Digital Health

Kap. 2: Kurze Einführung in die Telematik-Infrastruktur

Prof. Dr. Georgios Raptis

In diesem Kapitel behandeln wir allgemeine Prinzipien der Telematik-Infrastruktur, d.h. der landesweiten E-Health Infrastruktur in Deutschland

- Aus funktionaler Sicht, d.h. nicht technisch in allen Einzelheiten

- Ziel ist es, einige grundlegende Aspekte von E-Health sowie Anwendungen, wie sie in der Praxis konzipiert sind, zu verstehen

- Außerdem hat die Telematik-Infrastruktur als landesweite eHealth Infrastruktur in Deutschland eine besondere Bedeutung

Im Anschluss werden wir

- andere landesweite eHealth Infrastrukturen anderer Länder kennenlernen (Kap. 2.1)

- fortgeschrittene Identity-Management Konzepte für E-Health Anwendungen behandeln (Kap. 3)
  - Überleitend von der Telematik-Infrastruktur
  - hin zu möglichen (sicheren und unsicheren) Alternativen

Wir haben eine High-Tech Medizin

Diagnostik und Therapie sind auf einem exzellenten technologischen Niveau, insbesondere dank Medizintechnik und Medizinischer Informatik

Abb.: Von MBq - Selbst fotografiert, Copyrighted free use, https://commons.wikimedia.org/w/index.php?curid=32847845

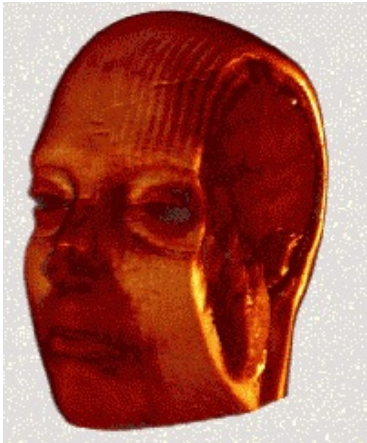


Abb.:Von Bionerd - Eigenes Werk, CC BY 3.0, https://commons.wikimedia.org/w/index.php?curid=11318838

Dennoch gibt es deutliche Defizite in der Vernetzung, Kommunikation und Zusammenarbeit im Gesundheitswesen

Anlass für die elektronische Gesundheitskarte und die TI

Im Jahr 2001 gab es das „Lipobay Skandal“

- Lipobay (Cerivastatin): ein Lipidsenker
- In Kombination mit einem anderen Medikament (Gemfibrozil) kann es zu Rabdomyolyse (Auflösung von Muskeln) und als Folge zu Nierenversagen kommen

- Diese unerwünschte Wirkung („Nebenwirkung“) war eigentlich bekannt
- Trotzdem wurde sie nicht erkannt oder beachtet
  - Der verordnende Arzt wusste evtl. nicht, welche andere Medikamente der Patient sonst nimmt
  - Nebenwirkung wurde nicht beachtet → es gibt sehr viele Medikamente, die miteinander irgendwie ungünstig interagieren. Maschinelle Unterstützung und insb. Information ist hier sinnvoll

Gesetzliche Grundlagen der Telematik-Infrastruktur

Die Politik wollte schon 2003 mit dem GKV-Modernisierungsgesetz gegensteuern, um solche Informationsdefizite zu beheben

- → § 291a SGB V: Elektronische Gesundheitskarte, Heilberufsausweise, Telematik-Infrastruktur mit benannten E-Health Anwendungen

Ziele: **Wirtschaftlichkeit, Qualität und Transparenz im Gesundheitswesen** steigern, durch:

- Vernetzung des deutschen Gesundheitswesens
- Schaffung einer Infrastruktur / Plattform / „Datenautobahn des Gesundheitswesens“
  → Bausteine und Werkzeuge für bereits geplante und zukünftige E-Health Anwendungen
- Sinnvolle und nutzbringende E-Health Anwendungen

E-Health Gesetz (2015), Terminservicegesetz (TSVG, 2019), Digitale Versorgungsgesetz (DVG, 2019), Patientendaten-Schutzgesetz (PDSG, 2020), Digitale Versorgung und Pflege Modernisierungs-Gesetz (DVPMG, 2021)

Umstrukturierung der Gematik, elektronische Patientenakte, Patientenkurzakte, Öffnung für Patient*innen mit Smartphones, Digitale Identitäten, „Zukunftskonnektoren“, Digitale Gesundheits- und Pflegeanwendungen, weitere Änderungen

Akteure

Wer baut die Telematik-Infrastruktur?

- gematik GmbH (Berlin) gegründet im gesetzlichen Auftrag
- Gesellschafter: Selbstverwaltung im Gesundheitswesen
  - Ärzte (Bundesärztekammer, Kassenärztliche Bundesvereinigung)
  - Zahnärzte (BZÄK, KZBV)
  - Apotheker (ABDA, DAV)
  - Krankenhäuser (Deutsche Krankenhausgesellschaft)

  - Krankenkassen (GKV-Spitzenverband) → ~~50% der Stimmen~~

Ab 2019: BMG hat 51% der Stimmrechte erhalten und die Kontrolle übernommen

Wieso baut man überhaupt *landesweite* eHealth Infrastrukturen?

- Landesweite **Interoperabilität**: Für eHealth Anwendungen muss es letztendlich egal sein, welche Software oder App und welchen Anbieter der Arzt, das Krankenhaus oder der Patient hat. Es muss so selbstverständlich klappen, wie telefonieren (= man kann jemanden problemlos anrufen, egal welches Endgerät oder Provider man hat).

Wie baut man eine landesweite eHealth Infrastruktur?

- **Top-Down**

oder

- **Bottom-Up**

Top-Down vs. Bottom-Up

Die Telematik-Infrastruktur : Top-Down Ansatz

- Der Gesetzgeber bestimmt
- Die Industrie baut
- Ärzte / Zahnärzte / Apotheker / Patienten usw. (müssen) machen

Andere E-Health Projekte verfolgen einen Bottom-Up Ansatz

- Einzelne Ärzte (Zahnärzte, Apotheker usw.) haben eine Idee
- Ein Krankenhaus kommt dazu
- Sie vernetzen sich, starten eine E-Health Anwendung
- Oder ein Software-Hersteller bietet eine E-Health Anwendung an
- Mehr Ärzte kommen hinzu, eine „Insel“ entsteht

- Entscheidender Punkt: gelingt die Integration mit weiteren Inseln?

