Fraunhofer Institut für Offene Kommunikationssysteme

gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Untersuchung zur Forderung nach Tests mit zusätzlichen dezentralen Speichermedien

Einführung der elektronischen Gesundheitskarte

Datum:	**30. April 2009**
Einstufung:	**Öffentlich**
Version / Status:	**1.0 / Freigegeben**
Autoren:	**Fraunhofer FOKUS, gematik GmbH**

---

gematik GmbH
Friedrichstraße 136, 10117 Berlin

Inhaltsverzeichnis

1 Zusammenfassung 4
2 Auftrag 7
3 Projektpartner 9
4 Vorgehensweise 9
5 Informationen zur dezentralen Datenspeicherung 10
6 Analyse des Konzepts der BÄK 11
7 Rahmenbedingungen für mögliche Testmaßnahmen 12
7.1 Anwender von dezentralen Speichermedien 12
7.2 Generelle Nutzung von Telematik-Anwendungen 12
7.3 Exemplarischer Anwendungskontext 13
7.3.1 Betrachtete Anwendungszwecke 14
7.3.2 Potentielle Anwendungen 15
7.3.3 Ermittlung geeigneter Fachanwendungen 18
7.3.4 Potentielle Einsatzszenarien 19
7.4 Abschätzung der Anforderungen an die dezentralen Komponenten 20
8 Mögliche Varianten des dezentralen Speichermediums 21
8.1 Dezentrale Speichermedien mit USB-Schnittstelle 21
8.1.1 Ungeschützter USB-Stick (STICK) 21
8.1.2 USB-Stick mit Schutzmechanismen (STICK_S) 22
8.2 Nutzung der eGK 23
8.2.1 eGK mit erweitertem Speichervolumen (eGK_M) 23
8.2.2 Karte mit eGK-Funktion und zusätzlichem Speicher (eGK_M+) 24
9 Definition der Bewertungskriterien 25
9.1 Konzeption der Bewertung 25
9.2 Detaillierte Beschreibung der Bewertungskriterien 26
9.2.1 Definition der Kriterien der Bewertungskategorie 1 “Konformität mit dem gesetzlichen Rahmen” 26
9.2.2 Definition der Kriterien der Bewertungskategorie 2 “Nutzung in Fachanwendungen” 28
9.2.3 Definition der Kriterien der Bewertungskategorie 3 “Integration in die TI” 31
9.2.4 Definition der Kriterien der Bewertungskategorie 4 “Eignung für den Wirkbetrieb” 32
10 Bewertung 35
10.1 Bewertungskategorie 1 “Konformität mit dem gesetzlichen Rahmen” 35
10.1.1 Zusammenfassung der Bewertungskategorie 1 40
10.2 Bewertungskategorie 2 “Nutzung in Fachanwendungen” 41
10.2.1 Datenvolumen 41
10.2.2 Anforderungen an den Datenerhalt 42
Handhabbarkeit für Versicherte und Leistungserbringer 43
10.2.3 Zusammenfassung der Bewertungskategorie 2 49
10.3 Bewertungskategorie 3 “Integration in die TI” 51
10.3.1 Zusammenfassung der Bewertungskategorie 3 55
10.4 Bewertungskategorie 4 “Eignung für den Wirkbetrieb” 58
10.4.1 Zusammenfassung der Bewertungskategorie 4 64
10.5 Zusammenfassung der Bewertungen 66
10.5.1 Einführung 66
10.5.2 Bewertung der generellen Eignung 66
10.5.3 Bewertung der Eignung der definierten Implementierungsvarianten 67
10.5.4 Ergebnis der Bewertung 69

Empfehlung zum weiteren Vorgehen....71
11 Generische Aufwandsabschätzung....72
12 Literaturverzeichnis....74
13 Anlagen....74
14 Abkürzungsverzeichnis....74
15 Glossar....75
A Anhang....76
A.1 Markterhebung: Auswertung von Marktstudien....76
A.2 Kurzbeschreibung Patienten-Kurzakte (Patient Summary)....77

Tabellenverzeichnis

Tabelle 7-1 Liste möglicher Anwendungen gemäß RVO....15
Tabelle 7-2 Liste möglicher Anwendungen nach SGB V, §291a....16
Tabelle 7-3 Liste weiterer möglicher Anwendungen....17
Tabelle 7-4 Plan zur Einführung geeigneter Anwendungen....18
Tabelle 8-1 Eigenschaften des ungeschützten USB-Sticks (STICK)....22
Tabelle 8-2 Eigenschaften des USB-Sticks mit Schutzmechanismen (STICK_S)....23
Tabelle 8-3 Eigenschaften der eGK mit erweitertem Speichervolumen (eGK_M)....24
Tabelle 8-4 Eigenschaften der eGK mit zusätzlichem Speicher (eGK_M+)....25
Tabelle 10-1 Bewertung Kategorie 1 „Konformität mit dem gesetzlichen Rahmen“....41
Tabelle 10-2 Bewertung Kriterium „Erforderliches Datenvolumen“....42
Tabelle 10-3 Bewertung Kriterium „Datenerhalt“....42
Tabelle 10-4 Bewertung Kriterium „Handhabbarkeit“....44
Tabelle 10-5 Bewertung Kriterium „Zeitbedarf des Anwendungsfalls“....47
Tabelle 10-6 Bewertung Kriterium „Unterstützung beim Schutz der Daten“....49
Tabelle 10-7 Bewertung Kategorie 2 „Nutzung in Fachanwendungen“....50
Tabelle 10-8 Ergebnisse Bewertungskategorie 3 „Integration in die TI“....58
Tabelle 10-9 Verfügbarkeit offener Spezifikationen....60
Tabelle 10-10 Verfügbarkeit von Prüfspezifikationen....62
Tabelle 10-11 Verfügbarkeit offener Spezifikationen....63
Tabelle 10-12 Ergebnisse Bewertungskategorie 4 „Eignung für den Wirkbetrieb“....66
Tabelle 10-13 Ergebnisse der Bewertungskategorien....68
Tabelle 12-1 Literaturverzeichnis....74
Tabelle 13-1 Anlagen....74
Tabelle 14-1 Abkürzungsverzeichnis....75
Tabelle 15-1 Glossar....75

Abbildungsverzeichnis

Abbildung 9-1 Vereinbarte Bewertungskriterien....25

Änderungsnachweis

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0	30.4.2009			Fraunhofer FOKUS, gematik

1 Zusammenfassung

Auftrag

Im Auftrag ihrer Gesellschafter hat die gematik eine *konzeptionelle Bewertung der Forderung der Bundesärztekammer (BÄK) zur Durchführung technik- und ergebnisoffener Tests von Speichermedien in der Hand von Versicherten als Alternative zu serverbasierter Speicherung* durchgeführt. Die Bewertungskriterien wurden mit dem Fachausschuss abgestimmt.

Durchführung der Untersuchung

Als Projektpartner konnte das Fraunhofer Institut für offene Kommunikationstechnik FOKUS gewonnen werden, das europaweit eine führende Stellung beim Entwurf von Lösungen für eIdentity-Systeme einnimmt. Die Untersuchung wurde gemeinsam von gematik und den unabhängigen Experten von FOKUS erstellt.

Grundlage der Untersuchung

Grundlage für die Bewertung waren das Konzeptpapier „Eckpunkte für ein Konzept zur dezentralen Speicherung medizinischer Daten in der Telematikinfrastruktur“ der Bundesärztekammer („Konzept“)“, die Beratungsvorlage zur 20. Gesellschafterversammlung der gematik und der darauf basierende Auftrag der Gesellschafter.

Danach soll im Rahmen der Telematikinfrastruktur den Versicherten die Möglichkeit geboten werden, persönliche medizinische Daten alternativ zur serverbasierten Speicherung in einem dezentralen Speichermedium ablegen zu können.

In Frage kommen hierfür insbesondere freiwillige Anwendungen nach § 291a Abs. 3 SGB V, deren Speicherung serverbasiert erfolgen soll. Das optionale USB-Speichermedium (STICK) würde ausschließlich innerhalb der Telematikinfrastruktur (TI) der eGK eingesetzt und vom Versicherten selbst beschafft werden. Von einem Einsatz des STICK am Praxisverwaltungssystem wird aus Sicherheitsgründen abgeraten. Der Anpassungsaufwand der Telematikinfrastruktur soll minimiert, potentielle Synergien sollen genutzt werden.

Um entsprechend der Forderung des „Konzepts“ den Anpassungsaufwand der Telematikinfrastruktur zu minimieren und potentielle Synergien zu nutzen und gleichzeitig dem Gesellschafterauftrag der Bewertung technikoffener Tests gerecht zu werden, hat die gematik nicht nur den STICK, sondern zusätzlich drei weitere Implementierungsvarianten dezentraler Speicherung in die Betrachtung einbezogen (STICK_S, eGK_M, eGK_M+).

Der STICK_S verfügt im Vergleich zum STICK über Sicherheitsfunktionen. Die eGK_M wird über die gleichen Eigenschaften wie die eGK verfügen, hat jedoch einen Speicher von ca. 1 MByte, also ca. das Zehnfache der eGK Generation 1. Die eGK_M+ wird voraussichtlich mehr als 100 MByte Speicher aufweisen.

Grundsätzliche Vor- und Nachteile dezentraler Speichermedien

Das Angebot von dezentralen Speichermedien in Versichertenhand könnte zwar zu einer Erhöhung der Akzeptanz der Telematikinfrastruktur der eGK führen, doch stehen diesem potentiellen Akzeptanzgewinn grundsätzliche Nachteile entgegen.

1. Die Verfügbarkeit der Daten ist bei der dezentralen Speicherung nicht gewährleistet. Ein Verlust des Mediums oder ein technischer Defekt sind nicht unwahrscheinlich und führen zu einem dauerhaften Verlust aller gespeicherten Daten. Die Wiederbeschaf-

fung ist ggf. mit erheblichen Aufwänden verbunden. Die Nichtverfügbarkeit der Daten kann die Behandlung des Versicherten beeinträchtigen.

2. Die Lebensdauer von Speichermedien und die Schutzwirkung von kryptografischen Verfahren sind zeitlich begrenzt. Die Daten müssen vor Ablauf einer Zeitspanne von ca. 5-10 Jahren auf ein neues Medium transferiert bzw. mit neuen Verfahren vor Zugriff geschützt, verschlüsselt und signiert werden.

Ergebnis der Bewertung

Das Ergebnis *der konzeptionellen Bewertung der Forderung zur Durchführung technik- und ergebnisoffener Tests von Speichermedien in der Hand von Versicherten als Alternative zu serverbasierter Speicherung* zeigt, dass ein ungeschütztes, unpersonalisiertes USB-Medium bei mehreren Kriterien aus verschiedenen Bewertungskategorien entweder als ungeeignet oder schlecht geeignet eingestuft werden muss. Die gesetzlichen Anforderungen des § 291 SGB V sind teilweise nicht erfüllt.

Zum Beispiel sind folgende Sachverhalte kritisch zu bewerten:

Die Anwendungen der TI der eGK müssen allen Versicherten und Leistungserbringern diskriminierungsfrei zugänglich sein. Das bedeutet, dass auch IT-Laien die Möglichkeit haben müssen, die feiwilligen Anwendungen sicher und unter Wahrung ihrer Personenrechte zu nutzen. Die Übertragung der alleinigen Verantwortung für ein dezentrales Speichermedium und die darauf gespeicherten Daten an den Versicherten setzt voraus, dass auch der IT-Laie durch die Systemlösung in die Lage versetzt wird, diese Verantwortung inhaltlich auch wahrnehmen zu können. Das vorgeschlagene Konzept berücksichtigt dies nicht hinreichend. Der Anwender verantwortet u. a. die Verwaltung und Pflege aller Daten auf dem STICK, muss selbst darauf achten, wann z.B. die Lebensdauer seines Mediums oder der verwendeten kryptografischen Verfahren endet, die Maßnahmen zum Erhalt der Daten einleiten und soll sich um die Archivierung der Daten kümmern.

Da die gespeicherten Daten bei einem Defekt verloren sind, muss die Zuverlässigkeit des Speichermediums für eine definierte Lebensdauer abgesichert sein. Für USB-Sticks gibt es jedoch keine offenen Prüfverfahren zur Sicherstellung der Wirkbetriebstauglichkeit hinsichtlich Lebensdauer und Robustheit. Es sind auch keine Referenzen der Verwendung in ähnlichen Projekten bekannt.

Die Handhabung von mehreren Medien (eGK und STICK für den Versicherten, eGK, STICK und ggf. HBA für den Leistungserbringer) ist nicht anwenderfreundlich.

Resultat der Betrachtung zusätzlicher Varianten von Speichermedien

Es ist ein Alleinstellungsmerkmal der Telematikinfrastruktur (TI) der eGK, dass sie die dezentrale Speicherung von Daten sicher und anwenderfreundlich unterstützt. Perspektivisch ist vorstellbar, dass mit eGK_M und eGK_M+ neue Typen dezentraler Speichermedien zur Verfügung stehen, die Funktionalität und Sicherheit der Telematikinfrastruktur mit einer dezentralen Speicherung sinnvoll verbinden.

Die vergleichsweise geringere Speicherkapazität von eGK_M (ca. 1 MByte) und eGK_M+ (> 100 MByte) scheint ein Nachteil gegenüber USB-Sticks zu sein, die über Speicher von bis zu 64GByte verfügen. Jedoch zeigt die Betrachtung der Anwendungssituation, dass die Speichergrößen von eGK_M und eGK_M+ für die heute vorhersehbaren Einsatzszenarien ausreichend sind. Versicherte, die die dezentrale Speicherung nutzen möchten, bräuchten kein zusätzliches Speichermedium, sondern eGK_M und eGK_M+ würden die heutige eGK ablösen.

Die Kosten für eine Nutzung werden deutlich niedriger geschätzt, als bei den Varianten eines USB-Stick, nicht zuletzt da die existierenden Schnittstellen der Kartenterminals weiterhin verwendet werden könnten. Leistungserbringer müssten keine neuen Geräte einführen, sondern könnten eGK_M und eGK_M+ mit den Kartenterminals des Basis-Rollout verwenden. USB-Schnittstellen sind für die aktuellen Geräte nicht spezifiziert. Eine Gesamtwirtschaftlichkeitsbetrachung für ein komplementäres Angebot dezentraler Speichermedien wurde im Rahmen der vorgelegten Untersuchung nicht vorgenommen und bedarf weiterer Untersuchungen, in die die Ergebnisse durchzuführender funktionaler Tests als auch Akzeptanzaspekte bei den Beteiligten (Versicherte/Ärzte) einfließen sollten.

Empfehlung zum weiteren Vorgehen

Fraunhofer FOKUS und gematik sind der Auffassung, dass das Angebot einer dezentralen Speicherung von Daten, die alternativ und optional zur Speicherung in einem Fachdienst angeboten wird, die Akzeptanz der TI der eGK erhöhen könnte.

Fraunhofer FOKUS und gematik halten es deshalb für sinnvoll, das Thema der dezentralen Speicherung zu vertiefen.

Eine Testung dezentraler Speichermedien auf Basis des vorgelegten Konzepts kann nicht empfohlen werden. Dennoch kann die Telematikinfrastruktur die Möglichkeit zur alternativen dezentralen Speicherung ohne Einbußen beim Schutz der personenbezogenen Daten unterstützen, sofern hierfür geeignete Medien verwendet werden. Hierfür sind weitere Konkretisierungen erforderlich.

Zunächst könnte für geeignete freiwillige Fachanwendungen geprüft werden, in welcher Form die Möglichkeit des Einsatzes dezentraler Speichermedien im Rahmen der Fachkonzepte für freiwillige Anwendungen realisiert werden könnte (Dauer: ca. vier Monate). In einem hierauf aufsetzenden nächsten Umsetzungsschritt könnte die Planung entsprechender Tests vorgenommen werden (Dauer: ca. 3 Monate).

Eine Kooperation zwischen der gematik, interessierten Gesellschaftern (insbesondere BÄK) und Fraunhofer FOKUS wäre denkbar. Die Arbeiten könnten nach dem erfolgreichen Abschluss der Konzeptphase des Online-Rollout starten und mit den Aktivitäten zur eGK G2 verbunden werden.

Die Entscheidung, ob entsprechende Arbeiten aufgenommen werden sollten, muss von den Gesellschaftern der gematik getroffen werden.

Es ist zu beachten, dass der potentielle Zeitpunkt eines Tests an den Ausbau der TI der eGK und die Einführung geeigneter freiwilliger Anwendungen gekoppelt ist. Dies entspricht auch der Intention der Beratungsvorlage und dem vorgelegten Konzept.

2 Auftrag

Die Geschäftsführung der gematik wurde in der 20. Gesellschafterversammlung folgendermaßen beauftragt:

> *„Die Geschäftsführung der gematik wird beauftragt, bis zur 22. Gesellschafterversammlung der gematik und unter Einbeziehung des Fachausschusses eine konzeptionelle Bewertung der Forderung zur Durchführung technik- und ergebnisoffener Tests von Speichermedien in der Hand von Versicherten als Alternative zu serverbasierter Speicherung vorzunehmen, eine Empfehlung zum weiteren Vorgehen auszusprechen und diese zur 22. Gesellschafterversammlung vorzulegen. Die Kostenwirkungen sind darzulegen."*

Der Beschluss wird einstimmig ohne Gegenstimme und ohne Enthaltung gefasst.

Der Beschluss referenziert das Dokument der Bundesärztekammer „Eckpunkte für ein Konzept zur dezentralen Speicherung medizinischer Daten in der Telematikinfrastruktur" (25.9.2008 / V1.0.0). Die vorliegende Bewertung erfolgt auf Basis dieses Konzepts.

