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.

1 Fragestellung

Am 29. Dezember 2015 ist das „Gesetz für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen (E-Health-Gesetz)“ in Kraft getreten. Dieses formuliert im Fünften Buch des Sozialgesetzbuches (SGB V), § 291b Satz 13, einen Prüfauftrag für die gematik mit folgender Fragestellung:

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.

Hintergrund dieser Fragestellung ist die zunehmende Nutzung von Smartphones und anderen mobilen Endgeräten für Gesundheitsanwendungen. Daher sollte die gematik bis Ende 2016 prüfen, ob die Versicherten solche Geräte etwa zur Wahrnehmung ihrer Zugriffsrechte und für die Kommunikation im Gesundheitswesen einsetzen können.[1]

Hierzu wurde geprüft, welche Möglichkeiten zur Anbindung mobiler und stationärer Endgeräte an die Telematikinfrastruktur bestehen und inwiefern entsprechende Szenarien bereits vorgesehen sind und wie Versicherte hiermit ihre Rechte wahrnehmen können.

Die Prüfung erfolgte auf Basis der veröffentlichten Konzepte und Spezifikationen der gematik zur elektronischen Gesundheitskarte (eGK) und zur Telematikinfrastruktur sowie auf Basis des aktuellen Stands des Aufbaus der Telematikinfrastruktur. Weiterhin floss der gegenwärtige Stand der Konzepte und Spezifikationen der gematik aus laufenden Projekten zur zukünftigen Erweiterung der Telematikinfrastruktur ein.

2 Wesentliche Prüfergebnisse

Die gematik hat entsprechend der an sie adressierten Fragestellung die Möglichkeit der Verwendung von Endgeräten der Versicherten geprüft.

Zunächst kann festgestellt werden, dass es sich bei den Geräten der Versicherten um eine sehr heterogene Landschaft handelt. Sie lässt sich in zwei grundsätzliche Geräteklassen einteilen

(1) mobile Endgeräte mit mobilen Betriebssystemplattformen sowie

(2) stationäre Endgeräte mit Desktop-Betriebssystemen.

Jedoch differieren die Eigenschaften der Geräte innerhalb einer Geräteklasse teilweise stark. Diese Diversität der Geräte der Versicherten sowie die damit einhergehenden sehr stark fragmentierten Sicherheitseigenschaften stellen neben den funktionalen Unterschieden eine der größten Herausforderungen zur Integration dieser Geräte in eine auf Sicherheit ausgerichtete Kommunikationslandschaft – wie die Telematikinfrastruktur – dar. Die Geräte der Versicherten befinden sich in deren Besitz und sind kein Teil der Telematikinfrastruktur, was mit einer Verantwortung der Versicherten für Sicherheit, Datenschutz sowie den Betrieb dieser Geräte einhergeht. Betrachtungen zur Diversität der Geräte und der Verantwortung der Versicherten finden sich im Kapitel 3.2 dieses Berichts.

Neben der Betrachtung der Geräte selbst erfolgte auch eine Analyse der für diese Geräte infrage kommenden Anwendungsfälle ausgehend von einer Betrachtung der im Zusammenhang mit der elektronischen Gesundheitskarte gesetzlich festgelegten Anwendungen. Je nach Anwendung erfolgt eine Speicherung der Daten dieser Anwendungen lokal auf der elektronischen Gesundheitskarte oder in einem Fachdienst der Telematikinfrastruktur. Obgleich die Versicherten das Recht haben, auf die Daten dieser Anwendungen zuzugreifen (§ 291a Absatz 4 Satz 2 SGB V), sind die Anwendungsfälle stark limitiert, da gemäß

§ 291a Absatz 5 Satz 5 SGB V der Zugriff auf den überwiegenden Teil der Daten mittels der elektronischen Gesundheitskarte unabhängig von der Existenz einer technischen Lösung nur in Verbindung mit einem Heilberufsausweis erfolgen darf. Eine kurze Analyse und Übersicht der möglichen Anwendungsfälle findet sich in den Kapiteln 4.1 und 4.2.

