gematik

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Sichere Telematikanwendungen der elektronischen Gesundheitskarte

Sven Marx

gematik - Gesellschaft für Telematikanwendungen
der Gesundheitskarte mbH
Friedrichstraße 136
10117 Berlin

Köln, 06.05.2009

Agenda

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

§ Die elektronische Gesundheitskarte

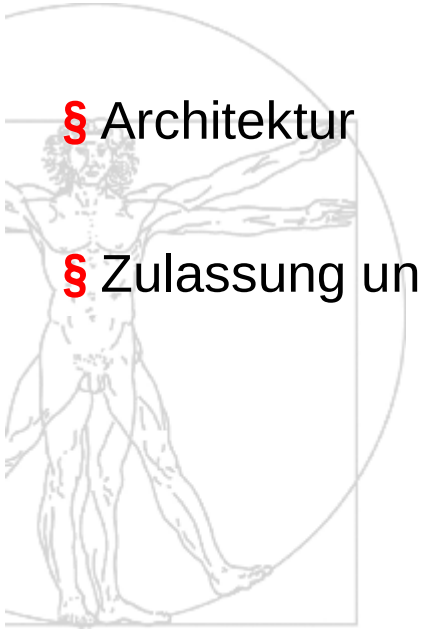
§ Beteiligte, Aufgaben und Grundlagen

§ Anwendungen mit der elektronischen Gesundheitskarte

§ Datenschutz & Datensicherheit

§ Architektur

§ Zulassung und Zertifizierung von Komponenten



gematik

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

§Die elektronische Gesundheitskarte

Elektronische Gesundheitskarte (eGK)

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Weiterentwicklung der Krankenversichertenkarte zur elektronischen Gesundheitskarte zur