Zum Verständnis des Auftrags ist die Beratungsvorlage der Bundesärztekammer zum betreffenden Tagesordnungspunkt der 20. GSV wichtig. Diese ist im Folgenden wiedergegeben:

> ***Sachstand***
>
> *Der 111. Deutsche Ärztetag hat sich im Mai 2008 erneut mit Fragen der Nutzung von Telematik im Gesundheitswesen befasst. Er hat festgestellt, dass der Schutz der Vertraulichkeit von Patientendaten und der Erhalt der ärztlichen Schweigepflicht unabdingbare Vorrausetzungen für den Einsatz telematischer Verfahren in der Medizin sind.*
>
> *In einer zukünftigen Telematikinfrastruktur werden – insbesondere im Kontext der so genannten freiwilligen Anwendungen wie z.B. einer Arzneimitteldokumentation oder elektronische Patientenakte – Datenspeicherungen aufgrund der zu erwartenden Datenmengen nicht ausschließlich auf der elektronischen Gesundheitskarte selbst erfolgen können. In den derzeitigen Konzepten für die Speicherung solcher Daten ist daher die serverbasierte und verschlüsselte Speicherung der patientenbezogenen Daten konzeptionell vorgesehen. Der 111. Deutsche Ärztetag hat sich (erneut) im Hinblick diese Form der Speicherung von Daten sehr kritisch geäußert und die „Erprobung von Speichermedien in der Hand des Patienten wie auch anderer Alternativen zur Datenspeicherung auf zentralen Servern" gefordert.*
>
> ***Bewertung und Handlungsempfehlung:***
>
> *a) Bewertung*
>
> *Die erwarteten medizinischen wie auch ökonomischen Vorteile des Einsatzes von Telematik im Gesundheitswesen werden sich nach übereinstimmender Auffassung nahezu aller Beteiligten besonders durch die Nutzung der so genannten freiwilligen Anwendungen nach § 291a Abs. 3 SGB V der elektronischen Gesundheitskarte realisieren lassen. Diese Anwendungen erfordern eine Speicherung patientenbezogener Daten in größerem Umfang um diese, in der Regel zum Zeitpunkt der Behandlung, nutzen zu können. Entscheidende Voraussetzung für den Erfolg der freiwilligen Anwendungen ist aber das uneingeschränkte Vertrauen des Patienten in die Sicherheit der notwendigerweise zu speichernden Daten vor dem unbefugten Zugriff Dritter.*
>
> *Es ist zu erwarten, dass bei grundsätzlicher Bereitschaft von ca. 2/3 der Patienten und Versicherten, die freiwilligen Anwendungen zu nutzen dennoch erhebliche Vorbehalte gegen eine Speicherung von Daten auf Servern bestehen. Immerhin beste-*

hen derzeit bei mehr als 1/3 der Versicherten „sehr große Bedenken", dass „die eGK von Unberechtigten eingesehen bzw. missbraucht" wird. Dies offenbar bei fast 1/3 selbst dann, wenn die verschlüsselte Speicherung „in einem speziellen Bereich" vorgesehen ist und ein „Datenschutzbeauftragter … Sicherheit garantiert"[1]. In der Folge kann daraus eine Situation entstehen, in der Patienten, die aus medizinischer Sicht von den freiwilligen Anwendungen profitieren könnten, diese dennoch nicht nutzen. Angesichts der Tatsache, dass sich heute bereits erhebliche Datenmengen auch auf Speichermedien wie bspw. USB-Sticks unter physischer Kontrolle des Versicherten ablegen lassen, erscheint es notwendig, die Nutzung solcher Speichermedien als Alternative zur serverbasierten Speicherung von Patientendaten systematisch und schrittweise zu erproben. Zur Schaffung von Vertrauen in die von der gematik angestrebte höchstmögliche Sicherheit der Telematikinfrastruktur erscheint eine solche Erprobung unumgänglich aber auch möglich. Sie macht keine grundsätzliche Veränderung der heute bereits vorgesehen Sicherheitsverfahren erforderlich vielmehr kann sie diese nutzen und ergänzen.

Ziel der technik- und ergebnisoffenen Tests muss die Schaffung einer Entscheidungsgrundlage für die Gesellschafter sein, ob und unter welchen Bedingungen im Rahmen der zukünftigen Telematikinfrastruktur Patienten zur Wahrung ihrer Rechte als Alternative zu serverbasierten Speicherung auch die Nutzung von unter ihrer persönlichen Kontrolle stehenden Speichermedien angeboten werden kann.

b) Handlungsempfehlung

In der Erprobung ist schrittweise vorzugehen, d.h. zunächst sind unter Einbeziehung und Bewertung der heute bereits von einigen Unternehmen angebotenen Lösungen in diesem Bereich die konzeptionellen Grundlagen für eine Erprobung zu legen. In Folge sind schrittweise Erprobungen und Labor- Anwender und Feldtest-Bedingungen durchzuführen. Hierbei ist neben der technischen Machbarkeit auch die Handhabbarkeit in der Praxis des Gesundheitswesens zu bewerten. Weiterhin sind alle heute bereits von der gematik konzipierten Sicherheitsverfahren (z.B. kryptographische Verfahren) in die konzeptionellen Überlegungen mit einzubeziehen und Lösungen zu suchen, die die geringst möglichen Auswirkungen auf die heute bereits vorliegenden Sicherheitskonzepte haben.

Die gematik soll die Forderung zur Durchführung technik- und ergebnisoffener Tests von Speichermedien in der Hand von Versicherten als Alternative zu serverbasierter Speicherung konzeptionell bewerten und den Gesellschaftern in der nächsten Gesellschafterversammlung einen Vorschlag zur möglichen schrittweisen Erprobung sowie eine Handlungsempfehlung für das weitere Vorgehen vorlegen.

Die von der Bundesärztekammer vorgelegten Eckpunkte für ein Konzept zur dezentralen Speicherung medizinischer Daten in der Telematikinfrastruktur (Anlage) sollten entsprechend berücksichtigt werden.

[1] Quelle: Forsa-Umfrage im Auftrag der Arbeitsgemeinschaft der Spitzenverbände der Krankenkassen, April 2008

3 Projektpartner

Die gematik hat das Fraunhofer Institut für offene Kommunikationstechnik FOKUS als Projektpartner gewinnen können.

Fraunhofer FOKUS hat europaweit eine führende Stellung beim Entwurf von Lösungen für kommende eIdentity-Systeme und ist mit den Anforderungen, Problemstellungen und künftigen technischen Möglichkeiten bestens vertraut. Fraunhofer FOKUS ist damit der ideale Partner bei der Erfüllung dieses Auftrags.

Das vorliegende Dokument ist gemeinschaftlich von Fraunhofer FOKUS und der gematik erstellt worden.

4 Vorgehensweise

Die Projektpartner möchten das Vorgehen und die Bewertung transparent und nachvollziehbar gestalten. Deshalb werden alle Kriterien und Bewertungsschritte offen in diesem Dokument dargelegt. Die Fachinformationen, auf denen die Bewertung beruht, wurden von Fraunhofer FOKUS und anderen unabhängigen Experten beigebracht oder überprüft.

Die gematik hat von den Gesellschaftern den Auftrag erhalten, die Forderung nach Tests zu bewerten.

Zur Umsetzung dieses Auftrags ist die gematik in folgenden Schritten vorgegangen:

1. Analyse des Konzepts der Bundesärztekammer [Konzept] und Ermittlung von zusätzlichem Definitionsbedarf um die konzeptionelle Bewertung der Forderung nach Tests durchführen zu können
2. Definition und Annahmen zur Konzeption der Tests
3. Definition der Bewertungskriterien
4. Bewertung
5. Zusammenfassung und Handlungsempfehlung

Der Aufwand und die Kosten eines Tests sind nur dann zu rechtfertigen, wenn vorausgesetzt werden kann, dass eine zu testende Lösung alle Bedingungen für einen erfolgreichen Einsatz im Wirkbetrieb erfüllen wird. Dies soll durch eine konzeptionelle Bewertung überprüft werden. Die Bewertungskategorien und die wesentlichen Kriterien wurden entsprechend ausgewählt und mit dem Fachausschuss abgestimmt.

Das Konzept der BÄK [Konzept] definiert einen ungeschützten USB-Stick als dezentrales Speichermedium. Der Auftrag der Gesellschafter fordert jedoch die Bewertung der Forderung nach u. a. technikoffenen Tests. Die gematik ist also beauftragt, neben dem ungeschützten USB-Stick auch alternative Technologien zu betrachten. Die gematik setzt dies um, indem neben ungeschützten USB-Sticks auch weitere Implementierungsvarianten von dezentralen Speichermedien in die Bewertung einbezogen werden.

5 Informationen zur dezentralen Datenspeicherung

Die Telematikinfrastruktur der eGK arbeitet im Gegensatz zu anderen nationalen eHealth-Infrastrukturen nicht nach dem Konzept einer zentralen Datenspeicherung, bei der alle Daten an einem Ort liegen und zentral verwaltet werden.

Das Konzept der TI der eGK unterstützt ausschließlich die verteilte Verwaltung von Daten. Konkret gibt es folgende Varianten:

1. Speicherung von Daten in anwendungsspezifischen verteilten Fachdiensten (z.B. Fachdienste für eVerordnungen und AMTS, etc). Die Fachdienste werden von verschiedenen Entitäten betreut. Eine Einsicht oder ein Abgleich der Daten in den verteilten und unterschiedlichen Fachdiensten von einer zentralen Stelle aus ist nicht möglich.
2. Speicherung von Daten auf der eGK. Beispiele: Neben den Versichertendaten werden der Notfalldatensatz und der Organspendeausweis auf der Karte gespeichert. Die beiden Letztgenannten werden ausschließlich auf der Karte gespeichert. eVerordnungen können alternativ zum Fachdienst auch auf der eGK gespeichert werden. Weiterhin werden neben einem Testkennzeichen Protokoll-, Verweis-, Einwilligungs- und Versionsdaten auf der Karte gespeichert.

Beide Formen der Implementierung in der TI der eGK sind aus Sicht des Datenschutzes sicher und für die Speicherung von personenbezogenen medizinischen Daten mit sehr hohem Schutzbedarf geeignet.

Das Prinzip der Speicherung von personenbezogenen Daten auf dezentralen Medien ist z.B. vom deutschen Reisepass oder vom künftigen Personalausweis her bekannt. Hier werden sensible Daten (Fingerabdrücke) nur im Dokument selbst, nicht aber in einem zentralen System gespeichert. Dies hat natürlich den Nachteil, dass bei Verlust des Dokuments, die gespeichert Daten ebenfalls verloren sind und neu erhoben werden müssen. Nichtsdestoweniger begrüßen viele Bürger das Gefühl „Herr der eigenen Daten“ zu sein.

Dies wäre beim Einsatz der Technik in der TI der eGK ebenfalls zu erwarten. Die Option, persönliche medizinische Daten alternativ zu einem Fachdienst in einem dezentralen Speichermedium zu speichern, kann die Akzeptanz des Systems der eGK erhöhen.

Eine Fraunhofer-Studie [eHealth_Infrastrukturen] aus dem Jahr 2008 stellt jedoch fest, dass die Verwendung von Speichermedien im Vergleich zu dezentral vernetzen Speicherdiensten nicht automatisch zu einer realen Erhöhung der Sicherheit gegen Missbrauch der Daten führt, da die eigentliche Datenverarbeitung in der Regel außerhalb des Speichermediums erfolgt.

eGK und TI bieten für Fachanwendungen beide Realisierungsmöglichkeiten. Abhängig von den jeweiligen fachspezifischen Anforderungen können Fachanwendungen mit Speicherung der Daten in einem Fachdienst oder auf einem dezentralen Medium realisiert werden. Falls eine Speicherung der Daten in einem dezentralen Medium verwendet wird, bietet die TI darüber hinaus die grundlegenden Funktionalitäten um den Versicherten beim Schutz seiner personenbezogenen medizinischen Daten zu unterstützen.

6 Analyse des Konzepts der BÄK

Das Konzept der BÄK baut auf der Telematikinfrastruktur (TI) der eGK auf. Es ist nicht als Alternative zu den Aktivitäten zur Einführung der eGK, sondern als Ergänzung zu verstehen. Es wird ein dezentrales Speichermedium als zusätzliches Speichermedium des Versicherten vorgeschlagen. Das Konzept sieht ausschließlich eine dezentrale Speicherung von medizinischen Daten auf diesem Speichermedium vor, das unter alleiniger physischer Kontrolle des Patienten ist, solange es nicht bei einem Leistungserbringer verwendet wird. Die Nutzung der TI der eGK, der eGK des Versicherten und des HBA des Leistungserbringers bleibt dabei verbindlich gefordert. Das Konzept schließt ausdrücklich aus, den Datenspeicher unmittelbar am Primärsystem anzuschließen. Es beschreibt den mobilen Datenspeicher als Bestandteil der Telematikinfrastruktur, der zusammen mit der eGK genutzt werden soll (siehe [Konzept, Kap. 3.2]). Eine Zusammenfassung der Aussagen des Konzeptes findet sich in Kapitel A 2.

Nach dem Vorschlag der BÄK könnte der Versicherte wählen, ob die Daten von freiwilligen Anwendungen, die nach heutigem Stand in einem speziellen Fachdienst abgelegt werden, alternativ auf einem dezentralen Speichermedium gespeichert werden sollen, womit die Verantwortung für den Schutz der Daten auf den Versicherten übergehen würde.

Zur Durchführung von Tests von dezentralen Speichermedien müssen der Kontext und die Rahmenbedingungen des Tests klar definiert sein. Das [Konzept] lässt hier wichtige konzeptionell erforderliche Bereiche offen. Dadurch ist eine Bewertung der Forderung nach Tests allein auf Basis des vorliegenden Konzepts der BÄK nicht möglich.

Um den Auftrag der Gesellschafter erfüllen zu können, hat sich die gematik entschieden, die offenen oder nicht hinreichend detaillierten Punkte durch eigene konzeptionelle Annahmen zu ergänzen. Konkret gilt dies für die folgenden Themen:

1. **Anforderungen der Zielgruppe für die Nutzung dezentraler Speichermedien**

   [Konzept] benennt die Versicherten als Anwender des dezentralen Speichermediums.

   Als Voraussetzung für einen potentiellen Test und die konzeptionelle Bewertung der Forderung zur Durchführung technik- und ergebnisoffener Tests von Speichermedien muss beschrieben werden, welche weiteren Anwendergruppen die dezentralen Speichermedien potentiell nutzen sollen, welche Rollen, Verantwortlichkeiten und Aufgaben ihnen zufallen und welche spezifischen Anforderungen von diesen Anwendern ausgehen.

2. **Definition des Anwendungskontextes**

   [Konzept] enthält keine konkreten Vorschläge zu Fachanwendungen. Die Erfahrungen aus den Tests der RVO R1 haben jedoch gezeigt, dass Tests nur erfolgreich sein können, wenn diese anwendungsbezogen ausgeführt werden, der Anwendungszweck und die Anwendungsprozesse definiert und letztere anwenderfreundlich implementiert sind.

   Die Eignung einer Komponente wie z.B. eines dezentralen Speichermediums muss immer in einem zugeordneten Anwendungskontext gesehen werden. In diesem Anwendungskontext ist demzufolge auch zu testen und zu bewerten.

3. **Ermittlung der Anforderungen an dezentrale Speichermedien**

   [Konzept] hat keine detaillierten Anforderungen an die dezentralen Speichermedien festgelegt.

Es ist es jedoch für einen Test erforderlich, die Eigenschaften der Komponenten so zu spezifizieren, dass sie insbesondere den Anforderungen der Anwender gerecht werden. Diese Anforderungen (z.B. Speichervolumen, Speicherdauer, etc) können aus den definierten Einsatzszenarien und den allgemeinen Anforderungen der Anwender abgeleitet werden.

4. **Einordnung in zeitlichen Rahmen**

   Sofern die Forderung nach einem Test positiv bewertet werden sollte, müssen diese Tests konzipiert werden. Es ist erforderlich, die potentielle Verfügbarkeit der einzelnen Einsatzszenarien abzuschätzen und in einen möglichen zeitlichen Ablauf von Tests einzuordnen.

Die Annahmen und Definitionen zu den vorstehenden Punkten sind im Kapitel 7 beschrieben.

7 Rahmenbedingungen für mögliche Testmaßnahmen

Die Bewertung der Forderung nach einem Test und dessen Realisierung mit spezifischen Komponenten erfordert eine Definition der Rahmenbedingungen eines solchen Tests.

In den folgenden Kapiteln werden Annahmen und Definitionen eingeführt, die aus heutiger Sicht eine plausible und realitätsnahe Komplettierung der Randbedingungen eines potentiellen Tests dezentraler Speichermedien darstellen. Diese Annahmen gehen in die Bewertung der Forderung nach einem Test ein.

7.1 Anwender von dezentralen Speichermedien

Für die weitere Betrachtung wird vorausgesetzt, dass ein potentielles Angebot der alternativen Nutzung dezentraler Speichermedien nicht nur einzelne Gruppen von Versicherten adressiert, sondern für alle interessierten Versicherten diskriminierungsfrei nutzbar sein muss. Es ist zu beachten, dass dem Versicherten bei der Speicherung auf einem eigenen dezentralen Speichermedium die Verantwortung für den Schutz der Daten zufällt. Die Lösung zur dezentralen Speicherung muss so gestaltet sein, dass auch Versicherte ohne IT-Kenntnisse in die Lage versetzt werden, die damit verbundenen Aufgaben inhaltlich wahrnehmen zu können. Sonst wären diese von der Nutzung ausgeschlossen.

Weitere Anwender des dezentralen Speichermediums sind die Leistungserbringer. Medizinische Daten werden von Leistungserbringern in das Speichermedium gespeichert oder ausgelesen.