---

[1] https://www.bundesgesundheitsministerium.de/themen/krankenversicherung/e-health-gesetz/e-health.html

Eine Lösung zur Anbindung der Geräte der Versicherten an die Telematikinfrastruktur durch Nutzung der elektronischen Gesundheitskarte ist in den Kapiteln 4.3 und 4.4 beschrieben. Diese Lösung wird durch die gematik als Teil des Projekts „Anwendungen der Versicherten“ bereits erarbeitet. Diese Lösung setzt auf einer technischen Umsetzung des Zwei-Karten-Prinzips auf und ist somit prinzipiell geeignet, weitere Anwendungsfälle zu ermöglichen. Vor dem Hintergrund der gesetzlichen Regelungen für die Zugriffsberechtigungen ist jedoch auch mit dieser Lösung aktuell nur ein eingeschränkter Zugriff der Versicherten auf ihre Daten möglich.

Der Stand der Umsetzung innerhalb des Projektes der gematik ist im Kapitel 4.5 aufgeführt.

3 Geräte der Versicherten

Zur Analyse der Fragestellung werden in diesem Kapitel zunächst die in Frage kommenden Geräte der Versicherten betrachtet.

3.1 Geräteklassen

Für die Verwendung stationärer Endgeräte durch die Versicherten wird von einer Nutzung dieser Geräte in der Heimumgebung, d. h. der heimischen IT-Infrastruktur, ausgegangen. Diese Umgebung ist jedoch nicht auf die Verwendung stationärer Endgeräte beschränkt, sondern umfasst auch die Verwendung mobiler Endgeräte.

Für die Verwendung mobiler Endgeräte ergeben sich weitere mögliche Einsatzszenarien der mobilen Nutzung dieser Endgeräte außerhalb der Heimumgebung.

Im Kontext der Anbindung der Endgeräte an die Telematikinfrastruktur und zur Nutzung der elektronischen Gesundheitskarte stellen diese Szenarien keinen Unterschied zur Nutzung mobiler Endgeräte in der Heimumgebung dar und werden damit darunter subsumiert.

Eine Klassifizierung der Geräte der Versicherten greift deren technische Ausstattung auf Basis meist grundsätzlich unterschiedlicher Betriebssystemplattformen auf. Hierbei erfolgt folgende Differenzierung:

(1) Mobile Endgeräte mit mobilen Betriebssystemplattformen

Dies umfasst hauptsächlich Smartphones und Tablets. Smart-Watches fallen auch unter diese Klasse, spielen jedoch aufgrund der eingeschränkten Visualisierung eine untergeordnete Rolle.

(2) Stationäre Endgeräte mit Desktop-Betriebssystemen

Dies umfasst PCs und Notebooks mit Desktop-Betriebssystemen sowie Smart-TV- Geräte oder TV-Geräte mit Set-Top-Boxen mit spezifisch an die Hardware angepassten Betriebssystemen, welche auch von mobilen Betriebssystemplattformen abgeleitet worden sein können. TV-Geräte spielen vermutlich für die in Kapitel 1 aufgeführte Fragestellung eine eher untergeordnete Rolle.

Mit fortschreitender Entwicklung der mobilen Betriebssysteme zeichnet sich, gerade bei Notebooks, ein fließender Übergang zwischen Desktop-Betriebssystemen und mobilen Betriebssystemplattformen ab, der auf eine zukünftige Konvergenz beider Plattformen hindeutet.

3.2 Diversität der Geräte

Der Zugriff auf die Daten der Anwendungen der elektronischen Gesundheitskarte und der Telematikinfrastruktur mit Geräten der Versicherten ist nicht auf bestimmte Geräteklassen, Geräteplattformen oder einzelne Geräte beschränkt. Die bereits genannten Geräte unterscheiden sich stark, beispielsweise hinsichtlich der verwendeten Technik, der Leistungsfähigkeit und der Verfügbarkeit.

Generell unterscheiden sich derzeit die beiden Geräteklassen stark voneinander.

Bei mobilen Endgeräten mit mobilen Betriebssystemplattformen ist das Betriebssystem zumeist an die Hardware der Geräte gebunden. Diese Geräte betten sich in ein eigenes Ökosystem aus Entwicklungs- und Verwaltungswerkzeugen ein. Für stationäre Endgeräte mit Desktop-Betriebssystemen ist dieser Grad der Integration in Ökosysteme derzeit nicht gegeben und die Kopplung des Betriebssystems an die Hardware deutlich geringer.

Zusätzlich gibt es teilweise erhebliche Unterschiede zwischen den Geräten innerhalb einer Geräteklasse. So sind die Ökosysteme der verschiedenen mobilen Betriebssystemplattformen komplett voneinander getrennt. Zumindest für die Softwareentwicklung auf mobilen Betriebssystemplattformen existieren Werkzeuge für eine sogenannte Cross-Plattform-Entwicklung, die eine Brücke zwischen den Ökosystem schlagen sollen. Andere Aspekte dieser Ökosysteme können damit jedoch nicht erreicht werden.

