TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

TeleTrusT-Informationstag "Elektronische Signatur und Vertrauensdienste"

Berlin, 27.09.2023

QES in der Telematikinfrastruktur

Sergej Suskov, Principal Engineer, gematik GmbH

gematik: Daten und Fakten

gematik
Nationale Agentur für Digitale Medizin

- Gründung in 2005
- Hauptsitz in Berlin
- Gesetzliche Basis § 310 SGB V
- Geschäftsführer: Dr. med. Markus Leyck Dieken (seit Juli 2019)
- Aktuell ca. 460 Mitarbeiter

Unsere Anwendungen

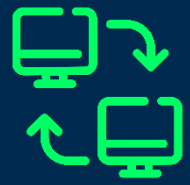
KIM

Elektronische Patientenakte (ePA)

E-Rezept

E-Medikationsplan

Notfalldaten-management

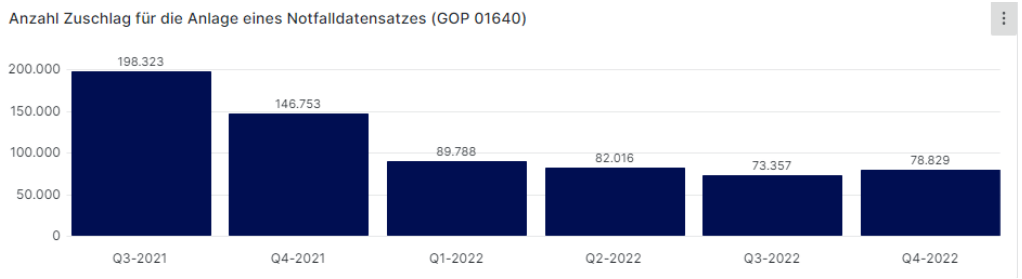


ISiK

DEMIS

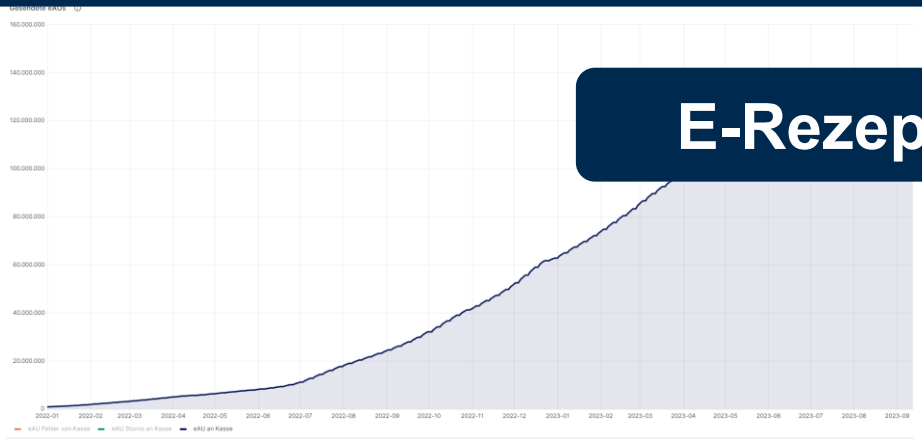
TI-Messenger

Anwendungsfälle mit QES



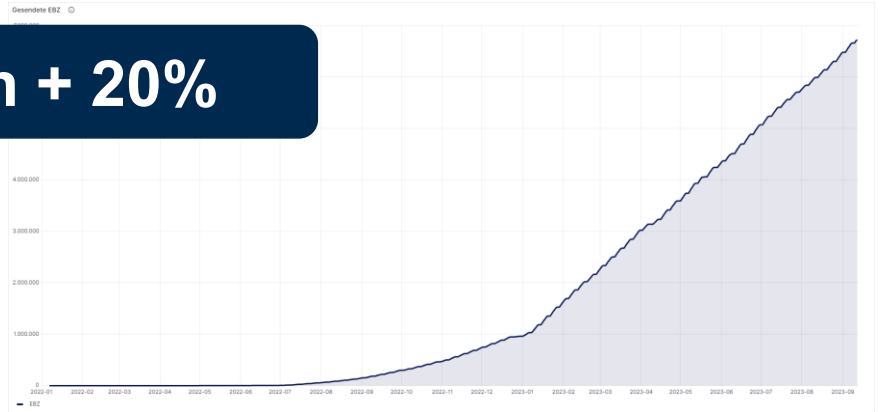
955.063 Notfalldatensätze (bis 31.12.2022)