7.2 Generelle Nutzung von Telematik-Anwendungen

Im Laufe der nächsten Jahre ist eine Vielzahl von Telematikanwendungen im Gesundheitswesen zu erwarten. Eine wesentliche Herausforderung wird darin bestehen, einem Leistungserbringer die verschiedenen Daten, die von diesen Anwendungen generiert werden, möglichst schnell und einfach nutzbar zu machen. Dabei muss folgenden Forderungen durch entsprechende Maßnahmen Rechnung getragen werden:

1. **Auffindbarkeit und Verarbeitbarkeit**: Der Leistungserbringer muss die für den jeweiligen Behandlungsfall relevanten Daten schnell und zuverlässig finden können. Dies führt zu folgenden Annahmen: Es reicht nicht, einen großen Datenspeicher bereitzustellen, der alle denkbaren Dateien aufnehmen kann. Im Gegenteil, je höher die Zahl der verschiedenen Dateien, umso länger dauert die Suche und umso größer ist die Gefahr, wichtige Daten zu übersehen. Daher müssen Strukturen und Standards für die Bezeichnung und Repräsentation von Daten festgelegt werden. Nach diesen Regeln werden dann die Daten der verschiedenen Anwendungen in Fachdiensten oder im dezentralen Medium abgelegt oder gesucht. Diese Struktur darf nicht durch Unberechtigte manipulierbar sein, die Update-Fähigkeit und die Weiterentwicklung von Strukturen bleibt davon unberührt. Weiterhin müssen einheitliche Dateiformate z.B. für Bilddaten oder zur Kompression als Standard vorgegeben werden, um sicherzustellen, dass der Leistungserbringer die jeweilige Datei mit einer Standardsoftware einsehen kann.
2. **Strukturierung:** Daten im Fachdienst und auf dem zentralen Medium müssen verwaltet werden. Ziel muss sein, den Datensatz überschaubar zu halten und z.B. nicht mehr benötigte Daten zu entfernen (Prinzip der Datensparsamkeit). Grundsätzlich werden weder Fachdienst noch dezentrales Speichermedium als Archiv für medizinische Daten vorgesehen. Prozesse und Verantwortlichkeiten zur Verwaltung der Daten müssen definiert werden.
3. **Authentizität und Integrität:** Der Leistungserbringer muss sich auf die Authentizität und Integrität der Daten verlassen können. Daten sind ggf. zu signieren oder anderweitig gegen Manipulation zu schützen.
4. **Performanz und Nutzerfreundlichkeit:** Die Nutzung künftiger Anwendungen und insbesondere das Lesen und Scheiben von Daten darf die Prozesse beim Leistungserbringer nicht verkomplizieren. Dezentrale Speichermedien müssen eine vergleichbare Performanz bieten wie der entsprechende Zugriff auf Fachdienste. Dem Leistungserbringer kann nicht zugemutet werden, mehr als z. B. 20 sec auf im Fachdienst hinterlegte Daten zu warten.
5. **Datenvolumen:** Gleichzeitig müssen die dezentralen Speichermedien Anwendungen und Anwendungsdaten bzw. Datengrößen nur in dem Umfang unterstützen, der auch auf der Seite der Fachdienste unterstützt wird. Viele Leistungserbringer verfügen über eine DSL-Anbindung mit nur 1024kBits/s. Durch die Kombination der geforderten Antwortzeit und der zur Verfügung stehenden Bandbreite bei der Nutzung der TI ergeben sich Obergrenzen für die zu übertragenden Datenvolumen. Dateigrößen sind daher durch geeignete Auswahl der Inhalte und durch Kompression auf einen sinnvollen Wert zu begrenzen. Zu unterstützende Mindestgrößen der Daten ergeben sich aus den relevanten Anwendungen.
6. **Interoperabilität:** Die Daten von Fachanwendungen müssen im Rahmen der Spezifikation und von Tests interoperabel sein. Die zu verwendenden Datenstrukturen, Datenformate und ggf. Kompressionsalgorithmen sind dabei im Rahmen der Facharchitekturen festzulegen.

7.3 Exemplarischer Anwendungskontext

Die Eignung einer Komponente wie z.B. eines dezentralen Speichermediums muss immer in einem zugeordneten Anwendungskontext gesehen werden. In diesem Anwendungskontext ist demzufolge auch zu testen und zu bewerten.

Da [Konzept] diesbezüglich keine hinreichenden Vorgaben macht, soll an dieser Stelle ein exemplarischer Anwendungskontext definiert werden. Dieser besteht grundsätzlich aus folgenden Komponenten:

1. Beschreibung des **Anwendungszwecks**, also der generellen Ziele, die Versicherte und Leistungserbringer mit der Nutzung von Anwendung und der Speicherung der Daten verbinden.
2. Auswahl und Beschreibung **geeigneter Fachanwendungen**, deren medizinische Daten entweder in einem Fachdienst gespeichert werden oder auf dem dezentralen Speichermedium abgelegt werden könnten.
3. Definition von **Einsatzszenarien** für die Nutzung der Komponenten. Hier wird zusammengefasst, welche Anwendungen und Anwendungszwecke von einem dezentralen Speichermedium in einer speziellen Nutzungsart des Versicherten unterstützt werden sollen.

Die Definitionen zu diesen Punkten sind in den folgenden Unterkapiteln beschrieben.

7.3.1 Betrachtete Anwendungszwecke

Grundsätzlich lassen sich folgende Anwendungszwecke unterscheiden:

- Private Nutzung:
  - Bereitstellung von Daten vom Leistungserbringer an den Versicherten zur nicht versorgungs-/behandlungsrelevanten privaten Nutzung außerhalb der TI
  - Bereitstellung von Daten im Patientenfach für den Versicherten
- Patientenzentrierter Transport von medizinischen Daten von Fachanwendungen innerhalb der TI von Leistungserbringer zu Leistungserbringer:
  - Transport einmalig (von LE „A“ nach LE „B“) -> kurzlebig
  - Ungerichteter Transport (Mitführung), mehrfacher Zugriff -> Dauerhafte Speicherung / langlebig

Anwendungen mit dem Zweck des direkten Transports von medizinischen Daten (Labordaten, Abrechnung, Befunde, Dokumente bildgebender Verfahren) zwischen Leistungserbringern, bei denen der Versicherte nicht eingebunden wird, sind für die eGK nicht relevant und begründen keine Rahmenbedingungen für einen Test von dezentralen Speichermedien.

Für den Bereich der privaten Nutzung, wenn also Daten dem Versicherten bereitgestellt werden, existieren bereits Lösungen, die die Speicherung von z. B. sehr großen Bilddaten für den Versicherten ermöglichen. Die Speicherung erfolgt in der Regel ungeschützt (unverschlüsselt) und nicht manipulationssicher (keine Signatur des Leistungserbringers), dabei werden dem Größenbedarf entsprechende Medien (z.B. DVD-ROMs) verwendet. Diese Daten sind nicht für einen mit der weiteren Behandlung betrauten Arzt bestimmt.

Für die Bereitstellung von Daten kann zukünftig auch die freiwillige Fachanwendung Patientenfach genutzt werden. Dies gilt unabhängig vom Inhalt, also gleichermaßen für kurzlebige und langlebige Inhalte.

Die freiwillige Anwendung Patientenfach[2] nimmt eine Sonderrolle ein, weil dieses den alleinigen Zugriff durch den Versicherten in den Vordergrund stellt. Nur hier kann der Patient, unter Berücksichtigung der Anforderungen an den Datenschutz (Protokollierung) Daten ohne die Anwesenheit eines Arztes (technisch: eines Heilberufsausweises) zur eigenen Verwendung erhalten oder bereitstellen. Welchen Inhalt dieses Patientenfach haben kann, ist noch nicht näher spezifiziert. Aus dem Blickwinkel der universellen Nutzbarkeit des Patientenfachs mit

[2] SGB V, §291a, Abs. 3 Nr. 5

einem dezentralen Speichermedium muss aber sichergestellt sein, dass auch hier die abweichenden gesetzlich vorgesehenen Regeln für den Zugriff auf das Patientenfach umsetzbar sind.

7.3.2 Potentielle Anwendungen

Die Gesundheitsversorgung kann potentiell durch eine Vielzahl von Fachanwendungen auf der Basis der TI verbessert werden. Für den Test von dezentralen Speichermedien kommen nur solche in Betracht, die unmittelbare Berührung mit dem Versicherten haben. Aus der Menge dieser Anwendungen sollen für die Herleitung von Rahmenbedingungen für einen Test Stellvertreter ausgewählt werden, die bereits durch die Release-Planung der RVO oder den §291a explizit benannt sind oder zurzeit in Fachkreisen diskutiert und erarbeitet werden.

Für diese Fachanwendungen ist zu überprüfen, ob und wie die Speicherung auf einem dezentralen Speichermedium hinsichtlich der fachlichen Vorgaben sinnvoll und praktikabel umzusetzen ist. Dies sollte zu allen Aspekten einer Fachanwendung erfolgen. Da für eine Reihe dieser Fachanwendungen noch keine Fachkonzepte existieren, können die Anforderungen für dezentrale Speichermedien nur abgeschätzt werden. Eine qualifizierte Schätzung ist z. B. in Bezug auf benötigte Datenvolumen und Datentransfergeschwindigkeit sowie Verwendungszweck und Daten-Lebensdauer möglich.

Zu den Anwendungen, die zukünftig durch ein dezentrales Speichermedium unter Einbeziehung der eGK unterstützt werden könnten, gehören nach RVO Release 3:

Anwendung	Beschreibung	Größe pro Eintrag	Zweck
A1: Daten zur Prüfung der Arzneimitteltherapiesicherheit (AMTS)	Die AMTS-Daten ermöglichen es sowohl dem Arzt oder Apotheker als auch deren jeweiligen Mitarbeitern, zum Verordnungs-, Applikations- oder Einlösezeitpunkt vorhandene Informationen zum Arzneimittel mit den individuell therapierelevanten Daten des Versicherten zur Prüfung der Arzneimitteltherapiesicherheit abzugleichen. Damit können sowohl die Verfügbarkeit als auch die Qualität von Informationen zur Medikation des Versicherten erheblich verbessert werden. Die bereitgestellten Daten können vom Leistungserbringer sowohl für eine intellektuelle als auch für eine technisch unterstützte Prüfung der Arzneimitteltherapiesicherheit genutzt werden. Die fachliche Konzeption der Bereitstellung von Daten zur Prüfung der Arzneimitteltherapiesicherheit wird von der gematik, im Kontext der RVO Release 3 auf Basis der fachlichen Beschreibung der AG AMTS der Leistungserbringerorganisationen erarbeitet.	3-5 kByte	Dauerhafte Speicherung (kumulativ)

Tabelle 7-1 Liste möglicher Anwendungen gemäß RVO

Zu den Anwendungen, die zukünftig durch ein dezentrales Speichermedium unter Einbeziehung der eGK unterstützt werden könnten, gehören nach §291a:

Anwendung	Beschreibung	Größe pro Eintrag	Zweck
A2: Arztbrief	In einem Arztbrief kann ein Arzt u. a. durchgeführte und geplante Untersuchungen und Behandlungen sowie Befunde weitere relevante Informationen dokumentieren und einem anderen Leistungserbringer zur Verfügung stellen. Es existieren bisher Implementierungsleitfäden des VHitG, die eine Abschätzung der Größe der Datenmenge ermöglichen aber noch keine fachliche Konzeption als Grundlage für einen Test enthalten. Der Bericht soll vorzugsweise als strukturiertes Dokument gemäß HL7 Clinical Document Architecture (CDA) übermittelt werden können. Es handelt sich in der Regel um Datentransport mit Hilfe des Speichermediums, eine dauerhafte Speicherung ist vorstellbar.	ca. 50-400 KByte (ggf. plus ca. 50 - 500 KByte bei Verwendung von z.B. Bildern (o. ä.))	Transport (nicht kumulativ)

Tabelle 7-2 Liste möglicher Anwendungen nach SGB V, §291a

Zu den Anwendungen, die zukünftig durch ein dezentrales Speichermedium unter Einbeziehung der eGK unterstützt werden könnten, gehören im Weiteren:

Anwendung	Beschreibung	Größe pro Eintrag	Zweck
A3: Elektronischer Impfpass	Bei dieser Anwendung handelt es sich um einen Teil der aus §291a vorgegebenen freiwilligen Anwendung elektronisches Patienakte (vgl. §291a: Daten über Befunde, Diagnosen, Therapiemaßnahmen, Behandlungsberichte sowie Impfungen für eine fall- und einrichtungsübergreifende Dokumentation über den Patienten (elektronische Patientenakte)). Ein Fachkonzept für den Einsatz in Deutschland existiert noch nicht.	< 50 kByte (geschätzt))	Dauerhafte Speicherung (kumulativ)
A4: Patienten-Kurzakte (Patient Summary)	Eine Patienten-Kurzakte ist eine Zusammenfassung von Gesundheitsinformationen über einen Patienten, die von mehreren Ärzten ergänzt und angepasst werden kann. Ein Fachkonzept steht noch nicht zur Verfügung. Im Rahmen des Pilotprojekt epSOS (vgl. Anhang A 2) wird eine Konzeption zur grenzübergreifenden Nutzung erarbeitet, die sich als Grundlage eignen könnte. Um technische Anforderungen in Bezug auf den benötigten Speicherplatz zum jetzigen Zeitpunkt zu beurteilen, können die Ansätze CCR und HL7 CCD (/CDA) als Beispiele betrachtet werden.	ca. 100-400 KByte.	Dauerhafte Speicherung (kumulativ)
A5: Befunde bildge-	Ergebnisse bildgebender Verfahren (z.B.	< 2 MByte	Transport

Anwendung	Beschreibung	Größe pro Eintrag	Zweck
bender Verfahren (DICOM – Strukturierter Bericht)	Röntgen-, Ultraschallbilder) werden in der Regel am Ort der Erstellung durch einen Radiologen befundet. Zur Speicherung der radiologischen Befunde als strukturierter Bericht kann der DICOM Standard genutzt werden, der es gleichzeitig erlaubt, zugehöriges Bildmaterial zu speichern. Diese Anwendung geht von Bildmaterial in geringer Menge und reduzierter Qualität aus, die nicht zur Nachbefundung, sonder lediglich zur Übersicht für den Empfänger gedacht ist. Ein Fachkonzept ist für diese Anwendung noch nicht definiert.	(es ist davon auszugehen, dass die untere Grenze bei bildgebenden Verfahren je nach Komprimierung bei ca. 100 kByte liegt)	(nicht kumulativ)
A6: Messdaten / Vitalparameter am EKG (HL7 oder GDT)	Viele Geräte zur Erstellung von Elektrokardiogrammen, die auch zur Langzeiterhebung vom Patienten zuhause eingesetzt werden, bieten die Möglichkeit, Messdaten als HL7 oder GDT-Daten auf einen Rechner oder Datenträger zu übertragen. Die eGK oder ein dezentrales Speichermedium könnte genutzt werden, um die Daten zur Auswertung vom Gerät zum Arzt zu transportieren. Vergleichbare Anwendungen werden zurzeit nur in proprietären Lösungen realisiert. Ein einheitliches Fachkonzept existiert nicht.	<100KB pro Woche (geschätzt)	Transport (kumulativ)
A7: Daten bildgebender Verfahren (CT, MRT, Ultraschall, etc)	Hier sollen sehr große Datenmengen dem Versicherten bereit gestellt werden, um ihm die Ansicht in vollem Umfang für die private Nutzung zu ermöglichen. Ein nutzerzentriertes Fachkonzept für diese Anwendung existiert jedoch nicht.	100 MByte - 100 GByte.	Dauerhafte Speicherung (kumulativ)

Tabelle 7-3 Liste weiterer möglicher Anwendungen

Tabelle 7-3 verdeutlicht, dass die Vielzahl der einzelnen Anwendungen weniger als ein Megabyte Speichervolumen benötigt. Einzelne Anwendungen, wie der DICOM-Bericht oder andere Anwendungen, die medizinische Bilddaten verarbeiten, können auch etwas oberhalb dieser Marke liegen, benötigen jedoch nicht wesentlich mehr Speicher. Das Anwendungsbeispiel A7 für Daten bildgebender Verfahren fällt im Bezug auf das benötigte Speichervolumen aus dem generellen Rahmen.

Die Daten aus Anwendungsbeispiel A7 unterstützen eine Informationsanwendung für den Versicherten. Sie haben keine Relevanz für die Leistungserbringer und den Behandlungsprozess. Es geht z. B. darum, die Daten nach Hause zu transportieren und in der privaten Umgebung zu nutzen. Im Folgenden wird diese Anwendung deshalb nicht weiter betrachtet. Weitere Anwendungen, die einen ähnlich hohen Speicherbedarf haben, sind nicht bekannt.

Das Fraunhofer-Institut FOKUS präsentiert in seiner Studie [eHealth_Medien] eine generellere Kategorisierung von Fachanwendungen unter Berücksichtigung von benötigtem Speichervolumen, verfügbarer Kommunikationsinfrastruktur sowie Dauerhaftigkeit und Kumulativität der Speicherung. Auf der Basis dieser Anwendungskategorien leitet FOKUS anhand von zwei lediglich generischen Anwendungsbeispielen allgemeine Anforderungen für Speichermedien ab. Auf dieser Basis konnten die vier potentiell geeigneten Lösungsansätze „Ungeschützter USB-Stick“, „USB-Stick mit Schutzmechanismen“, „eGK mit erweitertem Speicher“

und „eGK mit zusätzlichem Speicher“ identifiziert werden, die auch Grundlage dieses Dokuments sind.

7.3.3 Ermittlung geeigneter Fachanwendungen

Für alle Fachanwendungen gilt, dass der Speicherort für Transport oder Vorhaltung der jeweiligen Daten entsprechend der jeweiligen fachlichen Anforderungen festgelegt wird. Die Einführung und der Test von dezentralen Speichermedien sind daher prinzipiell möglich, sobald geeignete Anwendungen, die sich für eine alternative Speicherung der Daten auf einem dezentralen Medium eignen, verfügbar sind. Zurzeit liegen jedoch für keines der genannten Anwendungsbeispiele eine Implementierung und auch noch kein hierfür erforderliches Fachkonzept vor. Nach der Erarbeitung der Fachkonzepte müssen zur Durchführung eines Tests die Anwendungen sowohl auf der Seite der Primärsysteme wie auch in den TI-Komponenten implementiert und vorbereitet werden.

Der Zeitrahmen eines potentiellen Tests muss sich zudem an dem generellen Plan zur Einführung von geeigneten freiwilligen Anwendungen der TI der eGK orientieren. Dieser ist durch die Umsetzung der RVO2006 vorgegeben. Tabelle 7-4 benennt Anwendungen, die im Rahmen der Testvorhaben eingeplant sind, und gibt an, wie diese in die benannten freiwilligen Anwendungen gem. §291a einzuordnen sind und ob sie prinzipiell für die alternative dezentrale Speicherung in Frage kommen.