Telematik-Infrastruktur: Top-Down Ansatz

- Der Gesetzgeber bestimmt: viele eHealth Gesetze, welche auch die Technik bestimmen
- Die gematik baut im Auftrag ihrer Gesellschafter
- Die Ärzte / Zahnärzte / Apotheker / Krankenhäuser usw. müssen sich vernetzen und die eHealth Anwendungen bedienen

Vorteile

- **Flächendeckende** Vernetzung nach einem de-facto Standard
- Interoperabilität der so entwickelten E-Health Anwendungen
- Relevanter Markt für eHealth Hersteller (wirklich?)
- Kontrollierte Sicherheit

Nachteile

- „Zwangsinfrastruktur“, erzeugt Widerstände
- Die entwickelten Lösungen müssen nicht unbedingt die Besten sein (wir wissen es noch nicht)

Kontrollierte Sicherheit in der Telematik-Infrastruktur

- Vorgaben und Kontrolle durch das BSI (Bundesamt für Sicherheit in der Informationstechnik) und den BfDI
- Prüfung durch die Gesellschafter der Gematik
- Definiertes Sicherheitsniveau

- Veröffentlichung der Spezifikationen → Transparenz

- Security by Design
- Privacy by Design

Andere eHealth Projekte: Bottom-Up

Bottom-Up Ansatz anderer eHealth Lösungen

- Ärztenetze und Krankenhäuser, die sich selbst vernetzen und Anwendungen hochziehen
- Hersteller von KIS und PVS, die ihre Software mit eHealth Anwendungen anreichern

Vorteile

- Freiwillige Lösungen, bessere Motivation für die Anwender
- ~~Besserer Wettbewerb → nur gute Lösungen können sich etablieren~~ theoretisch ja, klappt aber nicht gut... Wettbewerb wird oft durch technische Abschottung mancher Anbieter behindert

Nachteile

- Insellösungen, in vielen Fällen inkompatibel untereinander
- Häufig Abschottung von Anwendungen seitens der Hersteller
- Keine flächendeckende Vernetzung
- Sicherheitsanforderungen / -architektur?
- Die Wahrscheinlichkeit für einen Patienten, dass alle seine Ärzte eine bestimmte Anwendung unterstützen, ist klein

Top-Down vs. Bottom-Up für landesweite eHealth Infrastruktur

Noch nie gab es in einem Land eine flächendeckende, interoperable, sichere, landesweite eHealth Infrastruktur nach dem Bottom-Up Ansatz

- **Sicherheit** und Datenschutz kosten, macht keiner freiwillig

- Für viele Unternehmen läuft **Interoperabilität** gegen ihre Geschäftsinteressen
  - Verteidigung von Marktanteilen durch Abschottung

- (Zu) viele Ärzte sehen keinen Grund, sich zu **vernetzen**
  - Verteidigung von Marktanteilen durch Abschottung
  - Unwilligkeit Daten herzugeben, Angst vor Transparenz

Bisherige internationale Erfahrungen: nur durch Regulierung des Staates (sogar in den USA) klappt es mit Flächendeckung, Interoperabilität und Sicherheit

Gesetzlich festgelegte Anwendungen, inkl. Zugriffsrechte (!)

- Versichertenstammdatenmanagement (VSDM, Pflichtanwendung)
- eRezept, Arbeitsunfähigkeitsbescheinigung (eAU-Bescheinigung)
- Notfalldatenmanagement (NFDM) → künftig Patientenkurzakte
- Kommunikation im Medizinwesen (KIM), TI-Messenger (TIM)
- eMedikationsplan / Arzneimitteltherapiesicherheitsprüfung (AMTS)
- ePatientenakte
  - darin: Patientenfach, Patientenquittung, Impfpass, Mutterpass, Anschluss DiGAs, weitere
- Organspendeerklärung
- Hinweise über Organspendeerklärung, Patientenverfügung, Vorsorgevollmacht

Grundlegende Architektur-Bestandteile der Telematik-Infrastruktur

- **Plattform**

- **Anwendungen**

TI-Architektur

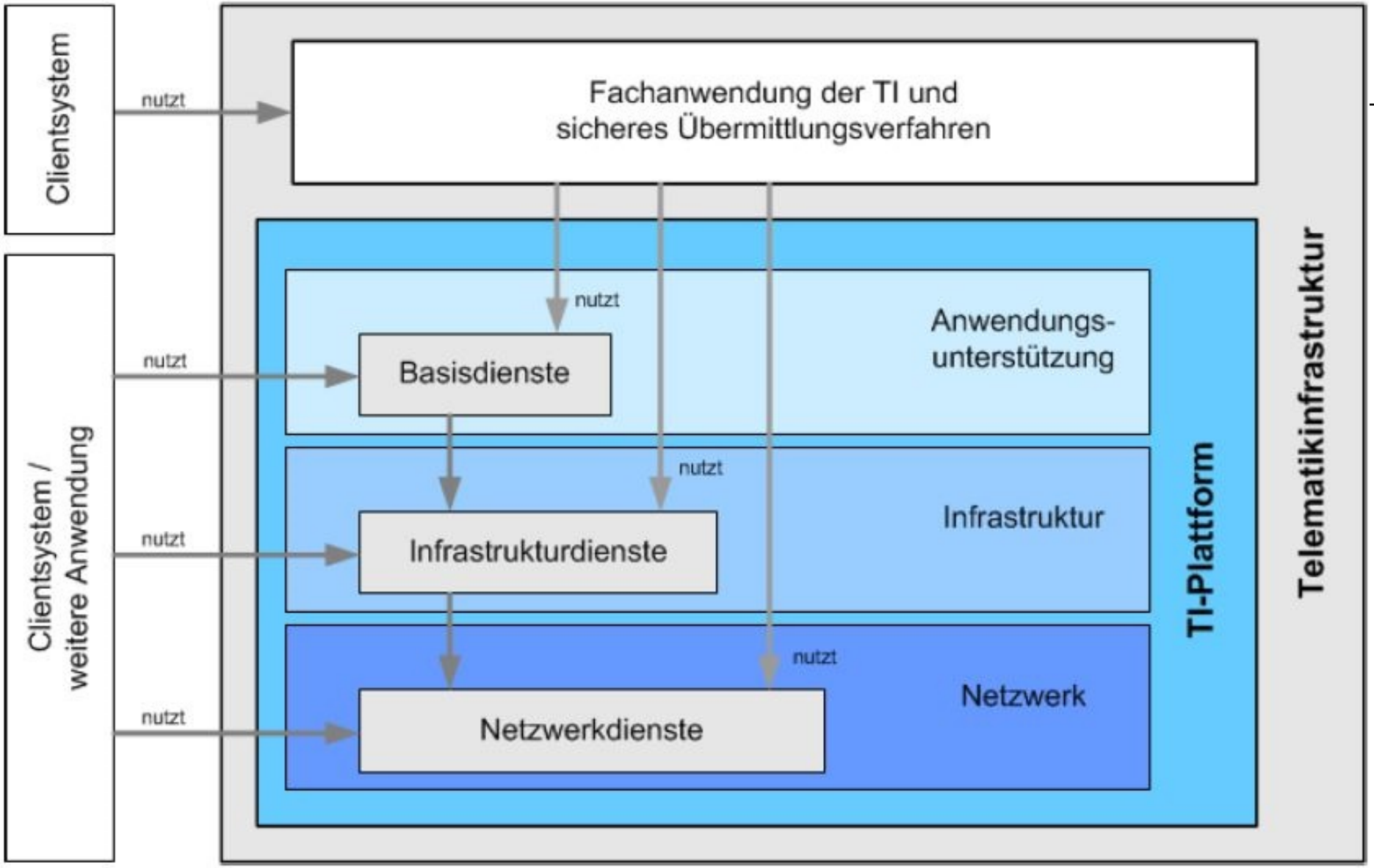
Telematik-Infrastruktur (TI) als Plattform

