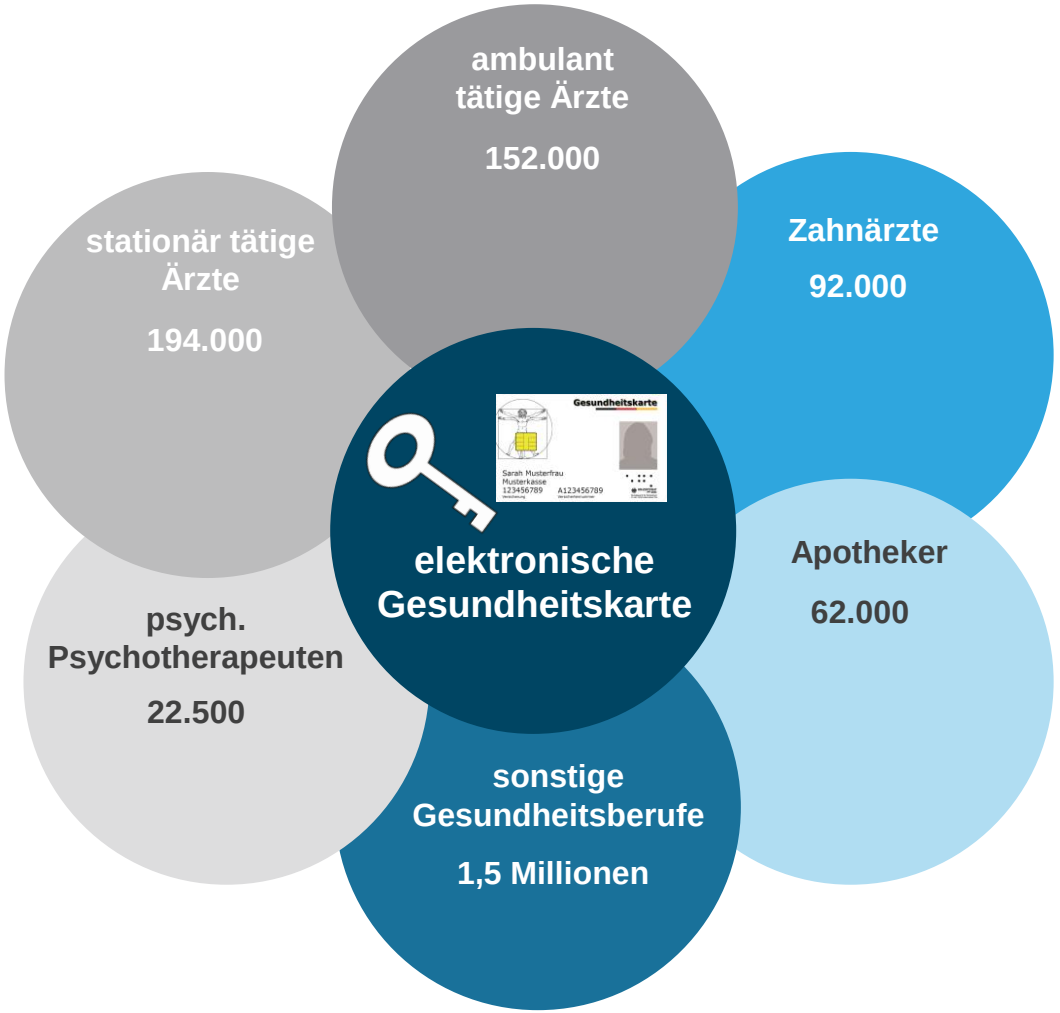
Sicherheitsmaßnahmen bei der Vernetzung der Akteure des Gesundheitswesens

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 %** (~71 Millionen) gesetzlich Versicherte
- **113** gesetzliche Krankenkassen
- **102.000** Arztpraxen
- **44.500** Zahnarztpraxen
- **20.500** psychologische Psychotherapeutenpraxen
- **2.000** Krankenhäuser
- **20.250** Apotheken
- **1.150** Vorsorge- oder Rehaeinrichtungen