11.874.272 eArztbriefe



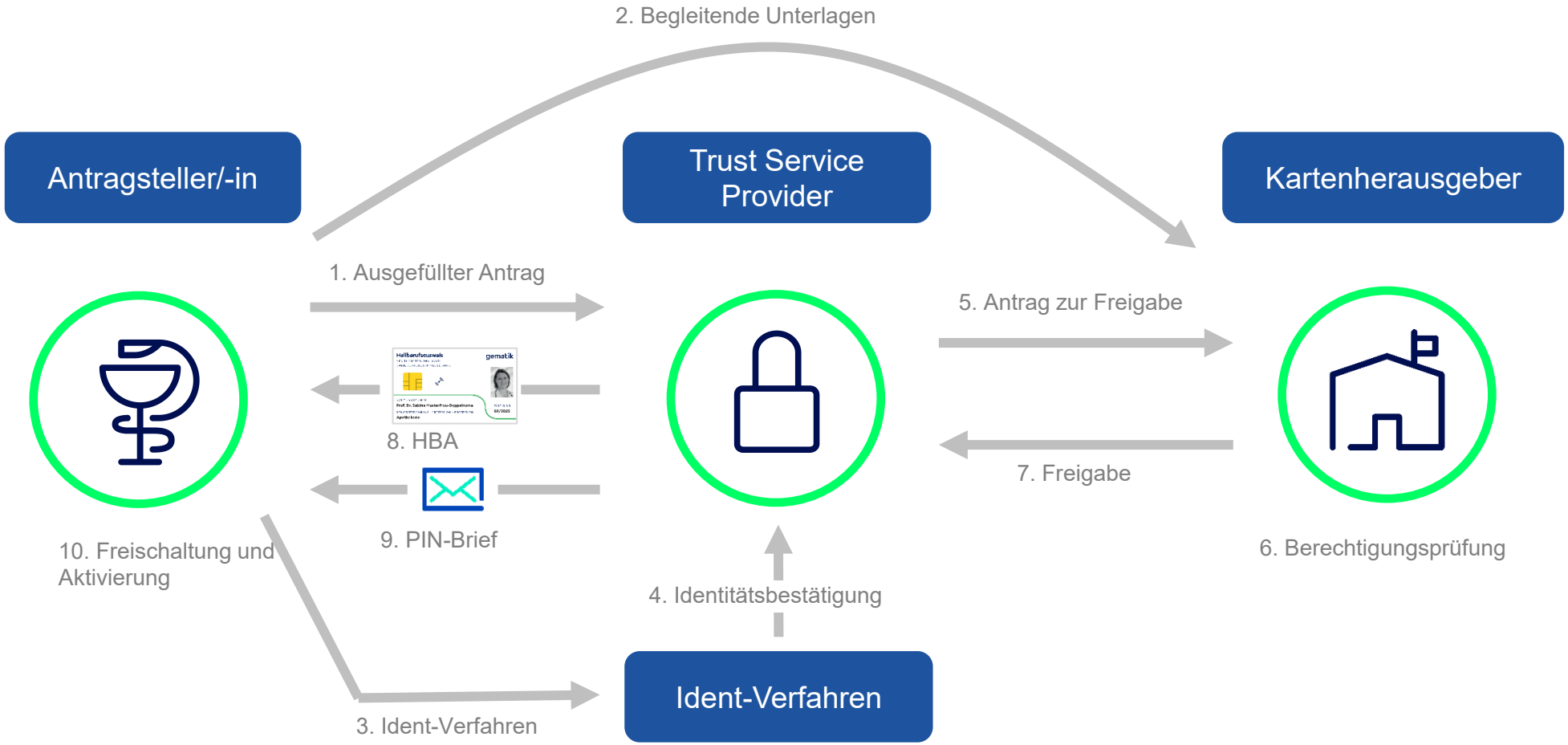
138.927.863 Arbeitsunfähigkeits-bescheinigungen, 50% QES signiert