- **Service-orientierte Architektur (SOA)**
  - Nachrichtenbasiert, hauptsächlich SOAP (nur eRezept ist REST), typischerweise mit Intermediär (Broker) für jede Anwendung
  - Mehrere Services (Fachdienste, Unterstützungsdienste)

- Zentrales Netz (VPN, MPLS-basiertes Backbone)
  - Sicherheitsgateways für Anbindung anderer geschlossener Netze und Anwendungen, Bestandssysteme der Krankenkassen sowie über Security Gateway zum Internet (!)

- Anbindung per “Konnektor“ für
  - Arzt- /Zahnarztpraxen
  - Krankenhäuser
  - Apotheken
  - weitere Einrichtungen des Gesundheitswesens

TI-Architektur, Plattform und Dienstehierarchie



Quelle: Gematik GmbH: Konzept Architektur der TI-Plattform Version 2.9.0

Telematik-Infrastruktur

- **Entkopplung von Plattform und Anwendungen**
  - Beliebige Anwendungen, die ins Architekturschema passen, können unterstützt werden, ohne Anpassung der Plattform
  - Gemeinsame Plattform-Dienste können unverändert von mehreren Anwendungen verwendet werden
  - Semantische Entkopplung (der Plattform ist egal, welche Informationen in der Anwendung ausgetauscht werden)
  - Entkopplung von Maßnahmen der Informationssicherheit

Komponenten der TI

- Backbone, mit Firewalls zur internen Segmentierung
- VPN-Konzentratoren für Praxen usw.,
- Security Gateways zu anderen Netzen, externe Anwendungen, Internet

→ Netz

- Elektronische Gesundheitskarten (eGK)
- Heilberufsausweise (HBA)
- Institutionskarten (SMC=Security Module Cards)
- Gerätekarten (SMC-{K|KT})
- Verzeichnisdienste, OCSP-Responder/Proxies
- PKIs für eGK, HBA, Geräteidentitäten, Dienste
- Authentifizierungsdienst (derzeit für ePA)
- Identity Provider (derzeit für eRezept)

→ ID-Management

- Konnektoren
- Kartenterminals

→ Dezentrale Komponenten

→ Plattform

- Unterstützungsdienste (SDS, DNS, NTP, UFS, CAMS usw.)
- Log-Dienste

- **Fachdienste (zentral und dezentral im Konnektor)**
- Fachdienst-spezifische Intermediäre (→ SOA)

