

Architekturzielbild

Dieses Dokument stellt den Arbeitsstand zum genannten Datum dar.

Projekt Digitale Identitäten

18. Februar 2021



In einer Wallet müssen nach eIDAS verschiedene Nachweisarten für öffentliche und private Anwendungsfälle integriert sein

Nachweis- und Identitätsmanagement

Nachweis

Beschreibung

Identitätsnachweise

Gliedert sich in 3 Stufen an Sicherheitsniveaus; bei hoheitlich regeltem Anwendungsfall („hoch“) ist Überprüfung der Verbindung zwischen (juristischer) Person, d.h. Daten des Personalausweises, und anderen Daten notwendig

Nachweisarten



Sicherheitsniveau „hoch“, bspw. für Anwendungsfälle wie staatlich hoheitliche OZG-Use Cases



Sicherheitsniveau „substanziell“, bspw. für Anwendungsfälle Hotel Check-in, Online Kontoeröffnung, Prepaid Aktivierung



Sicherheitsniveau „niedrig“, bspw. für Anwendungsfälle wie Kundenkonto-Registrierung im Online-Shop oder Online Zugänge via:



Identifizierung mit Benutzername



Authentifizierung mit Passwort

Identitätsmanagement

Weitere Nachweise

Nachweise, die über die Daten des Personalausweises hinausgehen, daher oftmals nicht hoheitlich geregelt und für verschiedene Arten von Anwendungsfällen einsetzbar sind



Beispiele für **weitere Nachweise**:







- Geburtsurkunde
- Führerschein¹
- Akademische Zeugnisse
- Impfnachweis
- Elektronische Gesundheitskarte
- Konto-, Zahlungs-, Bonitätsinformationen
- Versicherungsbescheinigungen
- Tickets für Mobilität/Kultur
- Mitarbeiter-/Mitgliedsausweis
- E-Mail oder Telefonnummer

1. In Deutschland ist ein Führerschein, obwohl er ein amtliches Dokument ist, kein Ausweisdokument, mit dem man sich identifizieren kann

Im langfristigen Zielbild soll SSI-Ansatz alle Sicherheitsniveaus und Nachweise abdecken, ...

Langfristiges Zielbild mit Kombination aus beiden Ansätzen

Nachweis- und Identitätsmanagement

Nachweis	Identitätsnachweise	Weitere Nachweise
Beschreibung	Gliedert sich in 3 Stufen an Sicherheitsniveaus; bei hoheitlich regeltem Anwendungsfall („hoch“) ist Überprüfung der Verbindung zwischen (juristischer) Person, d.h. Daten des Personalausweises, und anderen Daten notwendig	Nachweise, die über die Daten des Personalausweises hinausgehen, daher per se nicht hoheitlich geregelt und für verschiedene Arten von Anwendungsfällen einsetzbar sind
Nachweisarten	<div><div>SSI-Ansatz Sicherheitsniveau „hoch“, bspw. für staatlich hoheitliche OZG-Use Cases</div><div>SSI-Ansatz Sicherheitsniveau „substanziell“, bspw. für Hotel Check-in, Online Kontoeröffnung</div><div>SSI-Ansatz Sicherheitsniveau „niedrig“, bspw. für Kundenkonto-Registrierung im Online-Shop oder Online Zugänge via</div><div>Identifizierung mit Benutzererkennung</div><div>Authentifizierung mit Passwort</div><div>Identitätsmanagement</div></div> <div>Smart-eID eID¹/Hardwarebasierte Smart-eID Softwarebasierte Smart-eID²</div>	<div>Beispiele für weitere Nachweise:<ul style="list-style-type: none">• Geburtsurkunde• Führerschein• Akademische Zeugnisse• Impfnachweis• Elektronische Gesundheitskarte• Konto-, Identitätsinformationen• Versicherungsbescheinigungen• Tickets für Mobilität/Kultur• Mitarbeiter-/Mitgliedsausweis• E-Mail oder Telefonnummer</div>

1. Noch zu validieren, inwiefern eID-Protokoll Open-Source Standards gemäß der eIDAS 2.0 Verordnung entspricht; Hypothese, dass für langfristige europäische Interoperabilität „eIDAS Bridge“ keine Reichweite erzeugt, sodass eID-Protokoll standardisiert werden müsste
2. Lösung für bspw. TKG- und GWG-konformen Ansatz auf Sicherheitsniveau „substanziell“ aus der Wallet heraus erforderlich, die hohe Reichweite gewährleistet und ohne verpflichtende Unterstützung weiterer physischer Faktoren (wie z.B. eID, Fotos, Token etc.) funktioniert; Abhängig von BSI-Einstufung der Basis-ID und Verfügbarkeit von softwarebasierter Smart-eID
3. Gemäß ENISA, [Digital Identity: Leveraging the SSI Concept to Build Trust](#), Januar 2022