Diese Unterschiede zwischen den Plattformen beeinflussen insbesondere die Möglichkeiten der Geräte, gewünschte Funktionen und Sicherheitsmerkmale für Anwendungen gleichermaßen bereitzustellen.

Die notwendige Software auf den Geräten der Versicherten zum Zugriff auf Daten der gesetzlichen Anwendungen im Gesundheitswesen muss daher spezifisch für verschiedene Betriebssystemplattformen und ggf. auch spezifisch für bestimmte Versionen des Betriebssystems zur Verfügung gestellt werden.

3.2.1 Funktionalität

Die Geräte der Versicherten müssen mindestens folgende Leistungsmerkmale bieten:

(1) Internetanbindung,

(2) Möglichkeit der Darstellung der Daten sowie

(3) Möglichkeit zur Anbindung der eGK.

Da die funktionalen Eigenschaften der Geräte auch innerhalb der Geräteklassen differieren, muss eine Umsetzung dieser Leistungsmerkmale abhängig von den Eigenschaften der konkreten Geräte erfolgen, sodass eine pauschale Lösung für alle Geräte der Versicherten ausgeschlossen ist. Anbieter von Lösungen werden diese vermutlich daher jeweils auf bestimmte Gruppen von Geräten ausrichten.

3.2.2 Sicherheit

Die gesetzlichen Sicherheitsvorgaben in §§ 291a ff. SGB V sind auch im Zusammenhang mit den Geräten der Versicherten zu beachten.

Moderne Geräte verfügen heute über zahlreiche Sicherheitseigenschaften, die eine sichere Nutzung der Daten der gesetzlichen Anwendungen unterstützen. Allerdings unterscheiden sich die Geräte in Stärke und Umfang der unterstützten Sicherheitseigenschaften. Gerade mobile Betriebssystemplattformen bieten immer mehr Sicherheitseigenschaften, um die Vertraulichkeit der auf den Geräten gespeicherten und der vom Gerät übertragenen Daten zu wahren.

Aktuelle (mobile) Betriebssystemplattformen ermöglichen bereits eine im Betriebssystem eingebettete Trennung der Daten verschiedener Apps und entsprechende Steuerung der

Rechte von Apps zum Austausch von Daten mit anderen Apps oder zum Zugriff auf Hard- und Software-Ressourcen. Zusätzlich zur Möglichkeit der Verschlüsselung des gesamten oder Teile des Speichers sind dies nur einige Beispiele, die für eine Nutzung der Geräte eine wichtige Rolle spielen.

Es sei jedoch auch erwähnt, dass die Implementierungen dieser Sicherheitseigenschaften kein sicherheitszertifiziertes Niveau besitzen. Öffentlich bekannt gewordene Schwachstellen werden durch die Hersteller der Geräte oder Betriebssysteme in der Regel über entsprechende Software-Updates geschlossen. Gerade bei mobilen Geräten gewähren die Hersteller oft nur für einen kurzen Zeitraum nach Markteinführung der Geräte eine Möglichkeit des Software-Updates, auch für sicherheitskritische Updates.

Die Qualität der Sicherheitseigenschaften der Geräte der Versicherten ist wesentlich, um dem hohen Schutzbedarf der Daten der Versicherten gerecht zu werden und ein hohes Maß an Vertrauenswürdigkeit für die Versicherten zu gewährleisten. Aufgrund der Diversität der Geräte der Versicherten variiert diese Qualität, was sich im nutzbaren Leistungsumfang in den Lösungen der Anbieter widerspiegelt.

Die Geräte der Versicherten sind keine Geräte der Telematikinfrastruktur. Das bedeutet insbesondere, dass diese Geräte nicht durch die gematik zugelassen werden und damit kein Nachweis ihrer funktionalen und sicherheitstechnischen Eignung erfolgt. Die Versicherten tragen notwendigerweise selbst die Verantwortung für diese Geräte. Damit bestehen für die gematik organisatorisch und technisch nur wenige Regelungsmöglichkeiten. Zudem scheint eine Einbindung der Geräte der Versicherten angelehnt an eine im Unternehmensumfeld übliche Geräteverwaltung, welche eine sichere Konfiguration der Geräte steuert, aufgrund der Diversität und aufgrund der Verantwortung der Versicherten für diese Geräte nicht sinnvoll.