Anwendung	**RVO-Release**	**Einordnung in §291a**	**Speicherung auf dez. Speichermedien möglich**
A1: AMTS	RVO Release 3	Benannte Freiwillige Anwendung	Ja
A2: Arztbrief	keine RVO-Zuordnung,	Benannte Freiwillige Anwendung	Ja
A3: eImpfpass	keine RVO-Zuordnung,	“elektronische Patientenakte“ (Teilaspekt)	Ja
A4: Patienten-Kurzakte	keine RVO-Zuordnung,	“elektronische Patientenakte“ (Teilaspekt)	Ja
A5: Befunde bildgebender Verfahren (DICOM – Strukturierter Bericht)	keine RVO-Zuordnung	• evtl. Modul der Freiwilligen Anwendung „Arztbrief“ • evtl. Nutzung im Rahmen der Freiwilligen Anwendung „Patientenfach“	Ja
A6: Messdaten / Vitalparameter am EKG (HL7 oder GDT)	Keine RVO-Zuordnung,	evtl. Nutzung im Rahmen der Freiwilligen Anwendung „Patientenfach“	Ja

Tabelle 7-4 Plan zur Einführung geeigneter Anwendungen

Anhand der Tabelle 7-4 ergibt sich, dass die freiwillige Fachanwendung AMTS im zeitlichen Rahmen von RVO Release 3 zum Test vorgesehen ist. Eine weitere Anwendung, die ggf. in späteren Stufen für Tests von dezentralen Speichermedien nutzbar gemacht werden könnte, ist der Arztbrief, der im Rahmen der freiwilligen Anwendungen insbesondere den Anwendungszweck Transport sinnvoll abdeckt.

7.3.4 Potentielle Einsatzszenarien

Im Kapitel 7.3.3 sind Anwendungen identifiziert und beschrieben worden, die potentiell mit dezentralen Speichermedien verwendet werden können. Ein Versicherter wird üblicherweise eine Auswahl, also mehrere verfügbaren Anwendungen nutzen. Es lassen sich Annahmen zu derartigen Einsatzszenarien mit einer Auswahl von Anwendungen für die Nutzung von dezentralen Medien treffen, die die Rahmenbedingungen für den Test von dezentralen Speichermedien weiter konkretisieren. Insbesondere kann z.B. die Gesamtsumme an benötigtem Speichervolumen für mehrere gleichzeitig genutzte Anwendungen aus den Abschätzungen des Kapitels 7.3.2 bestimmt werden.

Die Einsatzszenarien – also die Frage, wie viele bzw. welche Anwendungen gleichzeitig oder nacheinander genutzt werden, hängen von den Anwendungszwecken der Versicherten ab. Heute kann jedoch nur schwer vorhergesehen werden, welche Anwendungszwecke von den Versicherten angestrebt werden. Es ist zu erwarten, dass sich erst im Laufe der Zeit Anforderungen und Erwartungen an das System herausbilden werden. Nichtsdestoweniger sollen an dieser Stelle Annahmen zu exemplarischen Einsatzszenarien getroffen werden. Mit diesem Ansatz kann die Bandbreite der Anforderungen an die dezentralen Speichermedien für die Bewertung der Forderung nach Tests plausibel abgeschätzt werden.

Die Anwendungszwecke, die in den Einsatzszenarien zum Ausdruck kommen, korrespondieren zur Gesamtheit der in Kapitel 7.3.1 beschriebenen Einzelanwendungszwecke einer passenden Auswahl von Anwendungen. Zum einen ergeben sich einheitlich geprägte Einsatzszenarien:

Beispieleinsatzszenario 1 „Allgemeine medizinische Übersichtsinformationen“

- Anwendungen: AMTS, eImpfpass, Kurzakte
- Anwendungszweck: Dauerhafte Speicherung von Daten zur mehrfachen Nutzung bei Leistungserbringern.
- Speicherzeitraum: Dauerhaft: Die Lebensdauer der Daten ist nicht beschränkt.
- Kumulativität: Daten können je nach Fachanwendung ggf. kumulativ gespeichert werden.
- Benötigtes Speichervolumen im Speicherzeitraum (Lebensdauer des Speichemediums (5-10 Jahre): ca. 100 - 250 KByte
- Verwaltung durch Leistungserbringer (z.B. Hausarzt): Die Bereitstellung und ggf. Ergänzung der Daten erfolgt durch verschiedene Leistungserbringer

Beispieleinsatzszenario 2„Transport von spezifischen Informationen zum aktuellen Behandlungsfall“

- Anwendungen: Arztbrief, Befunde bildgebender Verfahren (DICOM–Bericht)
- Anwendungszweck: patientenzentrierter Transport von Daten von Fachanwendungen zwischen Leistungserbringern.
- Speicherzeitraum: Transport: Die Lebensdauer der Daten ist auf den Transport (wenige Tage) beschränkt. Die Löschung der Daten erfolgt nach dem Transport.
- Kumulativität: Daten werden nicht kumulativ gespeichert, die Größe ist dadurch beschränkt.
- Benötigtes Speichervolumen im Speicherzeitraum: Maximum der benötigten Einzelspeichervolumen der angeführten Anwendungen ist ca. 2 MByte.

§ Verwaltung durch Leistungserbringer (z.B. Hausarzt)

Darüber hinaus sind aber auch beliebige Mischformen als Anwendungszweck eines Einsatzszenarios sowie Einsatzszenarien mit anderen als den beschriebenen Aspekten möglich, wie z.B. die Bereitstellung von Daten zur privaten Nutzung durch den Versicherten möglich.

7.4 Abschätzung der Anforderungen an die dezentralen Komponenten

Dezentrale Speichermedien, die in den Wirkbetrieb eingeführt werden sollen, müssen für den Anwendungszweck des Nutzers und die zu unterstützenden Prozesse beim Leistungserbringer geeignet sein.

Um die Strukturierung und Abgrenzung von Daten von einer oder mehreren Anwendungen auf dem Datenträger zu schützen, muss ein Datenträger anwendungsspezifischen feingranularen Zugriffsschutz bieten. Eine generelle Freischaltbarkeit des gesamten Speichermediums ist nicht ausreichend.

Nicht alle Fachanwendungen verwenden eine digitale Signatur, um die Authentizität der Daten zu sichern. Die Authentizität der Daten muss in diesen Fällen über die Vertrauenswürdigkeit des Mediums als nicht manipulierbarer Datenspeicher, der nur durch vertrauenswürdige Instanzen beschrieben werden kann, gesichert werden. Mit einem vom Versicherten frei beschreibbaren Speichermedium kann eine Authentizität der Daten nur bei Verwendung einer digitalen Signatur sichergestellt werden.

Um den Großteil der benannten Anwendungen einzeln realisieren zu können, ist ca. 1 MByte Speichervolumen auf einem Datenträger notwendig. Einsatzszenarien mit mehreren Anwendungen können zum Teil ebenfalls mit diesem Speichervolumen realisiert werden (vgl. Beispieleinsatzszenario 1). Es existieren auch mögliche Einsatzszenarien, die mehr als 1 MByte Speichervolumen benötigen (vgl. Beispieleinsatzszenario 2). Es sind jedoch zurzeit keine relevanten Einsatzszenarien erkennbar, die durch Summierung von Speichererfordernissen langlebiger Anwendungen oder durch Einzelanwendungen mit großen Daten in den Bereich von hundert(en) Megabyte kommen.

Die erforderliche Performanz eines Datenträgers hängt direkt mit den von Fachanwendungen gespeicherten Datenvolumen zusammen. Für diese Betrachtung sind nur die Datengrößen von Einzelanwendungen relevant. Um z.B. bis zu 1 MByte in maximal 20 Sekunden speichern oder laden zu können, sind Übertragungsraten bis zu 50KByte pro Sekunde erforderlich. Eine solche Performanz wird voraussichtlich für eine Vielzahl von Anwendungen ausreichen.

Für Anwendungen, die Daten dauerhaft speichern, ist die Langlebigkeit des Mediums relevant, da häufiges Migrieren von Daten einen erheblichen Aufwand verursacht. Hier sollte für die Datenträger mindestens eine Langlebigkeit angestrebt werden, die sich an den Aufbewahrungszeiträumen der Daten von Fachanwendungen bei den Leistungserbringern orientiert. Eine kürzere Lebensdauer der Medien erfordert eine rechtzeitige Migration der Daten auf ein anderes Medium und steigert die Gefahr des Datenverlusts. Für Anwendungen zum Transport der Daten geben der Transport- und Behandlungszeitraum die notwendige Langlebigkeit des Mediums vor.

8 Mögliche Varianten des dezentralen Speichermediums

Der Auftrag der Gesellschafter der gematik beinhaltet die Bewertung der Forderung nach technikoffenen Tests. Ein technikoffener Test ist im Wortsinn nicht umsetzbar, da in jedem Fall vor dem Test die Komponenten, Schnittstellen etc feststehen müssen.

Um die Bandbreite der technisch möglichen Implementierungsvarianten berücksichtigen zu können, werden in den folgenden Unterkapiteln verschiedene Optionen der technischen Umsetzung eines dezentralen Speichermediums definiert. Die Variante „Ungeschützter USB-Stick“ (siehe Kapitel 8.1.1) ist in [Konzept] benannt.

Alle Implementierungsformen werden in die Bewertung einbezogen, um individuell die Eignung für ein Testvorhaben zu prüfen.

8.1 Dezentrale Speichermedien mit USB-Schnittstelle

8.1.1 Ungeschützter USB-Stick (STICK)

Die BÄK schlägt in ihrem Konzept [Konzept] vor, handelsübliche USB-Sticks ohne Sicherheitsfunktionen zu benutzen. Eine Festlegung auf einen Hersteller oder Herausgeber ist nicht beschrieben. Spezielle Anforderungen an das Speichermedium werden nicht erhoben.

Diese ungeschützten USB-Sticks gibt es von einer Vielzahl von Herstellern und in einer großen Bandbreite von Implementierungen. Es kommen verschiedene Verfahren zur Ansteuerung der Speicher und unterschiedliche Speichertechnologien zum Einsatz. Üblicherweise verfügen handelsübliche ungeschützte USB-Sticks über die in Tabelle 8-1 beschriebenen Eigenschaften.

Eigenschaft	Wert
Schnittstelle	USB 2.0 (Mass Storage Class)
Speichervolumen	1-64 Gbyte
Datenübertragungsrate	nominal 480MBit/s, real 3-30MByte/s abhängig von Leistungsklasse/Preis des USB-Stick
Zugriffschutz	nein
Manipulationsschutz der Speicher	nein
Datenerhaltzeitraum	Bei Sticks gehobener Leistungsklasse z. T. Herstellererklärung bzgl. der maximalen Zahl der Schreibzyklen und Datenerhaltzeitraum.
Inbetriebnahme	Automatischer Ablauf. Kein nennenswerter Zeitbedarf
Definierte Strukturen für Anwendungsdaten	Herstellerseitig nicht vorgesehen, können aber vom Anwender aufgebracht werden. Struktur kann nicht gegen Manipulation geschützt werden.
Sicherheitszertifizierung	nein
Formfaktor	Nicht definiert
Optische Personalisierung - Erkennbarkeit	Keine optische Personalisierung durch den Hersteller. Personalisierung kann z.B. vom Versicherten aufgebracht werden. Die-

Eigenschaft	Wert
	se Personalisierung ist nicht fälschungssicher.
Elektronische Personalisierung	nein
Preis	Geschätzt < 2,50€ bei hohen Stückzahlen (z.B. > 5 Millionen Stück). Preis schwankt stark in Abhängigkeit der Leistungsklasse. Geräte hoher Leistungsklasse sind aufwändiger implementiert (z.B. in SLC-Technologie, siehe [eHealth_Medien]), was sich in höherer Datenerhaltzuverlässigkeit und Performanz niederschlägt.

Tabelle 8-1 Eigenschaften des ungeschützten USB-Sticks (STICK)

8.1.2 USB-Stick mit Schutzmechanismen (STICK_S)

Die USB-Schnittstelle ist für den Anschluss von Peripheriegeräten wie Drucker und Scanner an Personal Computer (PC) entworfen worden und wurde im Jahr 1996 von der Firma Intel in den Markt eingeführt. Aspekte der IT-Sicherheit spielten dabei eine untergeordnete Rolle. Mobile USB-Speicher setzten sich aufgrund der einfachen Anwendbarkeit weltweit durch. Allerdings traten bei der Nutzung in sensiblen Bereichen Sicherheitsprobleme auf. USB-Sticks können z.B. dazu genutzt werden, geschützte Daten zu entwenden oder Schadsoftware wie z.B. Viren zu verbreiten. Immer wieder kam es auch zu Verlust von USB-Sticks, was die Offenlegung der darauf gespeicherten Daten zur folge hatte. Aus diesem Grund gibt es Firmen und Einrichtungen, die ihren Mitarbeitern die Nutzung von ungeschützten USB-Sticks untersagen.

Um diese Schwachstelle zu adressieren, haben Hersteller von USB-Sticks Schutzmaßnahmen in ihre Produkte aufgenommen. Dabei wird auf dem Stick zusätzlich ein Prozessor zur Verschlüsselung von Daten oder zum Verbergen von Speicherbereichen genutzt, die Authentifizierung erfolgt abhängig vom Produkt durch eine PIN oder ein biometrisches Verfahren (vgl. Studie „Speichermedien in der Hand des Versicherten“ [Studie_Fokus_Speichermedien], Kap. 6.2 „Sichere USB-Speicher“). Für die Ansteuerung des Speichermediums ist meist spezielle Software nötig, die jedoch nicht die kryptografischen Operationen durchführt.

Regierungsinstitute in den USA haben eigene Entwicklungen gestartet, um USB-Sticks sicher genug für den Transport von sensiblen Daten zu machen und unbefugten Zugriff zu verhindern. Dabei wird Chipkartentechnologie in den USB-Stick eingebaut.

Ein handelsüblicher USB-Stick mit Schutzmechanismen verfügt üblicherweise über die folgenden Eigenschaften:

Eigenschaft	Wert
Schnittstelle	USB 2.0 (Mass Storage Class)
Speichervolumen	1-64 Gbyte
Datenübertragungsrate	nominal >480MBit/s, real 3-30MByte/s abhängig von Leistungsklasse/Preis des USB-Stick
Zugriffschutz	Zugriffschutz auf Speicherbereich mittels PIN
Manipulationsschutz der Speicher	nein
Datenerhaltzeitraum	Bei Sticks gehobener Leistungsklasse z. T. Herstellererklärung bzgl. der maximalen Zahl der Schreibzyklen und Datenerhalt-

Eigenschaft	Wert
	zeitraum.
Inbetriebnahme	Üblicherweise Installation von herstellerspezifischen Treibern für z.B. PIN auf Host-Rechner vor erster Inbetriebnahme erforderlich
Definierte Strukturen für Anwendungsdaten	Herstellerseitig nicht vorgesehen, können aber vom Anwender aufgebracht werden. Struktur kann nicht gegen Manipulation geschützt werden.
Sicherheitszertifizierung	Ein Beispiel mit FIPS 140-Zertifizierung und Zulassung als Transportmedium für amerikanische Behörden bekannt. Es wurde bisher jedoch kein Produkt nach weltweit relevanten Standard Common Criteria zertifiziert.
Formfaktor	Nicht definiert
Optische Personalisierung	Keine optische Personalisierung durch den Hersteller. Personalisierung kann z.B. vom Versicherten aufgebracht werden. Diese Personalisierung ist nicht fälschungssicher.
Elektronische Personalisierung	nein
Preis	Geschätzt < 5€ bei hohen Stückzahlen (z.B. > 5 Millionen Stück)

Tabelle 8-2 Eigenschaften des USB-Sticks mit Schutzmechanismen (STICK_S)

Eine Marktsichtung durch Fraunhofer FOKUS hat ergeben, dass alle gefundenen Produkte eine Installation von herstellerspezifischer Software vor der ersten Inbetriebnahme erfordern. Diese Software müsste im konkreten Fall im Konnektor oder den Kartenterminals des Leistungserbringers vorab installiert werden. Hierbei sind die evaluierungsrelevanten Prozesse zu beachten. Dies kann der Leistungserbringer nicht leisten. Eine Nutzung von beliebigen, am Markt erhältlichen STICK_S ist dadurch ausgeschlossen. Es müsste vielmehr eine spezielle Variante für die Nutzung in der TI der eGK spezifiziert werden. Die entsprechende Software könnte dann standardmäßig im Konnektor und in den KT verfügbar gemacht werden.

8.2 Nutzung der eGK

Der Einsatz der eGK des Versicherten ist nach dem Konzept der BÄK mit der Nutzung des dezentralen Speichermediums verbunden. Der Versicherte muss nach diesem Ansatz also zwei Medien, die eGK und ein zusätzliches Speichermedium, mit sich führen. Es soll deshalb überprüft werden, ob Implementierungsformen, die Form und Funktion der eGK mit einem erweiterten Speicher verbinden, im Sinne eines technikoffenen Tests geeignet sein könnten. Dies würde die Einführung eines zweiten Mediums überflüssig machen.

8.2.1 eGK mit erweitertem Speichervolumen (eGK_M)

Diese mögliche Variante der eGK unterscheidet sich durch die heutigen Implementierungen nur durch einen erheblich größeren Speicher. Alle anderen Funktionen und auch die Sicherheitseigenschaften sind gleich. Geeignete Sicherheitschips mit Speichervolumen von 0,5 – 2MByte Speicher sind heute bereits von einigen Anbietern lieferbar. In den nächsten Jahren ist ein weiterer Ausbau der Speichergrößen und eine breite Anbieterbasis zu erwarten.