Bestandteile einer integrierten Wallet im Zielbild







Laut eIDAS 2.0 Anforderung müssen **hochsichere Identitätsnachweise** in Wallet integriert sein – im **langfristigen Zielbild** wollen wir das als Option **auch über den SSI-Ansatz** ermöglichen

Vor dem Hintergrund neuer Anforderungen von eIDAS 2.0, insb. dem Wallet-Konzept und Nutzersouveränität, **empfiehlt auch ENISA³ selbstbestimmte Identitätslösungen (SSI)** als **fortschrittlichste Entwicklungsstufe** des Identitätsmanagements

... für kurzfristigen Relaunch braucht es jedoch (Smart-)eID für hochsichere Identitätsnachweise

Empfehlung für Relaunch mit Kombination aus beiden Ansätzen

Nachweis- und Identitätsmanagement

Nachweis	Identitätsnachweise	Weitere Nachweise
Beschreibung	Gliedert sich in 3 Stufen an Sicherheitsniveaus; bei hoheitlich regeltem Anwendungsfall („hoch“) ist Überprüfung der Verbindung zwischen (juristischer) Person, d.h. Daten des Personalausweises, und anderen Daten notwendig	Nachweise, die über die Daten des Personalausweises hinausgehen, daher per se nicht hoheitlich geregelt und für verschiedene Arten von Anwendungsfällen einsetzbar sind
Nachweisarten	<div><div>Sicherheitsniveau „hoch“, bspw. für Anwendungsfälle wie staatlich hoheitliche Smart-eID</div><div>Sicherheitsniveau „substanziell“, bspw. für Anwendungsfälle wie Hotel Check-in, Online Kontoeröffnung</div><div>Sicherheitsniveau „niedrig“, bspw. für Anwendungsfälle wie Kundenkonto-Registrierung im Online-Shop oder Online Zugänge via</div></div> <div><div> Identifizierung mit Benutzererkennung</div><div> Authentifizierung mit Passwort</div><div>SSI-Ansatz</div><div>Identitätsmanagement</div></div>	<div>Beispiele für weitere Nachweise:</div> <ul style="list-style-type: none">• Geburtsurkunde• Führerschein• Akademische Zeugnisse• Impfnachweis• Elektronische Gesundheitskarte• Konto-, SSI-Ansatz Identitätsinformationen• Versicherungsbescheinigungen• Tickets für Mobilität/Kultur• Mitarbeiter-/Mitgliedsausweis• E-Mail oder Telefonnummer

1. Noch zu validieren, inwiefern eID-Protokoll Open-Source Standards gemäß der eIDAS 2.0 Verordnung entspricht; Hypothese, dass für langfristige europäische Interoperabilität „eIDAS Bridge“ keine Reichweite erzeugt, sodass eID-Protokoll standardisiert werden müsste
2. Lösung für bspw. TKG- und GWG-konformen Ansatz auf Sicherheitsniveau „substanziell“ aus der Wallet heraus erforderlich, die hohe Reichweite gewährleistet und ohne verpflichtende Unterstützung weiterer physischer Faktoren (wie z.B. eID, Fotos, Token etc.) funktioniert; Abhängig von BSI-Einstufung der Basis-ID und Verfügbarkeit von softwarebasierter Smart-eID
3. Gemäß ENISA, [Digital Identity: Leveraging the SSI Concept to Build Trust](#), Januar 2022



Bestandteile einer integrierten Wallet für Relaunch

Um bei **kurzfristigem Relaunch hochsichere Identitätsnachweise** in Wallet zu integrieren, braucht es (Smart-)eID-Protokoll als **derzeit einziges deutsches eIDAS-notifiziertes System**, das Sicherheitsniveau „hoch“ erreicht