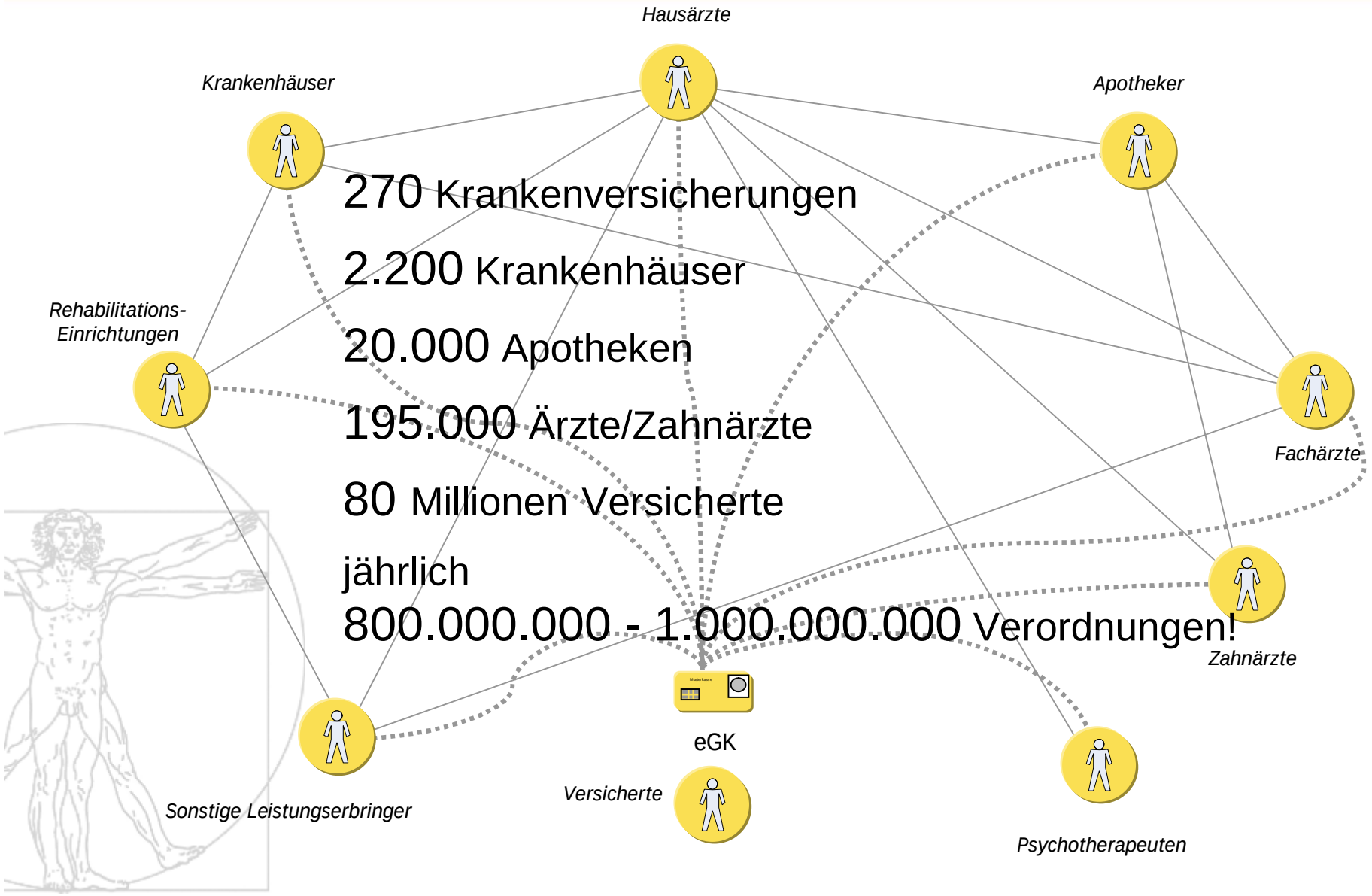
Verbesserung der

Wirtschaftlichkeit + **Transparenz** + **Qualität**

der Behandlung

Das Ziel: Sektorenübergreifende Vernetzung im Gesundheitswesen

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

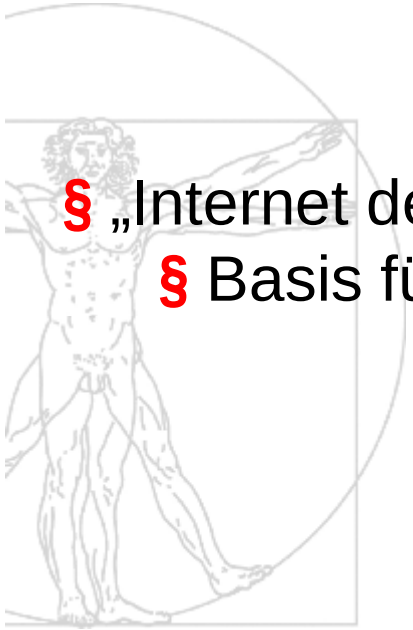


Das eGK Projekt ist ein Infrastrukturprojekt

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

- Kein „Kartenprojekt“: Im Vordergrund steht der Aufbau einer Telematikinfrastruktur

- Elektronische Gesundheitskarte (eGK) und der Heilberufsausweis (HBA) sind die Zugangsschlüssel

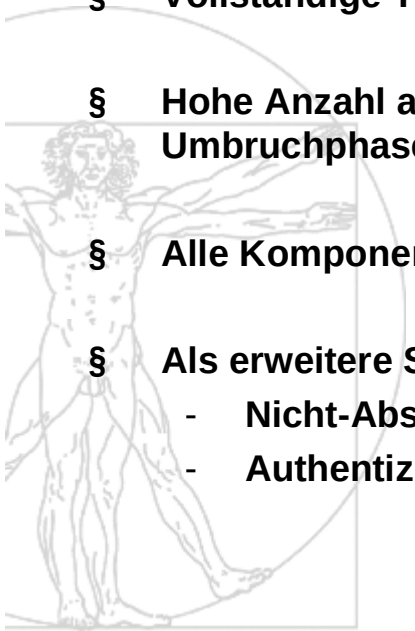


- „Internet des Gesundheitswesens“
  - Basis für weitere „Mehrwertanwendungen“

Die Herausforderung

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

- **Es werden Daten mit hohem und sehr hohem Schutzbedarf verarbeitet**
- **Sehr große Nutzerzahl (ohne IT-Affinität – „normale IT-User“)**
- **Etablierte Mechanismen des Risiko-Managements sind nicht oder nur sehr eingeschränkt anwendbar.**
- **Das Projekt erfährt eine sehr hohe öffentliche Aufmerksamkeit.**
- **Vollständige Transparenz aller Spezifikationen**
- **Hohe Anzahl an Beteiligten in einer Branche, die – unabhängig vom Projekt - durch eine Umbruchphase gekennzeichnet ist.**
- **Alle Komponenten müssen wettbewerbsneutral spezifiziert werden.**
- **Als erweitere Schutzziele müssen realisiert werden:**
  - **Nicht-Abstreitbarkeit und**
  - **Authentizität**