Deutsches Gesundheitswesen



Herausforderungen für die Telemedizin

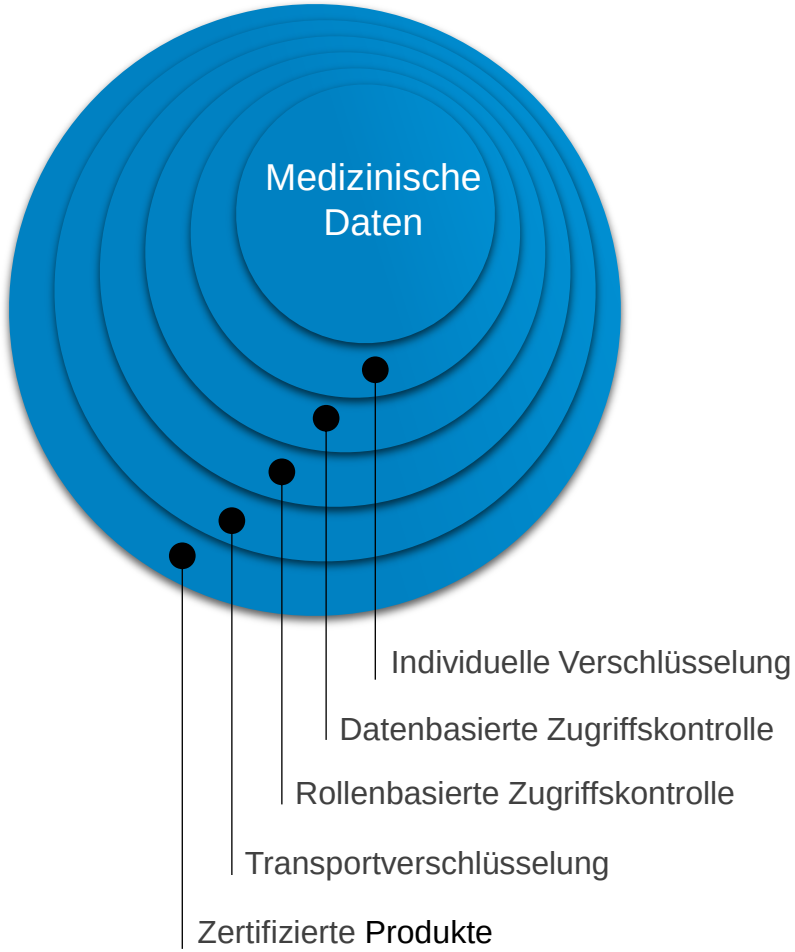
Telemedizin

- **Technische Umsetzung** erfordert große Initialbudgets
- Jedes Projekt benötigt **spezifische Kompetenzen** im Bereich Datenschutz und Sicherheit
- **Fehlendes Vertrauen** in Sicherheit von Projekten bei Nicht-IT-Akteuren
- Zahlreiche **Insellösungen** erschweren den Datenaustausch ohne Medienbrüche
- Häufig vorzeitiges „Abschließen“ innovativer Anwendungen durch Furcht vor **Folgekosten/ -risiken**
- Häufig bleibt es bei Projekten die nie in den **Regelbetrieb** gelangen

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



Ende-zu-Ende Verschlüsselung als zentrales Element zur Vermeidung von Datendiebstählen

- etwa 2,6 Milliarden kompromittierter Datensätze in 2017
- davon etwa 33,7 Millionen im Gesundheitswesen
- 1.765 Vorfälle, davon 27% im Gesundheitswesen
- in gerade einmal 3% aller Fälle (nicht nur Gesundheitswesen) waren die Datensätze verschlüsselt → in diesen Fällen waren die Daten für den Angreifer nutzlos

Kein erfolgreicher Angriff auf verschlüsselte Datensätze!