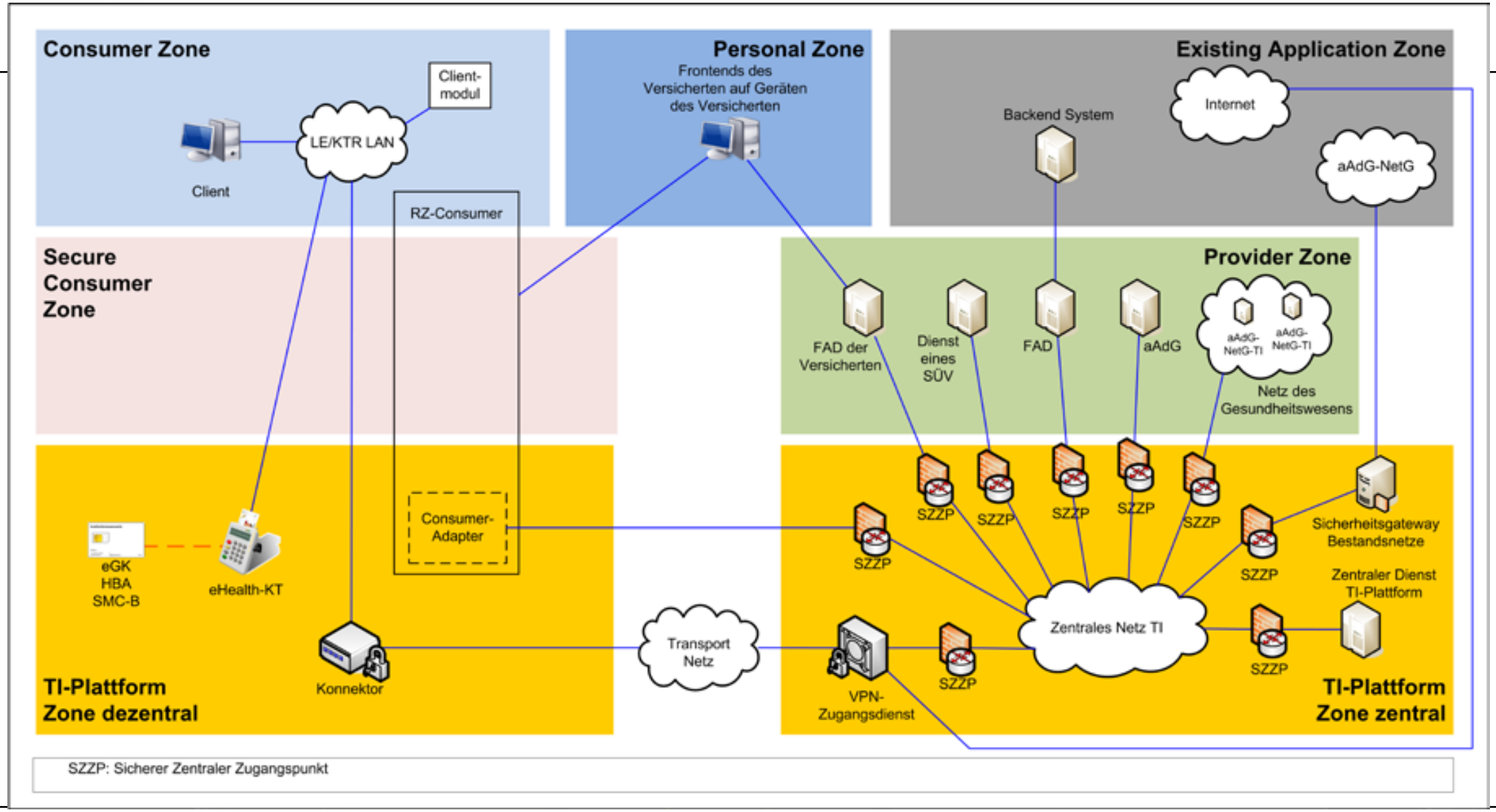
→ Anwendungen

- Gateways der Anbieter für Patientenzugang über Smartphones mit Vertrauenswürdiger Ausführungsumgebung, „Signaturdienst“
- Apps für Versicherte

→ Zugang Versicherte

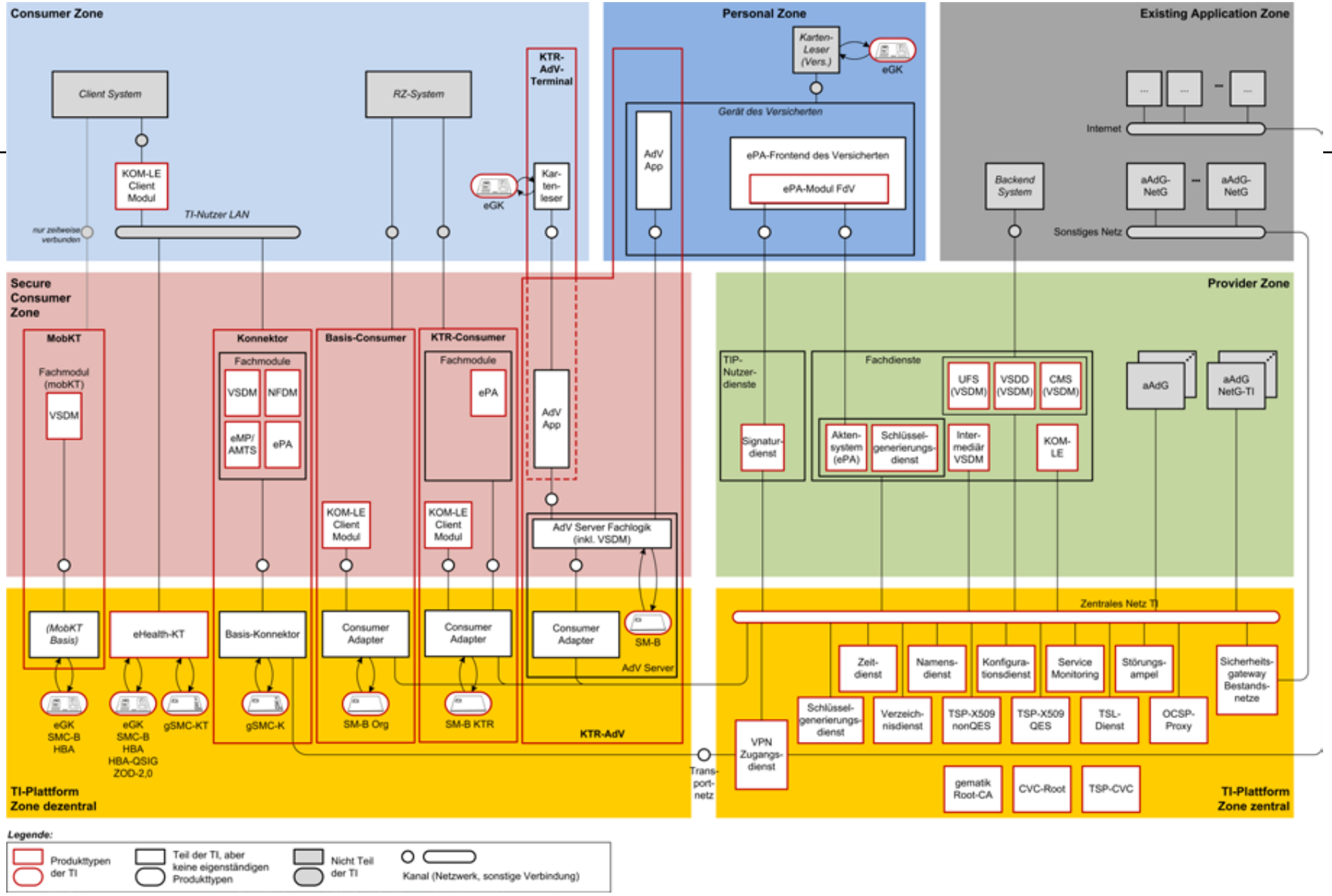
- Die Bestandssysteme („Primärsysteme“) der angebundenen Akteure gehören nicht zur TI (PVS, KIS, AVS, Krankenkassensysteme)