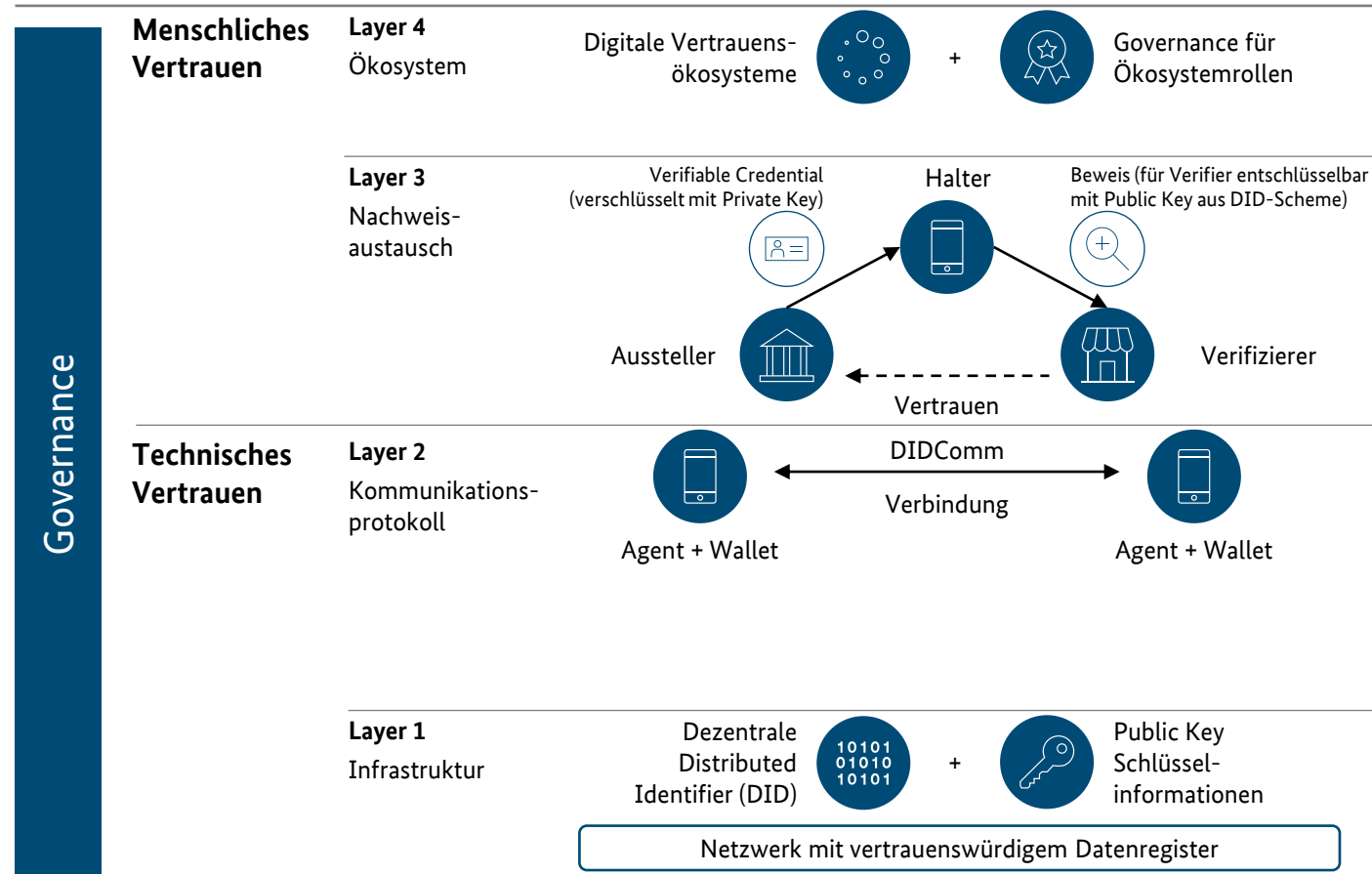
Lösung für bspw. **TKG- und GWG-konformen Ansatz** auf Sicherheitsniveau „substanziell“ **aus der Wallet heraus** erforderlich, die **hohe Reichweite** gewährleistet und ohne verpflichtende Unterstützung weiterer physischer Faktoren (z.B. eID, etc.) funktioniert

Für **Wallet-Konzept** und **Nutzersouveränitätsanforderung** empfehlen wir **SSI-Ansatz**, dessen **genaues Architekturdesign** es nochmal mit BMI, BSI, BfDI, weiteren Behörden und Wirtschaftspartnern **abzustimmen** gilt

Für die Architektur des SSI-Ansatzes im Zielbild und bei Relaunch müssen folgende Architekturdesignfragen beantwortet werden

Kernfragen

Layer der SSI-Architektur



Zu klärende Architekturdesignfragen

- 17 Wie kann die Vertrauenswürdigkeit der Aussteller sichergestellt werden?
- 18 Wie kann die Vertrauenswürdigkeit der Verifizierer sichergestellt werden?
- 19 Wie erzeugen wir die Vererbung von Vertrauen?
- 20 Welche Governance wird im Ökosystem verwendet?
- 12 Welche Wallets werden unterstützt?
- 13 Wie können Identitätsnachweise unterschiedlicher Sicherheitsniveaus aus einer Wallet heraus bereitgestellt werden?
- 14 Welches maximalen Vertrauensniveaus werden über welche Protokolle unterstützt?
- 15 Wie und in welcher Umgebung kann der Nutzer seine Credentials speichern?
- 16 Welche Signaturen werden verwendet?
- 6 Welche DID-Methoden/Protokolle werden unterstützt?
- 7 Welche Kommunikationsstandards für DIDs werden genutzt?
- 8 Wird ein Umschalter für verschiedene Protokolle benötigt?
- 9 Benötigen wir die Unterstützung der Protokolle OIDC und SIOP?
- 10 Welche Protokolle und DID-Methoden entwickeln wir weiter und tragen zu deren Standardisierung bei?
- 11 Welche Art von Verschlüsselung werden für Verifiable Credentials (VCs) und die Transportkommunikation verwendet?
- 1 Welches Netzwerke sind Teil des Ökosystems?
- 2 Wie und wo werden Daten im Netzwerk verarbeitet und gespeichert?
- 3 Benötigt man ein Cloud-Backup mit Restore-Möglichkeit?
- 4 Erfolgt eine Trennung von Storage, Secret-Verwaltung und Agent?
- 5 Werden für die Skalierung Observer-Nodes benötigt?

