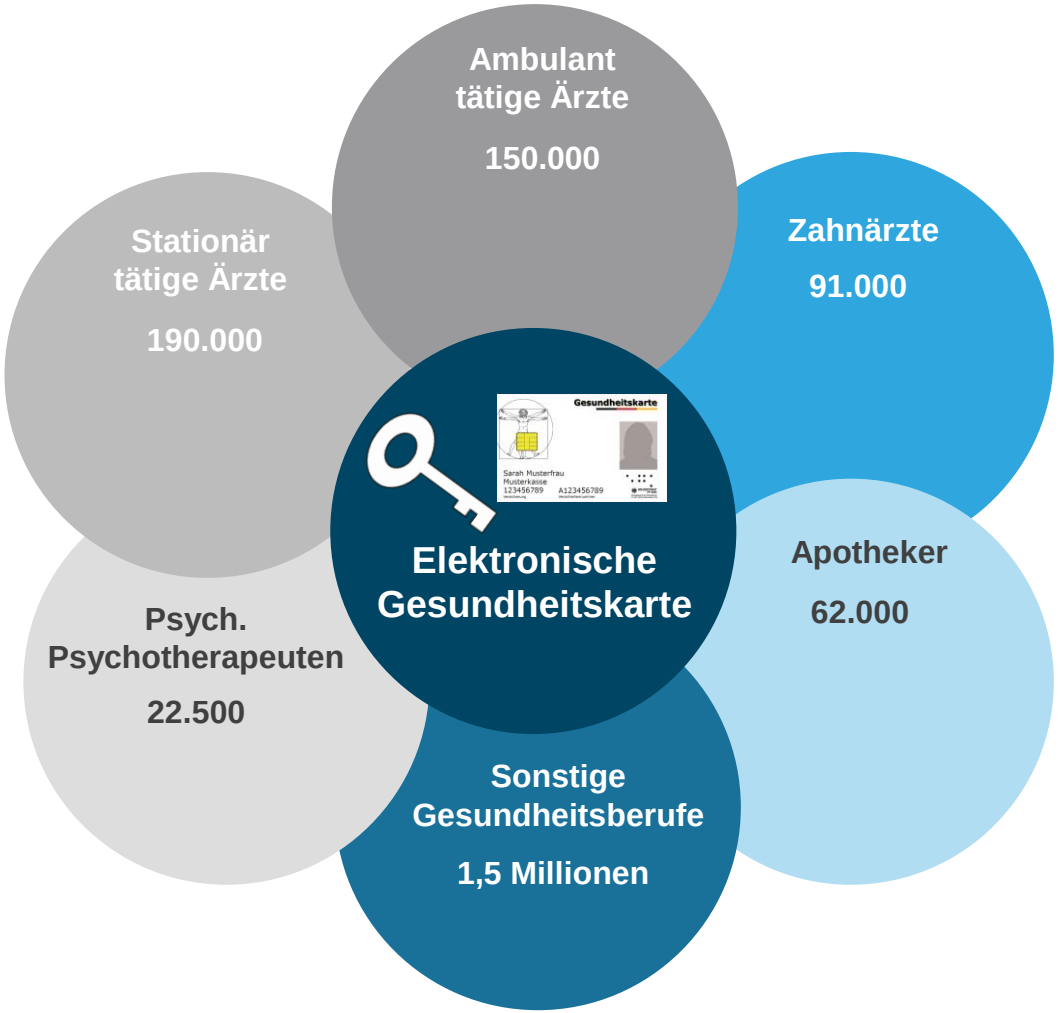
Datenschutz und Informationssicherheit in der Telematikinfrastruktur

Holm Diening, Abteilungsleiter Datenschutz und Informationssicherheit
gematik | Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH | Friedrichstraße 136 | 10117 Berlin

Das deutsche Gesundheitswesen

- **82,2** Millionen Einwohner
- **86%** (~70 Millionen) gesetzlich Versicherte
- **113** gesetzliche Krankenkassen
- **102.000** Arztpraxen
- **44.500** Zahnarztpraxen
- **20.500** Psychologische Psychotherapeutenpraxen
- **2.000** Krankenhäuser
- **20.500** Apotheken
- **1.150** Vorsorge- oder Rehaeinrichtungen