gematik

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

§ Beteiligte, Aufgaben und Grundlagen

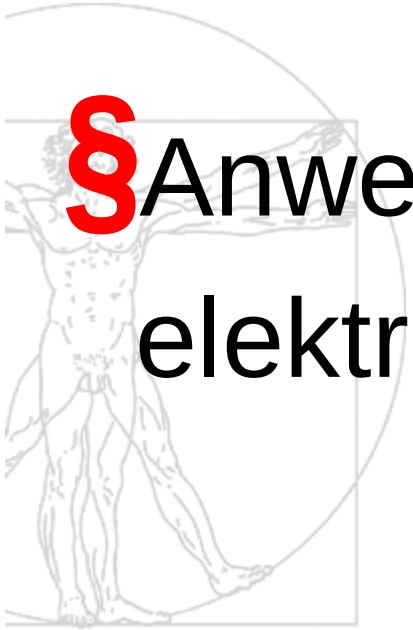
Beteiligte, Aufgaben und Grundlagen

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Gesellschafter	• Leistungserbringer erarbeiten unter begleitender Beratung der Kostenträger die freiwilligen Anwendungen	**§ 291a SGB V** **Gesellschaftsvertrag** **Grundsatzpositionen zur Telematik**
gematik	• Spezifiziert und zertifiziert • Teilaufgaben bei Einführung und Betrieb sektorübergreifender Komponenten • Stellt Interoperabilität aller Telematikkomponenten sicher • Stellt Wahrung der Patientenrechte sicher	**§ 291b SGB V** **Gesellschaftsvertrag**
Industrie	• Fertigt Komponenten nach gematik-Spezifikationen	
Testregionen	• Umsetzung der Telematik nach gematik-Vorgaben	**Rahmenvertrag** **Gesamtkonzept** **Rechtsverordnung**
BMG	• Rechtsaufsicht und Weisungen im Rahmen der Ersatzvornahme	**SGB V** **Rechtsverordnung**

gematik

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH



§Anwendungen mit der elektronischen Gesundheitskarte

Pflichtanwendungen mit der eGK nach § 291a SGB V

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

- § Versichertenstammdaten
  (Berechtigungsnachweis zur Inanspruchnahme von medizinischen Leistungen)

- § Elektronisches Rezept (eRezept)
  (Übermittlung ärztlicher Verordnungen mit Hilfe der eGK)

- § EHIC - European Health Insurance Card
  (Europäische Krankenversichertenkarte, zur Inanspruchnahme medizinischer Leistungen in Mitgliedsstaaten der Europäischen Union)

Freiwillige
eGK-Anwendungen nach § 291a SGB V

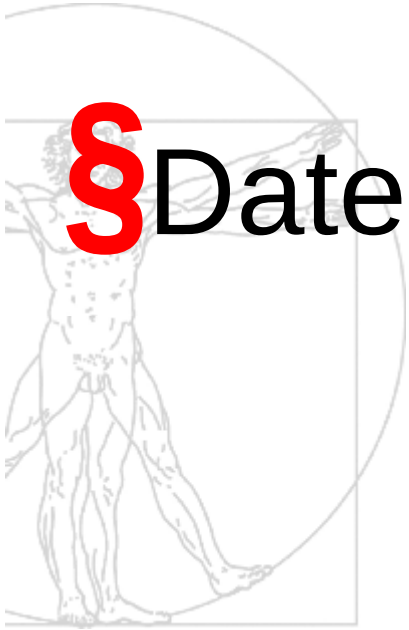
gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

- § Daten für die Notfallversorgung
  (z.B. Grunderkrankungen, individuelle Arzneimittelunverträglichkeiten und Allergien)
- § Elektronischer Arztbrief
  (z.B. Befunde, Diagnosen, Therapieempfehlungen, Behandlungsberichte)
- § Arzneimitteltherapiesicherheit
  (Dokumentation der vom Versicherten eingenommenen Arzneimittel durch Ärzte und Apotheker)
- § Elektronische Patientenakte
  (z.B. Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte, Röntgenbilder sowie Impfungen)
- § Eigene Dokumentationen des Versicherten
  (z.B. über einen Krankheitsverlauf, Diabetestagebuch)
- § Patientenquittung
  (Informationen in verständlicher Form über Leistungen und Kosten einer Behandlung)

Im Gegensatz zu den Pflichtanwendungen (Versichertenstammdaten, eRezept, EHIC) gilt bei den freiwilligen Anwendungen, dass der Versicherte ihnen zustimmen und sein Einverständnis erklären muss!

gematik

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH



§ Datenschutz & Datensicherheit

Datenschutz & Datensicherheit

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

- **Patient als Herr seiner Daten**

  Nutzung freiwilliger Anwendungen, z.B. elektronische Patientenakte, nur mit PIN-Bestätigung möglich

- **Protokollierung**

  Prozesse transparent für Patienten (wer, was, wann)

- **Physische Abschottung/Erkennung externer Angriffe**

  Transport der Daten erfolgt über geschlossenes Netzwerk, das Zugriff auf Daten unterbindet