Quelle: http://breachlevelindex.com/data-breach-database

Zentrale Sicherheitsmaßnahmen in der TI
Sichere Übertragung am Beispiel VSD-Update

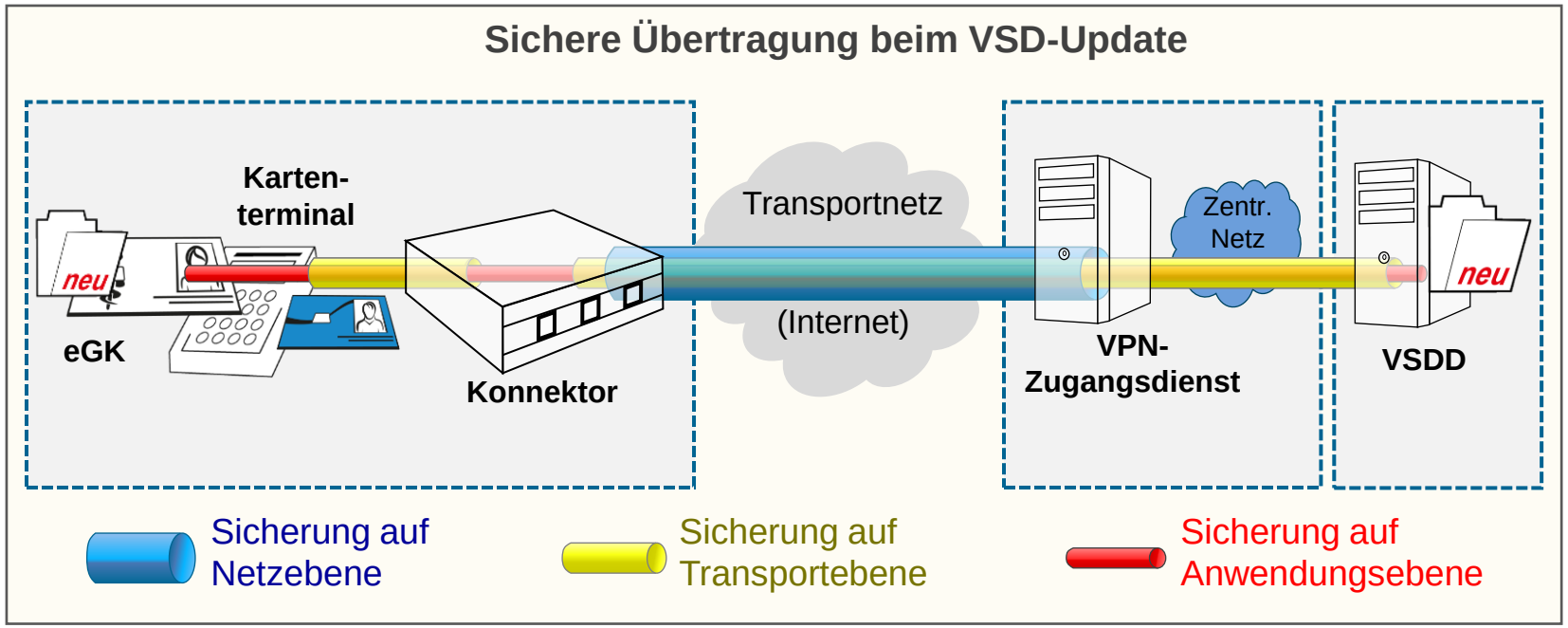
Vertraulichkeit und Integrität der VSD sind Ende-zu-Ende geschützt

Beim Übergang über das Transportnetz liegt ein dreifacher Schutz vor

Netzebene: IPsec

Transportebene: TLS

Anwendungsebene: Secure Messaging



Datenschutz- und Sicherheitsmanagement im gesamten Lebenszyklus

Datenschutz und Informations-sicherheit von Anfang an

- Nutzen von einheitlichen Methoden zur Erstellung von Datenschutz- und Sicherheitskonzepten