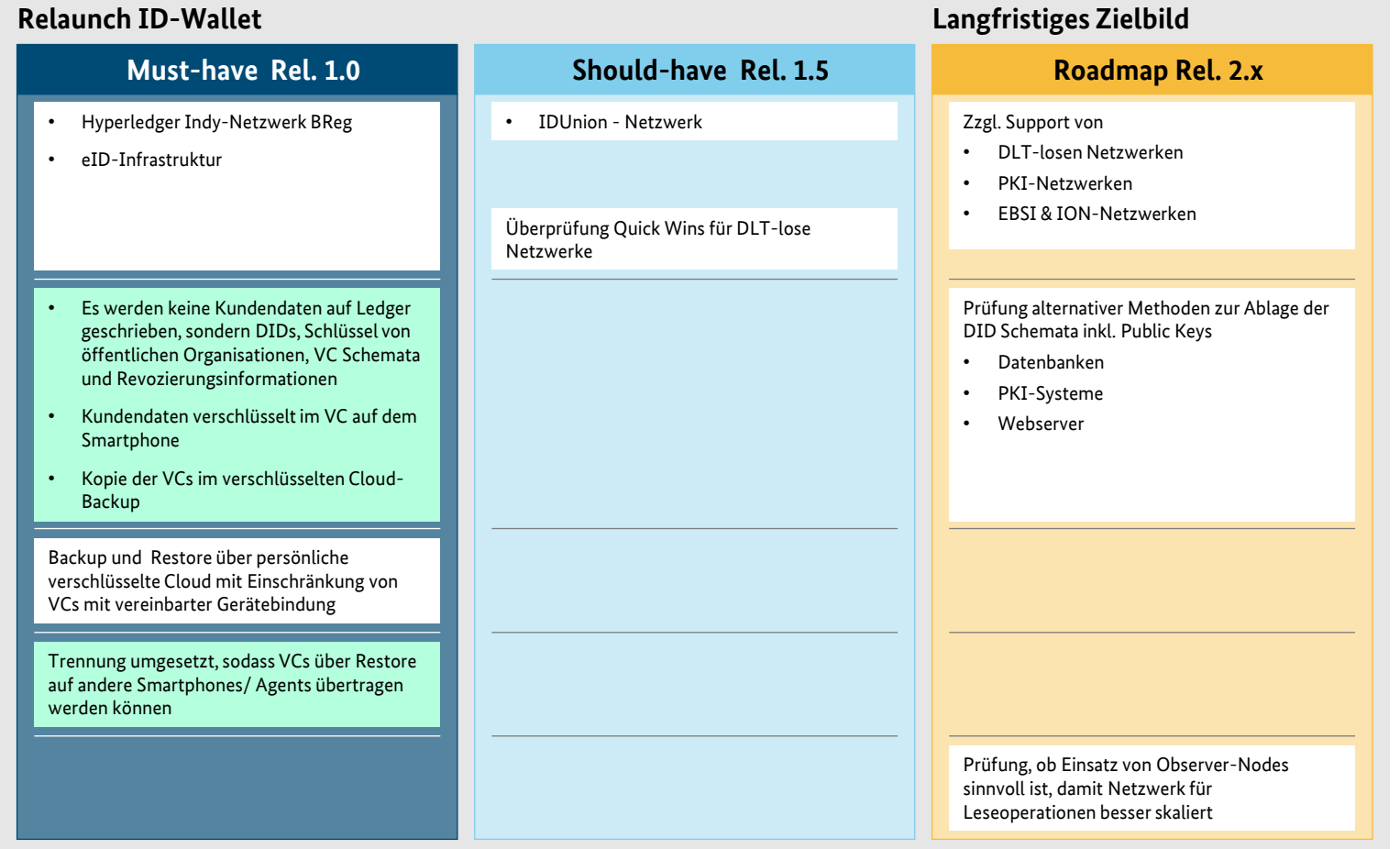
Nach gemeinsamer Definition des Zielbildes empfehlen wir folgendes Phasenmodell ab Relaunch (Layer 1: Infrastruktur*)