Die eGK mit erweitertem Speichervolumen verfügt über die folgenden Eigenschaften:

Eigenschaft	Wert
Schnittstelle	ISO/IEC7816
Speichervolumen	Bis zu 2 MByte
Datenübertragungsrate	nominal 115kBit/s, max 625 kBit/s
Zugriffschutz	Variabler, anwendungsspezifischer Zugriffschutz möglich
Manipulationsschutz der Speicher	ja
Datenerhaltzeitraum	>10 Jahre
Inbetriebnahme	Kein Aufwand erforderlich
Definierte Strukturen für Anwendungsdaten	Ja. Durch eGK-Spezifikation vorgegeben und durch Kartenherausgeber manipulationssicher aufgebracht.
Sicherheitszertifizierung	CC EAL4+ für Software, CC EAL5+ für Hardware, insgesamt also CC EAL4+
Formfaktor	ISO/IEC 7810 (Chipkarte)
Optische Personalisierung	Ja. Durch Kartenherausgeber durchgeführt.
Elektronische Personalisierung	Ja. Durch Kartenherausgeber durchgeführt.
Preis	Geschätzt < 2,50 € bei hohen Stückzahlen (z.B. > 5 Millionen Stück)

Tabelle 8-3 Eigenschaften der eGK mit erweitertem Speichervolumen (eGK_M)

8.2.2 Karte mit eGK-Funktion und zusätzlichem Speicher (eGK_M+)

Wesentliche größere Speichervolumen als bei der eGK_M lassen sich erreichen, wenn der sichere Chip, der die eGK-Funktion abbildet, durch einen zusätzlichen Speicherchip ergänzt wird. Beide Chips werden vom Chiphersteller in ein gemeinsames Gehäuse eingebracht und können vom Kartenhersteller auf klassische Weise in Karten eingebaut werden. Diese Karte verhält sich in der Anwendung wie eine eGK, bietet aber nach heutigem Stand Speichervolumen von mehr als 100MByte.

Eine Karte mit eGK-Funktion und zusätzlichem Speicher verfügt über die folgenden Eigenschaften:

Eigenschaft	Wert
Schnittstelle	ISO/IEC7816 Option: ISO/IEC 14443
Speichervolumen	Bis zu 2 GByte
Datenübertragungsrate	nominal 115kBit/s, max 625 kBit/s Option ISO/IEC14443 max 5 MBit/s
Zugriffschutz	Variabler, anwendungsspezifischer Zugriffschutz möglich
Manipulationsschutz der Speicher	Ja für sicheren Speicher des Security Controllers (analog zur eGK). Je nach Hersteller/Herstellungsprozess eingeschränkte Sicherheit für Zusatzspeicher.

Eigenschaft	Wert
Datenerhaltzeitraum	>5 Jahre
Inbetriebnahme	Kein Aufwand erforderlich
Definierte Strukturen für Anwendungsdaten	Ja
Sicherheitszertifizierung	CC EAL4+ für Software, CC EAL5+ für Hardware (ggf. außer Zusatzspeicher) , insgesamt also CC EAL4+
Formfaktor	ISO/IEC 7810 (Chipkarte)
Optische Personalisierung	Ja. Durch Kartenherausgeber durchgeführt.
Elektronische Personalisierung	Ja. Durch Kartenherausgeber durchgeführt.
Preis	Geschätzt < 4 € bei hohen Stückzahlen (z.B. > 5 Millionen Stück)

Tabelle 8-4 Eigenschaften der eGK mit zusätzlichem Speicher (eGK_M+)

9 Definition der Bewertungskriterien

9.1 Konzeption der Bewertung

Auftragsgemäß wurde von der gematik eine Konzeption zur Bewertung erstellt, die auf definierten Bewertungskriterien und der Nutzung des Wissens unabhängiger Experten beruht. Dieses konzeptionelle Vorgehen wurde mit dem Fachausschuss und dem Verwaltungsausschuss abgestimmt.

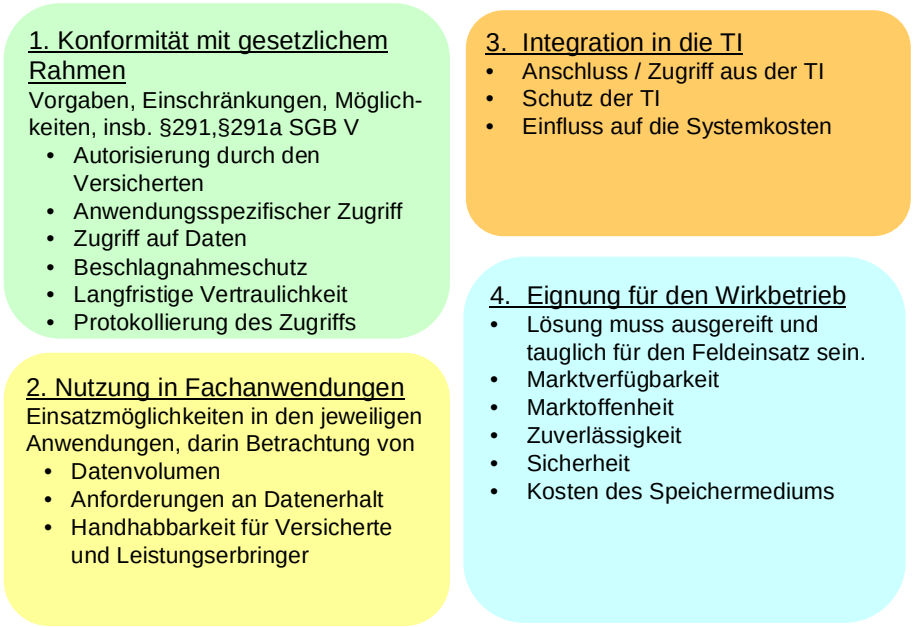


Abbildung 9-1 Vereinbarte Bewertungskriterien

Die Kriterien wurden in 4 Kategorien eingeteilt, die nachfolgend zur Gruppierung der Betrachtung verwendet werden.

Die Forderung nach einem Test kann nur unterstützt werden, wenn für eine Implementierungsform in allen Bewertungskategorien die Tauglichkeit für einen Einsatz im Wirkbetrieb nachgewiesen werden kann. Einzelne Kriterien sind von grundlegender Bedeutung und gelten als Ausschlusskriterien. Sofern eines dieser Ausschlusskriterien nicht erfüllt ist, kann der Forderung nach einem Test nicht entsprochen werden. Ausschlusskriterien werden bei der detaillierten Betrachtung der einzelnen Kriterien mit der Abkürzung AK gekennzeichnet.

9.2 Detaillierte Beschreibung der Bewertungskriterien

9.2.1 Definition der Kriterien der Bewertungskategorie 1 “Konformität mit dem gesetzlichen Rahmen”

Da im Konzept der BÄK das dezentrale Speichermedium in der Hand des Versicherten die Daten mit Hilfe der eGK verschlüsselt speichert, ist SGB V, §291a Abs. 3 anzuwenden: Die eGK wird dabei genutzt, um Daten im Kontext der freiwilligen Anwendungen zu erheben, verarbeiten oder zu nutzen.

Die Konformität zu den gesetzlichen Vorgaben ist eine Grundvoraussetzung für die Verwendung von Lösungen und Komponenten in der TI der eGK. Die folgenden Kriterien beschreiben wesentliche Anforderungen aus Gesetzen, der RVO und den Anforderungen an die Fachanwendungen, die für alle verwendeten dezentralen Komponenten verbindlich sind.

1.A Anwendungsspezifischer Zugriff, Einwilligung in die Nutzung freiwilliger Anwendungen

Für die Erhebung, Verarbeitung und Nutzung freiwilliger Anwendungen der eGK[3] ist das Einverständnis des Versicherten erforderlich[4]. Ausschließlich auf der eGK wird gespeichert, welche Fachanwendungen ein Versicherter nutzen möchte. Daten für freiwillige Fachanwendungen dürfen demnach durch den Arzt nur nach Prüfung der entsprechenden Stellen in der eGK genutzt werden. Liegt keine Einwilligung vor, dürfen Daten weder erhoben noch genutzt werden. Die Einwilligung des Versicherten muss dokumentiert vorliegen und fachanwendungsspezifisch sein. Die Dokumentation der Einwilligung muss manipulationssicher sein.

Es soll bewertet werden, ob diese Vorgaben generell und in der jeweiligen Implementierungsvariante technisch umgesetzt werden können.

Wird das Kriterium nicht erfüllt ist, führt dies zum Ausschluss des Mediums als geeignetes Verfahren (**AK**).

1.B Autorisierung durch den Versicherten

Es besteht die gesetzliche Vorgabe, dass der Versicherte den Zugriff auf seine personenbezogenen medizinischen Daten explizit (fallweise) autorisieren muss. Dies muss derart geschehen, das neben dem Vorlegen / Übergeben des Speichermediums auch technisch sicherzustellen ist, dass der Zugriff erst durch persönliche Willensbekundung (ausgedrückt durch das Eingeben der PIN) möglich ist[5].

[3] Vgl. SGB V, §291a, Abs. 3
[4] Vgl. SGB V, §291a, Abs 3, Sätze 3, 4
[5] Vgl. SGB V, § 291a Abs. 5 Satz 2

Mit diesem Kriterium soll bewertet werden, ob sichergestellt werden kann, dass der Zugriff auf Inhalte des Datenträgers generell nur nach der Zustimmung des Versicherten möglich ist und somit diese gesetzliche Vorgabe erfüllt werden kann.

Wird das Kriterium nicht erfüllt ist, führt dies zum Ausschluss des Mediums als geeignetes Verfahren (**AK**).

1.C Zugriff auf Daten

Gemäß § 291a Abs. 5 Satz 3 bis 5 SGB V ist sicherzustellen, dass der Zugriff auf Daten der Fachanwendungen nur im Zusammenhang mit den dort genannten Ausweisen / Signaturkarten / Autorisierungsverfahren möglich ist:

- Der Zugriff auf Daten der freiwilligen Anwendungen mittels der elektronischen Gesundheitskarte darf, mit Ausnahme der Fachanwendung „Patientenfach“, nur in Verbindung mit einem elektronischen Heilberufsausweis erfolgen[6].

- Der Zugriff auf Daten im Patientenfach darf durch den Versicherten ohne die Anwesenheit eines Heilberufsausweises geschehen, wenn der Zugriff protokolliert wird und der Zugriff mittels einer Karte autorisiert wird, die eine qualifizierte elektronische Signatur enthält.[7]

- Nur der Versicherte hat Zugriff auf Protokolldaten (vgl. 1.F).

Anhand dieses Kriteriums soll bewertet werden, ob der Zugriff auf Daten auf einem dezentralen Speichermedium mit diesen Vorgaben vereinbar ist.

Wird das Kriterium nicht erfüllt ist, führt dies zum Ausschluss des Mediums als geeignetes Verfahren (**AK**).

1.D Beschlagnahmeschutz

Gemäß §97 StPO ist eine Beschlagnahme der Gesundheitskarte bzw. von Daten der freiwilligen Anwendungen nicht möglich. Dies gilt auch für Daten, die zentral in der Telematikinfrastruktur gespeichert werden und auf die mittels der eGK zugegriffen werden kann[8]. Es ist zu klären, ob der Beschlagnahmeschutz auch für die Implementierungsvarianten des dezentralen Speichermediums gilt.

Eine juristisch eingehende Untersuchung zum Beschlagnahmeverbot eines USB-Datenspeichers, der optisch oder elektronisch nicht eindeutig zu einer bestimmten Person bzw. seiner eGK zuzuordnen ist, ist im Rahmen dieser Untersuchung nicht erfolgt.

Die Anwendbarkeit des Beschlagnahmeschutzes soll als Kriterium für die Bewertung der verschiedenen Implementierungsformen der dezentralen Medien herangezogen werden.

1.E Langfristige Vertraulichkeit, Vorgaben zu Verwaltung von Anwendungen

Für die Speicherung von medizinischen Daten müssen Verfahren angewendet werden, die eine langfristige Verfügbarkeit der Daten sicherstellen. Dies gilt auch für dezentral gespei-

[6] Vgl. SGB V, § 291a Abs. 5 Satz 3 SGB V:
[7] Vgl. SGB V, § 291a Abs. 5 Satz 3 SGB V:
[8] Vgl. [Gesundheitskarte_Rechtskommentare], S. 168-170, vgl. §97 StPO

cherte Daten. Die Herausforderung besteht darin, dass unter Berücksichtigung des zu erwartenden technischen Wandels von Speichertechnologien, Verschlüsselungsverfahren und Komponenten diese Daten im Maximalfall für die Lebensspanne des Versicherten verfügbar sein müssen. Dabei müssen auch die Maßnahmen zum Schutz der Daten den jeweiligen technischen Möglichkeiten folgen. So müssen z. B. verschlüsselte Daten auf neue, stärkere kryptografische Verfahren umgestellt werden können, ohne dass eine Entschlüsselung, selbst Jahre später, möglich wird. Alternativ muss durch das Speichermedium selbst ein wirksamer Schutz zur Verfügung gestellt werden, der den unberechtigten Zugriff auf Daten ausschließt.

Mit diesem Kriterium soll bewertet werden, ob diese Anforderung für die dezentrale Speicherung generell und für die einzelnen Implementierungsvarianten durch verschiedene Möglichkeiten umsetzbar ist.

Wird das Kriterium nicht erfüllt ist, führt dies zum Ausschluss des Mediums als geeignetes Verfahren (**AK**).

1.F Protokollierung des Zugriffs

Bei jedem Zugriff auf Daten muss technisch sichergestellt werden, dass eine Protokollierung des Zugriffs erfolgt. Als Bewertungskriterium soll betrachtet werden, ob eine nichtabstreitbare Protokollierung bei Einsatz des dezentralen Speichermediums sichergestellt ist[9].

Wird das Kriterium nicht erfüllt ist, führt dies zum Ausschluss des Mediums als geeignetes Verfahren (**AK**).

9.2.2 Definition der Kriterien der Bewertungskategorie 2 “Nutzung in Fachanwendungen”

Datenvolumen

2.A Einsatzszenariospezifische Betrachtung des erforderlichen Datenvolumens

Anhand der Definition der spezifischern Einsatzszenarien aus Kapitel 7.3.4 soll bewertet werden, ob die Implementierungsvarianten das erforderliche Speichervolumen bereitstellen.

Wird das Kriterium nicht erfüllt ist, führt dies zum Ausschluss des Mediums als geeignetes Verfahren (**AK**).

Anforderungen an den Datenerhalt

2.B Einsatzszenariospezifische Anforderungen an den Datenerhalt

Anhand der Definition der spezifischern Einsatzszenarien aus Kapitel 7.3.4 soll bewertet werden, ob das Speichermedium die die erforderlichen Prozesse zum Datenerhalt unterstützt.

[9] Vgl. § 291a Abs. 6 Satz 2 SGB V:

Handhabbarkeit für Versicherte und Leistungserbringer

2.C Handhabbarkeit

Mit diesem Kriterium soll die generelle Anwenderfreundlichkeit bewertet werden. Es gehen in die Bewertung ein:

1. Ist das Medium bequem und ohne Risiko mitzuführen?
2. Ist es möglich, das Medium ständig dabei zu haben? Dies vermindert das Risiko das Speichermedium bei Bedarf nicht zur Hand zu haben.
3. Müssen besondere Verfahren erlernt werden, um das Speichermedium einsetzen zu können?
4. Muss der Anwender zusätzliche Passworte oder PIN-Nummern anwenden?

2.D Zeitbedarf des Anwendungsfalls

Der Zeitbedarf bei der Speicherung oder dem Auslesen von Daten hängt von einer Reihe von Parametern ab. Die folgenden Einzelparameter sollen in die Bewertung einfließen:

1. Übertragungsrate zwischen Speichermedium und TI,
2. Zeitbedarf für Ver- und Entschlüsselung
3. Entsteht zusätzlicher Handhabungsaufwand durch z.B. das Wechseln des Mediums, das zusätzliche Eingeben von Pin-Nummern?
4. Performanz des KT, des Konnektors

Entscheidend für die Bewertung ist die Zeit, die ein Anwendungsfall insgesamt benötigt.

2.E Unterstützung beim Schutz der Daten

Bei der Speicherung in einem zusätzlichen dezentralen Speichermedium liegt der Schutz der personenbezogenen Daten in der Verantwortung des Patienten. Dabei ist zu beachten, dass Gefährdungen entstehen können, wenn z.B.

- § das Speichermedium gestohlen oder verloren wird,
- § ohne Wissen des Eigentümers ausgelesen werden kann,
- § die Daten zusätzlich auf unsicheren Systemen (z.B. dem Heim-PC) abgelegt werden.

Diese Gefährdungen entstehen auch dann, wenn die gespeicherten Daten durch Verschlüsselung oder Zugriffschutz geschützt sind. Kryptographische Maßnahmen haben eine endliche Lebensdauer. Üblicherweise wird ein Algorithmus für 6, maximal für 10 Jahre als sicher eingestuft. Danach besteht ggf. die Möglichkeit, die Schutzmaßnahmen mit relativ geringem Aufwand überwinden zu können.

Ein Konzept ist nur dann umsetzbar, wenn mit hinreichender Wahrscheinlichkeit davon ausgegangen werden kann, dass der Versicherte der Verantwortung für den Datenerhalt gerecht werden und für den Schutz seiner persönlichen Daten selbst sorgen kann.

Im konkreten Fall der TI der eGK muss jedoch davon ausgegangen werden, dass die große Mehrzahl der Versicherten keine IT-Experten sind, die die medizinischen Daten selbstständig verwalten, Backups in sicherer Umgebung selbstständig durchführen oder gar eine Umschlüsselung auf neue kryptographische Standards initiieren und begleiten können. Im Gegenteil, eine große Zahl der potentiellen Anwender auf Seiten der Versicherten haben keinerlei IT-Kenntnisse und wären bereits mit einem regelmäßigen Backup überfordert. Die

Lösungen der TI der eGK müssen jedoch diskriminierungsfrei jedem Interessenten zur Verfügung stehen. Es ist keine Option, nur IT-Experten die Nutzung der dezentralen Medien in Versichertenhand zu erlauben. Vielmehr muss die Systemlösung Verfahren bereitstellen, die die Nutzung für alle Interessenten sicher ermöglichen.