Geprüfter Datenschutz und geprüfte Informations-sicherheit

- Prüfung dezentraler Komponenten nach Vorgaben des BSI
- Prüfung zentraler Dienste durch unabhängige Sicherheitsgutachter

Datenschutz und Informations-sicherheit im laufenden Betrieb

- Kontrolle der Aufrechterhaltung des Datenschutzes und der Sicherheit im Betrieb

Common Criteria Evaluierung für dezentrale Komponenten

Bundesamt
für Sicherheit in der
Informationstechnik

- Erstellung von Protection Profiles für dezentrale Komponenten (Kartenterminal, Konnektor, Karten) durch BSI begleitend zu den Spezifikationen der gematik
- Vom BSI anerkannte Prüfstellen prüfen (evaluieren) die Produkte
- BSI zertifiziert evaluierte Produkte auf Grundlage der Prüfberichte

Prüfung mittels Sicherheitsgutachten für zentrale Dienste

- Anbieter zentraler Produkte müssen Sicherheitsgutachten im Rahmen der Zulassung bzw. Bestätigung einreichen
- Sicherheitsgutachter müssen eine Basisqualifikation vorweisen und werden zusätzlich von der gematik geschult (3 Tage Seminar mit Prüfung)
- Dokumentenprüfung, Interviews und Vor-Ort-Prüfungen
- Für jedes zentrale Produkt sind konkrete Anforderungen dem Sicherheitsgutachten zugewiesen
- gematik prüft die eingereichten Gutachten auf Vollständigkeit und Nachvollziehbarkeit
- Sicherheitsgutachten müssen alle 3 Jahre oder bei wesentlichen Änderungen erneuert werden

CERT – Behandlung von Schwachstellen und Sicherheitsvorfällen

- Identifikation von Schwachstellen und Sicherheitsvorfällen
- Verpflichtung der Anbieter zur Meldung
- Bewertung der Schwachstelle bzw. Sicherheitsvorfalls
- Einbindung des BSI und der Gesellschafter der gematik
- Abstimmung mit Anbieter und ggf. Anweisung von (Sofort-)Maßnahmen
- Ggf. weitere Eskalation an Notfallmanagement
- Überwachung und Verifikation der Umsetzung

Aufgaben des koordinierenden ISMS

Auditprogramm

- Auditrecht (anlassunabhängig und anlassbezogen) der gematik gegenüber Anbietern
- Jahresplanung der anlassunabhängigen Audits durch Auditprogrammmanager
- Planung und Durchführung der Audits beim Anbieter
- Abstimmung der Feststellungen und möglicher Gegenmaßnahmen mit Anbietern
- Nachverfolgung der Umsetzung abgestimmter Maßnahmen

