

Aktueller Stand der GesundheitsID

Versicherte – Leistungserbringer – LEI

gematik | 14.03.23

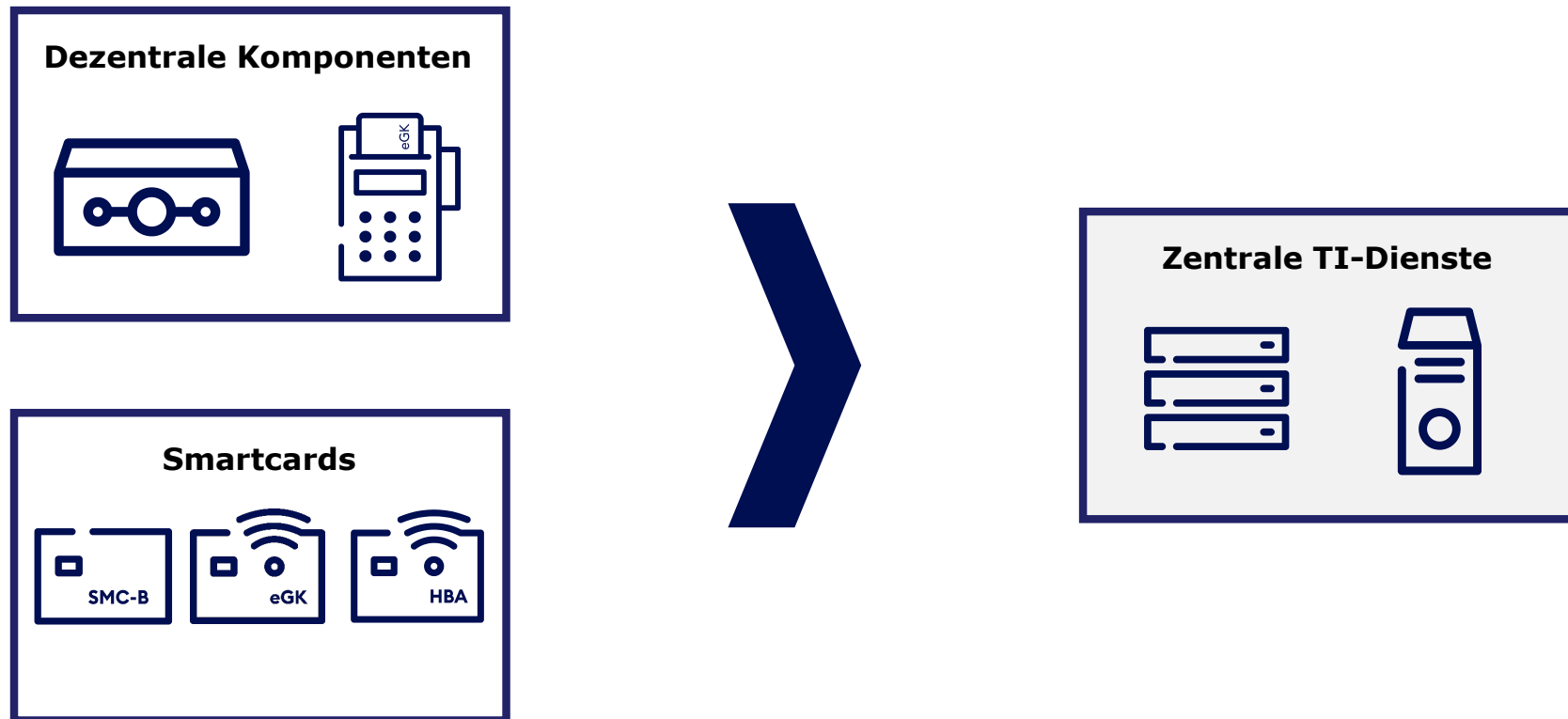
Agenda

1. Ausgangslage und Limitationen der TI 1.0
2. Digitale Identitäten als Wegbereiter der TI 2.0
3. Nutzergruppen der GesundheitsID
4. Stufenmodell der Einführung
5. Blickwinkel „Versicherter“
 1. Zielstellung
 2. Aktuelle Herausforderungen
6. Blickwinkel „Leistungserbringer“ und „Institutionen“
7. Status und Zeitschiene
8. Ausblick eIDAS 2.0 und EUdi Wallet



Ausgangslage TI 1.0

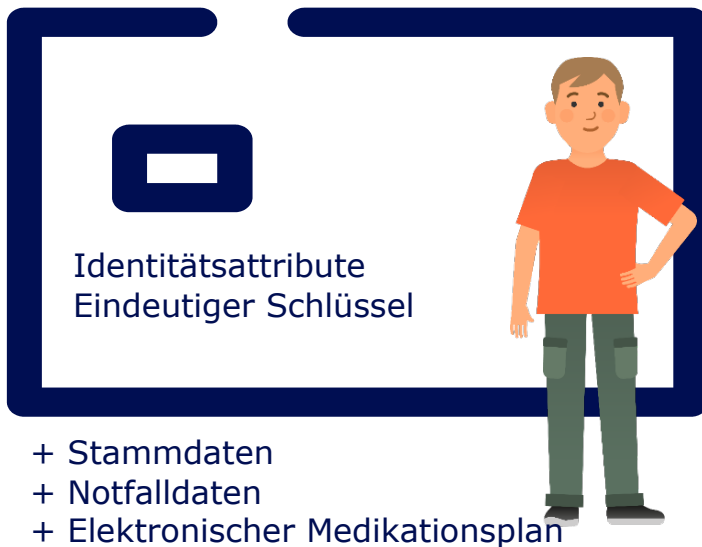
Zugangshürden durch dezentrale Komponenten und Smartcards