DETAILLIERTE BESCHREIBUNG UND BEGRÜNDUNG IM BACKUP

Architekturdesignfrage	Status quo
1 Welches Netzwerke sind Teil des Ökosystems?	Hyperledger Indy-Netzwerk BReg
2 Wie und wo werden Daten im Netzwerk verarbeitet und gespeichert?	<ul style="list-style-type: none"> Es werden keine Kundendaten auf Ledger geschrieben, sondern DIDs, Schlüssel von öffentlichen Organisationen, VC Schemata und Revozierungsinformationen Kundendaten verschlüsselt im VC auf dem Smartphone Kopie der VCs im verschlüsselten Cloud-Backup
3 Benötigt man ein Cloud-Backup mit Restore-Möglichkeit?	Cloud-Backup in ID Wallet funktionierte, wurde für Go-Live deaktiviert
4 Erfolgt eine Trennung von Storage, Secret-Verwaltung und Agent?	Trennung umgesetzt, sodass VCs über Restore auf andere Smartphones/Agents übertragen werden können
5 Werden für die Skalierung Observer-Nodes benötigt?	Bisher keine Observer-Nodes im Einsatz

Zusätzliche Feature/zunehmender Implementierungsaufwand →

■ Kernfragen ■ Bereits umgesetzt



* Keine 1:1 Zuordnung zu den Layern , Mehrfachzuordnung zu den Layern möglich

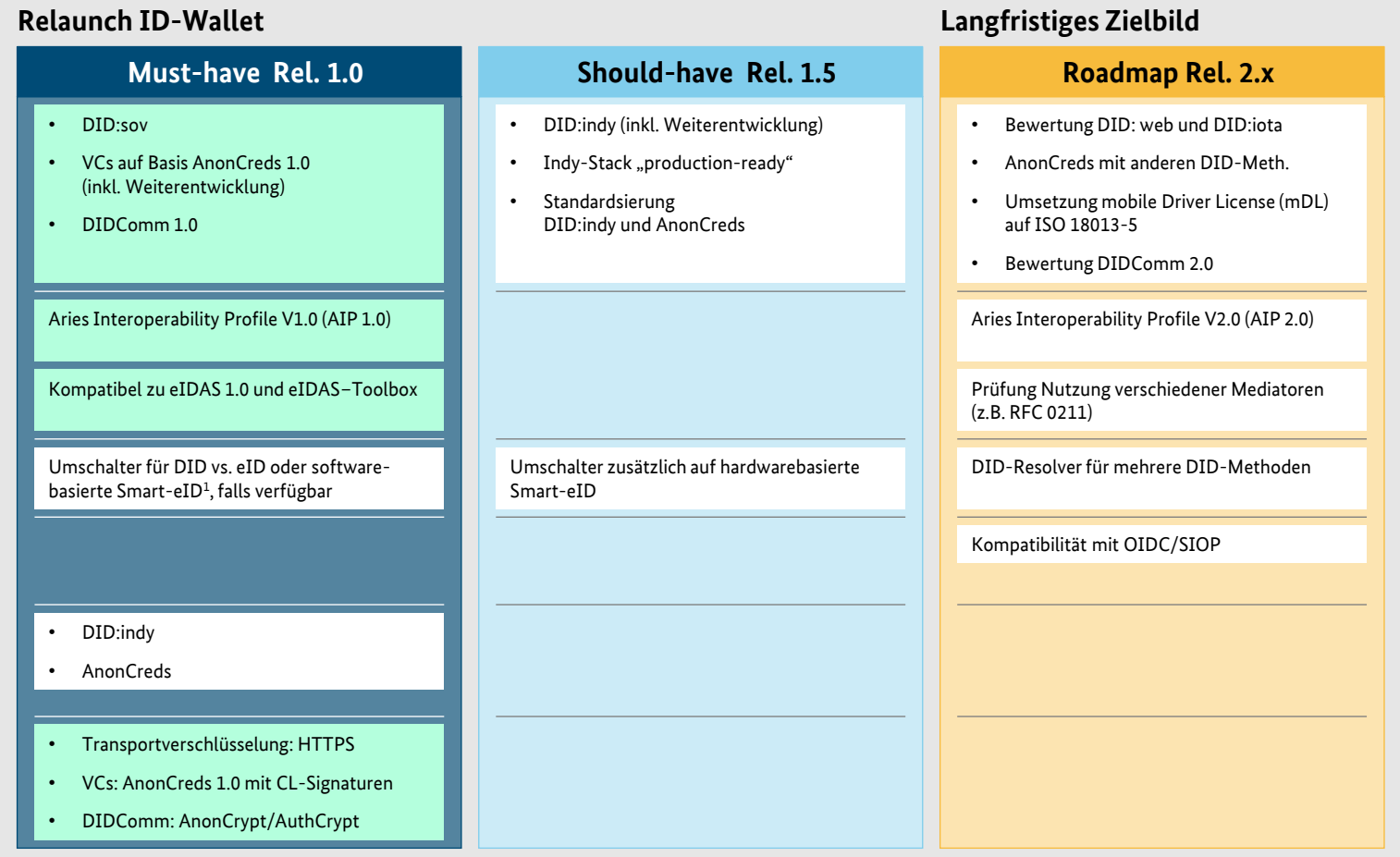
Nach gemeinsamer Definition des Zielbildes empfehlen wir folgendes Phasenmodell ab Relaunch (Layer 2: Kommunikationsprotokoll*)

