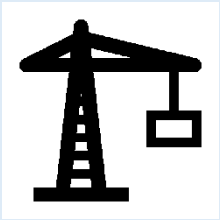


Fazit & Ausblick

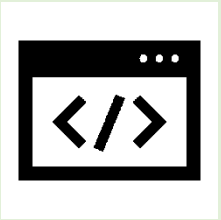
Abschluss

Empfehlungen für die Bundesverwaltung

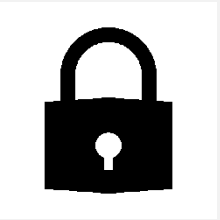
Zusammenfassung Kap. 2.9.



Architektur



Standards



Sicherheit & Wallet

Abschluss

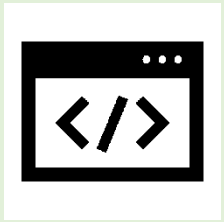
Zusammenfassung

Architektur

Transnationale Abstützung

26 Knoten in der Schweiz,
Knoten in jeder dritten Botschaft
im Ausland

→ Staat kann weiter operieren,
auch bei feindlicher Besetzung



Standards

Sicherheit & Wallet

Abschluss

Zusammenfassung

Architektur

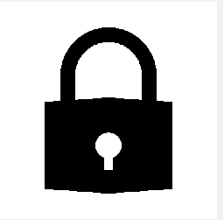
Transnationale Abstützung

26 Knoten in der Schweiz,
Knoten in jeder dritten Botschaft im Ausland

→ Staat kann weiter operieren, auch bei feindlicher Besetzung

Standards

- Eigene DID-Methode (analog EBSI)
- Internationale Standards (eSSIF, EBSI, W3C, DIF)
- Schaffung nationaler Arbeitsgruppen (analog W3C) zur Etablierung von Standards. (z.B. Hochschuldiplome)



Sicherheit & Wallet

Abschluss

Zusammenfassung

Architektur

Transnationale Abstützung

26 Knoten in der Schweiz,
Knoten in jeder dritten Botschaft im Ausland

→ Staat kann weiter operieren, auch bei feindlicher Besetzung

Standards

- Eigene DID-Methode (analog EBSI)
- Internationale Standards (eSSIF, EBSI, W3C, DIF)
- Schaffung nationaler Arbeitsgruppen (analog W3C) zur Etablierung von Standards. (z.B. Hochschuldiplome)

Sicherheit & Wallet

- Vorgaben zu IT-Sicherheit, Algorithmen und Hash-Funktionen.
- Upgrade der Blockchain, Anpassbarkeit Algorithmen (Post-Quanten-Zeit)
- Bund als Herausgeberin von Wallet App

Abschluss

Zusammenfassung

Erkenntnisse Forschung

Public Permissioned Blockchain für VDR eines Schweizer SSI-Ökosystems
(E-ID) am besten geeignet.

Alle Anforderungen im Kontext des VBS erfüllbar.

Erkenntnisse Proof of Concept

Ausbildungsgutschrift kann im SSI-Umfeld automatisiert realisiert werden.

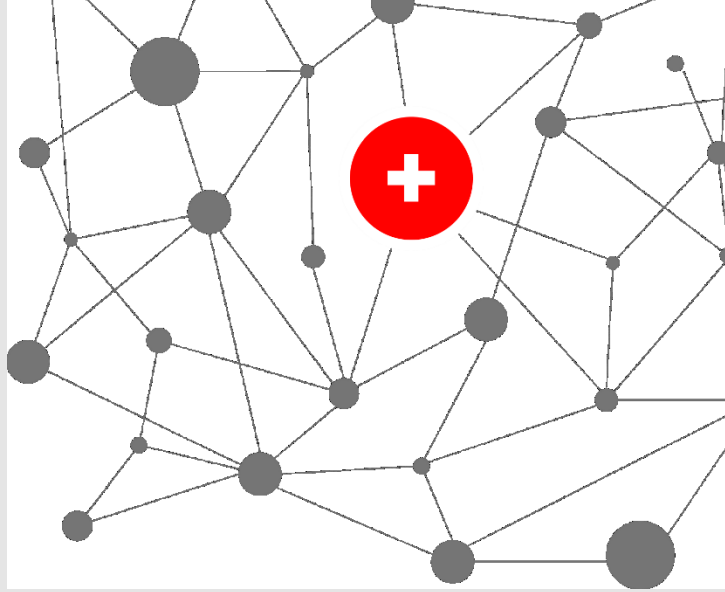
Durchlaufzeit reduziert sich von Wochen auf Minuten – bessere UX für AdA und VBS.

Jolocom-Framework geeignet, Teile noch nicht reif.

Ausblick

Analyse auf allgemeiner Basis durchgeführt. Evaluierung konkreter Technologien muss folgen.

Empfehlungen für die Bundesverwaltung in Bericht.



Thesis herunterladen

Herzlichen Dank!

Kontakt

Carlo Dietiker

carlo.dietiker@vtg.admin.ch

Luca Dietiker

luca.dietiker@swisscom.com