Zielstellung

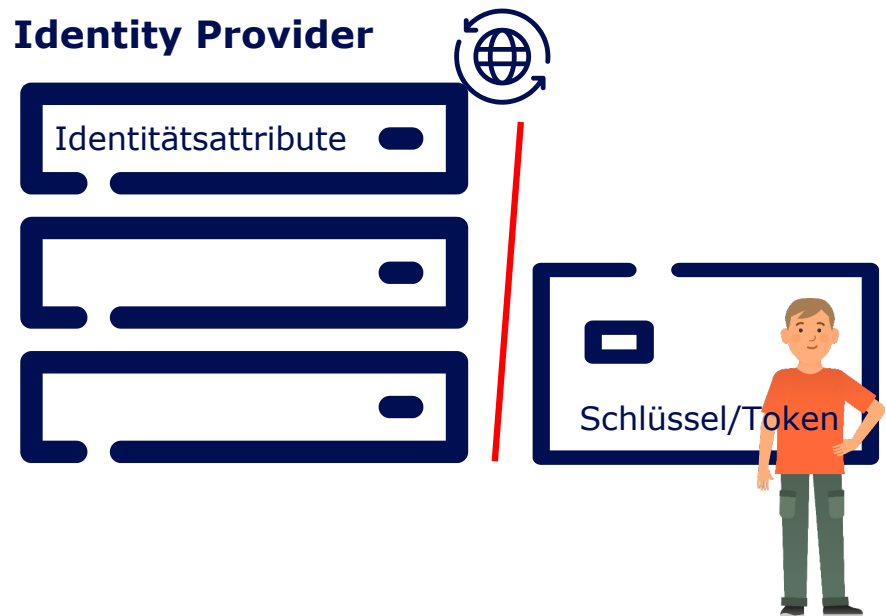
Alternative zu kartengebundenen Identitäten

Kartengebundene Identität



Daten von der Karte in
universell erreichbare
Datenbank

Identity Provider



Schlechte Usability in mobilen Szenarien

Aufwändiger **Herausgabeprozess**

Statische Attribute → Änderung oder
Erweiterung aufwändig

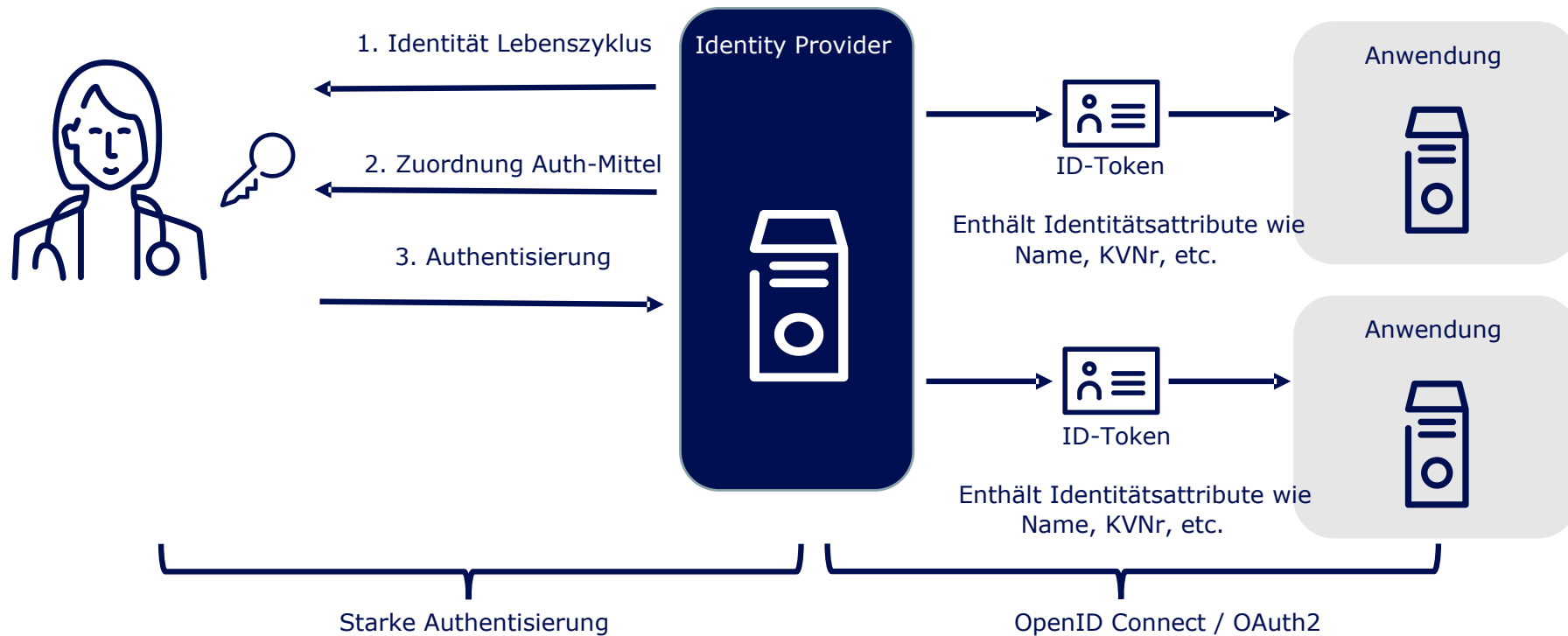
Selektive Nutzung von Identitätsattributen

