gematik
Nationale Agentur für Digitale Medizin

ID-Management in der Telematikinfrastruktur (TI) im Wandel

Von der Smartcard zur Smartphone-App

| Tim Ohlendorf, Karsten Kochan | OMNISECURE 2024 | 23.01.24 | öffentlich |

Sicherheit im Produktteam Identity Management

Tim Ohlendorf

IT Security Specialist

Security Engineering & Architectures

IAM, Zero Trust, Healthcare Confidential Computing

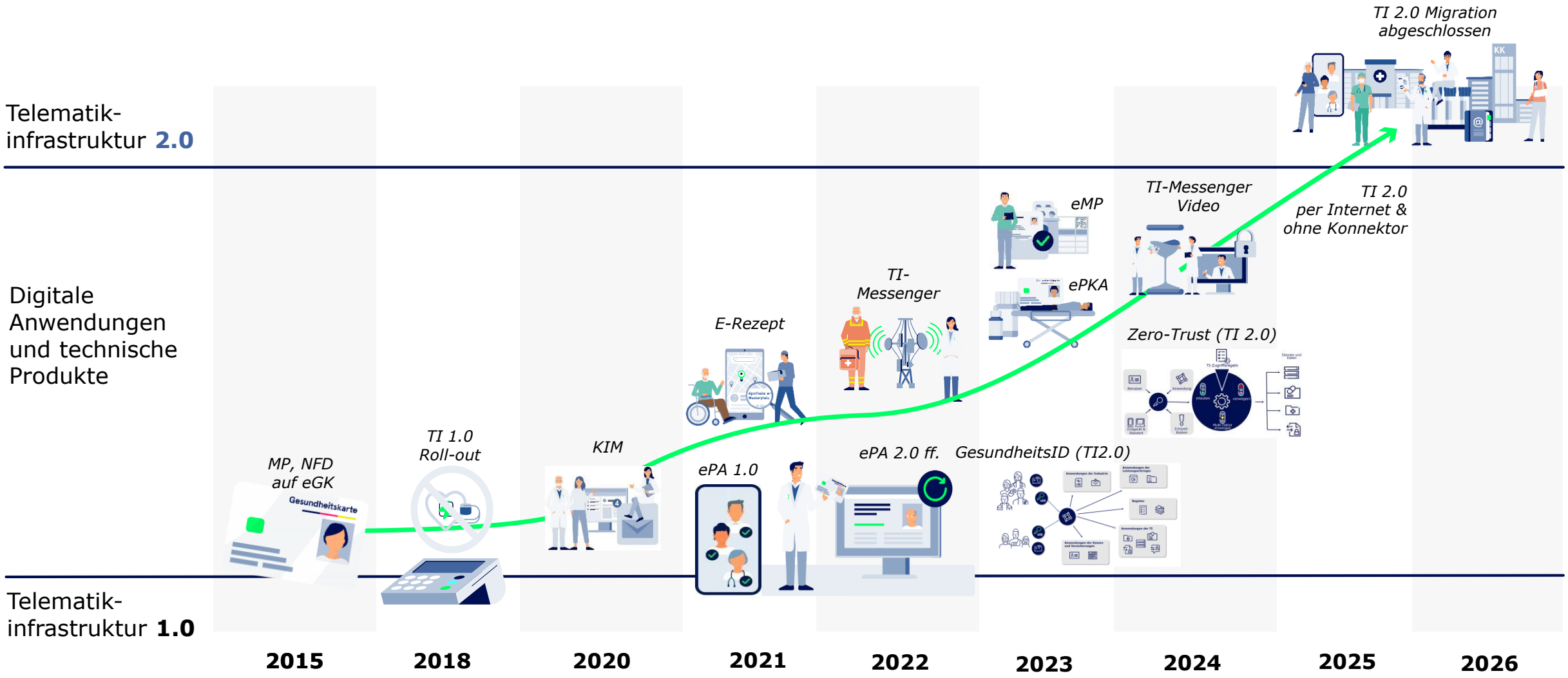
Karsten Kochan

IT Security Specialist

Security Engineering & Architectures

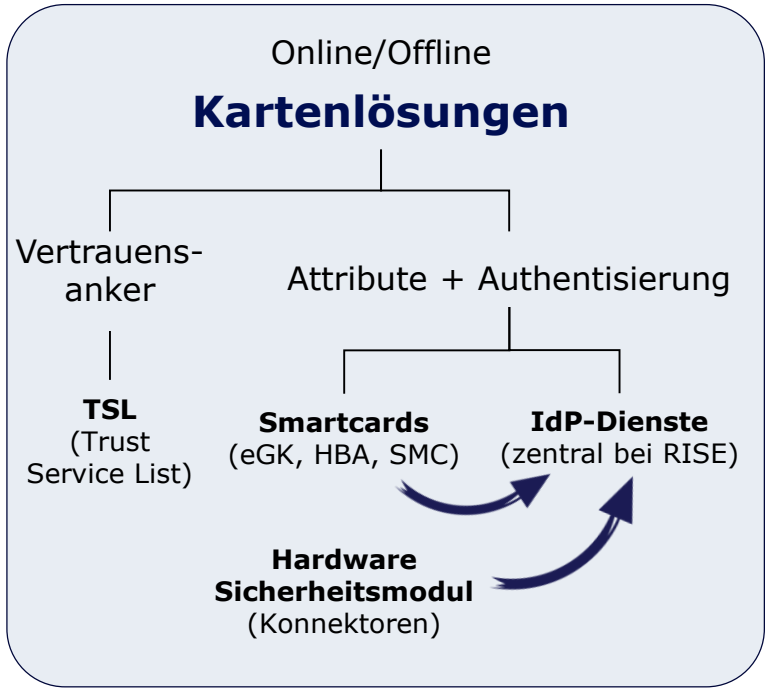
Vertrauensdienste, Regulatorik

Digitalisierung gewinnt deutlich an Schwung
Unser Ziel ist eine bessere Versorgung in Deutschland



Evolution des Identitätsmanagements in der TI

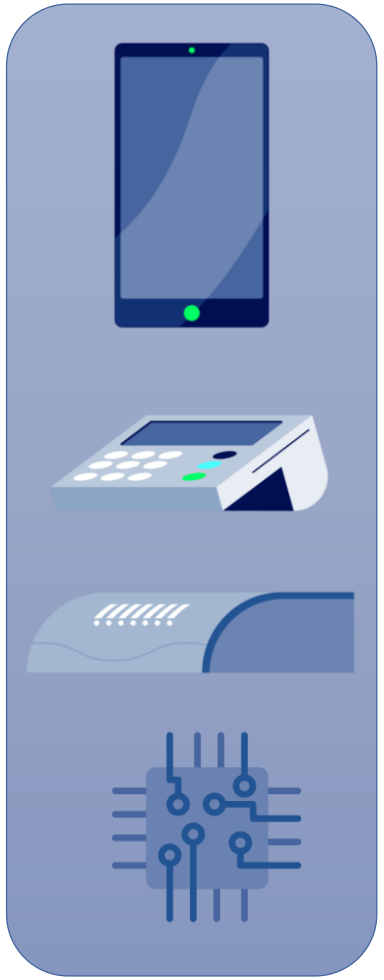
Bisher – PKI-basiert, X.509 Zertifikate, Smartcards