TI-Architektur, Netzwerktopologie



Quelle: Gematik GmbH: Konzept Architektur der TI-Plattform Version 2.9.0

TI-Architektur, Gesamtsystem

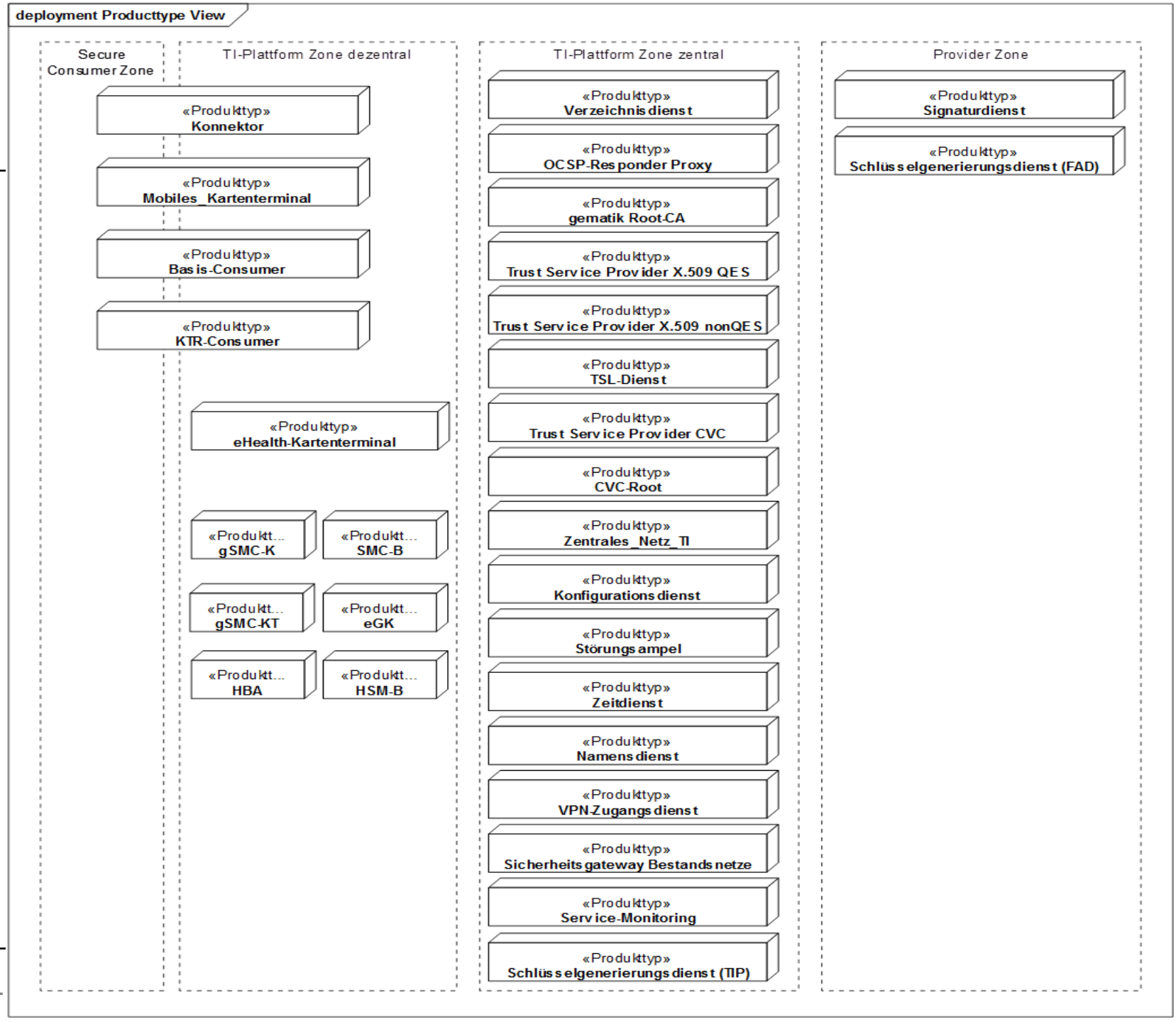


Quelle: Gematik GmbH: Konzept Architektur der TI-Plattform Version 2.9.0

OSTBAYERISCHE TECHNISCHE HOCHSCHULE REGENSBURG

INFORMATIK UND MATHEMATIK

TI-Architektur, Produkttypen der TI-Plattform



Quelle: Gematik GmbH: Konzept Architektur der TI-Plattform Version 2.9.0

Grundlegende Paradigmen in der TI

Die TI ist ein geschlossenes Netz/System

- Zugang ~~ausschließlich~~ / grundsätzlich über Konnektoren. Ausnahmen:
  - Legacy-Systeme der Krankenkassen sowie Kommunikationsanwendungen in Rechenzentren der Gesellschafter-Organisationen
  - Geplant für ePatientenakte („ePA“): Sicherheitsgateway (des ePA-Anbieters) für Patienten → Frontend des Versicherten
  - Für eRezept: App der Gematik für Smartphone des Versicherten, über Sicherheitsgateway
- Außenzugänge der TI:
  - Konnektor ←→ VPN-Konzentrator
  - Sicherheitsgateways/Proxies für externe (geschlossene) Netze und Anwendungen von Drittanbietern
  - Internet über Sicherheitsgateway (→ sicheres surfen im Internet)

Alle Akteure und Geräte in der TI haben eine kryptographische Identität, i.d.R. in Form einer Chipkarte (ID1, ID0 oder embedded)

- Gegenseitige Kryptographische Authentisierung aller Komponenten und Kommunikationsverbindungen
- Sperrung einer kryptographischen Identität jederzeit möglich
- Identitäten für den mobilen Zugang von Versicherten werden zentral gespeichert und über Authentifizierung freigeschaltet

Ende-zu-Ende Verschlüsselung

- Daten werden in einem Konnektor dezentral verschlüsselt und erst wieder in einem Konnektor oder in einer „Vertrauenswürdigen Ausführungsumgebung“ (VAU) für den Patientenzugang entschlüsselt
- Schlüsselmanagement jedoch zentral, insb. Verschlüsselungsschlüssel

Card-to-Card Authentisierung (C2C)

- Direkte Authentisierung zwischen 2 Chipkarten
- Mit Hilfe von Card Verifiable Certificates (CVC)
- Damit können bei der eGK Daten freigegeben werden
  - z.B. Lesen/Schreiben Notfalldaten ohne PIN
- Kryptographische Schlüssel können aktiviert werden
  - Zugriff mit Hilfe der eGK auf verschlüsselte Patientendaten nur bei Anwesenheit (also nach Freischaltung) eines HBA oder SMC

Card-to-Card Authentisierung (C2C)

- Attributsbasierte Autorisierung
    - z.B. Notfalldaten können nach Authentisierung eines eArztausweises, nicht aber eines eApothekerausweises auf die eGK geschrieben werden
- Sperrung der CVC (z.B. bei verlorenen oder gestohlenen Karten) jedoch nicht möglich
    - Theoretisch machbar & in den Karten vorbereitet, aber nicht „scharfgestellt“, Mechanismus dafür ist ziemlich kompliziert und wird voraussichtlich nicht in Betrieb gehen
- In Zukunft (nach Einführung „Digitaler Identitäten“) wird C2C-Authentisierung wahrscheinlich abgeschafft (wenngleich weiterhin die Identitäten von Patient und Arzt Aktionen autorisieren sollen, jedoch nicht über direkte gegenseitige Authentisierung zweier Chipkarten)

Offline vs. online Speicherung von medizinischen Daten

In der Telematik-Infrastruktur sind Anwendungen mit offline und auch welche mit online Speicherung von Patientendaten projektiert

- Offline, dezentral auf der eGK, oder nur Datenübertragung, keine langfristige zentrale Speicherung
  - Notfalldaten
  - Versichertenstammdaten
  - „Kommunikation im Medizinwesen“ → sichere E-Mail über S/MIME
  - Medikationsplan / AMTS (Arzneimitteltherapiesicherheitsprüfung)

- Online, serverbasiert
  - elektronische Patientenakte mit vielen Bestandteilen
  - eRezept, eAU (Arbeitsunfähigkeitsbescheinigung → Krankschreibung)