In diesem Zusammenhang kann nur auf allgemeine Verhaltensregeln für die Versicherten im Umgang mit ihren Geräten und eine sichere Konfiguration ihrer Geräte verwiesen werden, welche die Wahrscheinlichkeit einer Kompromittierung der Geräte einhergehend mit Verlust des Schutzes der darauf gespeicherten oder verarbeiteten Daten senken. Die Versicherten sind jedoch für eine Einhaltung dieser Verhaltensregeln und die Konfiguration ihrer Geräte selbst verantwortlich.

Die Versicherten können hierbei unterstützt werden, indem entsprechende Apps zum Zugriff auf die Daten der gesetzlichen Anwendungen zuvor von der gematik zugelassen werden und die Versicherten auf deren ausschließliche Verwendung hingewiesen werden. Im Rahmen des Zulassungsprozesses werden dann die von ihrer Ausführungsumgebung unabhängigen funktionalen und sicherheitstechnischen Eigenschaften dieser Apps geprüft.

Aufgrund der unterschiedlichen Qualität der Sicherheitseigenschaften der Geräte der Versicherten bestehen bei einer Nutzung der Geräte zum Zugriff auf die Daten der gesetzlichen Anwendungen zudem von den Sicherheitseigenschaften des eingesetzten Geräts abhängig unterschiedlich starke Restrisiken für eine Vertraulichkeit der in den genutzten Anwendungen gehaltenen Daten. Diese können zudem von den Versicherten durch die Wahl eines bestimmten Gerätes, die Art der Nutzung und Konfiguration des Gerätes beeinflusst werden.

Vor dem Hintergrund des freiwilligen selbstbestimmten Zugriffs auf Daten der gesetzlichen Anwendungen durch die Versicherten kann ein gewisses Maß an Zustimmung zur Übernahme von mit der Nutzung verbundenen Restrisiken vorausgesetzt werden. Eine explizite Einwilligung zur Nutzung von Lösungen zum Zugriff auf die Daten der gesetzlichen Anwendungen mit Geräten der Versicherten bedarf einer vorherigen Aufklärung der Versicherten über die Existenz und die Art der Restrisiken.

4 Datenzugriff mit Geräten der Versicherten

Zur weiteren Bestimmung der Fragestellung wird der Anwendungsbereich für die Geräte der Versicherten (GdV) im Kontext der im Zusammenhang mit der elektronischen Gesundheitskarte festgelegten gesetzlichen Anwendungen ermittelt.

4.1 Anwendungen mit der elektronischen Gesundheitskarte

Durch § 291a Absatz 2 Satz 1 und Absatz 3 Satz 1 SGB V werden die gesetzlichen Anwendungen im Zusammenhang mit der elektronischen Gesundheitskarte festgelegt. Die folgende Liste enthält die Bezeichnung dieser Anwendungen in Kurzform:

(1) eVerordnung

(2) Notfalldaten (NFD)

(3) eArztbrief/elektronische Fallakte (eFA)

(4) elektronischer Medikationsplan/Daten zur Prüfung der Arzneimitteltherapiesicherheit (eMP/AMTS)

(5) elektronische Patientenakte (ePA)

(6) elektronisches Patientenfach (ePF)

(7) Patientenquittung

(8) Organspendeerklärung (OSE)

(9) Hinweise zum Ablageort von Willenserklärungen der Versicherten (Persönliche Erklärungen, kurz: PE)

Weiterhin wird in § 291 Absatz 2 Satz 1 SGB V der Inhalt der auf der elektronischen Gesundheitskarte zu den Versicherten hinterlegten sogenannten Versichertenstammdaten (VSD) definiert.

Gemäß § 291a Absatz 3 Satz 1 SGB V werden Notfalldaten und gemäß § 291 Absatz 2 SGB V Versichertenstammdaten lokal auf der elektronischen Gesundheitskarte gespeichert. Für die Daten der anderen o. g. Anwendungen existieren keine gesetzlichen Festlegungen zur Speicherung der Daten. Derzeit werden folgende Speichermöglichkeiten durch die gematik betrachtet:

(1) lokale Speicherung auf der elektronischen Gesundheitskarte (eGK)

(2) Speicherung in einem Fachdienst der Telematikinfrastruktur (TI).