- Gesetzliche Versicherte

- Ärzte
- Apotheker
- Pflegekräfte

- Medizinisches Fachpersonal
- Institutionen
- Weitere Berufsgruppen



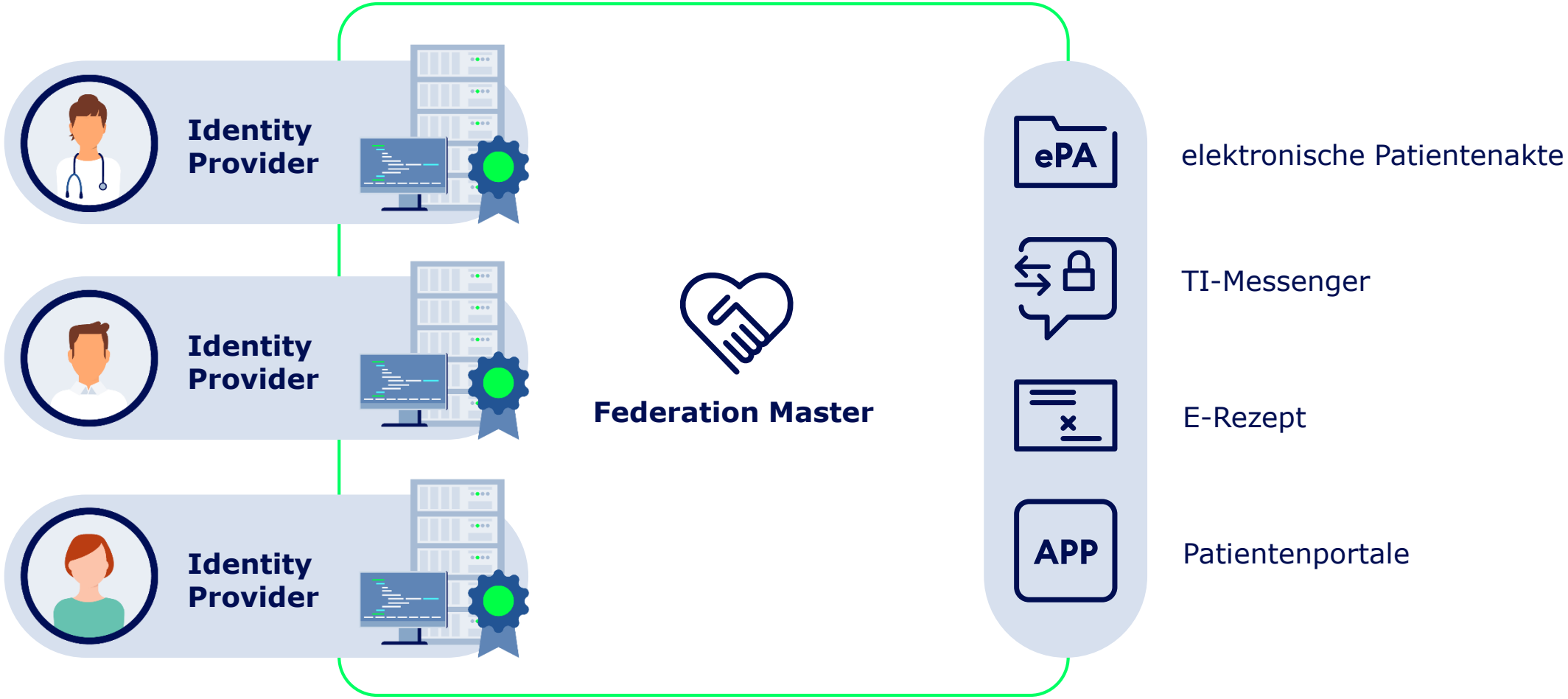
*weiter (Karten)-Identitäten: SMC-B ORG, SM-B ORG, SMC-B KTR, SM-B KTR, gSMC-KT