DETAILIERTE BESCHREIBUNG UND BEGRÜNDUNG IM BACKUP

Architekturdesignfrage	Status quo
6 Welche DID-Methoden/Protokolle werden unterstützt?	<ul style="list-style-type: none"> DID:sov VCs auf Basis AnonCreds 1.0 DIDComm 1.0
7 Welche Kommunikationsstandards für DIDs werden genutzt?	<ul style="list-style-type: none"> Aries Interoperability Profile V1.0 (AIP 1.0) Kompatibel zu eIDAS 1.0 und eIDAS – Toolbox
8 Wird ein Umschalter für verschiedene Protokolle benötigt?	Aktuell nur DID:sov, daher kein Umschalter implementiert
9 Benötigen wir die Unterstützung der Protokolle OIDC und SIOP?	Nicht implementiert
10 Welche Protokolle und DID-Methoden entwickeln wir weiter und tragen zu deren Standardisierung bei?	Standardisierung gestartet für <ul style="list-style-type: none"> DID:indy AnonCreds
11 Welche Art von Verschlüsselung werden für VCs und die Transportkommunikation verwendet?	<ul style="list-style-type: none"> Transportverschlüsselung: HTTPS VCs: AnonCreds 1.0 mit CL-Signaturen DIDComm: AnonCrypt/AuthCrypt

Zusätzliche Feature/zunehmender Implementierungsaufwand →

■ Kernfragen ■ Bereits umgesetzt



1. Abhängig von BSI-Einstufung der Basis-ID und Verfügbarkeit von softwarebasierter Smart-eID

* Keine 1:1 Zuordnung zu den Layern, Mehrfachzuordnung zu den Layern möglich

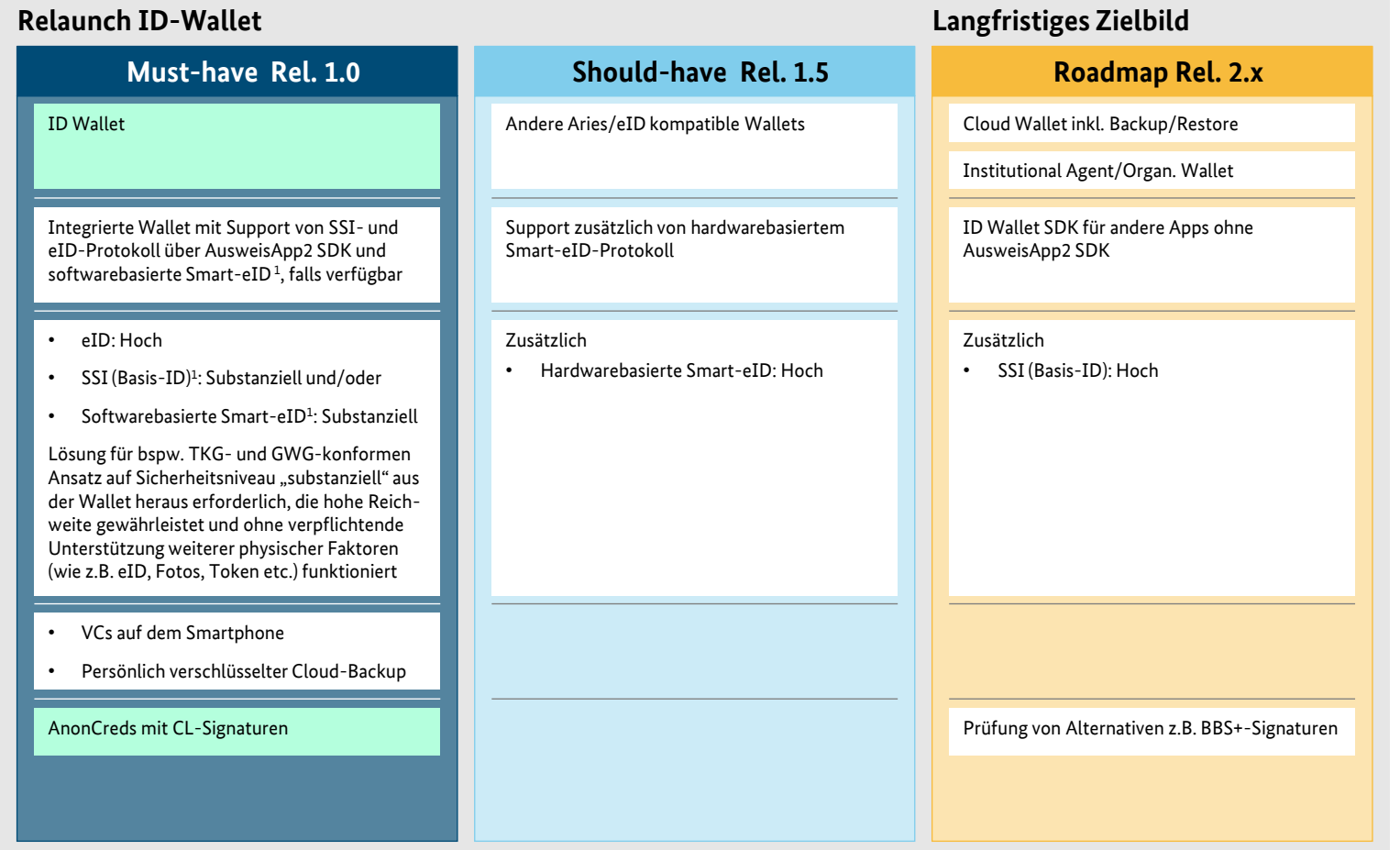
Nach gemeinsamer Definition des Zielbildes empfehlen wir folgendes Phasenmodell ab Relaunch (Layer 3: Nachweisaustausch*)