Bei der ersten Variante der lokalen Speicherung auf der elektronischen Gesundheitskarte wird diese als Speichermedium genutzt. Ein Zugriff auf die Daten erfolgt durch Nutzung der Smartcard-Funktionen der eGK und Zugriff auf deren Speicherstrukturen.

Bei der zweiten Variante der Speicherung in einem Fachdienst der TI erfolgt die Speicherung der Daten in einem speziellen daten- bzw. anwendungsspezifischen Speicherdienst, dem sogenannten Fachdienst. Dieser Dienst wird dabei an die Telematikinfrastruktur angebunden. Ein Zugriff auf die Daten einer Anwendung erfolgt dabei unter Nutzung von Funktionen bzw. Schnittstellen des Fachdienstes. Die eGK dient hierbei primär als Authentisierungsmittel für einen Online-Zugang zum entsprechenden Fachdienst der TI und ggf. zur Ver- und Entschlüsselung gespeicherter Daten.

Mit Bereitstellung einer Anwendung wird separat für diese Anwendung eine der beiden o. g. Varianten des Speicherorts festgelegt. Für die Daten der Anwendung eMP/AMTS wurde bereits festgelegt, dass diese zunächst lokal auf der eGK gespeichert werden. In einer späteren Stufe der Ausgestaltung dieser Anwendung werden die Daten in einem Fachdienst abgelegt.

4.2 Zugriffsrechte

Gemäß § 291a Absatz 4 Satz 2 SGB V haben die Versicherten das Recht, auf alle Daten der in Kapitel 4.1 genannten gesetzlichen Anwendungen zuzugreifen. Jedoch wird dieser grundsätzlich inhaltlich unbegrenzte Anspruch gemäß § 291a Absatz 5 Satz 5 eingeschränkt. Hiernach darf auf Daten der Anwendungen, die von Leistungserbringern erhoben werden, oft auch als medizinische Daten klassifiziert, mittels der eGK nur in Verbindung mit einem Heilberufsausweis (HBA) zugegriffen werden. Das gilt auch für den eigenständigen Zugriff durch die Versicherten. Als Beispiel seien die durch Ärzte zu erstellenden Notfalldaten genannt.

Berufsmäßige Gehilfen und sonstige zugriffsberechtigte Personen nach § 291a Absatz 4 Satz 1 Nummer 1 Buchstabe d und e sowie Nummer 2 Buchstabe d und e SGB V, die über keinen elektronischen Heilberufsausweis oder Berufsausweis verfügen, können auf die entsprechenden Daten zugreifen, wenn sie hierfür von Personen autorisiert wurden, die über einen elektronischen Heilberufsausweis oder Berufsausweis verfügen, und wenn nachprüfbar elektronisch protokolliert wird, wer auf die Daten zugegriffen hat und von welcher Person die zugreifende Person autorisiert wurde. Die technische Umsetzung des Zugriffs erfolgt durch die Verwendung der sogenannten Institutskarte des Leistungserbringers, welche die Identität der medizinischen Institution gegenüber der TI repräsentiert (SMC-B).

Diese Beschränkung der Versicherten hinsichtlich ihrer Rechte zum Zugriff auf diese sogenannten medizinischen Daten durch den Gesetzgeber wird in der Literatur mit dem Schutz der Versicherten begründet. Die Einsichtnahme in diese Daten soll damit nur in einer vertrauenswürdigen Umgebung bei Leistungserbringern erfolgen, die berufsmäßig mit diesen Daten arbeiten.

Technisch realisiert wird diese Beschränkung durch das sogenannte Zwei-Karten-Prinzip, welches beim Zugriff

auf die Daten mittels der eGK eine Autorisierung des Zugriffs durch einen HBA oder durch eine SMC-B eines Leistungserbringers erzwingt. Für Daten, die lokal auf der eGK gespeichert werden, sind die entsprechenden Zugriffsrechte auf der eGK hinterlegt und werden von dieser durchgesetzt.

Auf Daten für Anwendungen, die von den Versicherten selbst bereitgestellt werden, wie z. B. eine Organspendeerklärung oder Hinweise zum Ablageort von Willenserklärungen der Versicherten (Persönliche Erklärungen), können Versicherte ohne diese Beschränkung, d. h. eigenständig, zugreifen.