- **Authentifizierung**

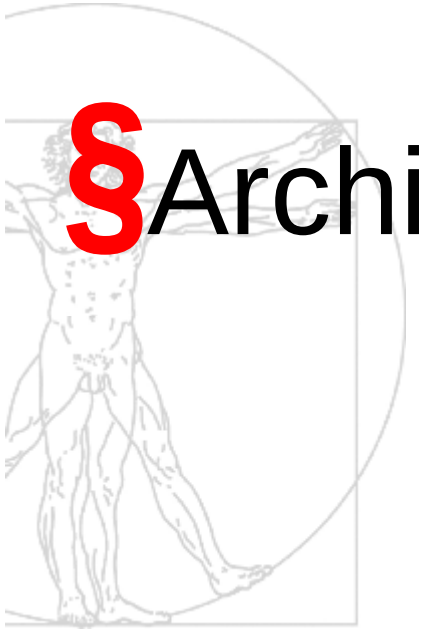
  Identitäten der Handelnden werden überprüft (z.B. eGK – HBA – Authentifizierung)

- **Kryptographie**

  Verschlüsselung von Informationen

gematik

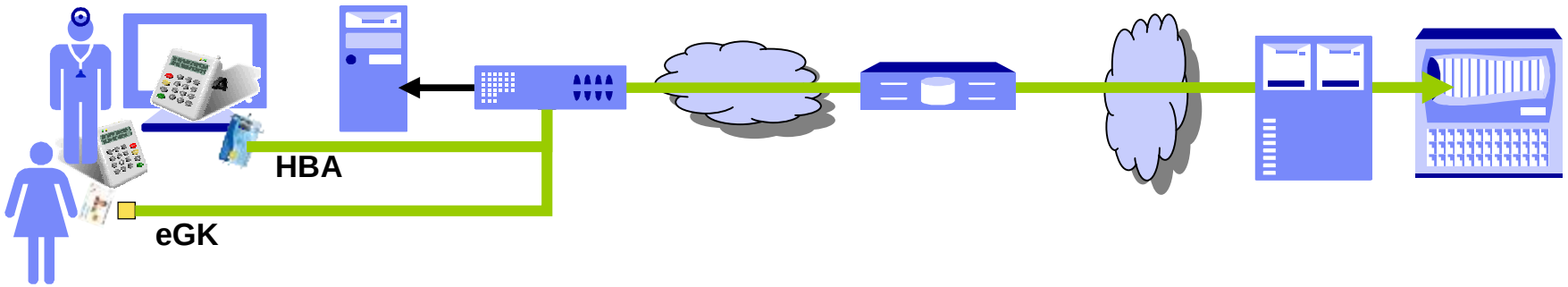
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