Flexible Authentisierungsmittel und -verfahren
(**Authentisierung as a Service**)

Dynamisch erweiterbare Attribute

Funktionsweise eines Identity Providers

Authentisierung gegenüber einem Identity Provider



Der Identity Provider übernimmt die sicheren Identifizierungs- und Authentisierungsprozesse, sodass Anwendungen diese nicht implementieren müssen und sich auf Ihre Kernfunktionalitäten konzentrieren können. Die Anwendung delegiert den Nutzer zur Anmeldung an eine App (Regelfall) des Identity Providers und bekommt nach erfolgreicher Authentisierung des Nutzers lediglich einen ID-Token mit den benötigten Informationen des Versicherten.

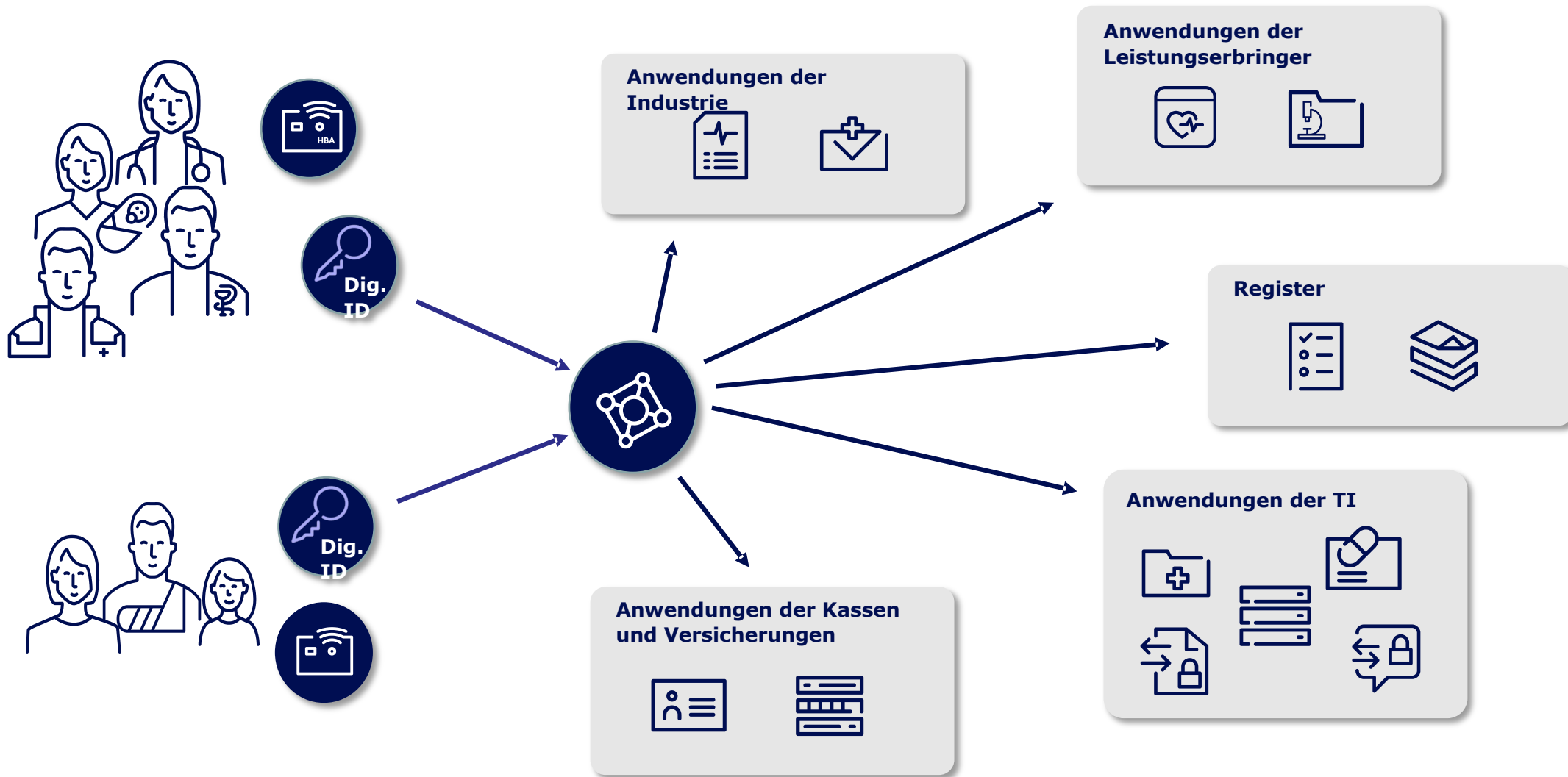
Nutzer- und Rollengruppen der digitalen Identitäten