E-Rezept: 4 Millionen + 20%



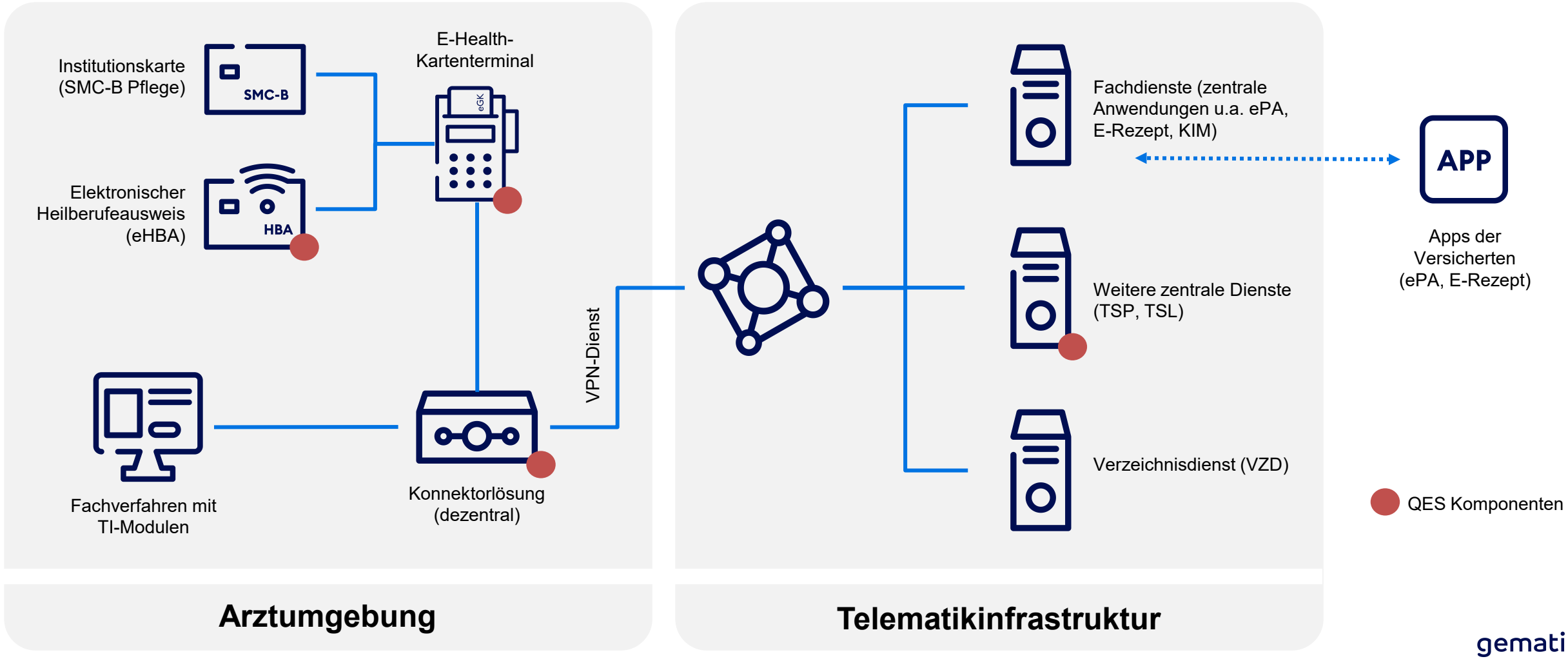
6.310.321 Elektronisches Beantragungs- und Genehmigungsverfahren (seit Februar 2022)

Der Antragsprozess HBA im Überblick



Zusammenspiel der einzelnen TI-Komponenten

Beispiel: Dezentrale Zugangslösung



Komfortsignatur, Stapelsignatur, Einfachsignatur

Einfachsignatur	Eine PIN-Eingabe zum Signieren eines einzelnen Dokuments
Stapelsignatur	Eine PIN-Eingabe zum Signieren mehrerer Dokumente mit einem Signaturauftrag
Komfortsignatur	Eine PIN-Eingabe zum Signieren mehrerer Dokumente über längeren Zeitraum ▪ Maximale Anzahl Dokumente: 250 ▪ Maximaler Zeitraum: 24 Stunden ▪ Das Primärsystem authentifiziert den Signierenden vor jeder Signatur

gematik

Starke UserId für HBA-Inhaber

- Individuelle, nicht zu erratende UserId für jeden HBA-Inhaber verpflichtend
- UserId = 128bit-Zufallszahl