DETAILLIERTE BESCHREIBUNG UND BEGRÜNDUNG IM BACKUP

Architekturdesignfrage	Status quo
12 Welche Wallets werden unterstützt?	ID Wallet
13 Wie können Identitätsnachweise unterschiedlicher Sicherheitsniveaus aus einer Wallet bereitgestellt werden?	Nur SSI-Protokoll
14 Welches maximalen Vertrauensniveaus werden über welche Protokolle unterstützt?	Nur SSI (Basis-ID): Niedrig
15 Wie und in welcher Umgebung kann der Nutzer seine Credentials speichern?	VCs nur auf dem Smartphone
16 Welche Signaturen werden verwendet?	AnonCreds mit CL-Signaturen

Zusätzliche Feature/zunehmender Implementierungsaufwand →

■ Kernfragen ■ Bereits umgesetzt



1. Abhängig von BSI-Einstufung der Basis-ID und Verfügbarkeit von softwarebasierter Smart-eID

* Keine 1:1 Zuordnung zu den Layern, Mehrfachzuordnung zu den Layern möglich

Nach gemeinsamer Definition des Zielbildes empfehlen wir folgendes Phasenmodell ab Relaunch (Layer 4: Ökosystem*)

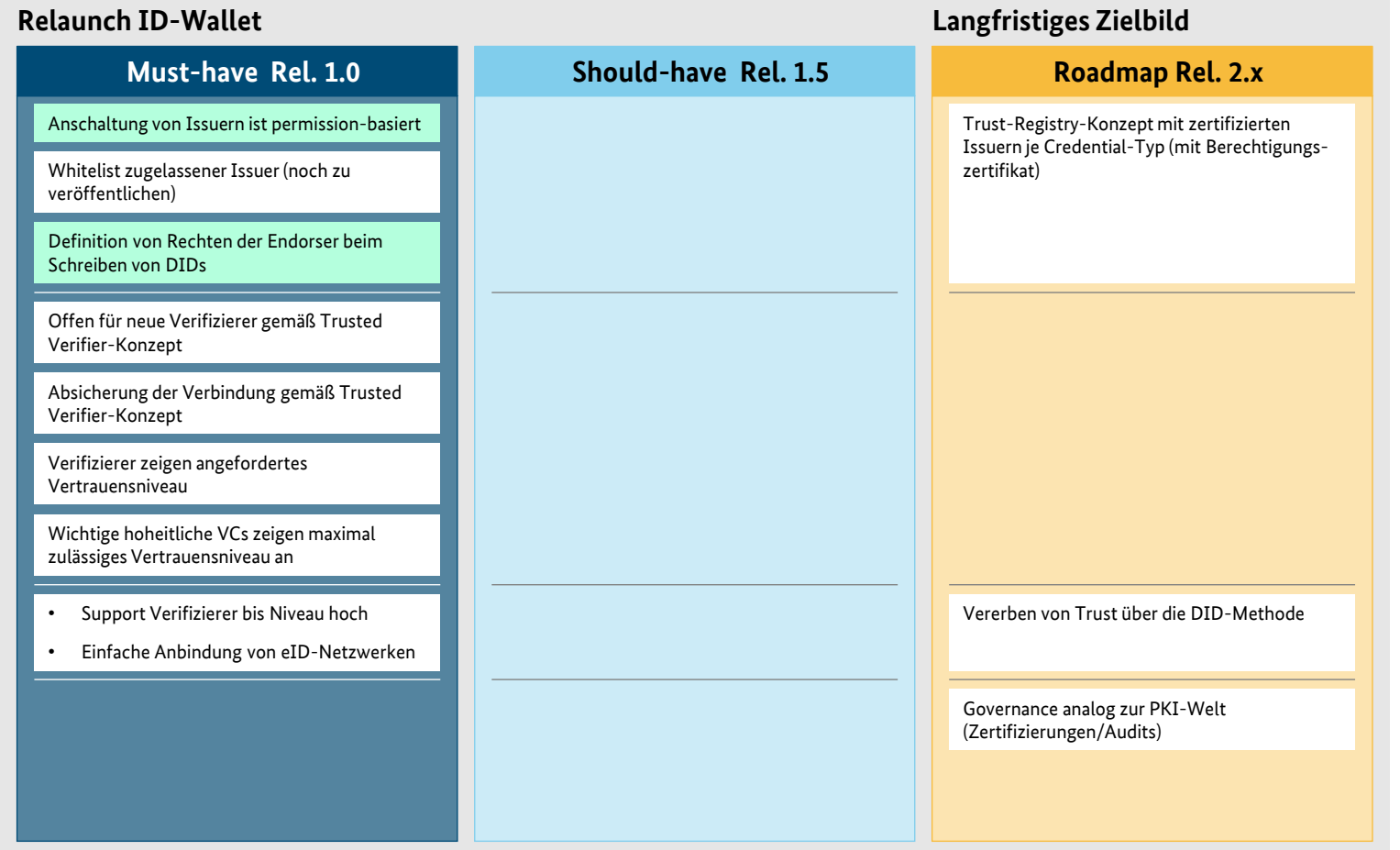
DETAILLIERTE BESCHREIBUNG UND BEGRÜNDUNG IM BACKUP

Architekturdesignfrage	Status quo
17 Wie kann die Vertrauenswürdigkeit der Aussteller sichergestellt werden?	Permission-basierte Zulassung von Issuern gemäß Governance-Vereinbarung/Whitelist zugelassener Issuer und deren Credentials (intern existent, aber noch nicht veröffentlicht)
18 Wie kann die Vertrauenswürdigkeit der Verifizierer sichergestellt werden?	Anzeige der HTTPS-URL des Verifizierers gegenüber dem Halter/Nutzer
19 Wie erzeugen wir die Vererbung von Vertrauen?	N/A
20 Welche Governance wird im Ökosystem verwendet?	N/A

Randbedingung: Agents und Protokolle müssen zum Launch performant sein!

Zusätzliche Feature/zunehmender Implementierungsaufwand

■ Kernfragen ■ Bereits umgesetzt



* Keine 1:1 Zuordnung zu den Layern , Mehrfachzuordnung zu den Layern möglich