In die Bewertung geht deshalb die Umsetzbarkeit verschiedener technischer Maßnahmen ein, die der Versicherte benötigt, um seiner Verantwortung für den Datenerhalt und den Schutz seiner persönlichen Daten gerecht werden zu können.

Die folgenden Maßnahmen sollen die Versicherten beim Schutz der Daten unterstützen:

1. **Anwendungsspezifischer Zugriffschutz, der das unberechtigte Auslesen verhindert**

Ein Zugriffsschutz verhindert das unberechtigte Auslesen der Daten. Dieser Zugriffsschutz muss die Anwendungsdaten individuell schützen, da der Versicherte dem Leistungserbringer nicht Zugriff zu allen Daten auf dem Medium gewähren muss. Das Prinzip der Datensparsamkeit ist auch hier als Sicherheitsziel zu verstehen.

Wird das Kriterium nicht erfüllt, führt dies zum Ausschluss des Mediums als geeignetes Verfahren (**AK**).

2. **Protokollieren von Zugriffen**

Das Protokollieren von Zugriffen auf das Speichermedium und die Fachdienste ist bei der Nutzung der TI der eGK gefordert. Bei Nutzung des dezentralen Speichermediums müssen auch die protokollierten Zugriffe manipulationssicher abgelegt werden.

Wird das Kriterium nicht erfüllt, führt dies zum Ausschluss des Mediums als geeignetes Verfahren (**AK**).

3. **Möglichkeit zum Sperren des Mediums**

Geht das dezentrale Speichermedium verloren oder wird es gestohlen, können die gespeicherten Daten potentiell in unberechtigte Hände fallen und das Medium kann von einer unberechtigten Person weiterverwendet werden. Das Sperren des Mediums auf Anfrage des rechtmäßigen Besitzers verhindert dies.

Sofern eine Verschlüsselung der Daten mithilfe der eGK des Versicherten durchgeführt wurde, wird diese auch zum Entschlüsseln benötigt. Ein Angreifer würde also auch die eGK benötigen. Wenn er im Besitz der eGK ist, kann diese bei Online-Kontakt zur TI gesperrt werden, wenn Online-Updates der eGK gemacht werden. In diesem Fall entsteht kein unmittelbares Risiko für die Daten.

Es ergibt sich ein Risiko in folgenden Fällen:

a. Speichermedium und eGK sind in Besitz des Angreifers. Die eGK wird niemals Online betrieben (dadurch wird ein Umsetzen der Sperrung der Karte unmöglich). Dies erlaubt bei Kenntnis der eGK-PIN das Lesen der Daten.

b. Der Angreifer wartet, bis der kryptografische Schutz der Daten veraltet ist.

Bewertet wird die Verfügbarkeit der Möglichkeit zur Sperrung des Mediums.

Wird das Kriterium nicht erfüllt, führt dies zum Ausschluss des Mediums als geeignetes Verfahren (**AK**).

4. Erneuerung des Mediums, Update des Verschlüsselungsschutzes

Beim Austausch eines dezentralen Speichermediums dürfen – in Abhängigkeit von der Anwendung und der Lebensdauer der Daten - die gespeicherten Daten nicht verloren gehen, sondern müssen auf das neue Medium transferiert werden.

Kryptografische Mechanismen sind ständig wachsenden Möglichkeiten der Angreifer ausgesetzt und haben deshalb eine begrenzte Lebensdauer. Nach Ablauf dieser Frist werden sie als unsicher eingestuft.

Es soll bewertet werden, ob Mechanismen vorhanden sind, die die Versicherten beim Update des Verschlüsselungsschutzes der im dezentralen Medium gespeicherten Daten unterstützen.

9.2.3 Definition der Kriterien der Bewertungskategorie 3 “Integration in die TI”

Anschluss / Zugriff aus der TI

3.A Schnittstelle des Mediums zur TI

Zur Bewertung soll herangezogen werden, ob die passenden Schnittstellen für die verschiedenen Varianten des dezentralen Speichermediums an KT und Konnektor vorhanden sind oder ob diese Schnittstelle in die Geräte noch implementiert werden muss.

3.B Umsetzung der geforderten Funktionen in der TI

Das Konzept der BÄK sieht vor, dass die Verschlüsselung der Daten im Konnektor ausgeführt wird.

Zur Bewertung soll herangezogen werden, ob die notwendigen Verfahren (z.B. Verschlüsselung und Entschlüsselung) in der TI vorhanden sind oder noch hinzugefügt werden müssen.

3.C Erkennung des dezentralen Datenspeichers in der TI

Insbesondere in Umgebungen, in denen mehrere Kartenterminals und demzufolge auch mehrere weitere dezentrale Datenspeicher zum Einsatz kommen können, muss der Zugriff technisch und organisatorisch derart vorgenommen werden, dass der Zugriff nur auf dem vom Versicherten bereitgestellten Medium erfolgt. Dazu gehören Mechanismen, die das dezentrale Speichermedium anhand elektronischer Merkmale in der TI sicher erkennen können und optische Merkmale, die es dem Leistungserbringer oder seinem Personal ermöglichen, das Medium einer Person und seinen Daten verlässlich zuzuordnen.

Zur Bewertung soll herangezogen werden, ob es Vorkehrungen gibt, die es erlauben, das Medium eindeutig zu erkennen und dem Versicherten zuzuordnen.

Wird das Kriterium nicht erfüllt, führt dies zum Ausschluss des Mediums als geeignetes Verfahren (**AK**).

Schutz der TI

3.D Gefährdungen durch das Medium

Für alle Komponenten, die an die TI angeschlossen werden, muss sichergestellt sein, dass sie die Sicherheit und Verfügbarkeit der TI der eGK nicht beinträchtigen.

Es soll betrachtet werden, ob durch die Anwendung des Speichermediums Gefahren für die TI entstehen. Dies kann z.B. durch das Einbringen von Software bei der Erstnutzung geschehen.

Es muss bei dieser Betrachtung beachtet werden, dass zum Speichermedium und der notwendigen Schnittstelle keine Sicherheitsvorfälle größeren Ausmaßes bekannt sind bzw. es müssen die in diesem Fall getroffenen Gegenmaßnahmen Beachtung finden.

3.E Gefährdungen durch Dateninhalte

Durch die im dezentralen Speichermedium gespeicherten Daten kann Schadsoftware in die TI und insbesondere in die Primärsysteme eingebracht werden, da z. B. gewisse Bilddatenformate ausführbare Komponenten enthalten können.

Einfluss auf die Systemkosten

3.F Kosten durch neue Schnittstellen und Funktionen

Zur Bewertung soll der Aufwand herangezogen werden, der durch das Hinzufügen neuer Schnittstellen und die Umsetzung der geforderten Funktionen entsteht.

3.G Kosten durch zusätzlichen Arbeitsaufwand

Es soll abgeschätzt und bewertet werden, in welchem Maß durch die Speicherung in einem dezentralen Speichermedium zusätzliche Arbeitsaufwände beim Leistungserbringer entstehen. Hier soll auch die Speicherung im Fachdienst in den Vergleich aufgenommen werden.

3.H Risiken und Kosten durch Nichtverfügbarkeit von Daten

Die dezentrale Speicherung birgt die Gefahr des Datenverlustes, wenn das dezentrale Speichermedium verloren geht, gestohlen wird oder aufgrund eines Defekts nicht mehr ausgelesen werden kann. Außerdem kann es vorkommen, dass die Daten dem Leistungserbringer nicht zur Verfügung stehen, weil der Versicherte das dezentrale Speichermedium vergessen hat.

Es soll betrachtet werden, inwieweit dies generell gegen die Einführung der dezentralen Speicherung spricht und welche Unterschiede sich für die Implementierungsvarianten des Mediums ergeben.

Abschließend ist die Kostenwirkung abzuschätzen.

9.2.4 Definition der Kriterien der Bewertungskategorie 4 “Eignung für den Wirkbetrieb”

Die Lösungen, die in den Test aufgenommen werden, müssen eine klare Perspektive für die Tauglichkeit zum Einsatz im Wirkbetrieb haben.

4.A Marktverfügbarkeit der Speichermedien

Es soll betrachtet werden, ob zum geforderten Zeitpunkt eine hinreichende Anzahl von Herstellern die Komponente auf Anfrage entwickeln und liefern kann. Ziel ist es zu beurteilen, ob ein funktionierendes Marktgeschehen zustande kommen kann.

4.B Referenzen im Einsatzgebiet

Die TI der eGK und insbesondere die eGK und das dezentrale Speichermedium sind dem Einsatzgebiet Secure eIdenty zuzuordnen. Als Anwendungsgebiete zählen hierzu z.B. eHealth-Projekte mit dem Versicherten/Patienten als Anwender, nationale ID-Karten und Bürgerkarten, elektronische Führerscheine, Ausweis- und Reisedokumente. Wesentliche Randbedingungen dieses Einsatzgebiets sind ein hoher Schutzbedarf der Daten (z.B. bei personenbezogener Daten), hohe Zuverlässigkeit bei jahrelanger Nutzung durch den Anwender und sehr große Einsatzfelder (z.B. nationale Lösungen). Kleine Insellösungen mit fehlender Interoperabilität sind als Referenzen nicht aussagekräftig.

Selbst nach umfangreichen technischen Tests stellt die Einführung neuer Technologien in den Wirkbetrieb eines speziellen Einsatzgebiets ein Risiko dar, wenn keine realen Einsatzerfahrungen vorliegen.

In die Bewertung soll daher einfließen, ob positive Referenzen für einzelne technologische Lösungsansätze im Einsatzgebiet eIdentity existieren.

4.C Marktoffenheit

Das Ziel der Implementierung ist ein diskriminierungsfreier Marktzugang für alle interessierten Lieferanten, um ein funktionierendes Marktgeschehen zu erreichen.

Es dürfen nur Lösungen eingesetzt werden, die auf Normen oder offenen Spezifikationen beruhen. Proprietäre Konzepte sind ein Ausschlusskriterium. Um den Implementierungsaufwand und die erforderliche Entwicklungszeit abschätzen zu können, soll weiterhin bewertet werden, inwieweit bei den Implementierungsformen auf bereits bestehende Spezifikationen zurückgegriffen kann.

Wird das Kriterium nicht erfüllt, führt dies zum Ausschluss des Mediums als geeignetes Verfahren (**AK**).

4.D Zuverlässigkeit

Die ausschließliche Speicherung von personenbezogenen medizinischen Daten auf einem Speichermedium in Händen des Versicherten bedingt das Risiko des Datenverlustes, wenn das Medium verloren oder gestohlen wird und insbesondere auch bei einem Defekt. Der letzte Fall soll hier betrachtet werden.

Es müssen besondere Qualitätsmaßnahmen ergriffen werden, um die Funktion des Speichermediums für einen definierten Zeitraum mit hoher Wahrscheinlichkeit sicherzustellen zu können. Dazu müssen Prüfungen bzgl. Interoperabilität, Lebensdauer und Stabilität nach offenen Prüfspezifikationen durchgeführt werden. Diese Prüfungen müssen von neutralen, kompetenten Prüfinstituten durchgeführt und die Ergebnisse bestätigt werden. Die Erstellung der Prüfstandards und der Aufbau von Prüflaboren sind sehr zeitaufwendig und würden die Einführung der betreffenden Komponente erheblich verzögern.

In die Bewertung soll deshalb die Verfügbarkeit von Prüfspezifikationen und neutralen Prüflaboren für alle Tests eingehen. Für folgende Bereiche müssen Prüfspezifikationen und Prüfmöglichkeiten vorliegen:

1. Konformität und Interoperabilität der physikalischen Eigenschaften, Protokollebene und Anwendungsebene der Schnittstelle
2. Belastbarkeit des Gehäuses

3. Lebensdauer- und Zuverlässigkeitsprüfungen

4.E Nachweis der Sicherheit

Der Schutz der personenbezogenen medizinischen Daten ist ein wesentliches Bewertungskriterium. Insbesondere weil dezentrale Speichermedien in unberechtigte Hände gelangen können, ist der Schutz der Daten vor einem Auslesen oder einer Manipulation wichtig.

Aus diesem Grund müssen besondere Maßnahmen ergriffen werden, um die Sicherheit des dezentralen Speichermediums für einen definierten Zeitraum mit hoher Wahrscheinlichkeit sicherzustellen zu können. Dazu müssen offene Schutzprofile erstellt werden, nach denen die Evaluation und Zertifikation durchgeführt wird. Diese Prüfungen müssen von neutralen Prüfinstituten durchgeführt und die Ergebnisse nach einem anerkannten Verfahren bestätigt werden.

In die Bewertung soll deshalb die Verfügbarkeit von Schutzprofilen und neutralen Prüflaboren für alle Tests eingehen.

4.F Kosten des Speichermediums

Das dezentrale Speichermedium soll möglichst preisgünstig sein. Die Kosten sollen deshalb in die Bewertung eingehen.

4.G Migrationsunterstützung.

Die Anforderungen an die TI der eGK und auch an diejenigen des dezentralen Speichermediums können sich im Laufe der Zeit ändern. Dies kann dazu führen, dass die Implementierung geändert werden muss. Eine Migration von einem Implementierungsstand zum nächsten kann aus fachlichen Gründen oder auch aufgrund von veränderten Sicherheitsanforderungen erforderlich sein.

Die Lösungen müssen z.B. eine fachlich bedingte Datenmigration unterstützen. Eine Datenmigration kann erforderlich werden, wenn Änderungen aus dem Kontext einer Fachanwendung entstehen. Die Systeme der TI und die verwendeten Primärsysteme beim Leistungserbringer sind durch eine Software-Update entsprechend anzupassen und bereits existierende medizinische langlebige Daten sind gemäß eines definierten Vorgehensweise in einen weiterhin verarbeitbaren Stand zu überführen - Migration. Dieser Fall tritt dann ein, wenn die Grenze der Abwärtskompatibilät bei den beteiligten Systemen der TI erreicht ist und ein „altes Format“ abgekündigt wird.

Weiterhin ist sicherzustellen, dass mit Austausch der eGK – z.B. im Fall einer neuen Kartengeneration – die Bindung zwischen vorhandenem dezentralen Speichermedium und alter Karte auf die neue Karte übergeht.

Es ist zu betrachten, inwieweit dezentrale Speichermedien notwendige Migrationsanforderungen unterstützen

4.H Kontrollierter Austausch von dezentralen Speichermedien

Es ist zu betrachten, wie dezentrale Speichermedien, die aufgrund eines Sicherheitsvorfalls als unsicher oder sogar als Bedrohung für die Telematikinfrastruktur, die Umgebung des Leistungserbringers, die Umgebung des Kostenträgers oder des Versicherten eingestuft werden, vom Betrieb ausgeschlossen werden können.

Die durch einen Sicherheitsvorfall als unsicher oder als Bedrohung eingestuften dezentralen Speichermedien müssen von einer weiteren Nutzung technisch ausgeschlossen werden. Al-

ternativ kann dem Besitzer des Mediums die Bedrohung bekannt gemacht werden. Der Besitzer muss dann die weitere Nutzung sicher unterbinden.

Wird das Kriterium nicht erfüllt, führt dies zum Ausschluss des Medium als geeignetes Verfahren (**AK**).

10 Bewertung

Die Bewertung kann für jedes Kriterium aus den folgenden Perspektiven erfolgen:

(1) Bewertung bezogen auf die generelle Eignung der Speicherung in einem dezentralen Speichermedium für das spezielle Kriterium

(2) Bewertung der Eignung der einzelnen Implementierungsvarianten des Speichermediums für das spezielle Kriterium

Sofern sich keine relevanten Aspekte ergeben wird auch keine Beschreibung zu dem jeweiligen Punkt erstellt.

Um die Eignung der jeweiligen Lösungsvariante zu kennzeichnen, werden folgende Symbole verwendet:

Symbol	Bewertung
ì	Gut geeignet
è	Grundsätzlich geeignet
î	Schlecht geeignet
AK	Ungeeignet. Führt zum Ausschluss für die betrachtete Lösung

10.1 Bewertungskategorie 1 “Konformität mit dem gesetzlichen Rahmen”

1.A Einwilligung in die Nutzung freiwilliger Anwendungen (AK)

Mit der Nutzung einer freiwilligen Anwendung darf gemäß § 291a[10] erst begonnen werden, wenn der Versicherte gegenüber dem Leistungserbringer dazu seine Einwilligung erklärt hat. Die Information über die Einwilligung des Versicherten ist durch den Leistungserbringer auf der eGK zu dokumentieren. Es ist sicherzustellen, dass die Einwilligungsdokumentation auf Folgekarten übertragen werden kann. Weiterhin ist zu beachten, dass die Kostenträger keine Kenntnis über Daten der freiwilligen Anwendungen des Versicherten haben dürfen.

[10] Vgl. §291, Abs 3 Satz 1 SGB V

Die Einwilligung in das Betreiben einer freiwilligen Anwendung ist nach § 291a[11] durch den Versicherten jederzeit widerruflich und kann auf einzelne Anwendungen beschränkt werden. Der Widerruf der Einwilligung ist auf der eGK des Versicherten zu dokumentieren und die gesamten medizinischen und administrativen Daten dieser freiwilligen Anwendung sind automatisch zu löschen. Alle für diese freiwillige Anwendung erteilten Zugriffsberechtigungen müssen automatisch enden.

eGK_M und eGK_M+ enthalten wie die für den Basis Rollout vorgesehene eGK der Generation 1 die erforderlichen Strukturen und Mechanismen zur Speicherung der Einwilligungsinformationen für den Versicherten, da es sich um eine Folgegeneration der eGK handelt. Damit werden automatisch alle Anforderungen in Bezug auf die Nutzung und die damit verbundenen Einwilligungs- und Widerrufsprozeduren abgedeckt.

Für die freiwillige Anwendung „Notfalldaten“ wird die dezentrale Speicherung auf der eGK bereits genutzt. Somit kann angenommen werden, dass für weitere freiwillige Anwendungen die Speicherung von Daten auf dezentralen Speichermedien in Bezug auf die Berücksichtigung der Einwilligung nach dem gleichen Prinzip erfolgen wird. Die eGK erlaubt für die Notfalldaten keinen Zugriff ohne einen HBA, auch der Versicherte kann ohne den Leistungserbringer lediglich die Einwilligung dieser freiwilligen Anwendung verwalten.