Einführung der digitalen Identitäten

Das Stufenmodell bis 2026

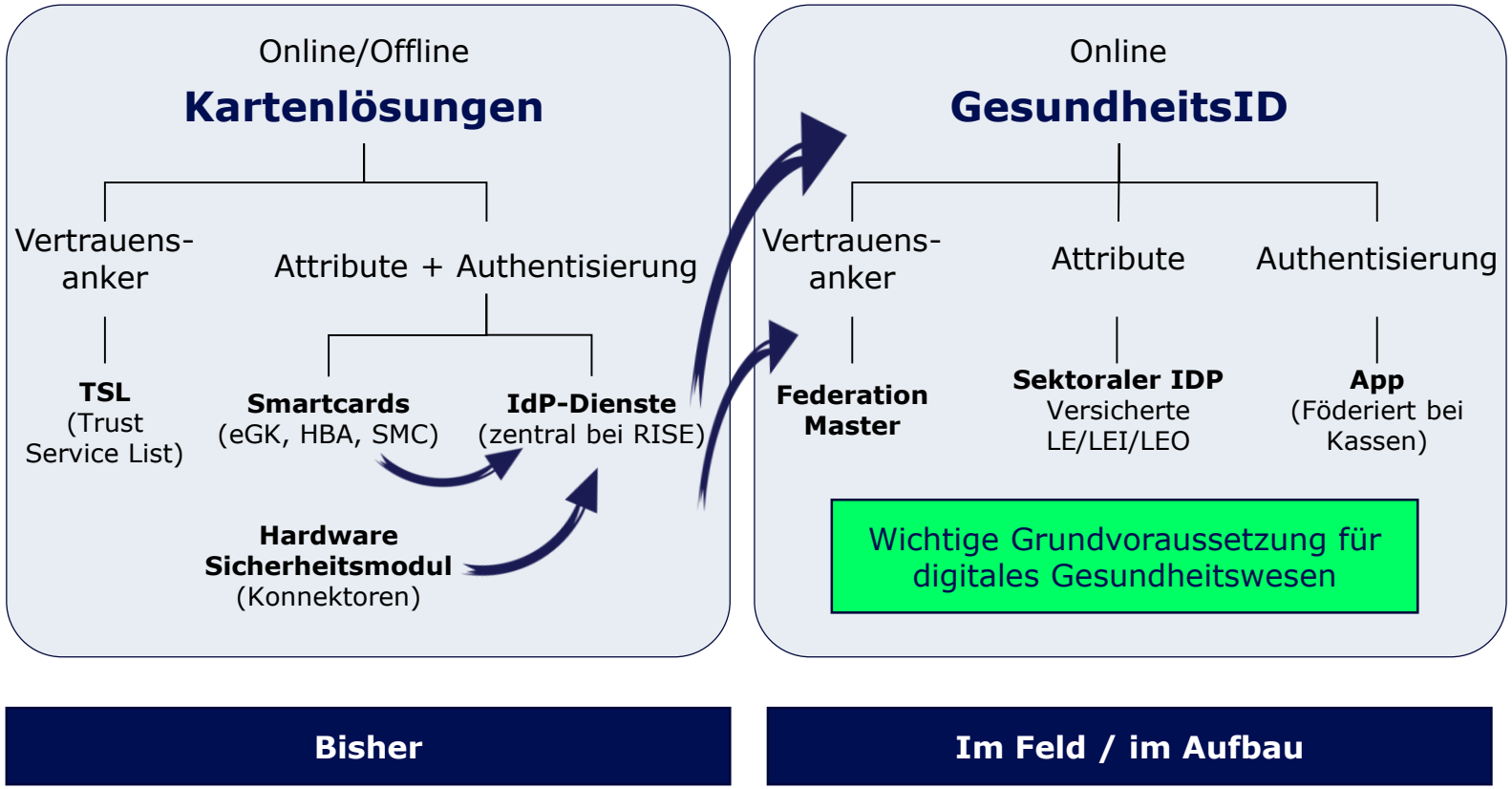
Föderiertes Identitätsmanagement der TI 2.0