- Die Diskussion online/zentral vs. offline/dezentral wurde zwischen den Gesellschaftern häufig ideologisch geführt

- Die strategische Ausrichtung des BMG geht in Richtung einer künftigen reinen online-Speicherung

Patientenindividuelle Verschlüsselung

- Frühere Konzepte: Alle (künftig) online gespeicherten Daten sollten mit dem öffentlichen Schlüssel der eGK des Patienten (oder HBA/SMC eines berechtigten Heilberuflers) verschlüsselt werden
  - Für die privaten eGK/HBA-Schlüssel gibt es keine Backups!
  - Kryptographische Berechtigungskonzepte erforderlich, wenn ein Patient z.B. einem neuen Arzt dauerhaften Zugang (ohne eGK-Anwesenheit) auf Daten gewähren möchte
  - Umschlüsselungskonzepte notwendig, damit die Daten bei Verlust/Austausch der Karte zugänglich bleiben
- Aktuelle Konzepte: Patientenindividuelle Verschlüsselung, **jedoch mit einem Server-Schlüssel nach Authentisierung des Patienten oder eines berechtigten Arztes**

Nachrichtenbasierte Kommunikation über SOAP und inzwischen auch REST

- Sessionbasierte Anwendungen, wie z.B. Videokonsultation sind in der Architektur noch nicht berücksichtigt

Zwei-Schlüssel-Prinzip

- Für jeden Datenzugriff müssen 2 Chipkarten zusammenarbeiten
  - die eGK des Patienten
  - der HBA oder Institutionskarte (SMC-B) eines Leistungserbringers

- aber nicht zwangsweise gleichzeitig: Berechtigungskonzepte angedacht, so dass ein HBA/SMC mit Hilfe der eGK berechtigt wird, auch in Abwesenheit der eGK auf Daten zuzugreifen

- Ausnahmen davon: Zugriff des Versicherten (i.d.R. über mobile Geräte)

Logging zur Datenschutzkontrolle

- Alle Zugriffe auf Daten und möglichst alle Zugriffsversuche
- Erst loggen, dann zugreifen
- Log auf eGK (50 Einträge Ringspeicher)
- und (falls online-Anwendung) Fachdienst online

Technische Autorisierung (gesetzlich festgelegt)

- PIN-Eingabe für alle freiwilligen Anwendungen
- Zusätzlich zur C2C-Authentisierung eines HBA/SMC
- „Virtuelle“ PINs für jede Anwendung („Multireferenz-PIN“)
  - Es gibt nur **eine „reale“ Karten-PIN** der eGK („PIN.CH“)
  - jede Anwendung hat eine PIN-Referenz (vergleichbar mit einem Soft-Link unter Linux)
    - zeigt auf PIN.CH, hat aber eigenen Security Status
  - → nach PIN-Eingabe wird nur **eine** Anwendung freigegeben und **nicht global** alle Anwendungen auf die Karte
- Keine PIN-Eingabe für Notfalldaten
  - nur C2C-Authentisierung

Online Aktualisierung von Chipkarten durch CAMS

- Card Application Management System
- Authentifiziert sich über ein CV-Zertifikat gegenüber der Chipkarte
- CAMS darf nicht alles machen, definierte Rechte
- Authentifizierte Verbindung oder signiertes Datenpaket

Für jede „Datei“ und möglichem Kartenbefehl auf einer Chipkarte sind Rechte in Form einer ACL festgelegt

- PIN und/oder Authentisierung eines HBA/SMC mit bestimmtem Attribut (Arzt, Apotheker, Krankenhaus usw.) oder eines CAMS
- „Datei“: Elementary File (EF) mit Daten (z.B. Notfalldaten) oder Schlüssel (z.B. für die Authentisierung online)

Der Konnektor

Quelle Bild: KoCo Connector AG / CGM

Funktionen des Konnektors

- Netzkonnektor: VPN-Device
  - Sichere Netzanbindung in die Telematik-Infrastruktur
- Anwendungskonnektor:
  - Basisdienste
  - Module mit Fachlogik für E-Health Anwendungen
- Anwendungsproxy / -server
  - Keine direkte Verbindung der Praxis-IT in die TI
    - Schutz der Praxis-IT / Schutz der TI / Schutz der E-Health Anwendungen in der TI
    - Aber sehr wohl DURCH die TI zu anderen Netzen und Anwendungen
  - PVS steuert E-Health Anwendung über Modul im Konnektor
  - Modul im Konnektor steuert Intermediäre / Fachdienste in der TI
- Anbindung und Steuerung der Kartenterminals

Funktionen des Konnektors

- Steuerung der Chipkarten
- Anbieten von Basis-Diensten, wie Ver-/Entschlüsselung, Authentisierung
- Signaturanwendungskomponente
  (Erzeugen und Prüfen von elektronischen Signaturen)
- Vermitteln einer sicheren Internetverbindung
  → (über Security Gateway in der TI)
- Verbindung zu anderen mit der TI verbundenen Netzen und Anwendungen