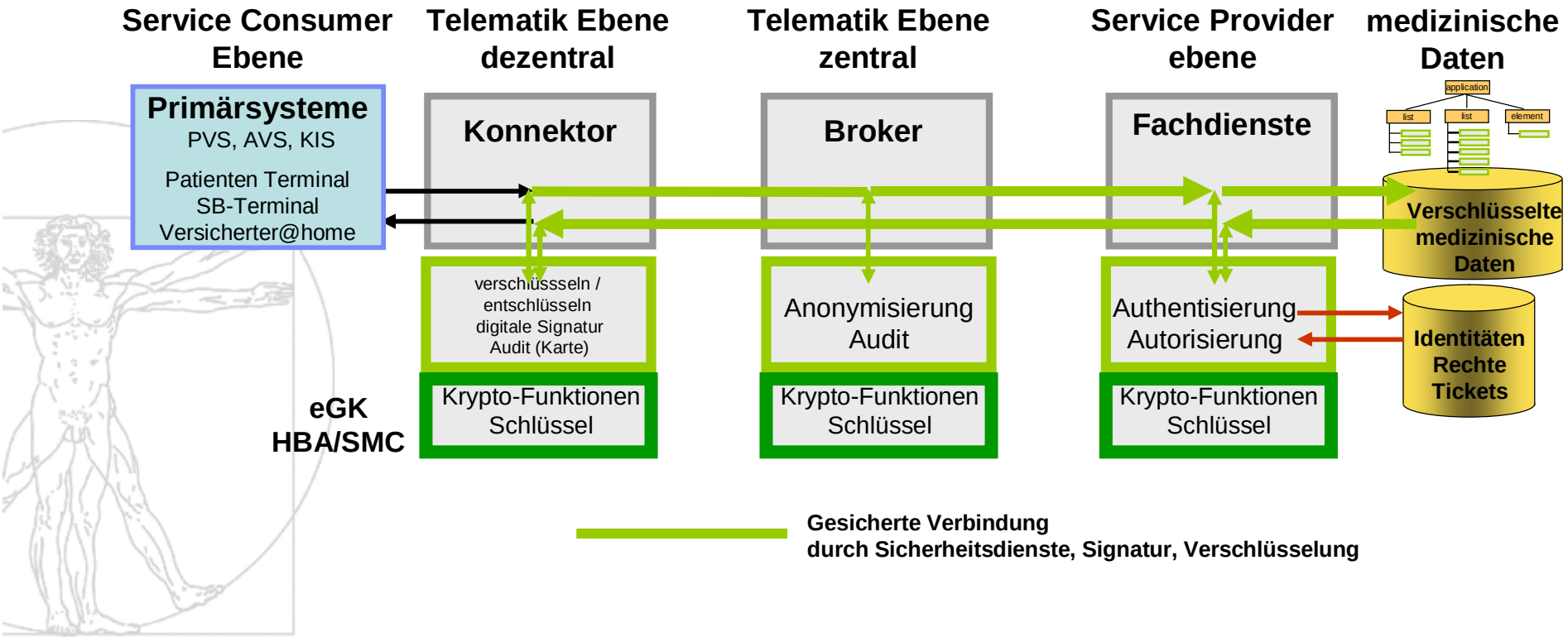


§Architektur

Technische Realisierung

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH



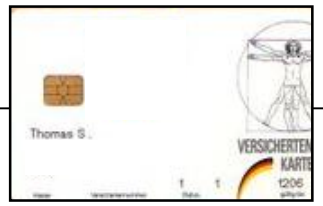


Kartentypen

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Alt: Krankenversichertenkarte

- Speicherkarte (Memory Card) ohne Betriebssystem
- 256 Bytes Speicher
- Statische Sicherheitslogik