Für eGK_M und eGK_M+ kann daher dieses Kriterium als erfüllt angesehen werden.

Für die Nutzung von STICK und STICK_S beim Leistungserbringer, wo eGK, HBA und Stick vorliegen, kann der Konnektor die Zugriffe auf den Stick unterbinden, wenn die erforderlichen Voraussetzungen (Einwilligung, HBA) nicht gegeben sind.

Als wichtige Bedingung wird aber deutlich, dass eine Erkennung des STICK durch den Konnektor möglich sein muss. Werden mehrere Kartenterminals an einem Konnektor betrieben darf die nur auf den zur eGK gehörigen Stick zugegriffen werden. Daher muss in einem weiteren Kriterium (vgl. 9.2.3 Abschnitt 3.C) bewertet werden, ob eine eindeutige Zuordnung des dezentralen Datenspeichers zum Versicherten möglich ist.

Das Lesen von auf STICK oder STICK_S gespeicherten und mit der eGK verschlüsselten Daten einer freiwilligen Anwendung ist technisch allerdings auch ohne die Anwesenheit eines HBA und eines Konnektors möglich. Zwar sind die Daten nicht unmittelbar nutzbar, aber ein Kopieren, bei dem es sich gemäß §3 BDSG bereits um eine Verarbeitung handelt, und ein etwaiges späteres Entschlüsseln können nicht verhindert werden, obwohl dann die Einwilligung zur Nutzung evtl. nicht mehr vorliegt.

Der Entzug einer Einwilligung in Abwesenheit des Sticks (z. B. bei Verlust des Sticks) kann eine Löschung der Daten nicht erzwingen. Der Versicherte muss sich in diesem Fall vergewissern, dass die Daten bzw. der Stick tatsächlich nicht mehr nutzbar sind oder in Kopien vorliegen, die ggf. kopiert werden können oder worden sind. Eine ggf. nicht mehr vorhandene Einwilligung kann im Gegensatz zur Speicherung auf der eGK nicht immer für STICK und STICK_S berücksichtigt werden.

Somit erfüllen STICK und STICK_S nicht in allen Fällen dieses Kriterium. Die Löschung der Daten von freiwilligen Anwendungen bei Entzug der Einwilligung kann nicht immer erzwungen werden.

Die Verarbeitung (z. B. „Übermittlung“) der verschlüsselten Daten durch ggf. nicht zugriffsberechtigte Personen kann außerhalb der TI nicht unterbunden werden (vgl. 1.C).

1.B Fallweise Autorisierung des Zugriffs (AK)

Zusätzlich zum in 1.A betrachteten Kriterium muss der Zugriff auf Daten einer freiwilligen Anwendung fallweise explizit autorisiert werden.

[11] Vgl. §291, Abs 3 Satz 4 SGB V

Das Konzept der BÄK, [Konzept], Kapitel 3.3 geht davon aus, dass ein Berechtigungskonzept für den Zugriff auf Daten nicht erforderlich sei, „wenn die Daten physisch vom Patienten an den Arzt übergeben werden“. Für alle Zugriffe auf Daten der freiwilligen Fachanwendungen gilt jedoch, dass eine bloße „Übergabe“ oder das „Vorhandensein“ des Mediums bzw. der Daten nicht ausreicht. SGB V verlangt ausdrücklich eine fachanwendungsbezogene Autorisierung durch technische Vorkehrungen durch den Versicherten, bevor die Daten der freiwilligen Anwendung durch die berechtigte Person genutzt werden dürfen.

Analog zur Betrachtung in 1.A. kann der Konnektor - bei entsprechender Anpassung - zusammen mit der eGK auch die fallweise Autorisierung (PIN-Eingabe) für den Zugriff auf den STICK sicherstellen, die Ver- und Entschlüsselung der Daten würde dann als Folgeschritt erfolgen. Auch hier gilt die Bedingung, dass eine eindeutige Identifikation des STICK gegeben sein muss.

Die Verarbeitung als solche kann aber auch hier ohne den Konnektor (also außerhalb der TI) nicht verhindert werden (vgl. 1.A). Anders als bei der Einwilligung muss für die hier betrachtete fallweise Autorisierung aber nur sichergestellt sein, dass ein Zugriff auf die Daten nicht möglich ist, wenn keine Autorisierung vorliegt. Der unautorisierte Zugriff auf Daten wird durch die Verschlüsselung verhindert, die Entschlüsselung würde damit implizit die Autorisierung bedeuten. Damit kann für den STICK das Kriterium als erfüllt betrachtet werden, wenngleich nicht abschließend geklärt werden konnte, ob dieses Verfahren alle Anforderungen aus gesetzlicher Sicht erfüllt.

Für STICK_S ist die Autorisierung ggf. in Abhängigkeit der konkreten Sicherheitsfunktionen auf dem Stick technisch umsetzbar. Dazu muss der STICK_S einen Zugriffsschutz für fachanwendungsbezogene Dateien bereitstellen, die z. B. für den Zugriff auf eine gespeicherte Datei in einem bestimmten Bereich eine Bestätigung des Nutzers verlangt.

Mit der im Rahmen dieser Studie untersuchte Variante STICK_S ist dies nicht möglich. Damit kann STICK_S dieses Kriterium nur erfüllen, wenn auch hier die Daten zusätzlich mit der eGK verschlüsselt werden. Somit geht ein Vorteil von STICK_S teilweise verloren, da dessen Sicherheitsmechanismen alleine nicht ausreichen und ein weiterer Schritt zur fallweisen fachanwendungsbezogenen Autorisierung erforderlich ist.

Für eGK_M und eGK_M+ kann dieses Kriterium als erfüllt angesehen, da die gleichen Regelungen wie für die eGK gelten, die die Autorisierung durch den Versicherten berücksichtigt.

Für STICK und STICK_S wird das Kriterium ebenfalls erfüllt, da der Konnektor die Funktion bereitstellen kann, sofern eine feste Zuordnung zwischen eGK und STICK bzw. STICK_S gegeben ist.

1.C Zugriff auf Daten (AK)

Das Erheben, Verarbeiten oder Nutzen[12] von medizinischen Daten ist nur den gesetzlich festgelegten Personenkreisen gestattet, d. h. nur den gesetzlich definierten Leistungserbringern ist der Zugriff gestattet. „Verarbeiten“ umfasst nach §3 Abs. 4 BDSG das „Speichern, Verändern, Übermitteln, Sperren, und Löschen personenbezogener Daten“.

Bei der Verwendung der eGK-Varianten eGK_M und eGK_M+ ist aufgrund der technischen Umsetzung im Zusammenhang mit dem HBA sichergestellt, dass ein Zugriff auf Daten freiwilliger Anwendungen nur erfolgen kann, wenn eine gegenseitige Authentisierung stattgefunden hat (Card2Card). Die eGK ist somit für freiwillige medizinische Fachanwendungen (mit Ausnahme des Patientenfachs) alleine nicht nutzbar, auch die Notfalldaten können nur im Beisein eines Leistungserbringers eingesehen werden.

Dementsprechend erfüllen die eGK-Varianten das Kriterium, dass nur die berechtigten Personen Zugriff auf personenbezogene medizinische Daten erhalten.

[12] Vgl. §291a, Abs 4 Satz 1

Die dezentralen Speichermedien STICK und STICK_S können die Verarbeitung durch nicht berechtigte Personenkreise technisch nicht verhindern. In der Umgebung des Leistungserbringers kann der Konnektor die Einhaltung der Zugriffsbeschränkung durchsetzen, außerhalb der TI ist dies nicht möglich.

Somit kann jeder, der Zugriff auf den Stick hat, Daten vom ihm kopieren oder löschen, d. h. „verarbeiten“ gemäß BDSG, unabhängig davon, ob er zum Zugriff auf medizinische Daten berechtigt ist. Bei STICK_S ist allerdings neben dem Besitz auch Wissen (PIN) oder eine biometrische Eigenschaft nötig (je nach Hardware des STICK_S), um diese Daten zu verarbeiten.

Für STICK und STICK_S bedeutet dies, dass selbst die Verwaltung gemäß [Konzept] von auf diesen Medien gespeicherten Daten nicht durch den Versicherten alleine erfolgen darf, wenn der Personenbezug der Daten erkennbar ist. [Konzept] sieht dazu vor, „Objekt-Tickets mit Metadaten und Schlüsselmaterial“ auf dem Stick zu speichern. Das vorgestellte Verfahren der hybriden Verschlüsselung bedeutet, dass alle Daten auf dem USB-Stick mit technischen Mitteln alleine durch den Versicherten sogar ohne Beisein eines Berechtigten (z.B. eines Arztes) einsehbar wären, da alle dafür erforderlichen Daten und die eGK beim Patienten vorliegen. Das gesetzliche vorgesehene 4-Augen-Prinzip kann damit umgangen werden.

Bezogen auf die Implementierungsvarianten STICK und STICK_S bedeutet dies, dass der rollenbezogene Zugriff für Daten von freiwilligen Anwendungen nicht sichergestellt werden kann.

Betrachtung für die freiwillige Anwendung Patientenfach

Eine Sonderrolle unter den freiwilligen Anwendungen nimmt das Patientenfach ein, das „von Versicherten selbst oder für sie zur Verfügung gestellte Daten“[13] enthalten kann. Nur auf Daten des Patientenfachs darf durch den Versicherten ohne die Anwesenheit eines Heilberufsausweises zugegriffen werden, wenn der Zugriff „mittels einer eigenen Signaturkarte, die über eine qualifizierte elektronische Signatur verfügt“[14] erfolgt. Daher wird im Folgenden betrachtet, unter welchen Voraussetzungen die Nutzung von dezentralen Speichermedien für die Fachanwendung Patientenfach möglich ist.

Für die eGK_M und eGK_M+ ist die Speicherung von Daten eines Patientenfachs auf eGK_M oder eGK_M+ dann möglich, wenn eine Signaturkarte des Versicherten zum Einsatz kommt, die tatsächlich eine qualifizierte elektronische Signatur enthält.

Für STICK und STICK_S wäre ggf. eine Nutzung als Patientenfach denkbar, da hier eine Nutzung der Daten durch den Versicherten außerhalb der TI explizit vorgesehen ist. Dennoch muss das dezentrale Medium zumindest für die Nutzung innerhalb der TI (z. B. beim Arzt, der Daten bereit stellt) Anforderungen der TI genügen, auch hier müssen Einwilligung, Autorisierung, Protokollierung (vgl. 1.F), Zugriffsberechtigung und Erkennbarkeit des Speichermediums in der TI (vgl. 9.2.3, Abschnitt 3.C) sichergestellt sein. Mit der derzeitigen Technik von STICK und STICK_S und der von der BÄK vorgeschlagenen Lösung scheint die Umsetzung noch nicht möglich, weitere Bewertungen im Dokument müssen dazu herangezogen werden.

STICK und STICK_S erfüllen somit dieses Kriterium nicht.

1.D Beschlagnahmeschutz

Daten der freiwilligen Anwendungen der eGK unterliegen dem Beschlagnahmeverbot. Im Zusammenhang mit dem Zeugnisverweigerungsrecht wird somit sichergestellt, dass z. B.

[13] §291a, Abs 3 Nr. 5
[14] §291a, Abs 4 Satz 3 vierter Halbsatz

ärztliche Unterlagen nicht indirekt durch Einsicht in die Daten eines Versicherten eingesehen werden können. Dies gilt sinngemäß auch für Datenträger, die ärztliche Aufzeichnungen speichern, die z.B. Befunde und Ergebnisse bildgebender Verfahren enthalten können.

Die eGK (damit auch die Varianten eGK_M, eGK_M+) ist zwar gemäß §97 StPO nicht explizit als beschlagnahmefreier Gegenstand aufgeführt, es kann aber nach [Gesundheitskarte_Rechtskommentare] davon ausgegangen werden, dass ein Beschlagnahmeschutz auch für die eGK besteht. Daten in der TI sind gemäß §97 StPO Satz 2 vor der Beschlagnahme geschützt.

Für einen STICK oder einen STICK_S kann man davon ausgehen, dass der Beschlagnahmeschutz nicht automatisch gilt, nur weil auf ihm mit der eGK verschlüsselte Daten abgelegt sein könnten. Der Nachweis, dass es sich um mit der eGK verschlüsselte Daten handelt, ist durch den Versicherten schwer zu erbringen, zumal auch andere verschlüsselte oder unverschlüsselte Daten auf dem Stick gespeichert werden könnten, die nicht mit der eGK in Beziehung stehen.

Eine juristisch eingehende Untersuchung zum Beschlagnahmeverbot eines USB-Datenspeichers, der optisch oder elektronisch nicht eindeutig zu einer bestimmten Person bzw. seiner eGK zuzuordnen ist, ist im Rahmen dieser Studie nicht erfolgt. Es erscheint aber unwahrscheinlich, dass ein handelsüblicher STICK oder STICK_S nicht beschlagnahmt werden könnte, nur weil der Inhaber (angeblich) Daten von freiwilligen Anwendungen der eGK auf ihm gespeichert hat. Selbst wenn die Daten nicht unmittelbar ohne die eGK entschlüsselt und genutzt werden können, stehen sie dem Versicherten nicht mehr zu Verfügung.

Somit ist anzunehmen, dass STICK und STICK_S dieses Kriterium nicht erfüllen.

1.E Langfristige Vertraulichkeit (AK)

Für die eGK-Varianten ist ein Zugriff durch Dritte (ohne HBA) auf die Daten der eGK (mit Ausnahme der ungeschützten VSD) z. B. bei Verlust nicht möglich, somit können Daten der freiwillig genutzten Anwendungen auf diese Weise auch dann nicht von der eGK ausgelesen werden, wenn die PIN des Versicherten vorliegt.

Bei STICK - und eingeschränkt auch bei STICK_S - kann die Sicherheit der Daten nicht durch die Komponente allein gewährleistet werden (wie das bei der Telematikinfrastruktur als Ganzes der Fall wäre), sondern der Versicherte muss selbst für deren Sicherheit sorgen.

Ein Verlust des STICK und damit der verschlüsselten Daten würde bedeuten, dass diese Verschlüsselung die einzige Barriere vor dem unerlaubten Zugriff ist. Werden zudem Datenobjekte auf dem Datenträger als personenbezogene Daten mit medizinischem Inhalt erkennbar, z. B. durch beigefügte Metainformationen, ist das Risiko für eine spätere Entschlüsselung eventuell sogar noch erhöht. Für STICK_S ist das Risiko geringer, da eine weitere Schutzmaßnahme den direkten Zugriff auf die gespeicherten Daten verhindert. Diese Schutzmaßnahme kann aber im Vergleich zu eGK_M und eGK_M+ leichter überwunden werden.

Alle Verschlüsselungsverfahren können über die Zeit ihre Wirksamkeit verlieren und müssen zur Aufrechterhaltung des Sicherheitsniveaus entsprechend angepasst werden. Auch die auf dem dezentralen Speichermedium gespeicherten verschlüsselten Daten müssten dieser Anpassung folgen, d. h. umgeschlüsselt werden. Da das nicht wie bei den Varianten eGK_M und eGK_M+ sichergestellt ist, verschlechtert sich das Sicherheitsniveau für STICK und STICK_S.

STICK und STICK_S erfüllen dieses Kriterium, jedoch zeitlich beschränkt.

1.F Protokollierung des Zugriffs (AK)

Zugriffe auf medizinische Daten müssen protokolliert werden, so dass der Versicherte den Datenschutz seiner Daten kontrollieren kann. Damit soll nichtabstreitbar dokumentiert werden, durch wen und wann ein Zugriff auf die Daten des Versicherten erfolgt ist.

Die eGK stellt technisch sicher, dass die Protokollierung des Zugriffs erfolgt, die Varianten mit großem Speicher könnten zukünftig auch mehr als die gesetzlich vorgeschriebene Mindestanzahl von 50 Einträgen speichern.

Ein Zugriff auf Inhalte auf einem STICK oder STICK_S kann nur dann auf ihnen selbst protokolliert werden, wenn dabei keine Möglichkeit der Manipulation der Protokolleinträge (z.B. durch Löschen) möglich ist. Eine Protokollierung der Zugriffe auf STICK oder STICK_S auf der eGK ist ohne technische Anpassungen an der eGK und an den STICK-Varianten nicht möglich, zumindest müsste eine eindeutige Zuordnung des STICKS zu einer eGK technisch möglich sein, damit Protokolle auf der eGK eine Relevanz haben. Die bloße Protokollierung, dass auf Daten auf einem „externen“ STICK oder STICK_S zugegriffen wurde, reicht spätestens bei Verlust eines der beiden dezentralen Medien nicht aus.

STICK und STICK_S erfüllen dieses Kriterium nicht.

10.1.1 Zusammenfassung der Bewertungskategorie 1

Die Zusammenfassung der Bewertung für die Kategorie „Konformität mit dem gesetzlichen Rahmen“ zeigt zwei wesentliche Ergebnisse:

1. Es ist möglich, die Option der Nutzung von dezentralen Speichermedien rechtskonform anzubieten. Des gelingt uneingeschränkt mit den Implementierungsvarianten eGK_M und eGK_M+.
2. Die Speichermedien STICK und STICK_S sind dagegen ungeeignet, da klare Ausschlusskriterien erfüllt sind.

Tabelle 10-1 stellt die Bewertungen für alle Kriterien und die abschließende Bewertung für die Kategorie „Konformität mit dem gesetzlichen Rahmen“ für alle Implementierungsvarianten dar.