Primärsystem	• erzeugt bei jedem Aktivieren des Komfortsignaturmodus für jeden Nutzer/HBA eine neue UserId • Verwendet diese UserId bei jedem Zugriff des Nutzers auf den HBA • Setzt den HBA vor Aktivierung des Komfortsignaturmodus zurück (oder bei Fehler 4081)
Konnektor	• prüft Länge der UserId • prüft Eindeutigkeit der UserId über 1.000 Vorgänge

Telematikinfrastruktur 2.0

TeleTrusT
Pioneers in IT security.
Bundesverband IT-Sicherheit e.V.

1

Föderiertes Identitätsmanagement

Mehr Flexibilität und Nutzerfreundlichkeit durch einfache Nutzung von Identitätsbestätigungen der TI

2

Universelle Erreichbarkeit der Dienste

Wegfall proprietärer IT-Lösungen (z.B. Konnektor) mit reduzierten Kosten und stabilisiertem Betrieb

3

Moderne Sicherheitsarchitektur

Eigenständige Bereitstellung von Diensten durch unterschiedliche Anbieter mit mehr Sicherheit und Effizienz

4

TI-Regelwerk

Vertrauen in die TI durch automatisierte Überprüfung von Sicherheit und Datenschutz sowie von Interoperabilität und Verfügbarkeit

5

Verteilte Dienste

Verknüpfung von Daten aus verschiedenen Quellen für optimierte Versorgungsprozesse