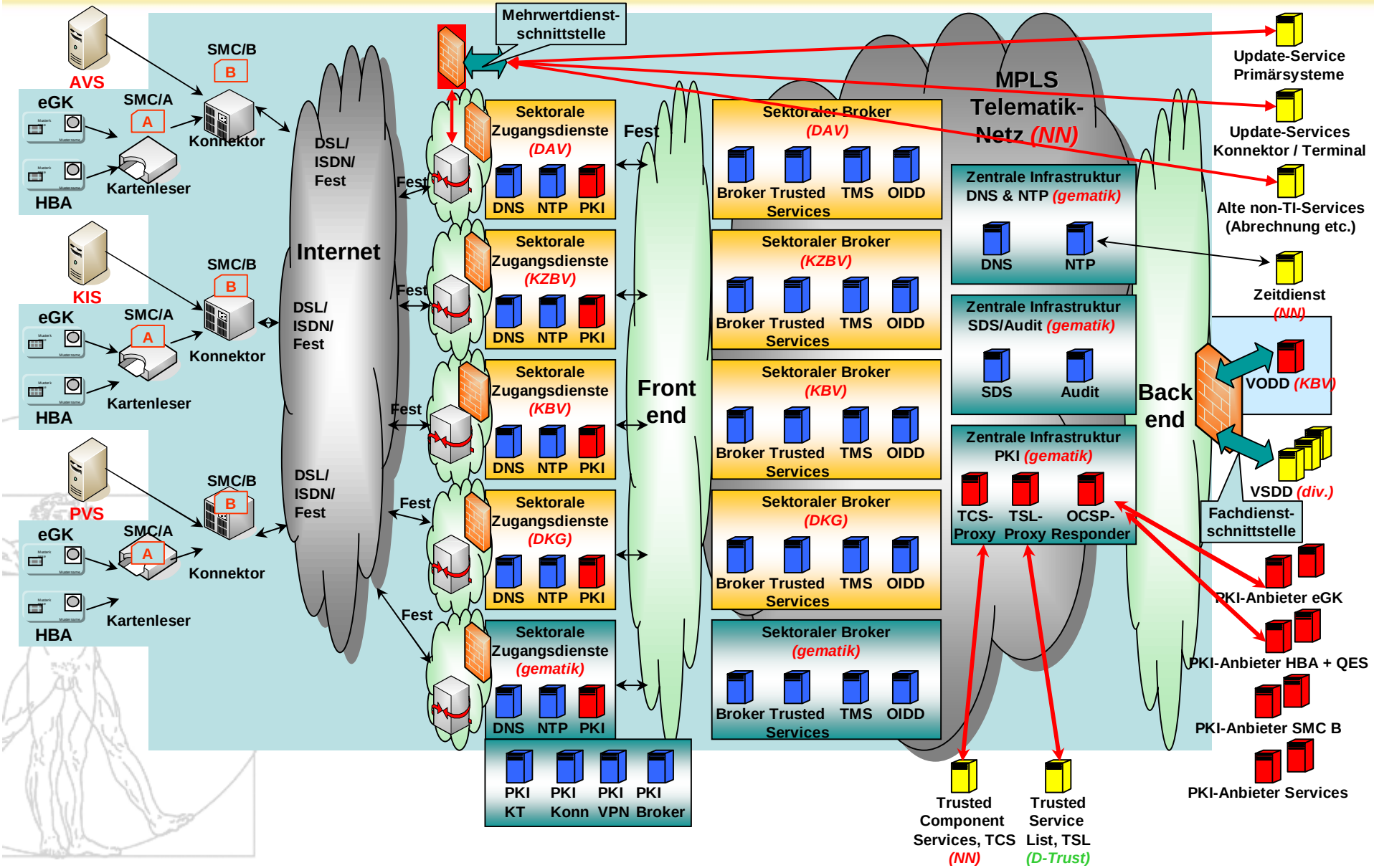


Neu: eGK

- Mikroprozessorkarte (Smart Card) mit Betriebssystem
- frei konfigurierbare Anwendungen
- 65.536 Bytes Speicher
- Konfigurierbare Sicherheitsfunktionen:
  - Authentifikation
  - Verschlüsselung
  - Signatur