eGK, eHBA und SMC-B bekommen eine kartenunabhängige Alternative



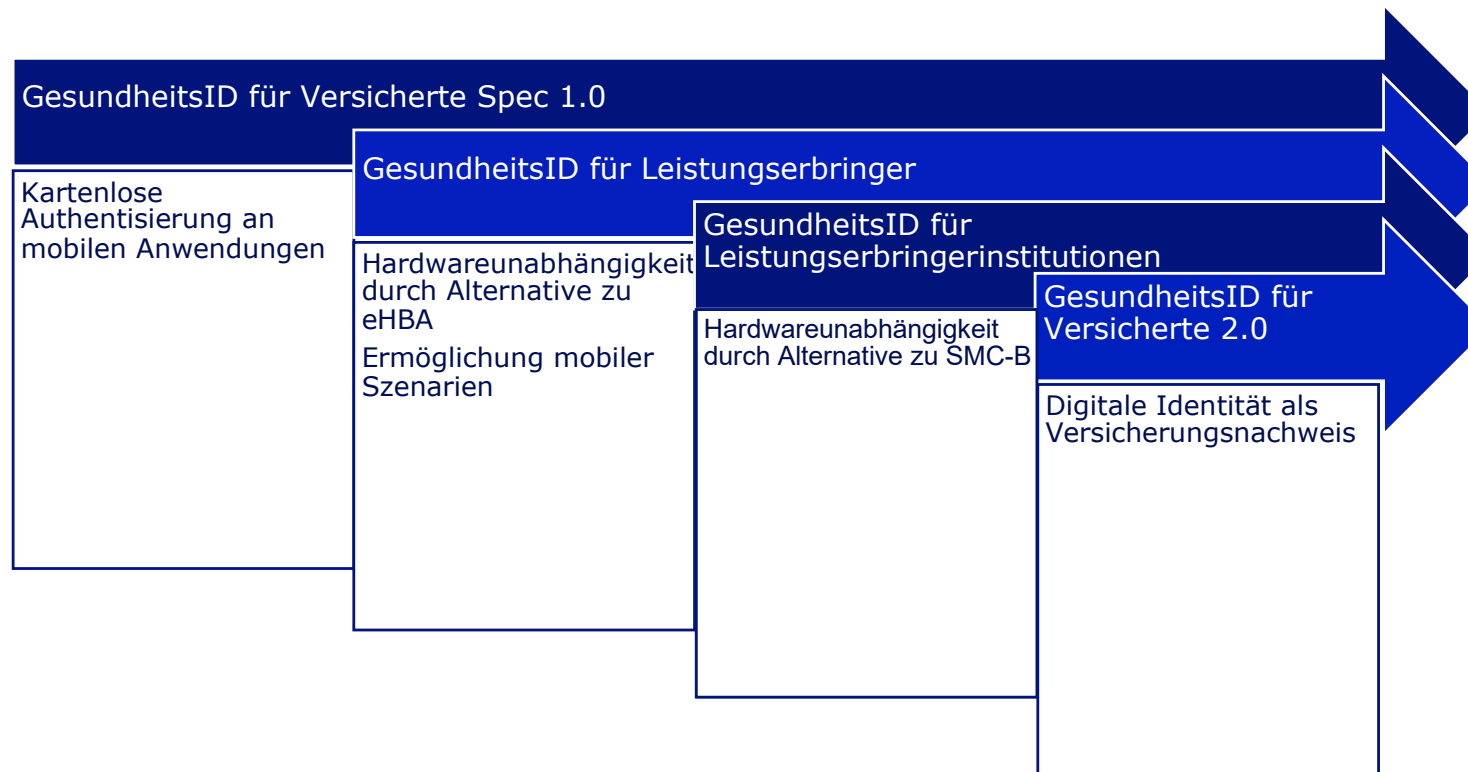
Föderiertes Identitätsmanagement

Die erste Säule der TI 2.0



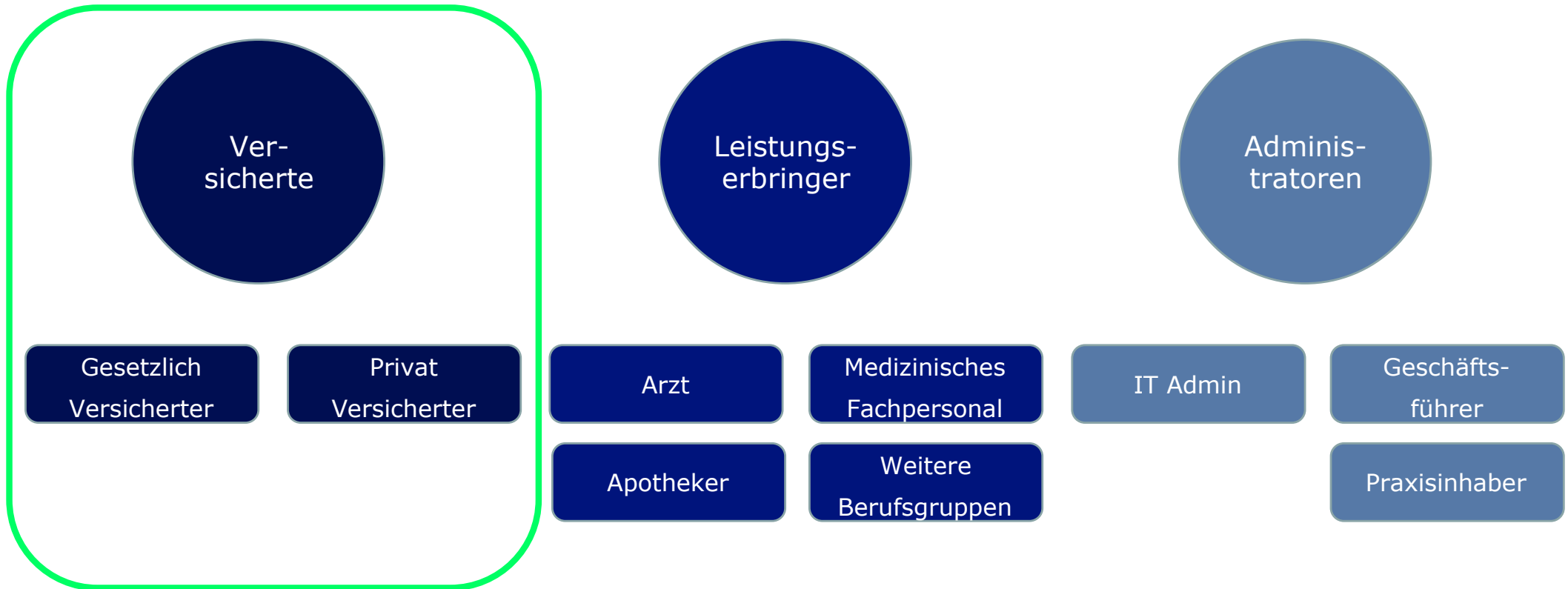
Stufenmodell bei der Einführung digitale Identitäten

Digitale Identitäten für LE und LEI folgen denen der Versicherten



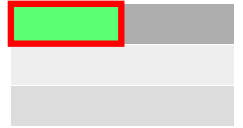
Nutzer- und Rollengruppen der digitalen Identitäten

eGK, eHBA und SMC-B bekommen eine kartenunabhängige Alternative