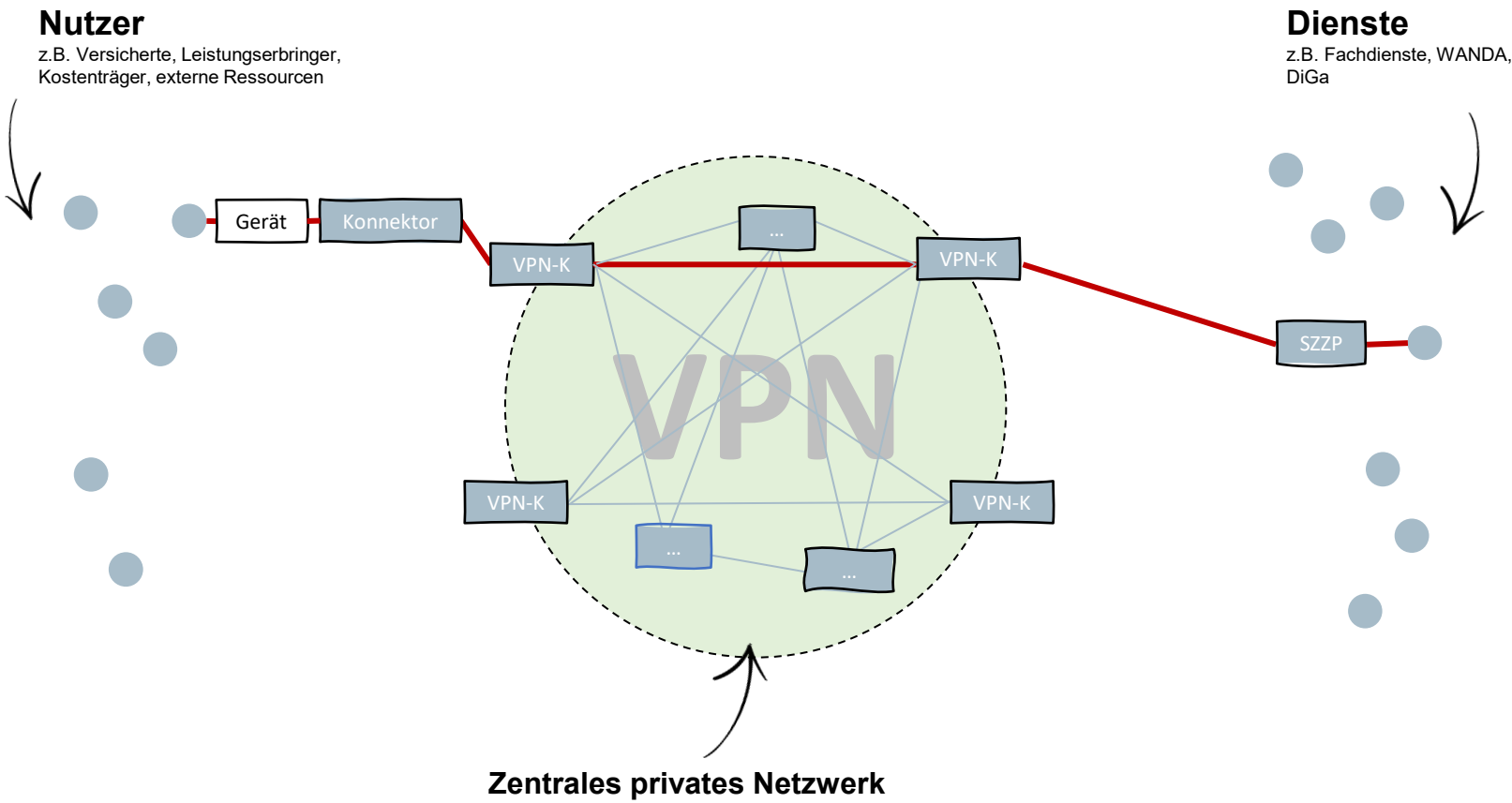
6

Interoperabilität und strukturierte Daten

Höhe Datenqualität für anwendungsfallbezogene Versorgung und Forschung und bessere Integration von Produkten und Services