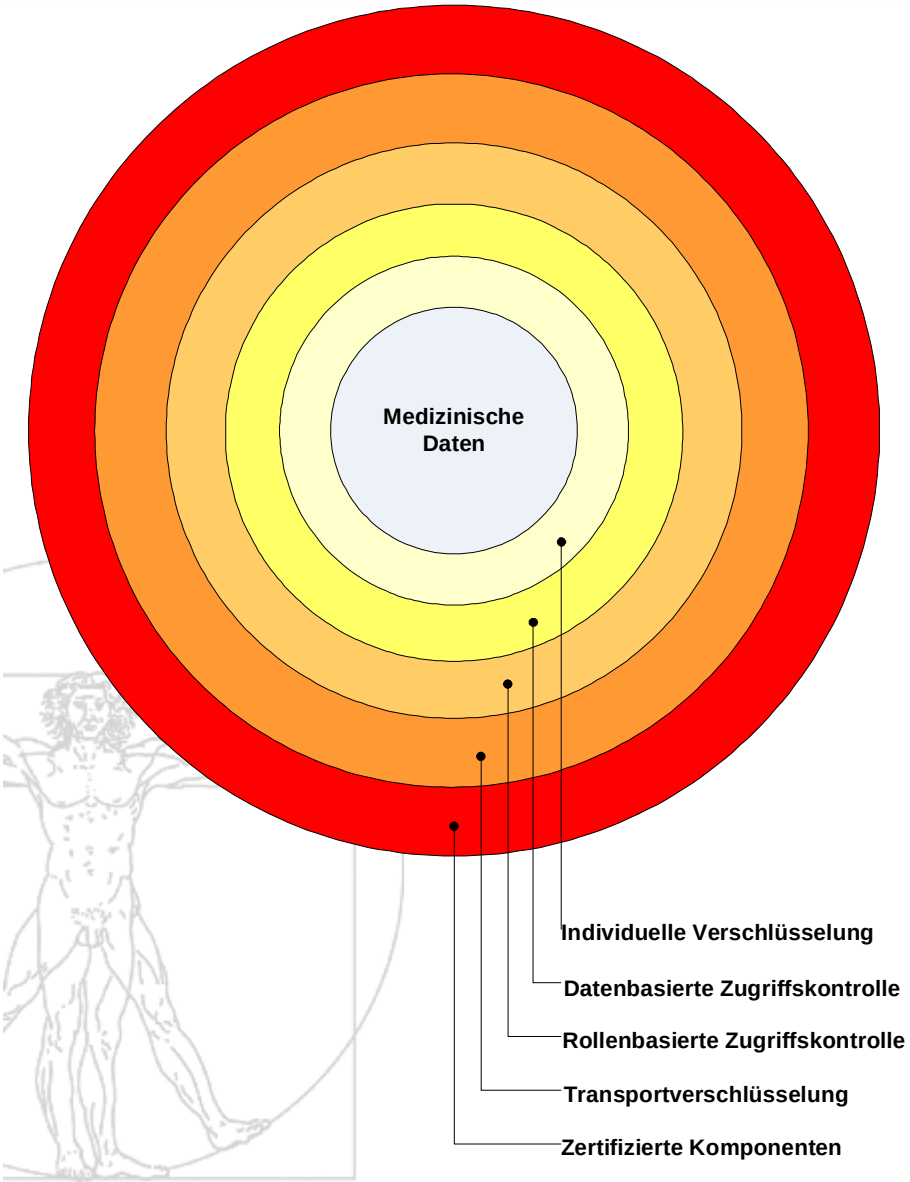
Betriebsumgebung Telematikinfrastruktur

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH



Mehrschichtige Sicherheitsmechanismen in der Telematikinfrastruktur

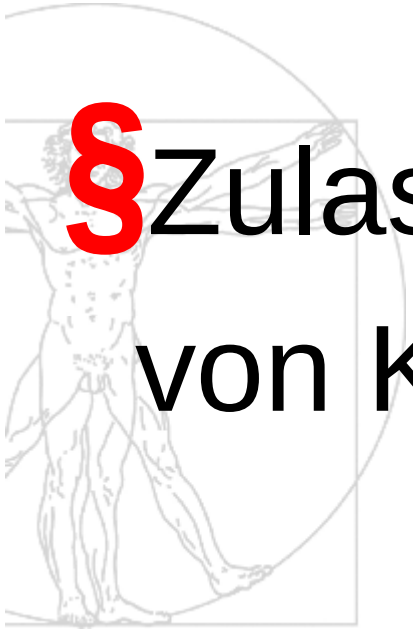
gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH



- § Zugriffe erfolgen über abgesicherte, zertifizierte und zugelassene Komponenten (Konnektor, Kartenterminals, Karten)
- § Kommunikation erfolgt über abgesicherte Kanäle - Client- und Serverauthentifizierung
- § Zugriffe dürfen nur durch Personen erfolgen, die für die Art des Zugriffs zugelassen sind. Die Identifikation erfolgt über den HBA.
- § Zugriffe dürfen nur nach Autorisierung durch den Versicherten erfolgen. Die Autorisierung erfolgt entweder durch die eGK des Versicherten oder durch zuvor explizit vergebene Berechtigung.
- § Die individuelle Verschlüsselung der Daten wird erst auf den Systemen des jeweiligen Leistungserbringers entfernt.

gematik

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH



§Zulassung und Zertifizierung von Komponenten

Systematik der Zulassungsarten nach dem Gesetz

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Zulassungsdienstleistung		Zulassungsnehmer	Zulassungsvoraussetzungen
Komponenten- u. Dienstezulassung *gemäß § 291b Abs. 1a SGB V*	**Dezentrale Komponenten**	Komponentenhersteller	1. Bestätigung der Funktionsfähigkeit, Interoperabilität u. Sicherheit durch Testlabor der gematik 2. IT-Sicherheitszertifizierung u. Bestätigung (nach SigG) durch BSI bzw. eine von der BNetzA anerkannte Prüf- und Bestätigungsstelle 3. Bestätigung der bestandenen elektrischen u. physikalischen Tests durch Prüfstellen
	Zentrale Komponenten	Komponentenhersteller	1. Bestätigung der Funktionsfähigkeit, Interoperabilität u. Sicherheit durch Testlabor der gematik bzw. in der Betriebsumgebung des Betreibers ***2. Bestätigung der sicherheitstechnischen und datenschutzrechtlichen Eignung durch einen unabhängigen Sicherheitsgutachter (unabhängigen Begutachtung des Sicherheitskonzepts) u. Prüfung dieser Gutachten durch gematik-Sicherheit***
	Zentrale Dienste u. Fachdienste	Technischer Diensteprovider	
	eGK-Herausgabeprozesse	eGK-Herausgeber	1. Absolvieren sicherheitstechnischer Audits, die durch akkreditierte Sicherheitsgutachter durchgeführt werden, u. Prüfung dieser Gutachten durch gematik-Zulassungsstelle
Anbieterzulassung *gemäß § 291b Abs. 1b SGB V*		Anbieter	1. Nachweis der Verwendung zugelassener Komponenten und Dienste durch Zulassungsbescheid der Komponenten- u. Dienstezulassung ***2. Bestätigung der sicherheitstechnischen und datenschutzrechtlichen Eignung durch einen unabhängigen Sicherheitsgutachter (unabhängigen Begutachtung des Sicherheitskonzepts) u. Prüfung dieser Gutachten durch gematik-Sicherheit*** 3. Bestätigung der Verfügbarkeit der Betriebsleistung durch Prüfung des Betriebs- u. des Notfallskonzeptes durch gematik-Betrieb 4. Vertragliche Verpflichtung des Anbieters, die Rahmenbedingungen für Betriebsleistungen der gematik einzuhalten

Zulassungskriterium für Dienste- und Anbieterzulassung

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Bestätigung der sicherheitstechnischen und datenschutzrechtlichen Eignung durch einen unabhängigen Sicherheitsgutachter (unabhängige Begutachtung des Sicherheitskonzepts) u. Prüfung dieser Gutachten durch gematik-Sicherheit

- **Dienstezulassung**

  Vorlage eines durch einen unabhängigen Sicherheitsgutachter erstellten Sicherheitsgutachtens, in dem der Gutachter bestätigt, dass alle Anforderungen an einen Dienst und speziell an diesen Dienst in einem Sicherheitskonzept betrachtet und umgesetzt sind.