Neben Anwendungsfällen zum Zugriff auf die in Kapitel 4.1 genannten gesetzlichen Anwendungen sind, abhängig von der Anwendung, weitere fachliche Anwendungsfälle und Verwaltungsfunktionen sinnvoll. Weitere fachliche Anwendungsfälle ergeben sich aus der Notwendigkeit, Daten auf der eGK zu verbergen oder verborgene Daten wieder sichtbar zu machen. Unter Verwaltungsfunktionen verstehen sich allgemeine und anwendungsübergreifende Anwendungsfälle zum Ändern und Entsperren von PINs, zum Ein- und Ausschalten des PIN-Schutzes sowie zum Einsehen von Protokollierungsdaten.

Die folgende Tabelle gibt einen Überblick, welche der für Versicherte infrage kommenden Anwendungsfälle durch die Versicherten eigenständig ausgeführt werden können. Diese sind in der letzten Spalte mit einem Kreuz gekennzeichnet. Über diese Anwendungsfälle hinaus existieren noch weitere Anwendungsfälle, z. B. des schreibenden Zugriffs, die gesetzlich nicht für die Versicherten in der Heimumgebung vorgesehen sind.

Tabelle 1

Anwendungsfälle für Versicherte und Berechtigung

Anwendung	**Anwendungsfall**	**eigenständiger Zugriff durch Versicherte möglich**
Verwaltungsfunktionen	PIN ändern	X
	PIN entsperren	X
	PIN-Schutz für Anwendungen ein- oder ausschalten	X
	Gültigkeit der eGK prüfen	X
	Zugriffsprotokoll lesen	X
	Aktivierung/Deaktivierung einer Anwendung (Daten einer Anwendung verbergen bzw. sichtbar machen)	[2]
VSD	Versichertenstammdaten der eGK anzeigen	X
	Abgleich der Versichertenstammdaten	[2]
PE	Persönliche Erklärungen anzeigen	X
	Persönliche Erklärungen erstellen, aktualisieren oder löschen	[2]
OSE	Organspendeerklärung anzeigen	X
	Organspendeerklärung erstellen, aktualisieren oder löschen	[2]
NFD	Notfalldaten anzeigen	
eFA	elektronischen Arztbrief bzw. elektronische Fallakte anzeigen	
eMP/AMTS	e-Medikationsplan anzeigen	
eVerordnung	eVerordnung anzeigen	[3]
Patientenquittung	Patientenquittung anzeigen	

[2] Ein eigenständiger Zugriff der Versicherten wäre zulässig, jedoch ist eine technische Autorisierung im Sine des Zwei-Karten-Prinzips, wie in Kapitel 4.3 beschrieben, notwendig.

[3] Bei einer alternativen Autorisierung durch die Versicherten kann gemäß § 291a Absatz 5 Satz 7 SGB V vom Zwei-Karten-Prinzip abgewichen werden.

Anwendung	Anwendungsfall	eigen-ständiger Zugriff durch Versicherte möglich
ePA	elektronische Patientenakte anzeigen	
ePF	Daten des elektronischen Patientenfachs anzeigen	[4]
	eigene Daten im elektronischen Patientenfach bereitstellen	[4]
	Daten im elektronischen Patientenfach löschen	[4]

Aus dieser Tabelle ist ersichtlich, dass aufgrund der gesetzlichen Beschränkungen ein eigenständiger Zugriff der Versicherten auf die Daten der gesetzlichen Anwendungen nur in einem sehr eingeschränkten Maß möglich ist. Anwendungsfälle auch mit nur lesendem Zugriff auf die im Kapitel 4.1 beschriebenen Daten der medizinischen Anwendungen, wie z. B. das Lesen des elektronischen Medikationsplans, sind daher für Geräte der Versicherten ausgeschlossen. Technisch könnten jedoch auch diese Anwendungsfälle mit der in Kapitel 4.3 beschriebenen Lösung des Projektes „Anwendungen der Versicherten“ realisiert werden.

Zusätzlich hat der Gesetzgeber jedoch den Versicherten das Recht eingeräumt, über das elektronische Patientenfach auf diese Daten zuzugreifen. Dazu müssen Leistungserbringer gemäß § 291a Absatz 5 Satz 9 SGB V auf Wunsch des Versicherten diese Daten im elektronischen Patientenfach bereitstellen. Für den Zugriff auf das elektronische Patientenfach kann gemäß § 291a Absatz 5 Satz 8 SGB V von der gesetzlichen Beschränkung des Zugriffs auf Daten der eGK nur in Verbindung mit einem Heilberufsausweis abgewichen werden, sofern die Versicherten sich mittels eines geeigneten technischen Verfahrens authentifizieren.

