

ISO mDL vs SSI

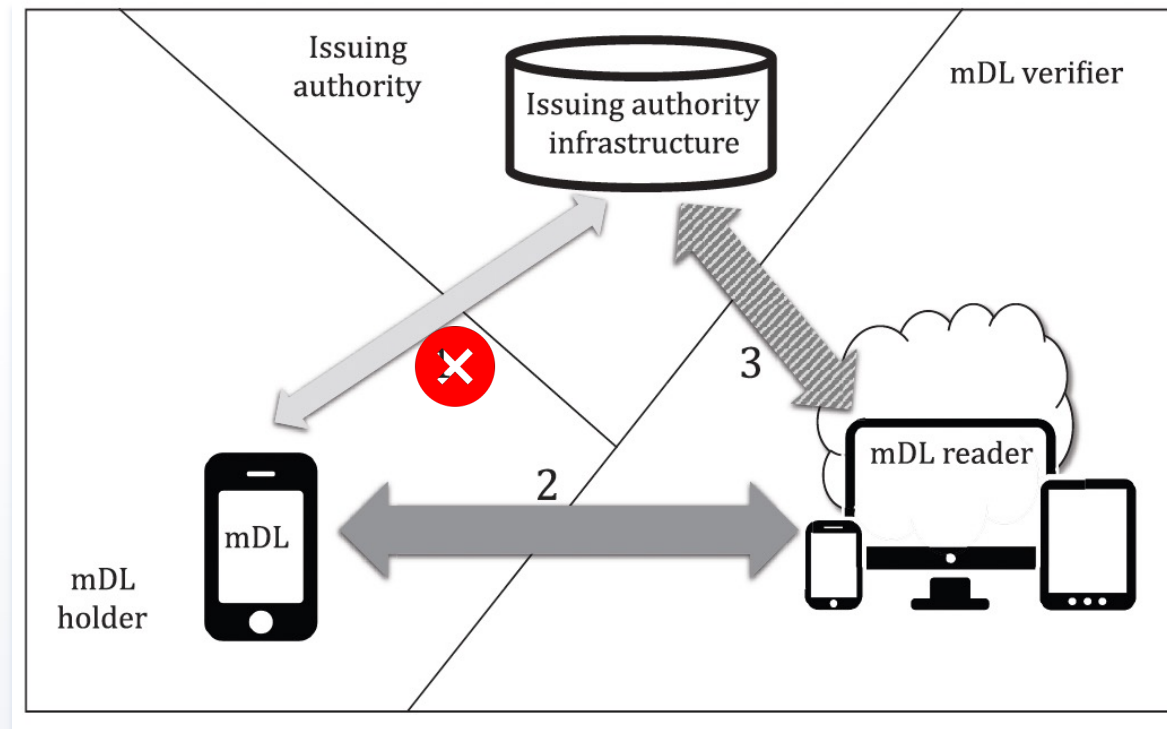
ISO 18013-5 Mobile driving licence (mDL) im Kontext von SSI



Einführung zu ISO 18013-5

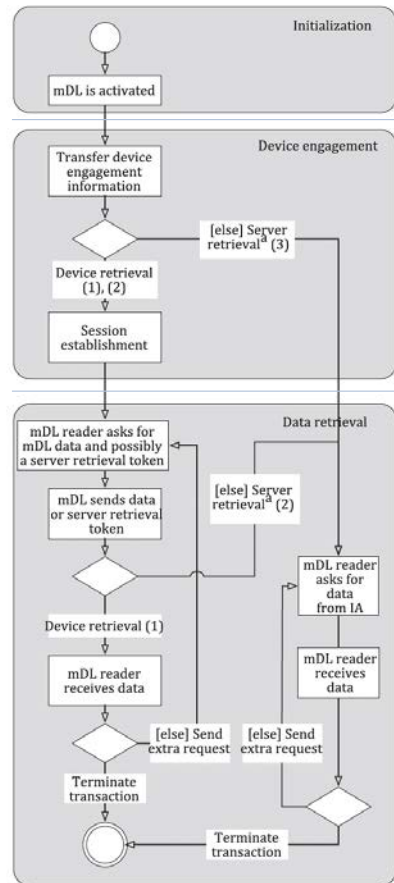
- > Publizierter ISO Standard seit September 2021
 - Grosses Industrieinteresse: UL, Apple, Google, Microsoft, IDEMIA, etc.
 - Bereits unterstützt in Apple Wallet und angekündigt für mehrere US Bundesstaaten
- > PKI basiert mit x509 Zertifikaten (Aussteller)
- > Übertragung vom Führerschein via NFC, BLE, Wifi ("offline") und Web APIs ("online")