gematik

TI Heute

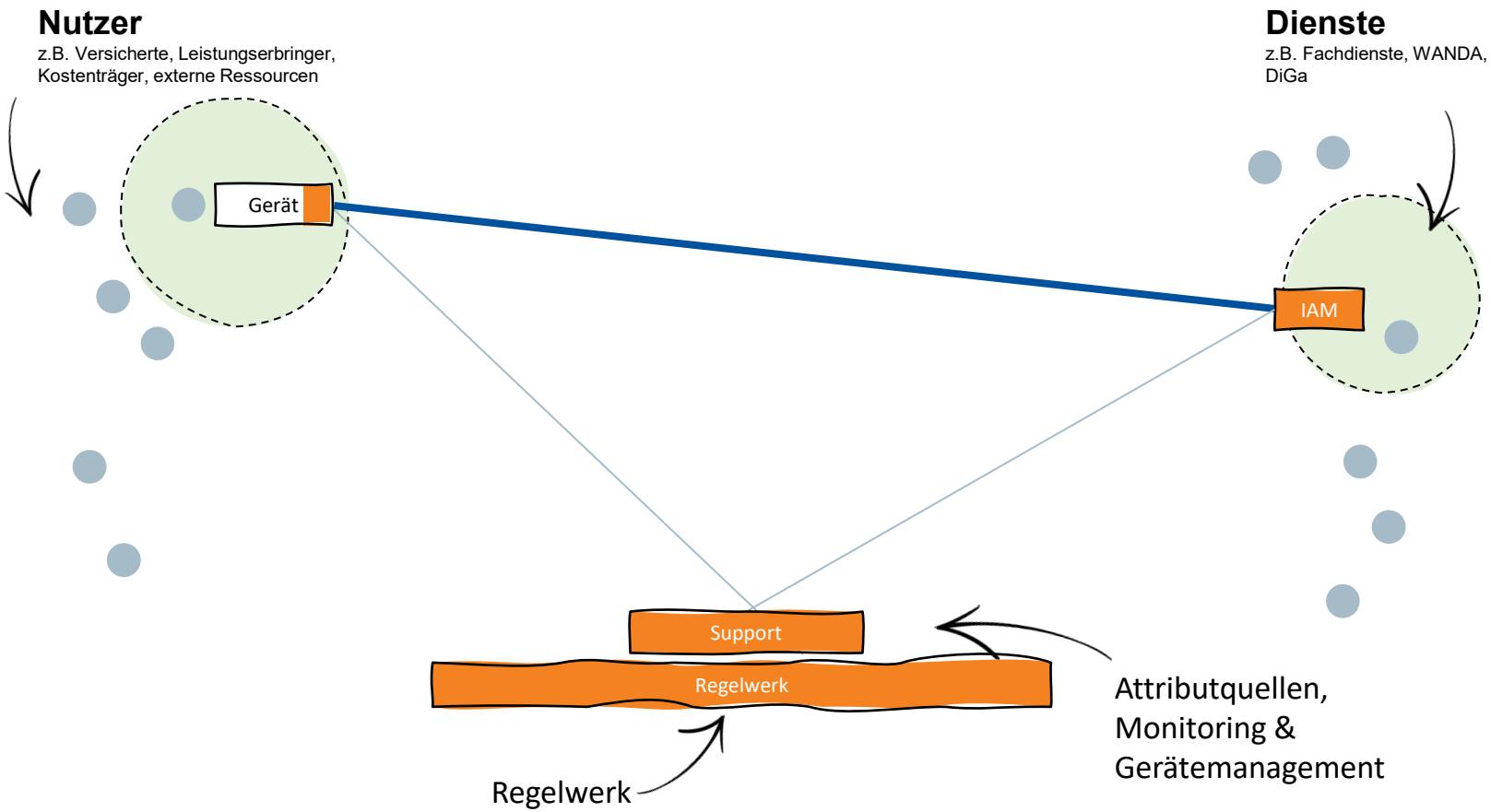


TI heute

- heutige TI über zentrales, vertrauenswürdiges Netz
- Einsatz proprietärer Komponenten mit teurer und fehleranfälliger Hardware, keine durchgehende Sicherheit
- Ortsbindung, limitierte Nutzerfreundlichkeit, geringe Flexibilität und Skalierbarkeit
- Wachsende Komplexität und Fehleranfälligkeit Gesamtarchitektur (VPN, SZZP, VAU etc.)
- Limitierte Innovations-geschwindigkeit bei Fachdiensten

Heutiger Architekturansatz der TI trägt nicht mehr

TI mit Zero Trust



TI mit Zero Trust

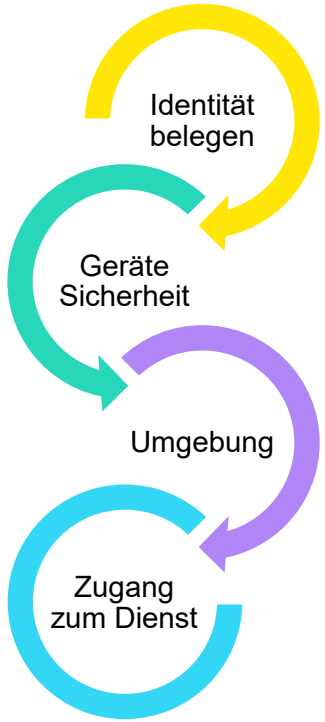
- Direktkommunikation zwischen Nutzern und (Fach-)diensten ohne Einwahl in zentrales Netz
- Vertrauen durch kontinuierliches und flexibilisiertes Prüfen und Steuern der Zugriffe
- Verzicht auf ortsgebundene Zugangshardware

- Erhöhung Mobilität, Nutzungs-komfort und Steuerbarkeit
- Senkung von Kosten und Fehleranfälligkeit
- Höhere Agilität bei Entwicklung von Fachdiensten

Neue Sicherheitsarchitektur

1. Identität mit n Rollen (Arzt, Versicherter, ...)
2. OS, Virenscanner, Updates, Jailbreak…
3. Geo Location! DE, kein TOR, Ip-Adresse…

Fachlogik, Zugriff auf Daten, Login…



Elektronische Identitäten für Versicherte

Zugang zu

ePA

E-Rezept

TI-Messenger

Patientenportale

APP

Kasseneigene Anwendungen

APP

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

Elektronische Identitäten für Leistungserbringer

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:
  - nutzerfreundlichen Authentisierungsmethoden
  - **„Vollwertiger Ersatz zum HBA“** ➔ Faktischer Mehrwert ergibt sich in Kombination mit einem Fernsignaturdienst

Initiative Fernsignatur

Auslösen von Signaturen im Behandlungskontext auch ortsunabhängig ermöglichen – ohne Smartcard