Sektoren treten als Identitätsgeber auf



Evolution des Identitätsmanagements in der TI

Jetzt – IdP Föderation, OpenID Connect-basiert



GesundheitsID – Kartenloser Zugang im Gesundheitswesen

- 3 Anbieter sind für die GesundheitsID zugelassen: T-Systems, RISE, IBM
- Gesetzliche Krankenkassen termingerecht seit Ende 2023 mit der GesundheitsID produktiv
- Inkrafttreten DigiG (vls. Q2 2024): Grundlage für Erweiterung um Akzeptanzfeatures
- 3 Monate nach DigiG (vls. Q3 2024): Verfügbarkeit der Akzeptanzfeatures:
  - Verzicht auf regelmäßige kartenbasierte Authentisierung
  - Biometrische Authentisierungsverfahren

Regulatorische Ausprägungen der GesundheitsID

normativ

gematik-ehealth-loa-high:

- angelehnt an BSI TR-03107-1 hoch / ISO 18045 high attack potential
- Abweichungen:
  - Haben-Faktor auch in SW, TEE, unzertifizierter TRH möglich, dann aber Laufzeitbegrenzung
  - Wissen-Faktor darf auch System-PIN sein
- bestehende Zertifizierungen / Notifizierungen dürfen potentiell nachgenutzt werden

Ausblick

niederschwellige Authentisierung (gematik-ehealth-loa-substantial):

- nach Einwilligung, nur für Versicherte
- angelehnt an BSI TR-03107-1 substantiell
- Abweichungen:
  - Haben-Faktor: Nachnutzung gängiger Industriezertifizierungen
  - Biometrie als 2. Faktor, SSO erlaubt

Zulässige Identifizierungs- und Authentisierungsverfahren

Kompromisslose Identifizierung – komfortable Authentisierung

Identifizierungsverfahren

- **Online-Ausweisfunktion**
- **eGK + PIN**
- **Vor-Ort-Verfahren:**
  - POSTIDENT Filiale
  - Identifizierung in der Geschäftsstelle
  - WIP: Apotheken-Ident

Authentisierungsverfahren

- **Online-Ausweisfunktion**
- **eGK + PIN**
- **Gerätebindung** (+ zweiter Faktor)
  - App-PIN oder System-PIN
  - Aktuell keine Biometrie!

Weitere ausgewählte technische Aspekte

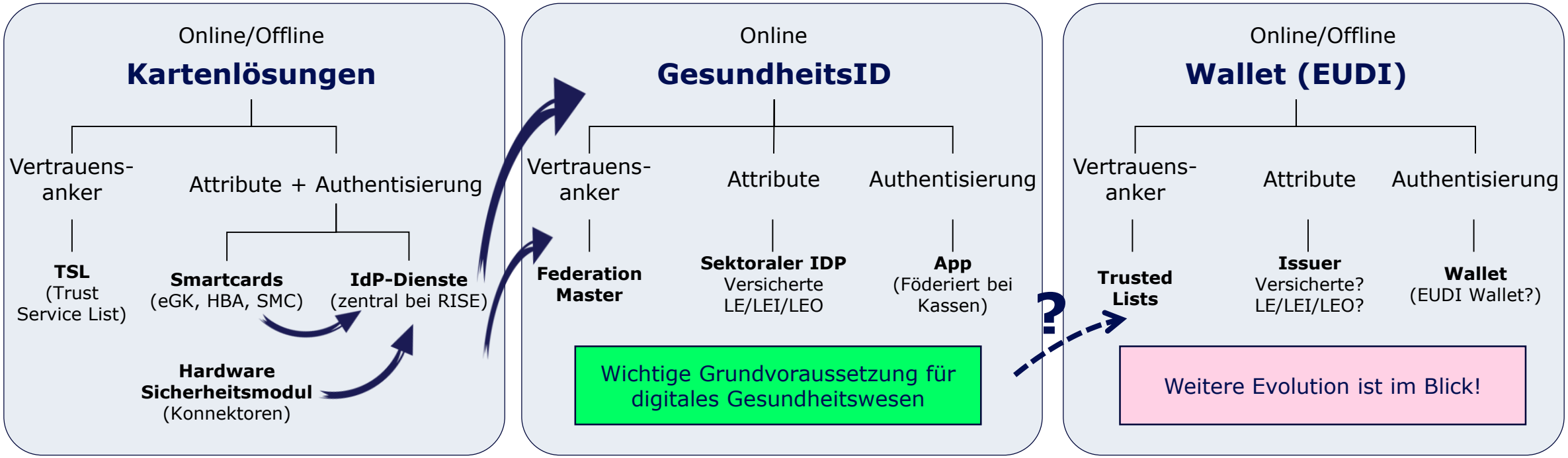
Key Attestation für Nachweis der Gerätebindung
- kryptographischen Nachweis und serverseitige Prüfung
- über Android Key & ID Attestation oder Apple App Attest API