Funktionen des Konnektors

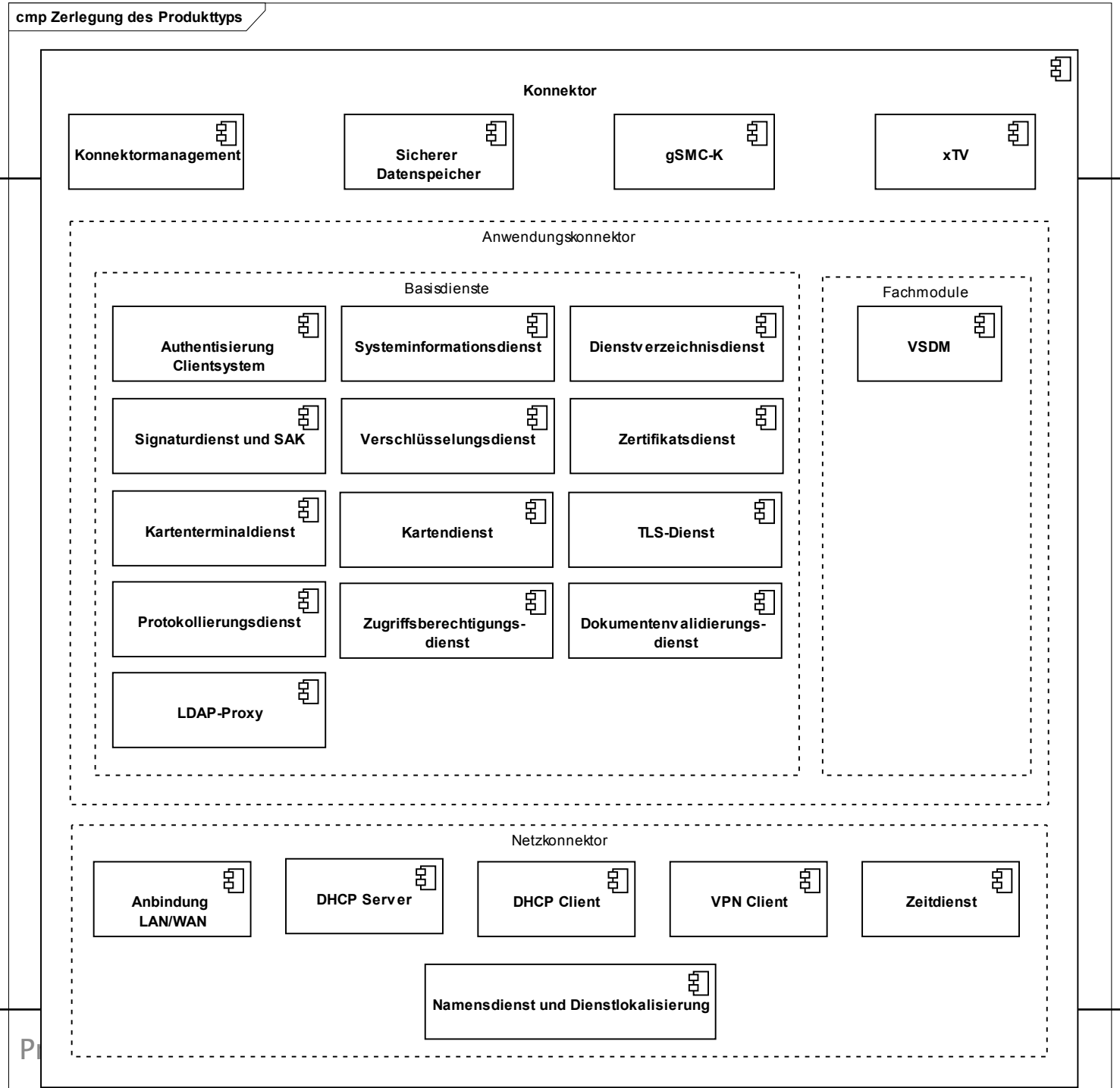
Konzeption als modularer Konnektor

- Basisdienste
  - Stehen den Modulen, manche sogar dem PVS zur Verfügung

- Jede Anwendung (z.B. NFDM) hat im Konnektor ein eigenes Fachmodul, welches die Fachlogik der Anwendung implementiert

- PVS schickt SOAP-Aufruf an Konnektor, Modul nutzt die Basisdienste

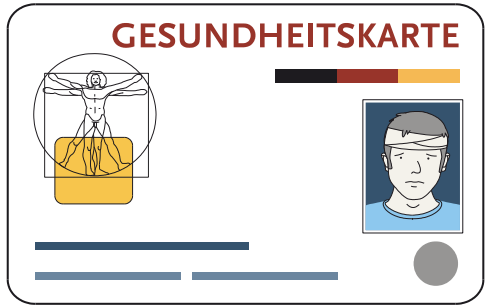
Der Konnektor



Quelle: Gematik GmbH,
Konnektor Spezifikation V4.7.0

Modularer Konnektor

- Idee: Modul „scriptet“ Basisdienst-Aufrufe mit anwendungsspezifischen Parametern und Logik
  - Z.B. Notfalldaten auf eGK schreiben
    - Prüfung Gültigkeit eGK / HBA
    - Schema-Prüfung XML-Dokument NFD
    - Signatur der NFD, inkl. online-Validierung der Signatur
    - C2C-Authentisierung SMC←→eGK
    - Ggf. PIN-Eingabe für eGK, falls NFDM-PIN aktiv
    - Schreiben der signierten NFD auf eGK



Elektronische Gesundheitskarten (eGK)

- Werden von Krankenkassen ausgegeben, mit Foto
- PIN (6stellig)
- 96kB-128kB geschützter Speicher
- sicherheitszertifizierter Chip und Betriebssystem (COS)
- Nicht-auslesbare private Schlüssel und öffentliche Zertifikate (CVC und X.509-Zertifikate) zum Nachweis der Echtheit der Karte, technische Signatur/Authentisierung, Ver-/Entschlüsselung von Daten
- Root-CV-Zertifikate zur Validierung (Prüfung) der C2C-Authentisierung eines HBA/SMC oder CAMS
- ~~Option für~~ kontaktlose NFC-Schnittstelle sowie qualifizierte elektronische Signatur (werden nicht genutzt)
  - NFC ab Dezember 2019 Pflicht
  - Bisher wird die PIN der eGK dem Versicherten (noch) nicht mitgeteilt

HBA (Heilberufsausweise) und SMC (Institutionskarten)

© Bundesärztekammer

- Werden von den Kammern (HBA) bzw. Kassen(zahn)ärztlichen Vereinigungen / Krankenhausgesellschaften (SMC-B) ausgegeben
  - HBAs mit Foto
- HBA: Signaturkarte: rechtsverbindliche „qualifizierte“ elektronische Signatur gemäß eIDAS-EU-Verordnung
- Card Verifiable Zertifikate (CVC) mit Berufsattribut zur Authentisierung und Autorisierung gegenüber der eGK

HBA (Heilberufsausweise) und SMC (Institutionskarten)

- X.509 Public Key Zertifikate inkl. Berufsattribut und Schlüssel für
  - Qualifizierte elektronische Signatur
  - Authentisierung (z.B. im Rahmen einer TLS-Verbindung)
  - Ver-/Entschlüsselung von Daten (inzwischen nur HBA, außerhalb der TI)

- 2 PINs (6stellig): für Signatur und alle anderen Funktionen
  - PUK (8stellig) zur Entsperrung der PIN

- sicherheitszertifizierter Chip und Betriebssystem (COS)

- zusätzlich (für HBA, noch nicht SMC) kontaktlose Schnittstelle (RFID/NFC, ISO14443)

Stationäre Kartenterminals

- Kommunikation mit Konnektor über Ethernet / TLS-abgesichert
- Eigene kryptographische Identität (Pairing mit Konnektor)
- 2 Einsteckplätze: HBA und eGK
- PIN-Pad
- Kleiner Bildschirm für Statusmeldungen (z.B. „Bitte geben Sie Ihre PIN zum Schreiben von Notfalldaten ein“)
- Abgeschirmt, sicherheitszertifiziert