Ausgewählte Prio-Themen Rel. 1.0 für Einstieg in die Umsetzungsdiskussion



Priorisierte Themen für die Umsetzungsdiskussion

Integration eID / SSI im Wallet und im Netzwerk

Nutzung Ausweis-App / Smart eID mit und ohne App /
SDK-only

Abbildung Backup / Restore –Funktion

Zusammenspiel ID-Wallet Deutschland mit EU-ID-Wallet
Ausschreibung

Governance Rahmen (für Abbildung Trust Level,
zugelassene Issuer und Trusted Verifier-Konzept und
Security wichtig)

Zur Abstimmung der Relaunch-Empfehlungen und langfristigem Architekturzielbild schlagen wir einen partizipativen Prozess vor

VORSCHLAG DER WIRTSCHAFTSUNTERNEHMEN – ZUR DISKUSSION

■ Abgeschlossene Prozessphase

Partizipativer Prozess zur Definition von SSI-Architekturdesign

Einbindung von Experten der Wirtschaftspartner

Ziel: Erarbeitung von langfristigem Zielbild und Relaunch-Empfehlung nach Vornehmen initialer Expertenbewertungen



Einsammeln von Rückmeldungen/Feedback nach Architekturzirkel

Ziel: Sicherstellung gemeinsamer Projektsicht auf Zielbild und Relaunch-Empfehlungen durch Rückmeldungen bis Freitag, 25. Februar 2022



Bilden von Expertengremien mit BMI, BSI, BfDI, weiteren Behörden und Wirtschaftspartnern

Ziel: Validierung der Zielbild- und Relaunchkomponenten sowie Expertenbewertungen unter Einbeziehung der Wirtschaftspartner



Architekturentscheidung für Relaunch und langfristiges Zielbild

Ziel: Zusammenführung aller Experteneinschätzungen, Synthese und Validierung der Empfehlungen mit gemeinsamer Empfehlung



Behördenübergreifende Konsensfindung zu SSI-Architekturdesign unter Einbindung der Expertise der Wirtschaftspartner wird als Voraussetzung für Relaunch gesehen – genaue Packetierung für Umsetzung muss nach Aufwandsschätzungen gemeinsam definiert werden