Elektronische Identitäten

Stufe 1: Authentisierung an (mobilen) Anwendungen



Zugang zu

ePA



E-Rezept



TI-Messenger



Patientenportale



Kasseneigene
Anwendungen



Medizinische
Einrichtungen



Nutzen

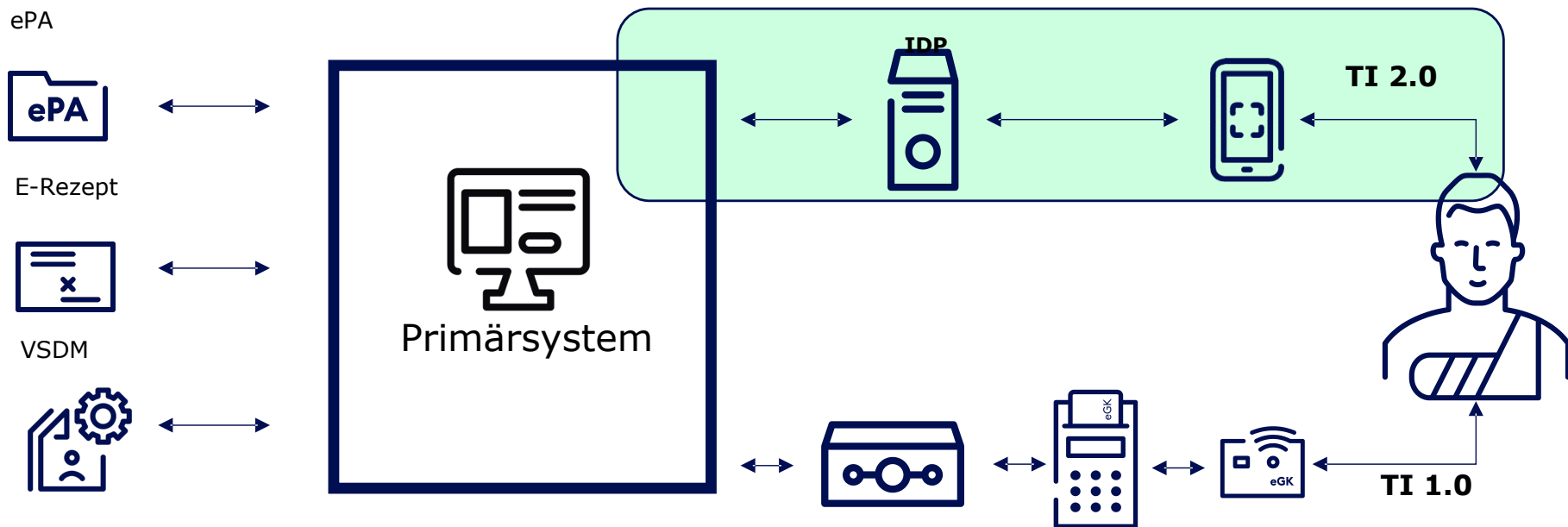
- Komfortabler und niederschwelliger Login mit dem Smartphone an mobilen Anwendungen
- Einmaliger Registrierungsprozess für Nutzende
- Anwendungen müssen die (komplexen) Anmeldeprozesse nicht selbst implementieren