Weitere Chipkarten (in verschiedenen Formen)

- SMC-KT: Kryptographische Identität eines Kartenterminals
- SMC-K: Kryptographische Identität eines Konnektors
- (künftig) HSM-K: Hardware Security Modul (eine übergroße und schnelle Chipkarte z.B. als 19“-Gerät) → SMC für große Krankenhäuser (noch nicht verfügbar)

Warum Chipkarten?
→ Sichere, unauslesbare, unkopierbare Schlüsselspeicher
→ Extreme Sicherheitsmaßnahmen
→ die für die langfristige Verschlüsselung von Patientendaten leider nicht mehr genutzt werden

Mobile Kartenterminals

- Zwischenspeicher zur Speicherung mobil erfasster Daten
- Daten werden für HBA des Arztes verschlüsselt gespeichert
- (viel zu kleiner) Bildschirm gemäß Spec
- Kleiner integrierter Anwendungskonnektor mit Fachlogik
- → Unzureichend für medizinische Anwendungen, wie z.B. Notfalldaten.

"**Primärsysteme**" = Systeme der Leistungserbringer

- Praxisverwaltungssystem (PVS), AVS, Krankenhausinformationssystem (KIS) usw.

- Keine direkte Verbindung zur TI, nachrichtenbasierte (SOAP) Kommunikation über Konnektor
  - Ausnahme bzw. neues Paradigma: eRezept-Anwendung
    → Direkte Verbindung des Fachmoduls des Primärsystems auf einen Fachdienst der TI

- Verbindung mit Konnektor über TLS1.2 mit *möglichst* gegenseitiger Authentisierung

- Keine direkte Steuerung von Fachdiensten der TI
  - Anwendungen nur über Module des Konnektors, welche dann die eigentlichen Fachdienste der TI steuern
  - Ausnahme / neues Paradigma: eRezept

- „Implementierungsleitfäden": Empfehlungen, wie Primärsysteme die Anwendungen der TI nutzen sollen, z.B. User-Interface

Anwendungen der Versicherten

„Umgebung zur Wahrnehmung der Rechte des Versicherten“ („UzWdRdV“)
- Automaten-artige Geräte, die irgendwo stehen sollten

„Anwendungen der Versicherten in einer Leistungserbringerumgebung"
- Geräte, die im geschützten Bereich von Einrichtungen des Gesundheitswesens (z.B. Arztpraxen, Krankenhäuser, Apotheken) aufgestellt werden sollen
- Dort können Versicherte künftig Daten lesen, verbergen/sichtbar machen, Rechte vergeben, Logs lesen, Organspendeerklärungen schreiben/löschen/verbergen usw

“Umgebung im Auftrag der Kostenträger“
- wie o.g. allerdings nicht in der Umgebung einer Einrichtung des Gesundheitswesens
- Weniger Rechte: keine med. Daten lesen / schreiben. Logs lesen und Anwendungen verbergen / sichtbar machen. Ggf. Rechteverwaltung

- PIN@home
  - Nutzung von bestimmten Anwendungen der TI zu Hause. Handelsüblicher Kartenleser erforderlich

→ Apps in Smartphones

Aktuelle Konzeption für ein User Interface für Versicherte

- Nutzung von Tablets und Smartphones
- Einführung mit elektronischer Patientenakte (wird später in der Vorlesung behandelt)
- eRezept
- Digitale Identitäten

Aktueller Stand der TI (Anfang 2022)

Was ist schon da?

- Elektronische Gesundheitskarten der Generation 2.1
  - G1 und G1+ sind inzwischen ungültig, Grund ist, vom BSI nicht mehr als geeignet eingestufte Kryptoalgorithmen. G2 weiterhin im Umlauf und gültig
  - Ab Dez. 2019 (ok, jetzt ganz langsam...): eGKs mit NFC-Schnittstelle
  - KEINE flächendeckende PIN-Brief Ausgabe → medizinische Anwendungen können effektiv noch nicht genutzt werden.

- Heilberufsausweise nach Generation 2.1 (und einige Vorläuferkarten, nicht eGK-kompatibel)
- Kartenterminals (KT), die eGKs einlesen können
- Inzwischen ~~4~~ 3 Konnektoren zugelassen
- Versichertenstammdaten online
- Sicherer Internetzugang, Zugang zum anderen Netzen im Gesundheitswesen, Signaturen
- Die meisten Arztpraxen /Krankenhäuser sind mit der TI verbunden, Rollout gilt als abgeschlossen

Aktueller Stand der TI (Anfang 2022)

Was ist da?

- “eHealth PTV-4 Konnektoren“, mit Support für Signatur, KIM, Notfalldaten, eMedikationsplan, ePA
- “Kommunikation im Medizinwesen“ (KIM) → sichere E-Mail wird langsam ausgerollt
- ~~Authentisierung gegenüber einem Server über TLS~~
- Notfalldatenmanagement (NFDM)
- Elektronische Patientenakte u.a. mit Mutterpass, Impfpass
- eMedikationsplan und AMTS

Was kommt demnächst?

- eRezept und eAU (kurz vor Einführung)
- TI-Messenger

Strategie zur Weiterentwicklung der TI

Neuestes Digitalisierungsgesetz (DVPMG)

- „Zukunftskonnektor“: Software-Konnektor und/oder App
  - Derzeitiger Hardware-Konnektor zu unflexibel und teuer, damit können unmöglich 2 Millionen Angehörige weiterer Heilberufe und Gesundheitsfachberufe angeschlossen werden
- Digitale Identitäten, zusätzlich zu eGKs und HBAs
  - Schlüsselmaterial in Smartphones, Tablets, Computer in Kombination mit Identity Providern
- Patientenkurzakte statt Notfalldaten
- Alles Online statt Offline-Anwendungen und Speicherung auf der eGK
- Anschluss von Pflege, Physiotherapie, Hebammen usw. an die TI
- Anschluss von Digitalen Gesundheits- und Pflegeanwendungen (DiGA / DiPA) an die ePA

Strategie zur Weiterentwicklung der TI

Die Gematik hat ein Strategiepapier für eine „TI 2.0“ veröffentlicht, geplant ab 2025

- Es ist aber unklar, ob alles so kommt, wie derzeit geplant (und wann…)
- Statt Zukunftskonnektor → gar kein Konnektor
- Statt geschlossenes Netz (VPN) → alle Dienste über das Internet erreichbar
- Statt eGKs und HBAs: nur Authentisierung gegenüber Identity Provider, Nutzung von Fachdiensten mit openID Connect Tokens
- Fachdienste sollen Policy-Dokumente enthalten, welche das jeweilige Sicherheitsniveau attestieren