4.3 Anbindung an die TI

Für die in Tabelle 1 aufgeführten Anwendungsfälle, bei denen die Daten lokal auf der eGK gespeichert sind und bei denen kein HBA, keine SMC-B eines Leistungserbringers bzw. andere berechtigte Karte (SMC-B) notwendig ist (siehe Tabelle 1, Spalte „eigenständiger Zugriff durch Versicherte möglich“), ist eine Verbindung zur Telematikinfrastruktur nicht erforderlich.

Andere Anwendungsfälle benötigen jedoch eine zusätzliche, ggf. nur technische Autorisierung des Zugriffs auf die Daten der eGK mittels einer zweiten berechtigten Karte, einem Heilberufsausweis/Berufsausweis (HBA), einer Institutskarte eines Leistungserbringers bzw. einer anderen berechtigten Karte (SMC-B).

Für die im Kapitel 3.1 beschriebenen Einsatzszenarien der Geräte der Versicherten wird im Projekt „Anwendungen der Versicherten (AdV)“ der gematik eine Lösung erarbeitet, mit der auch in diesen Szenarien das Zwei-Karten-Prinzip ermöglicht werden kann. Für die Realisierung ist im Rahmen der in diesem Projekt erarbeiteten Lösungsarchitektur der sogenannte AdV-Server vorgesehen.

Der AdV-Server bindet auf der einen Seite die Geräte der Versicherten an und stellt auf der anderen Seite die Verbindung zur Telematikinfrastruktur und den angeschlossenen Fachdiensten, zunächst nur den Fachdienst VSDM, dar. Ein an den AdV-Server angeschlossenes oder integriertes Hardware-Sicherheitsmodul stellt die für das Zwei-Karten-Prinzip notwendige zweite Karte bereit.

Zur Wahrung des Datenschutzes der Daten der Versicherten wird die Verbindung zwischen dem AdV-Server und den Geräten der Versicherten der über eine kryptografisch gesicherte Verbindung erfolgen, die dem aktuellen Stand der Technik entspricht.

[4] Ein Zugriff auf das elektronische Patientenfach kann gemäß § 291a Absatz 5 Satz 8 SGB V auch unter Verwendung eines geeigneten technischen Verfahrens zur Authentisierung der Versicherten erfolgen.

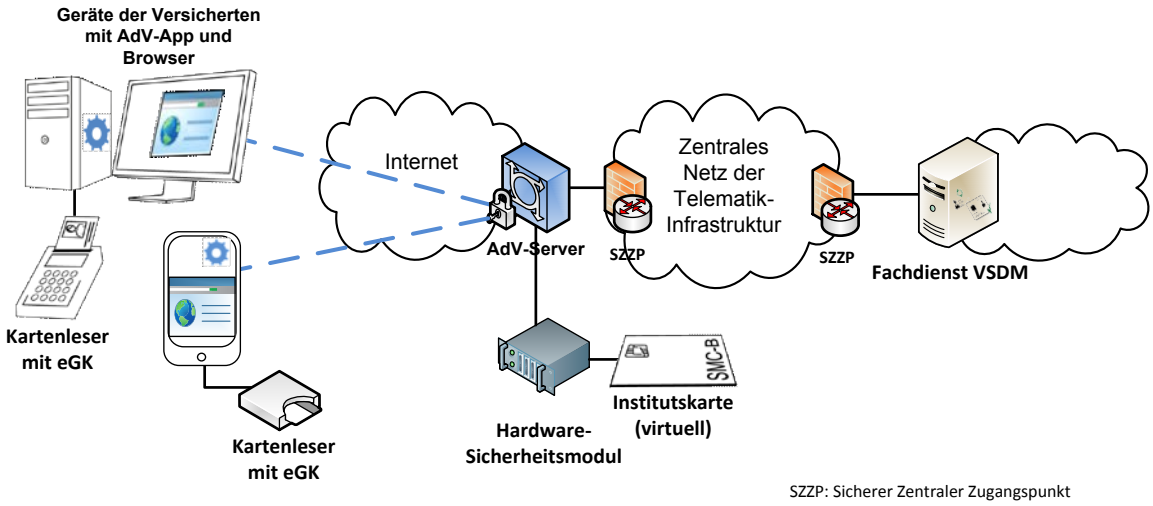
Im Rahmen der für den Verbindungsaufbau notwendigen Authentisierung der Versicherten erfolgt in Verbindung mit der über diesen Dienst bereit gestellten zweiten Karte eine Prüfung der Authentizität und Echtheit der eGK der Versicherten. Durch die Nutzung von Anwendungen oder Verwaltungsfunktionen ist ggf. zusätzlich die PIN-Eingabe der eGK durch die Versicherten erforderlich. Je nach Anbindung der Karte über einen externen Kartenleser erfolgt diese PIN-Eingabe der Versicherten am externen Kartenleser oder an den Geräten der Versicherten direkt.