Eckpunkte

- Krankenversicherungen stellen digitale Identitäten für ihren Sektor nach OpenID Connect bereit
- eGK weiterhin als Authentisierungsmittel nutzbar, digitale Identität als Ergänzung
- Größte Herausforderung ist Einvernehmen mit BSI und BfDI zu nutzerfreundlichen Authentisierungsmethoden
- Ab 2024 verpflichtend anzubieten ab 2026 Versicherungsnachweis

Digitale Identität als Alternative zu eGK

Stufe 2: GesundheitsID als alternativer Versicherungsnachweis <



Fachanwendung

Infrastruktur

Zulässige Identifizierungs- und Authentisierungsverfahren

Zielvorgabe: Vertrauensniveau „hoch“ muss erreicht werden

Identifizierungsverfahren

- **Online-Ausweisfunktion**
- **eGK + PIN**
- Vor-Ort-Verfahren:
 - POSTIDENT + POSTIDENT Zustellung
 - Identifizierung in der Geschäftsstelle
 - WIP: Apothekenident

Authentisierungsverfahren

- **Online-Ausweisfunktion**
- **eGK + PIN**
- Gerätebindung (+ zweiter Faktor)
 - ➔ Hardwareabhängigkeit
 - Zertifiziertes SE: Unbegrenzt
 - SE ohne Zertifizierung: 6 Monate
 - Kein SE: 24 h
- Biometrienutzung als zweiter Faktor
 - ➔ Zulässigkeit setzt Listung auf der Allow-Liste des BSI voraus

WIP!

Wir streben an, per Einwilligung niederschwellige Verfahren zuzulassen.

Hürden digitaler Identitäten im Versichertenkontext

Breite Nutzerakzeptanz durch BSI und BfDI-Vorgabe kaum möglich

Die **Bereitstellung** von **komfortablen** und in der **Breite akzeptierten Anmeldeverfahren** unter den strengen Vorgaben des BSI und BfDI ist die **größte Herausforderung** bei der Konzeption von eID-Lösungen!



- 1. Geringe Anzahl an zulässigen Anmeldeverfahren**, die das geforderte Sicherheitsniveau ‚hoch‘ erreichen
 - nPA/eGK + PIN, externe Hardware, Samsung Galaxy S20 als langfristig nutzbares Authentisierungsmittel
 - Nutzer ohne NFC-fähiges Smartphone sind von mobilen Szenarien ausgeschlossen



2. Ein (Groß)Teil der **biometrische Anmeldeverfahren** nach BSI-Vorgaben **nicht zulässig**



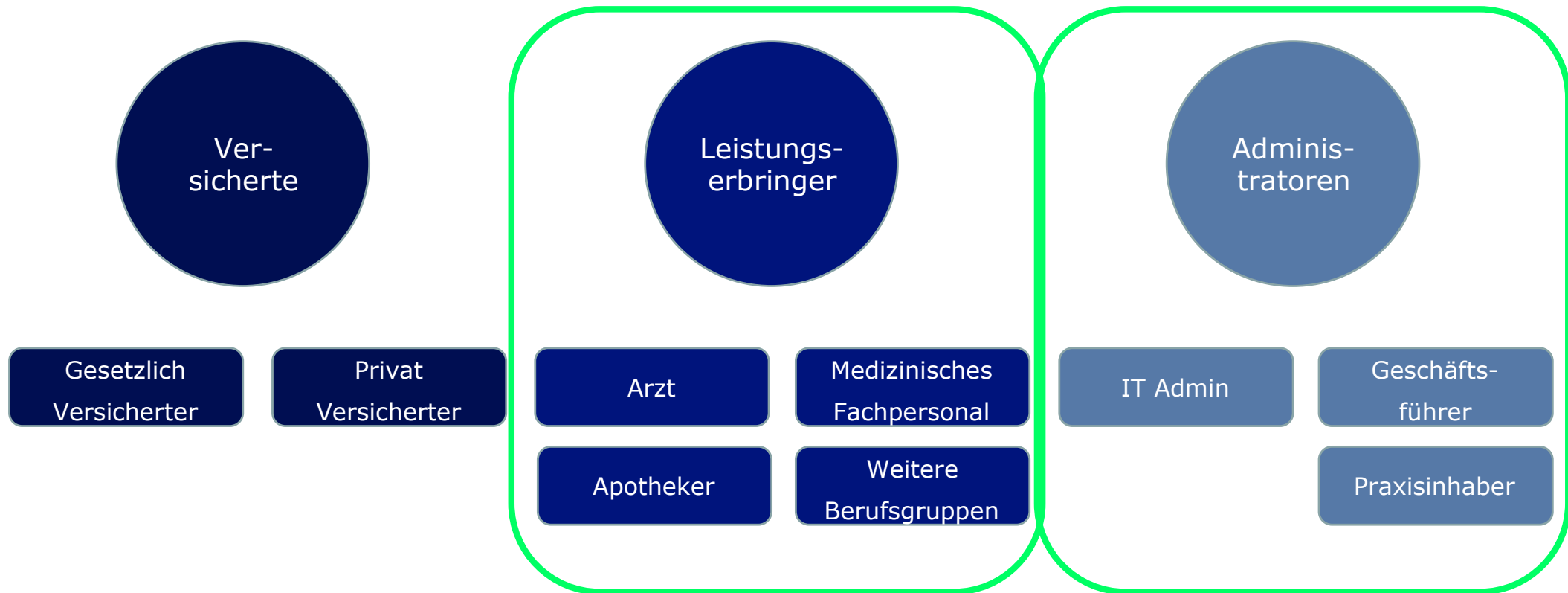
- 3. Single Sign-On** für Gesundheitsanwendungen **nicht zulässig**