- **Anbieterzulassung**

  Vorlage eines durch einen unabhängigen Sicherheitsgutachter erstellten Sicherheitsgutachtens, in dem der Gutachter bestätigt, dass alle Anforderungen an einen Anbieter (insb. das Informationssicherheits- und Datenschutz-managementsystem) in einem Sicherheitskonzept betrachtet und umgesetzt sind.

Welche Qualifikation benötigen Sicherheitsgutachter?

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Basisqualifikation

BSI gelisteter akkreditierter Sicherheitsdienstleister

(Das BSI plant, eine Liste aller beim BSI akkreditierten IT-Sicherheitsdienstleister zu veröffentlichen. In einem Akkreditierungsverfahren werden diese Dienstleister ihre Vertrauenswürdigkeit und Fachkompetenz gegenüber dem BSI nachweisen müssen.)

ODER

ISO-27001-Auditor

(Lizenz vom BSI [ISO-27001 auf der Basis von IT-Grundschutz zertifizierte Auditoren] oder anderen anerkannten Zertifizierungsstellen)

ODER

IT-Grundschutz-Auditor

(Lizenz vom BSI)

UND

- **Zusatzqualifikation „Telematikinfrastruktur“**

Kompakte Schulung zur Gesetzeslage, den speziellen Datenschutzaspekten, den technologischen Grundlagen inkl. Sicherheitsarchitektur.
Die konkreten Details werden derzeit noch von Seiten der gematik erarbeitet und abgestimmt.

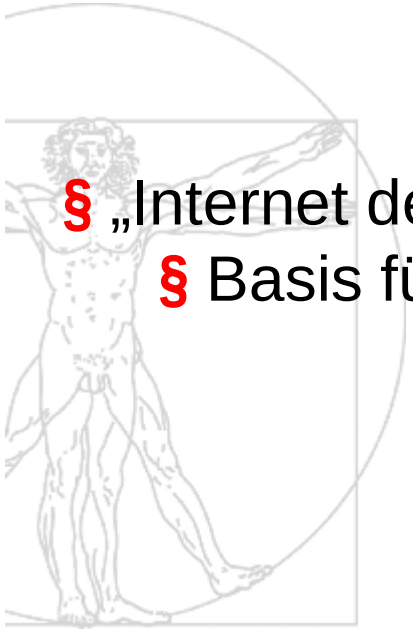
§Fazit

Das eGK Projekt ist ein Infrastrukturprojekt

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

- Kein „Kartenprojekt“: Im Vordergrund steht der Aufbau einer Telematikinfrastruktur

- Elektronische Gesundheitskarte (eGK) und der Heilberufsausweis (HBA) sind die Zugangsschlüssel



- „Internet des Gesundheitswesens“
  - Basis für weitere „Mehrwertanwendungen“

Vergleich der Konzepte

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Parameter	Offene gematik TI		Proprietäre TI	
Vorbereitungsaufwand	Hoch. Offenlegung und Konsentierung aller Spezifikationen. Vorbereitung für Test und Zulassung.	↑	Gering - mittel	→
Beschaffungs- und Erhaltungskosten	Dauerhafte Optimierung der Beschaffungskosten durch Anbieterwettbewerb	↓	Kein oder eingeschränkter Wettbewerb	↑
Sicherheit und Datenschutz	Bestätigung durch unabhängige Prüfer	↓	Üblicherweise Lieferantenerklärung	↑
Zugang für zusätzliche Lieferanten und Systemdienstleister	Komponenten basieren auf offenen Spezifikationen. Zulassungsverfahren.	↓	Eingeschränkt	↑
Zugang für zusätzliche Dienste und Dienstanbieter	Offene TI. Zulassungsverfahren.	↓	Eingeschränkt	→
Skalierbarkeit Dienste	Von low-end bis high-security, reliabilty	↓	High-security nur mit sicherem Medium	→

Weitere Informationen zu den Themen Datenschutz und Informationssicherheit

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

- **Informationen zur Sicherheitsarchitektur finden Sie auf der WebSite der gematik unter http://www.gematik.de/ (Aktuelles Release 2.3.4)**

- **Eine Grundlageneinführung zu den verwendeten Sicherheitsmechanismen kann das Whitepaper Sicherheit geben:**

  http://gematik.de/upload/gematik_whitepaper_sicherheit_3571.pdf

Vielen Dank für Ihre Aufmerksamkeit

gematik

Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

info@gematik.de ▪ **www.gematik.de**