Aufgaben des koordinierenden ISMS

Notfallmanagement TI

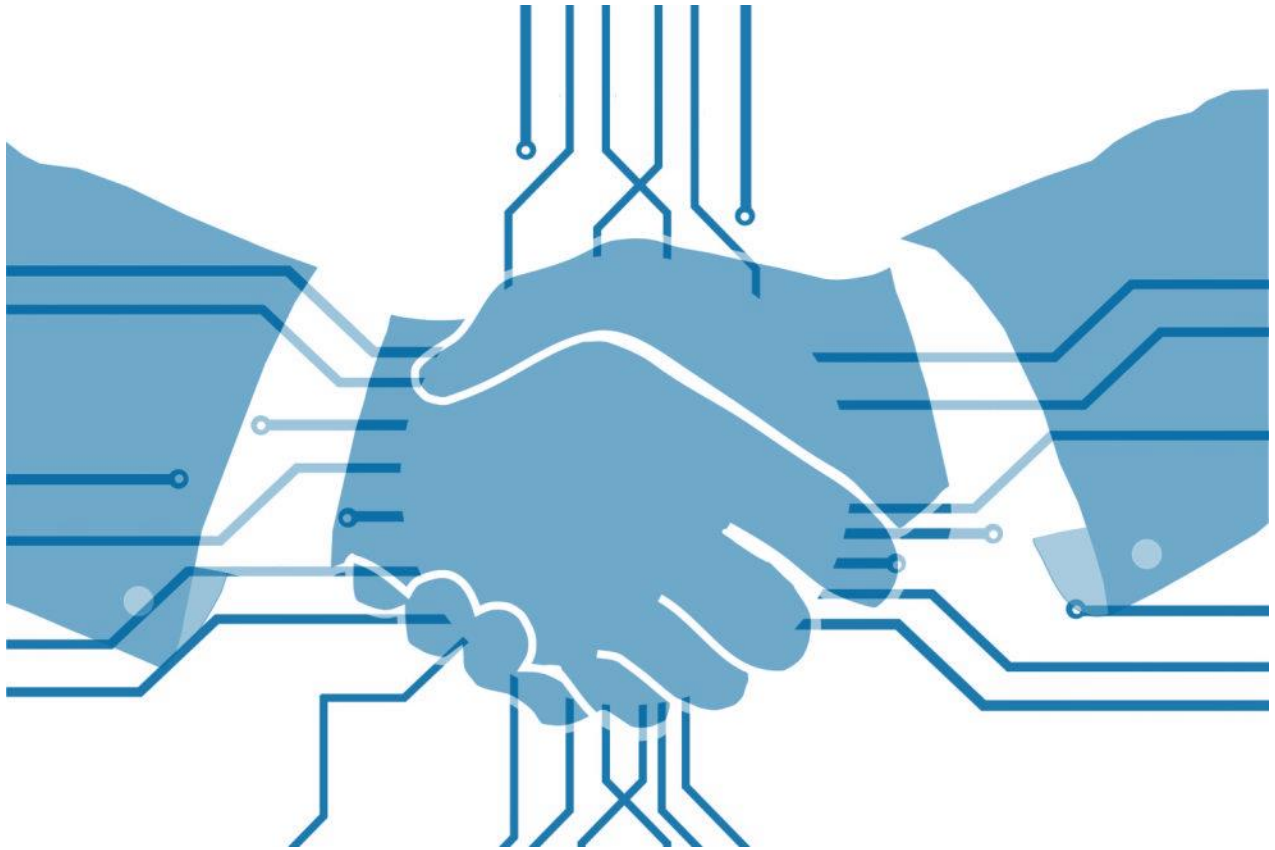
- Präventive Maßnahmen zur Verhinderung von TI-Notfällen (Vorsorge)
- Maßnahmen, um Auswirkungen von Notfällen auf die TI gering zu halten (Bewältigung)
- Etablierung eines lokalen Notfallmanagements bei allen Anbietern
- Etablierung Notfallmanagement der TI (gematik)
- Enge Abstimmung zwischen gematik und Anbietern (Notfallkriterien wie BIA, Vorsorge- und Bewältigungsstrategien sowie Kommunikation)
- Durchführung von Notfallübungen

Aufgaben des koordinierenden ISMS

Grünes Licht für erste Komponenten der Industrie

- 11. November 2017: Konnektor, E-Health-Kartenterminal, VPN-Zugangsdienst und Praxisausweis **zugelassen für Einsatz** in der Telematikinfrastruktur (TI)
- **Alle Anforderungen** an die Funktionalität, Interoperabilität und Sicherheit zum Einsatz in der TI sind **erfüllt**
- **Weitere Produkte** verschiedener Unternehmen **durchlaufen** derzeit die **Zulassungsverfahren**

Erste Komponenten zugelassen



WIR VERNETZEN DAS GESUNDHEITSWESEN. SICHER.

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