- 4. Nutzer darf nicht** informiert und selbstbestimmt **in niederschwellige Verfahren einwilligen**

Nutzer- und Rollengruppen der digitalen Identitäten

eGK, eHBA und SMC-B bekommen eine kartenunabhängige Alternative



Elektronische Identitäten

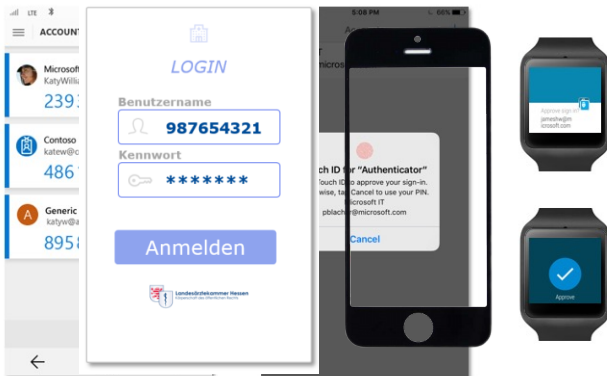
Authentisierung von Leistungserbringern



Das Authentisierungsmittel eHBA
des Leistungserbringers...



...soll durch gewohnte, komfortable
Verfahren ergänzt werden.



Nutzen

- Komfortabler und niederschwelliger Login, z.B. mit dem Smartphone an Gesundheitsanwendungen
- Einmaliger Registrierungsprozess für Ärzte und Apotheker
- Enabler für Fernsignaturdienst

Eckpunkte

- Bereitstellung der IDPs wird im Gesellschafterkreis zentral durch die gematik gewünscht
- HBA weiterhin als Authentisierungsmittel nutzbar, digitale Identität als Ergänzung
- 2 große Herausforderungen:
 - Einvernehmen mit BSI und BfDI zu nutzerfreundlichen Authentisierungsmethoden
 - Externe Erwartungshaltung: „**Vollwertiger Ersatz zum HBA**“ → Faktischer Mehrwert ergibt sich in Kombination mit einem Fernsignaturdienst
- Ab 2024 auf Verlangen bereitzustellen, Verschiebung auf 2025 angestoßen

Elektronische Identitäten

Authentisierung von Institutionen/Organisationen



Nutzenpotenzial

- LE kann in **unterschiedlichen Behandlungskontexten** ohne Zusatzaufwand im Namen der jeweiligen Institution auftreten (bspw. heute KH, morgen Praxis)
- **Nahtloser Prozess für LE und MFAs/Gehilfen** durch „Konsolidierung“ bzw. Verbindung der lokalen Identitäten im Primärsystem und der TI-Identitäten
- Enabler **mobiler Szenarien**

Eckpunkte

- Primäre Prämisse: **Keine Schaffung zusätzlicher Prozesshürden** für den operativen Praxis-/Klinikprozess



Keine Spezialhardware



Nicht verschiedene Identitäten für kleinteilige Zwecke



Möglichkeit ortsunabhängig zu agieren (mobil)



Flexible Prozesse zum Onboarding (Self-Service für vertretungsberechtigte)



Sicherheitsniveaus erfüllen, um auf TI Dienste zuzugreifen

Zusätzliche Herausforderungen im LE-Kontext

LE haben (noch) weniger Toleranz für komplexe Anmeldeprozesse

Herausforderung 1

Diskrepanz zwischen BSI und Realität

Massive Diskrepanz zwischen aktuellen und im Feld **genutzten Anmeldeprozessen** in den Primärsystemen zu den **strengen BSI-Vorgaben** für Anmeldungen nach Vertrauensniveau ‚hoch‘
Akzeptanzkriterien: Schnelle und nahtlose Prozesse!

Herausforderung 2

Erwartungshaltung bezgl. komfortabler Signatur

Erwartungshaltung der LE, dass die digitale Identität sowohl Anmelde- **als auch** **Signaturprozesse** wesentlich **komfortabler** machen als aktuell mit dem HBA

Herausforderung 3

Behandlungsteam-Patienten Verhältnis

Abbildung des in der Realität existierenden **Behandlungsteam-Patienten-Verhältnis** (anstatt Arzt-Patienten-Verhältnis) durch den genutzten technischen Standard **OpenID Connect**.

Die eID-Lösung muss es ermöglichen, dass das gesamte Behandlungsteam gemäß Ihrer Rollen und Rechte auf (TI-)Anwendungen im Verlauf der Behandlungsepisode zugreifen kann.