IdP Betreiberausschluss mittels **Vertrauenswürdiger Ausführungsumgebung (VAU)** um
- Omnipotenz innerhalb der Föderation und
- Profilbildung über die Versicherten zu verhindern.

Certificate Transparency Monitoring
- sowohl durch IdP als auch durch Federation Master
- Detektion von falsch ausgestellten oder gefälschten IDP-TLS-Zertifikaten

Evolution des Identitätsmanagements in der TI

Wallets am Horizont



Q&A

gematik.
Gesunde Aussichten.

Kontakt

Tim Ohlendorf
mobile +49 160 3664 702
tel +49 30 40041-541
e-mail tim.ohlendorf@gematik.de

Backup Folien

Systemkontext – sektoraler IdP

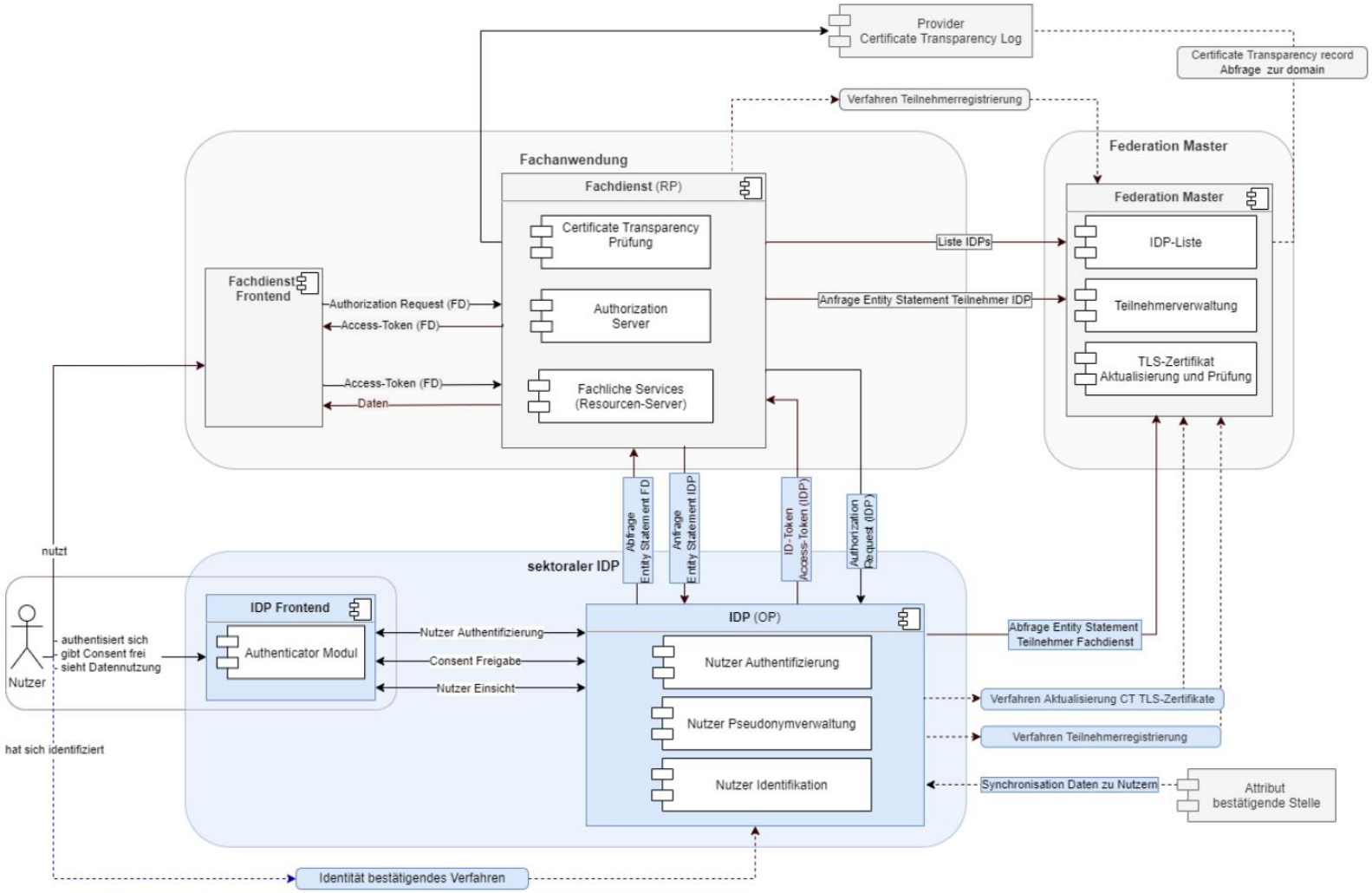


Abbildung 2: Systemkontext

Gerätebindung – gematik-ehealth-loa-high

Gerätenutzung	Authentisierung
ohne Hardware Keystore	Die Gerätebindung kann a) durch Identifikation, welche dem Niveau "gematik-ehealth-loa-high" entspricht oder b) mit einer 2FA, welche dem Niveau "gematik-ehealth-loa-high" entspricht, angelegt werden. Die Gerätebindung kann für 24 Stunden zusammen mit einem Faktor aus den Bereichen Wissen oder Inhärenz auf dem Niveau "gematik-ehealth-loa-high" genutzt werden.

Gerätenutzung	Authentisierung
mit Hardware Keystore	Die Gerätebindung kann a) durch Identifikation, welche dem Niveau "gematik-ehealth-loa-high" entspricht oder b) mit einer 2FA, welche dem Niveau "gematik-ehealth-loa-high" entspricht, angelegt werden. Die Gerätebindung kann für 6 Monate zusammen mit einem Faktor aus den Bereichen Wissen oder Inhärenz auf dem Niveau "gematik-ehealth-loa-high" genutzt werden.