Stand QES heute

- Chipkarten, Kartenlesegerät sowie Signatursoftware im Konnektor

Zukünftig soll es auch Fernsignaturlösungen geben

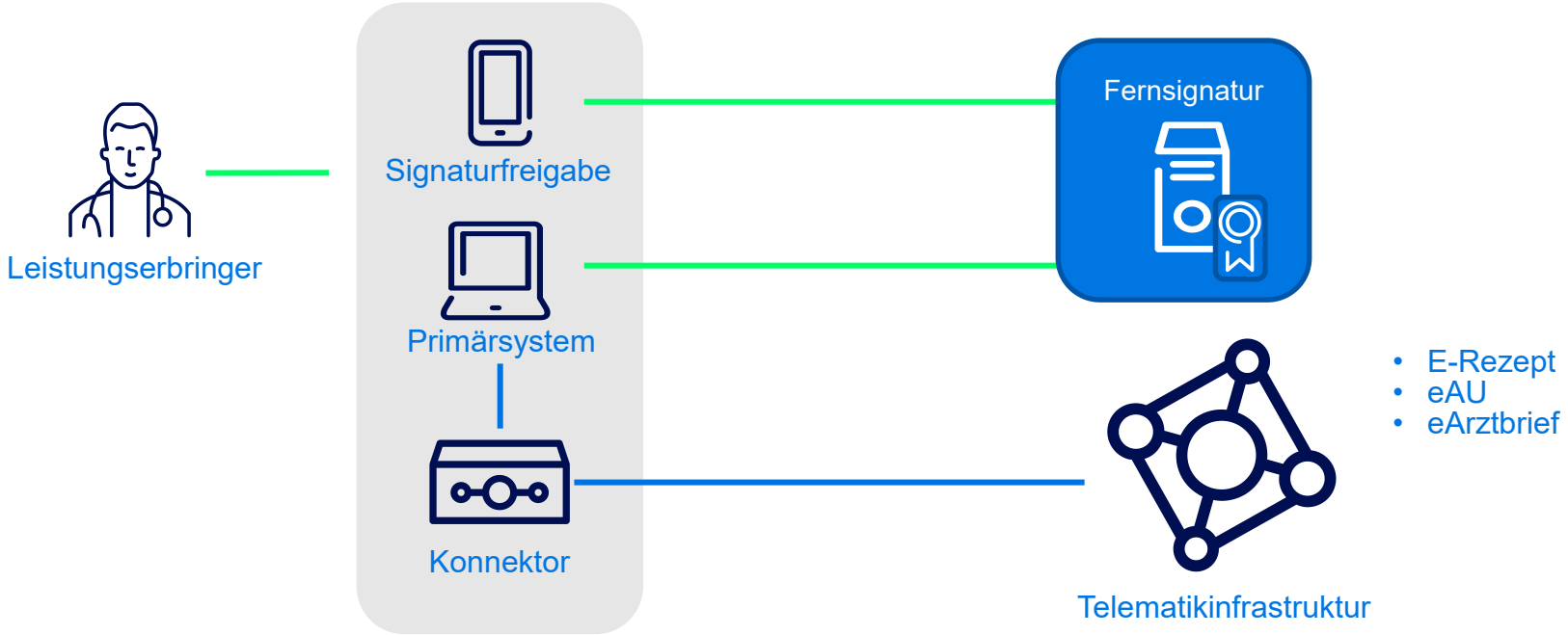
- QES wird von einem qualifizierten Vertrauensdiensteanbieter im Auftrag der unterzeichnenden Person erstellt
- Qualifizierter Vertrauensdiensteanbieter ist nach eIDAS zertifiziert
- Zusätzliche Zulassung durch gematik für spezifische Anforderungen im Gesundheitswesen
- Interoperabilität mit Konnektoren (Prüfung)

Signaturanwendung

- Integration mir Primärsystemen muss möglich sein
- Authentisierung / Freigabe eines Signaturvorgangs muss durch LE als benutzerfreundlich akzeptiert sein
- Benutzerkomfort ist zu berücksichtigen (Stichwort Komfortsignatur)

Ein Pilotprojekt mit konkreten Benutzergruppe und entsprechenden Gutachten/Datenschutzbewertungen erforderlich

Pilotierung Fernsignatur



Pilotierung mit D-Trust ab Q4/2023

- Fernsignaturzertifikate auf Basis der HBA Prozesse
- eIDAS zugelassener qVDA
- Direkte Integration in Primärsysteme
- Zeitlich begrenzt, Teilnehmerzahl begrenzt
- Hauptfokus: Nachweis der Nutzerakzeptanz und Interoperabilität

Danke ...