Herausforderung 4

Multisektorale Tätigkeit einzelner LEs

Tätigkeit einzelner Leistungserbringer für **unterschiedlichen Sektoren bzw. Institutionen**

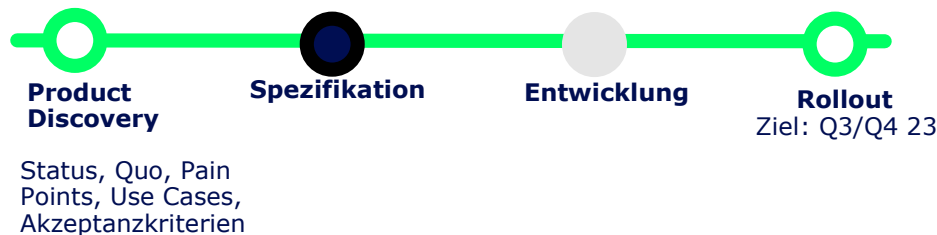
Die eID-Lösung muss schnell und reibungslos eine Zuordnung einer Person zu einer Institution ermöglichen und den LEs eine komfortable Möglichkeit liefern, den Institutionskontext zu wählen bzw. zu wechseln!

Status digitale Identitäten im Gesundheitswesen

Versicherten-ID vor Leistungserbringer-ID

GesundheitsID für Versicherte

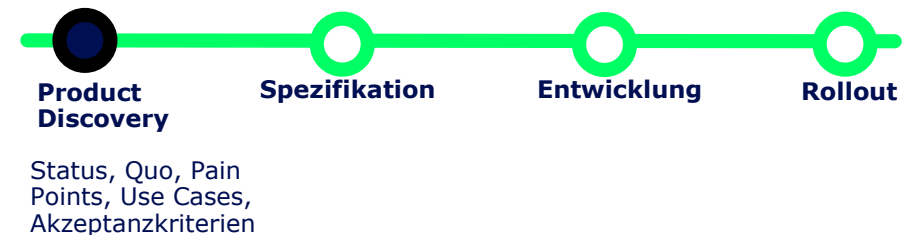
- Spezifikation mit Kostenträgern abgestimmt
- Einvernahme mit BfDI und BSI aktuell nicht hergestellt
- Rechtsrahmen wird Anfang 2023 angepasst



GesundheitsID für Leistungserbringer

Product Discovery Phase:

- Analyse der Anwendungsfälle, Akzeptanzkriterien & Lösungsraum
- Etablierung von Arbeitsgruppen/Taskforces, um Konzeption früh abzustimmen und zu validieren

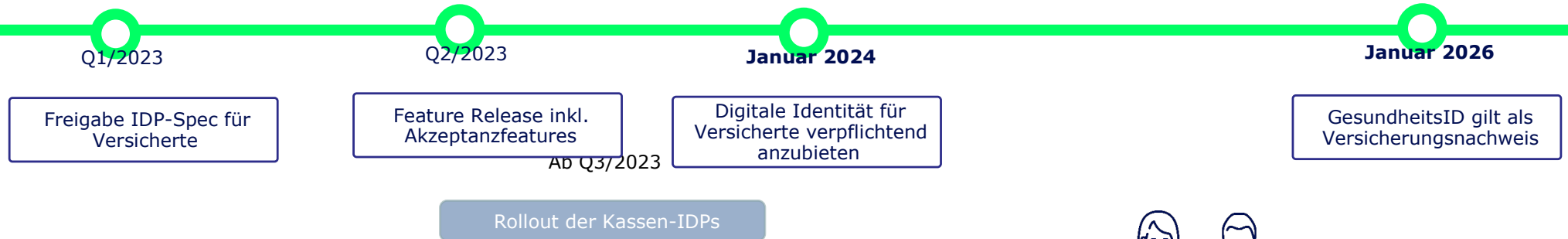


Digitale Identität als Alternative zu eGK, HBA und SMC-B

Ein kartenloser Zugang für alle Anwendungen

Roadmap digitaler Versichertenidentitäten

Stand: Kabinettsfassung KHPfIEG



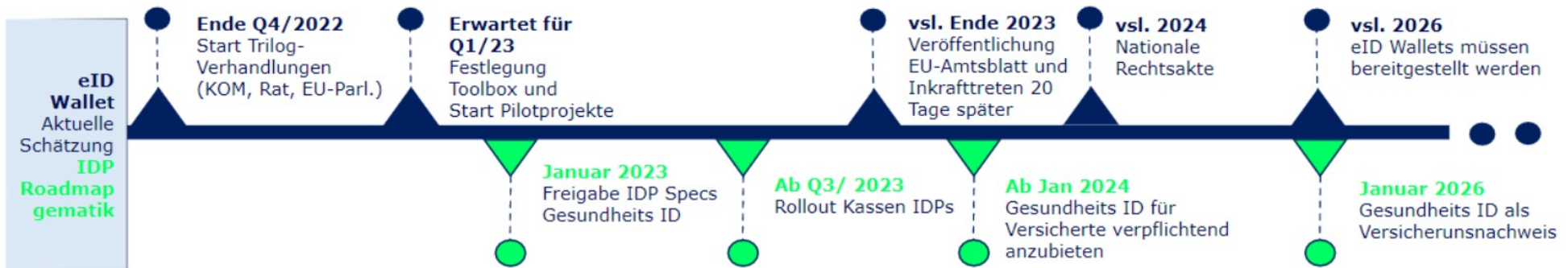
Roadmap digitaler Identitäten für Leistungserbringer(-institutionen)



*Verschiebung auf 2025 angekündigt

Einordnung der EUid Wallet nach eIDAS 2.0

Aktuelle Devise lautet: Beobachten & Vorbereiten



gematik. Gesunde Aussichten.