Deutsches Gesundheitswesen



Projekte Online-Rollout

Basis-Telematikinfrastruktur

Spitzenverband KBV

Stufe 1

Versicherten-stammdaten-management (VSDM)

Spitzenverband

Stufe 1

Qualifizierte elektronische Signatur (QES)

KBV Spitzenverband

Stufe 1

Kommunikation Leistungserbringer (KOM-LE)

KBV

Stufe 2.1

Notfalldaten-management (NFDM)

Bundesärztekammer

Stufe 2.1

Gesundheitsdaten-dienste/elektronische Fallakte (GDD/EFA)

Deutsche Krankenhaus Gesellschaft DKG

Stufe 2.1

eMedikationsplan (eMP)/ Arzneimittel-therapiesicherheit (AMTS)

Bundesärztekammer DAV

Stufe 2.1

Anwendungen des Versicherten (AdV)

Spitzenverband

Stufe 2.1

ePatientenakte (ePA)/ ePatientenfach (ePF)

gematik

Stufe 2.2

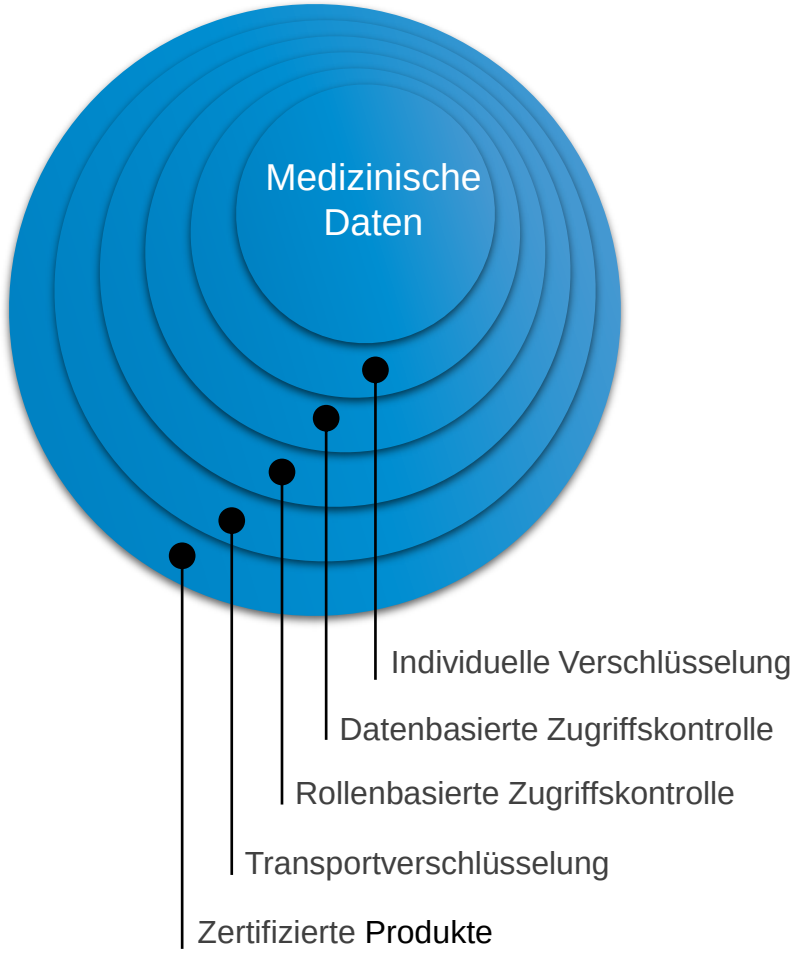
Organspende-erklärung (OSE)

Bundesärztekammer Deutsche Krankenhaus Gesellschaft DKG Spitzenverband

Mehrschichtige Sicherheitsmechanismen

- Zugriffe erfolgen über abgesicherte und durch die gematik und das BSI zertifizierte und zugelassene Produkte (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 in der Umgebung der Leistungserbringer entfernt.