Eine zum AdV-Server gehörige App sorgt auf den Geräten der Versicherten für den gesicherten Verbindungsaufbau zu diesem AdV-Server, den Zugriff auf die eGK über den an den Geräten der Versicherten angeschlossenen Kartenleser sowie die lokale Anzeige und Verarbeitung der gelesenen Daten.

Folgende Abbildung zeigt den prinzipiellen Aufbau der im Projekt AdV verfolgten Lösungsarchitektur zur Anbindung der Geräte der Versicherten.

Abbildung

Beispielhafte Anbindung der Geräte der Versicherten an die Telematikinfrastruktur



SZZP: Sicherer Zentraler Zugangspunkt

4.4 Anbindung der eGK

Für die in der Tabelle 1 aufgeführten Anwendungsfälle mit Geräten der Versicherten ist zum Zwecke

(1) des Zugriffs auf die auf der eGK lokal gespeicherten Daten und

(2) zur Authentisierung der oder des Versicherten

eine Anbindung der eGK an die Geräte der Versicherten unumgänglich. Für den Zugriff auf eine Smartcard wie die eGK ist ein entsprechender Kartenleser erforderlich. Die Anbindung der Smartcard an den Kartenleser könnte hierbei grundsätzlich über die auf der Smartcard aufgebrachten Kontakte oder über eine kontaktlose (NFC-)Schnittstelle erfolgen.

Diese kontaktlose (NFC-)Schnittstelle ist in der Spezifikation optional vorgesehen. Da aktuell für kontaktlose Karten im Gesundheitswesen, bspw. in Ermangelung entsprechen- der zugelassener Kartenleser, keine Anwendungsszenarien existieren, gibt es derzeit keine eGK mit kontaktloser (NFC-)Schnittstelle.

Daher ist bei der Anbindung der eGK an die Geräte der Versicherten derzeit immer von einer Nutzung eines separaten Kartenlesegerätes auszugehen. Solche Kartenlesegeräte können drahtlos (z. B. über Bluetooth) oder kabelgebunden (z. B. über USB) mit dem Endgerät verbunden werden.

4.5 Stand der Umsetzung

Um den Versicherten technisch die Möglichkeit zu geben, ihre Zugriffsrechte in Bezug auf die mittels der eGK gespeicherten Daten wahrzunehmen, wurde die gematik durch ihre Gesellschafter mit dem Projekt „Anwendungen des Versicherten“ beauftragt. Im Rahmen der Konzeption des Lösungsansatzes dieses Projektes wurden die in Kapitel 4 beschriebenen technischen Voraussetzungen und organisatorischen Rahmenbedingungen zur Anbindung der Geräte der Versicherten an die Telematikinfrastruktur bereits berücksichtigt.

Hierzu erarbeitet die gematik eine Lösungskonzeption und Spezifikationen, welche nach der Finalisierung veröffentlicht werden und von Anbietern für die Entwicklung von AdV-Lösungen genutzt werden können.

Mit der Finalisierung der Lösungskonzeption wird sich die gematik mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) abstimmen, um notwendige sicherheitstechnische Anforderungen an die Lösung zu klären.

Anhang A

A1 – Abkürzungen

BSI	Bundesamt für Sicherheit in der Informationstechnik
eFA	elektronische Fallakte
eGK	elektronische Gesundheitskarte
ePA	elektronische Patientenakte
ePF	elektronisches Patientenfach
GdV	Geräte der Versicherten
HBA	Heilberufsausweis
NFC	Near Field Communication
NFD	Notfalldaten
OSE	Organspendeerklärung
PE	Persönliche Erklärungen
PIN	Personal Identification Number
PS	Primärsystem
SMC-B	Secure Module Card Typ B
TI	Telematikinfrastruktur

A2 – Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

A3 – Abbildungsverzeichnis

A4 – Tabellenverzeichnis

A5 – Referenzierte Dokumente

A5.1 – Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Einführung der Gesundheitskarte – Glossar

Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333