ISO mDL Schnittstellen



Source: ISO 18013-5

ISO mDL Transaktionen



Device engagement technologies

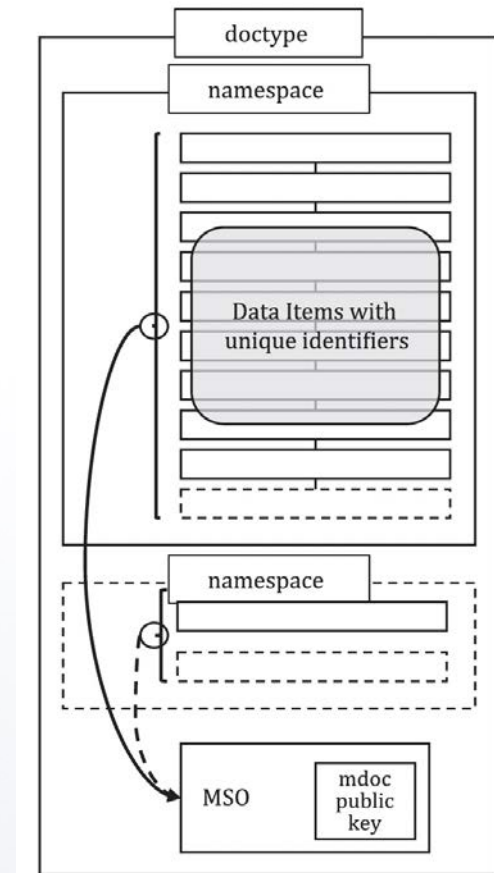
Transmission technology	Support	
	mDL holder	mDL reader
NFC	Conditional	Mandatory
QR code	Conditional	Mandatory

Data retrieval methods

Data retrieval method	Transmission technology	Support	
		mDL holder	mDL reader
Device retrieval	BLE	Conditional	Mandatory
	NFC	Conditional	Mandatory
	Wifi Aware	Optional	Recommended
Server retrieval	WebAPI	Optional	Recommended
	OIDC	Optional	Recommended

ISO mDL Datenmodell

- > mDL Datenmodell analog physischer Variante (ISO 18013-1)
- > Wallets speichern vom Aussteller signiertes Mobile Security Object (MSO)
 - Enthält Public Key, Referenzen der einzelnen Attribute sowie Ausstellzeitpunkt
 - Wird zur Prüfung an Reader übertragen
 - Attribute können einzeln geteilt werden



Typische ISO mDL Architektur



Zusammenführung ISO mDL & SSI

Verlgeich mDL und SSI: Vorteile und Nachteile

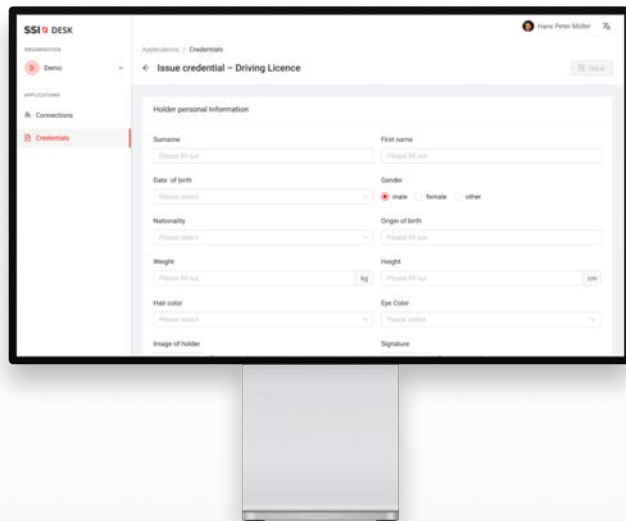
	mDL	SSI
Vorteile	<ul style="list-style-type: none"> • Klar spezifizierte Protokolle für Verbindungsaufbau und Datenübertragung 	<ul style="list-style-type: none"> • Nicht-korrelierbare Identifier • Keine zentralisierte Infrastruktur • Grosse Open-Source Community
Nachteile	<ul style="list-style-type: none"> • Korrelierbarer Identifier • Übertragungsmethoden teilweise basierend auf zentraler Infrastruktur (analog IdP Ansatz) • Revozierung nicht spezifiziert • Proprietäres Ökosystem 	<ul style="list-style-type: none"> • Früh in der Entwicklung • Offenheit der Standards führt zu hoher Diversität

mDL als Verifiable Credential

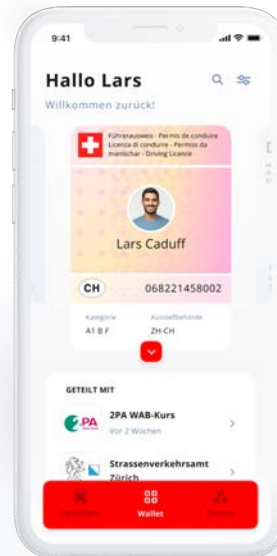
Die Vorteile von SSI und mDL könnten folgendermassen kombiniert werden:

- > Ausstellung des mDL als Verifiable Credential: ISO 18013-1 Datenelemente als reguläre Attribute und einbetten des mDL Mobile Security Object (MSO)
- > Das MSO muss regelmässig durch den Issuer erneuert werden
- > Die SSI Wallet soll die ISO 18013-5 offline Schnittstellen unterstützen (NFC & BLE)
- > Die ISO 18013-5 online Schnittstellen sollen aus Privatsphärengründen nicht implementiert werden
- > Das mDL Verifiable Credential wird mit den regulären SSI Mechanismen revoziert

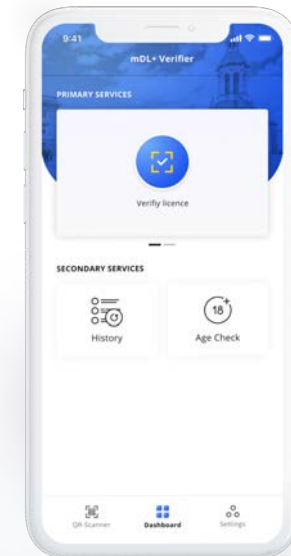
Mobiler Führerschein – mit Procivis SSI+ & Procivis mDL+



SSI Issuer
SSI+ Desk



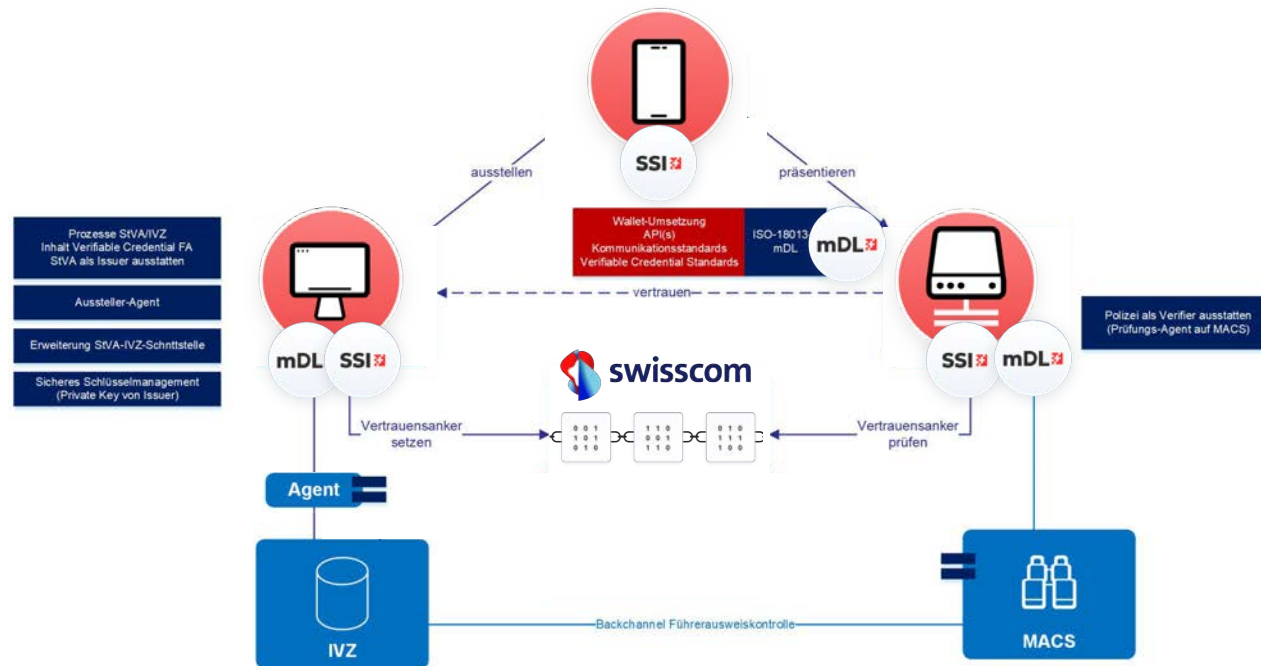
SSI Wallet
SSI+ Wallet



ISO 18013-5 Verifier
mDL+ Verifier



Architekturskizze der Pilotprojekte (mDL)



Fragen