Sicherheitsmechanismen

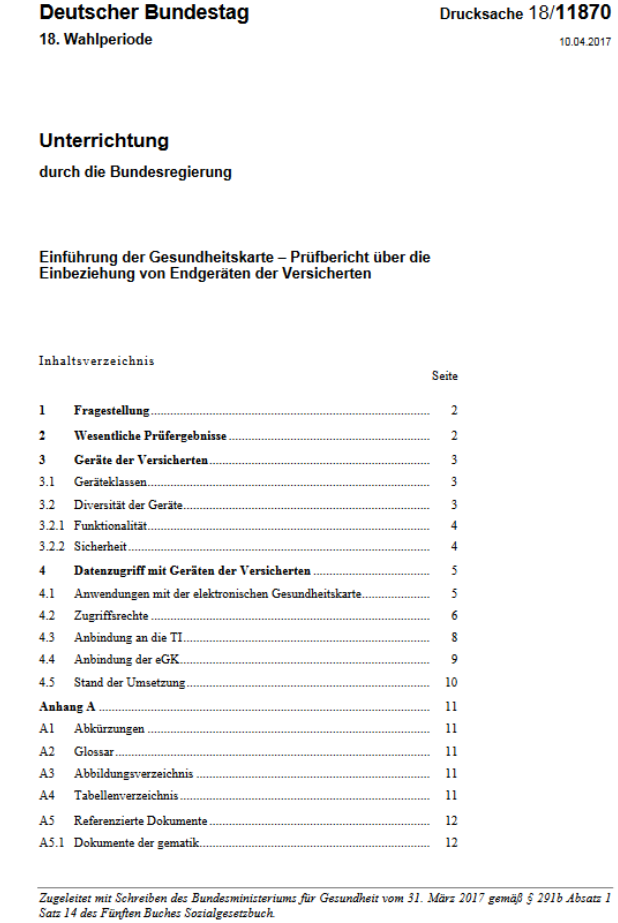


Einbindung von Geräten der Versicherten

Bis zum 31. Dezember 2016 hat die Gesellschaft für Telematik zu prüfen, inwieweit mobile und stationäre Endgeräte der Versicherten zur Wahrnehmung ihrer Rechte, insbesondere der Zugriffsrechte gemäß § 291a Absatz 4 Satz 2, und für die Kommunikation im Gesundheitswesen einbezogen werden können.

- **Prüfbericht wurde im April veröffentlicht** ✓

Auftrag



Deutscher Bundestag Drucksache 18/**11870**
18. Wahlperiode 10.04.2017

Unterrichtung
durch die Bundesregierung

Einführung der Gesundheitskarte – Prüfbericht über die Einbeziehung von Endgeräten der Versicherten

Inhaltsverzeichnis

Zugeleitet mit Schreiben des Bundesministeriums für Gesundheit vom 31. März 2017 gemäß § 291b Absatz 1 Satz 14 des Fünften Buches Sozialgesetzbuch.

Geräteklassen

1. mobile Endgeräte mit mobilen Betriebssystem-plattformen
   - Smartphones
   - Tablets
   - eher untergeordnet: Smart-Watches
2. stationäre Endgeräte mit Desktop-Betriebssystemen
   - PCs
   - Notebooks
   - eher untergeordnet: Smart-TVs

Rahmenbedingungen:

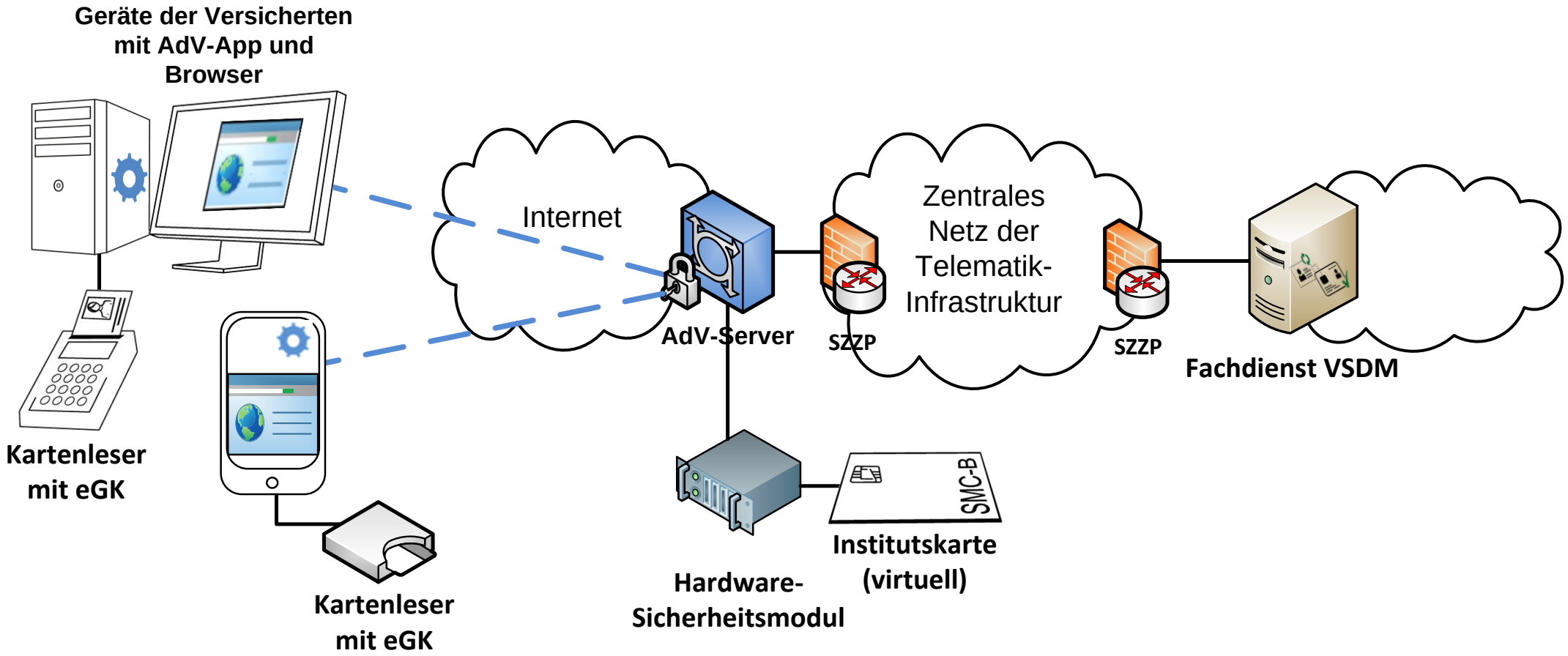
- Diversität der Geräte der Versicherten
- Unterschiedliche Sicherheitseigenschaften
- Keine Geräte der TI, Verantwortung liegt beim Versicherten

Geräteklassen

Anwendungsfälle und Zugriffsrechte

Anwendungsfall	Zugriff durch Versicherte?
PIN ändern, PIN entsperren, PIN-Schutz für Anwendungen ein- oder ausschalten	eigenständig
Gültigkeit der eGK prüfen	eigenständig
Zugriffsprotokoll lesen	eigenständig
Daten einer Anwendung verbergen bzw. sichtbar machen	eigenständig, mit Zweikartenprinzip
Versichertenstammdaten der eGK anzeigen	eigenständig
Abgleich der Versichertenstammdaten	eigenständig, mit Zweikartenprinzip
Organspendeerklärung und Persönliche Erklärung anzeigen	eigenständig
Organspendeerklärung und Persönliche Erklärung erstellen, aktualisieren, löschen	eigenständig, mit Zweikartenprinzip
Notfalldaten, elektronischen Medikationsplan oder elektronische Patientenakte anzeigen	mit Zweikartenprinzip, nur in der Leistungserbringerumgebung
Daten im elektronischen Patientenfach anzeigen, bereitstellen, löschen	Authentisierung notwendig

Technische Lösung zum Zweikartenprinzip für Anwendungen des Versicherten



SZZP: Sicherer Zentraler Zugangspunkt

WIR VERNETZEN DAS GESUNDHEITSWESEN. SICHER.

Holm Diening, Abteilungsleiter Datenschutz und Informationssicherheit
gematik | Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH | Friedrichstraße 136 | 10117 Berlin