mit zertifiziertem Secure Element	Die Gerätebindung kann a) durch Identifikation, welche dem Niveau "gematik-ehealth-loa-high" entspricht oder b) mit einer 2FA, welche dem Niveau "gematik-ehealth-loa-high" entspricht, angelegt werden. Die Gerätebindung kann unbegrenzt zusammen mit einem Faktor aus den Bereichen Wissen oder Inhärenz auf dem Niveau "gematik-ehealth-loa-high" genutzt werden.

Regulatorische Anforderungen an die GesundheitsID

Jurisdiktion	Richtlinien & Standards		
EU	eIDAS Regulation (on electronic identification and trust services)	eIDAS 2.0 (Toolbox, ARF, …)	
National	BSI TR-03147 (Vertrauensniveaubewertung von Verfahren zur Identitätsprüfung natürlicher Personen)	BSI TR-03107-1 (Elektronische Identitäten und Vertrauensdienste im E-Government Teil 1) BSI TR-03166 (Biometric Authentication Components in Devices for Authentication)	ISO / IEC 18045 (Methodology for IT security evaluation) BSI TR-03161 (Anforderungen an Anwendungen im Gesundheitswesen)
Telematik-infrastruktur	gemSpec_IDP_Sek (sektoraler Identity Provider) OpenID Connect Core 1.0	gemSpec_Krypt (Übergreifende Spezifikation Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur) OpenID Connect Federation 1.0 (Draft 21)	