	Kriterium	**Ungeschützter USB-Stick (STICK)**		**USB-Stick mit Schutzmaßnahmen (STICK_S)**		**eGK mit erweitertem Speicher (eGK_M)**		**eGK mit Zusatzspeicher (eGK_M+)**	
1.A	Prüfung der Einwilligung vor dem Zugriff	Nicht möglich	AK	Nicht möglich	AK	Kann wie bei eGK unterstützt werden	ì	Kann wie bei eGK unterstützt werden	ì
1.B	Fallweise Autorisierung des Zugriffs	Nicht möglich ohne Zuordnung von eGK und STICK (vgl. 3.C)	î	Nicht möglich ohne Zuordnung von eGK und STICK (vgl. 3.C)	î	Kann wie bei eGK unterstützt werden	ì	Kann wie bei eGK unterstützt werden	ì
1.C	Prüfung des Zugriffsberechtigten	Nicht möglich	AK	Nicht möglich	AK	Kann wie bei eGK unterstützt werden	ì	Kann wie bei eGK unterstützt werden	ì

	Kriterium	Ungeschützter USB-Stick (STICK)		USB-Stick mit Schutzmaßnahmen (STICK_S)		eGK mit erweitertem Speicher (eGK_M)		eGK mit Zusatzspeicher (eGK_M+)	
1.D	Beschlagnahmeschutz	Nicht gegeben	î	Nicht gegeben	î	Wie bei eGK	è	Wie bei eGK	è
1.E	Langfristige Vertraulichkeit	Eingeschränkt, aber kein Zugriffsschutz	è	Eingeschränkt Zugriffsschutz vorhanden	è	Wie bei der eGK gewährleistet	ì	Wie bei der eGK gewährleistet	ì
1.F	Protokollierung des Zugriffs	Nicht erzwungen. Nichtabstreitbarkeit kann technisch nicht erzwungen werden	AK	Nicht erzwungen. Nichtabstreitbarkeit kann technisch nicht erzwungen werden	AK	Kann wie bei eGK unterstützt werden	ì	Kann wie bei eGK unterstützt werden	ì
KAT1	Bewertung Kategorie 1: Konformität mit dem gesetzlichen Rahmen	Ungeeignet, da Ausschlusskriterien erfüllt.	AK	Ungeeignet, da Ausschlusskriterien erfüllt.	AK	In vollem Umfang wie bei eGK erfüllt.	ì	In vollem Umfang wie bei eGK erfüllt.	ì

Tabelle 10-1 Bewertung Kategorie 1 „Konformität mit dem gesetzlichen Rahmen“

10.2 Bewertungskategorie 2 “Nutzung in Fachanwendungen”

10.2.1 Datenvolumen

Der Speicherbedarf eines dezentralen Speichermediums und der Zeitraum der Speicherung von anwendungsspezifischen Daten werden durch die Art des Einsatzes des Speichermediums, die Anwendungen und den Anwendungszweck des Versicherten bestimmt. Exemplarische Testeinsatzszenarien sind in Kapitel 7.3.4 definiert worden.

2.A Einsatzszenariospezifische Betrachtung des erforderlichen Datenvolumens (AK)

Alle vier betrachteten Varianten der dezentralen Speichermedien verfügen für Testeinsatzszenario 1, der langfristigen Speicherung von Daten, über ausreichend Speicherplatz.

Für die ggf. zusätzliche Speicherung von kurzfristig relevanten Daten sind die Medien grundsätzlich ebenfalls geeignet, Lediglich bei großen Datenmengen, die sich z.B. beim Speichern von Dokumenten bildgebender Verfahren ergeben, kann die eGK_M in Abhängigkeit der Dateninhalte nicht ausreichend sein.

Somit erfüllt die eGK_M dieses Kriterium nicht.

	Kriterium	Ungeschützter USB-Stick (STICK)		USB-Stick mit Schutzmaßnahmen (STICK_S)		eGK mit erweitertem Speicher (eGK_M)		eGK mit Zusatzspeicher (eGK_M+)	
2.A.1	Erforderliches Datenvolumen Testeinsatzszenario 1	Deutlich mehr Speichervolumen als benötigt	ì	Deutlich mehr Speichervolumen als benötigt	ì	Benötigtes Speichervolumen vorhanden	ì	Deutlich mehr Speichervolumen als benötigt	ì
2.A.2	Erforderliches Datenvolumen Testeinsatzszenario 2	Deutlich mehr Speichervolumen als benötigt	ì	Deutlich mehr Speichervolumen als benötigt	ì	Benötigtes Speichervolumen nicht vorhanden	AK	Benötigtes Speichervolumen vorhanden	ì
2.A	Datenvolumen	Deutlich mehr Speichervolumen als benötigt	ì	Deutlich mehr Speichervolumen als benötigt	ì	Benötigtes Speichervolumen nicht vorhanden	AK	Benötigtes Speichervolumen vorhanden	ì

Tabelle 10-2 Bewertung Kriterium „Erforderliches Datenvolumen“

10.2.2 Anforderungen an den Datenerhalt

2.B Einsatzszenariospezifische Anforderungen an den Datenerhalt (AK)

Die TI der eGK wird ein Konzept zum Datenerhalt bereitstellen. Dieses Konzept für die eGK kann unverändert auch für eGK_M und eGK_M+ angewendet werden. Der Lebenszyklus der eGK wird vom Kartenherausgeber verwaltet.

Das Datenerhaltskonzept der TI könnte grundsätzlich auch für STICK und STICK_S erweitert werden, Allerdings liegt die Verantwortung für die rechtzeitige Initiierung des Datenerhaltsprozesses für STICK und STICK_S ausschließlich beim Versicherten. Dies bedingt Kenntnisse und ein entsprechendes Sicherheitsbewusstsein beim Versicherten. Daraus erwächst ein Risiko, dass der Datenerhalt nicht sachgerecht oder rechtzeitig umgesetzt wird.

	Kriterium	Ungeschützter USB-Stick (STICK)		USB-Stick mit Schutzmaßnahmen (STICK_S)		eGK mit erweitertem Speicher (eGK_M)		eGK mit Zusatzspeicher (eGK_M+)	
2.B	Datenerhalt	*bedingt geeignet*	è	*bedingt geeignet*	è	Geeignet	ì	Geeignet	ì

Tabelle 10-3 Bewertung Kriterium „Datenerhalt“

Handhabbarkeit für Versicherte und Leistungserbringer

2.C Handhabbarkeit

In die Bewertung des Kriteriums der Handhabbarkeit gehen mehrere Aspekte ein, die im Folgenden für die 4 Implementierungsvarianten besprochen werden sollen.

2.C.1 Ist das Medium bequem und ohne Risiko mitzuführen?

Für die Medien mit dem Formfaktor Karte (eGK_M und eGK_M+) kann dies uneingeschränkt bejaht werden. Die Beispiele der KVK und der Bankkarten zeigen, dass eine Karte bequem und ständig z.B. in der Brieftasche mitgeführt werden kann.

Prinzipiell gilt dies auch für einen USB-Stick. Allerdings wirkt sich in diesem Fall hinderlich aus, dass er zusätzlich zur eGK mitgeführt werden muss. Es ergibt sich daraus ein klarer Vorteil für die Varianten eGK_M und eGK _M+.

2.C.2 Ist es möglich, das Medium ständig mitzuführen?

Für die Medien mit dem Formfaktor Karte (eGK_M und eGK_M+) kann dies uneingeschränkt bejaht werden. Die Beispiele der KVK und der Bankkarten zeigen, dass eine Karte bequem und ständig z.B. in der Brieftasche mitgeführt werden kann.

Für einen USB-Stick gilt dies nur eingeschränkt. Dies insbesondere auch, weil handelsübliche USB-Sticks nicht auf die Eignung für den jahrelangen Einsatz z.B. als Schlüsselanhänger geprüft sind. Zusätzlich ist es recht unbequem und deshalb unwahrscheinlich, dass ein Patient dauerhaft eGK und Stick mitführt. Daraus ergibt sich ein Risiko, das die Daten bei Bedarf nicht zur Verfügung stehen.

Insgesamt sind die Varianten eGK_M und eGK _M+ gut geeignet, ständig mitgeführt zu werden. Die Varianten STICK und STICK_S unterstützen diesen Fall dagegen eher nicht.

2.C.3 Müssen besondere Verfahren erlernt werden, um das Speichermedium einsetzen zu können?

Die Handhabung eines Systems muss möglichst unkompliziert sein, um die Einarbeitung zu erleichtern und Anwendungsfehler zu vermeiden.

Bei der Nutzung der Varianten STICK und STICK_S kommt zusätzlich zur Verwendung der eGK ein weiteres Speichermedium hinzu, das in eine neue Schnittstelle eingesteckt werden muss. Es gibt damit für den Leistungserbringer komplett neue Anwendungsfälle zu bearbeiten.

Die beiden Varianten der eGK erfordern nur ein Medium und letztlich nur eine Abfrage, ob die Daten im Fachdienst oder auf der Karte gespeichert werden sollen. Die Verfahren sind gegenüber der klassischen Anwendung der eGK also nahezu unverändert.

2.C.4 Muss der Anwender zusätzliche Passworte oder PIN-Nummern anwenden?

Bei den Tests der eGK hat sich gezeigt, dass die Verwendung einer PIN für viele Versicherte schwierig ist. Die Verwendung einer weiteren PIN stellt ein zusätzliches Anwendungshemmnis dar. Die eGK_M und eGK_M+ kommen mit der bereits defi-

nierten PIN aus. Die Variante STICK ist nicht geschützt. Nur beim dezentralen Speichermedium STICK_S kommt ggf. eine zusätzliche PIN zum Einsatz. In den meisten Fällen wird es zumindest möglich sein, diese auf den gleichen Wert wie die eGK Pin zu setzen. Dadurch wäre zwar eine zusätzliche PIN einzugeben, der Versicherte müsste sich aber zumindest keine neue PIN merken.

Gesamtbewertung der Handhabbarkeit

Die Gesamtbewertung der Handhabbarkeit ergibt klare Vorteile für die erweiterten Implementierungen der eGK.

	Kriterium	Ungeschützter USB-Stick (STICK)		USB-Stick mit Schutzmaßnahmen (STICK_S)		eGK mit erweitertem Speicher (eGK_M)		eGK mit Zusatzspeicher (eGK_M+)	
2.C.1	*Bequemes Mitführen*	*Zwei Medien (eGK + Stick) erforderlich*	è	*Zwei Medien (eGK + Stick) erforderlich*	è	*Nur ein Medium (eGK) erforderlich,*	ì	*Nur ein Medium (eGK) erforderlich,*	ì
2.C.2	*Ständiges Mitführen möglich?*	*Formfaktor ist für dauerhaftes Mitführen als unbequem einzustufen. Dauerhaftes Mitführen unwahrscheinlich.*	í	*Formfaktor ist für dauerhaftes Mitführen als unbequem einzustufen Dauerhaftes Mitführen unwahrscheinlich*	í	*Karte im ID1-Format für dauerhaftes Mitführen gut geeignet*	ì	*Karte im ID1-Format für dauerhaftes Mitführen gut geeignet*	ì
2.C.3	*Besondere Verfahren erforderlich?*	*Ja. insbesondere durch zweites Medium des Patienten.*	è	*Ja. insbesondere durch zweites Medium des Patienten.*	è	*Nur neue Abfrage ob Speicherung im Fachdienst oder Speichermedium*	ì	*Nur neue Abfrage ob Speicherung im Fachdienst oder Speichermedium*	ì
2.C.4	*Zusätzliche PIN erforderlich?*	*Nein. STICK ist nicht durch eine PIN geschützt. Eingabe eGK-PIN ausreichend..*	ì	*Ja. Zusätzlich zur eGK-PIN muss eine PIN STICK_S eingegeben werden.*	è	*Nein. Einmalige Eingabe der eGK PIN reicht aus*	ì	*Nein. Einmalige Eingabe der eGK PIN reicht aus*	ì
2.C	Gesamtbewertung der Handhabbarkeit	Zweites Medium erforderlich	è	Zweites Medium erforderlich, zusätzliche PIN-Eingabe	í	Gleicher Prozess wie bei eGK. Kein Zusatzaufwand	ì	Gleicher Prozess wie bei eGK. Kein Zusatzaufwand	ì

Tabelle 10-4 Bewertung Kriterium „Handhabbarkeit“

2.D Zeitbedarf des Anwendungsfalls

In die Bewertung des Kriteriums der Handhabbarkeit gehen mehrere Aspekte ein, die im Folgenden einzeln bewertet werden sollen.

2.D.1 Übertragungsrate zwischen Speichermedium und TI

Bei der Übertragungsrate sind die beiden Implementierungen mit USB2.0 - Schnittstelle (STICK, STICK_S) den beiden Varianten der eGK nominal weit überlegen. Für Datenmengen >2 Mbyte ist die Schnittstelle nach ISO7816-3 ungeeignet. Die Übertragungszeiten kommen dann in den Bereich über 25 Sekunden. Sollen größere Datenmengen übertragen werden, müssen eGK_M und eGK_M+ schnellere Schnittstellen wie ISO7816-12 (max. 12 MBit/s, real bis zu 8 MBit/s) oder ISO14443 (max. 5MBit/s) benutzen. Dies würde allerdings wie bei STICK und STICK_S eine Spezifikationserweiterung der Kartenterminals bzw. ggf. des Konnektors erfordern.

2.D.2 Zeitbedarf für Ver- und Entschlüsselung

Das Konzept der BÄK fordert zu Recht eine Verschlüsselung der Daten, bevor diese auf dem Speichermedium USB-Stick gespeichert werden. Dies ist immer dann erforderlich, wenn kein sicherer Zugriffschutz existiert und der Speicherchip, in dem die Daten abgelegt werden, keinen hinreichenden Schutz gegen Angriffe aufweist. Dieser Schutz wird durch die Sicherheitszertifizierung nachgewiesen. Eine Verschlüsselung ist daher für STICK, STICK_S und – sofern der Zusatzspeicher nicht als sicher eingestuft ist - für eGK_M+ erforderlich. Für die eGK die eGK_M und ggf. auch die eGK_M+ gilt dies nicht, da deren Speicher als sicher eingestuft ist. Es bedarf deshalb keiner Verschlüsselung der Daten.

Die Verschlüsselung der Daten durch den Konnektor macht einen Teil des Zeitbedarfs des Anwendungsfalls aus. Die Verschlüsselung großer Datensätze kann mit der von der BÄK vorgeschlagenen Methode performant gelöst werden. Im konkreten Fall STICK und STICK_S stellt die Verschlüsselung einen untergeordneten Faktor für die Performanz der Schreib- und Lesevorgänge dar.

Die Verschlüsselung kann bei eGK, eGK_M und ggf. eGK_M+ entfallen, sofern der Anwendungskontext dies zulässt.

2.D.3 Zusätzlicher Handhabungsaufwand

Durch die Verwendung eines zweiten Speichermediums entsteht bei Nutzung von STICK und STICK_S ein zusätzlicher Handhabungs- und damit auch Zeitaufwand. Der Zeitbedarf für das Stecken und Entnehmen des USB-Stick zusätzlich zur Nutzung der eGK ist allerdings nicht erheblich. Gravierender ist, dass bei Nutzung des STICK_S eine zusätzliche PIN eingegeben werden muss. Dies erhöht den Zeitbedarf und insbesondere das Risiko durch operativen Problemen (Vergessen der PIN, Eingabe einer falschen PIN, etc).

2.D.4 Performanz des KT, des Konnektors

Die aktuell zugelassenen Kartenterminals unterstützen keine USB-Schnittstelle, die zum Anschluss von STICK und STICK_S benötigt wird. Auch sind diese Terminals nicht für sehr hohen Datendurchsatz (z.B. zum Konnektor) ausgelegt. Insgesamt stellen KT und Konnektor jedoch nicht den begrenzenden Faktor der Übertragungsgeschwindigkeit dar. Die Dimensionierung dieser Komponenten ist also angemessen.

Es gibt keinen prinzipiellen Unterschied in Abhängigkeit der Implementierungsvariante des dezentralen Speichermediums.

Gesamtbewertung Zeitbedarf

Der Zeitbedarf des Anwendungsfalls der Speicherung oder des Auslesens von Daten von einem dezentralen Speichermedium wird durch die Übertragungsgeschwindigkeit zwischen dem Medium und der TI und der Zeit, die eine ggf. erforderliche Ver- und Entschlüsselung der Daten benötigt, bestimmt. Die Vorteile, die STICK, STICK_S bei der Übertragungsrate haben, werden von eGK_M teilweise ausgeglichen, weil hier kein Zeitaufwand für die Verschlüsselung anfällt. Gleiches gilt für eGK_M+, sofern der Zusatzspeicher sicher implementiert wird. Insgesamt ist eGK_M bei Datenvolumen << 1MByte die effizienteste Implementierung bzgl. des Zeitbedarfs. Bei großen Datenvolumen schneidet eGK_M+ am besten ab, sofern ein sicherer Zusatzspeicher implementiert und ein schnelles Interface (ISO7816-12 oder ISO14443) verwendet wird. Tabelle 10-5 bietet eine Übersicht über die Bewertung zum Zeitbedarf des Anwendungsfalls.

Vergleich zur Speicherung in einem Fachdienst

Die Speicherung von Daten in einem Fachdienst unterliegt ebenfalls Randbedingungen, die die Performanz einschränken und den Zeitbedarf des Anwendungsfalls der Speicherung oder des Auslesens von Daten negativ beeinflussen. Ein Beispiel dafür ist die begrenzte Bandbreite einer DSL-Verbindung, die der limitierende Faktor für die Übertragungsgeschwindigkeit ist. Diese liegt z.B. beim Telekom-Produkt DSL1000 mit mind. 256kBit/s bei der Speicherung im Bereich der Bandbreite der Schnittstelle ISO7816-3. Das Lesen funktioniert ca. fünfmal schneller.

Der Vorteil der Speicherung im Fachdienst besteht darin, dass dieser Prozess im Hintergrund abgeschlossen werden kann. Der Leistungserbringer muss nicht abwarten, bis die Speicherung komplett erfolgt ist, sondern kann den Anwendungsfall abschließen und parallel neue Arbeiten aufnehmen. Die Dauer der Behandlung oder des Beratungsvorgangs wird also nicht durch die Speicherdauer beeinflusst.

Bei der versichertenzentrierten Kommunikation besteht allerdings die Vorraussetzung, dass der Versicherte dem Arzt dafür die Berechtigung erteilt, die Speicherung im Fehlerfall zu wiederholen. Die Umsetzung des entsprechenden Berechtigungskonzepts im Rahmen der Gesamtarchitektur ist in R3 vorgesehen. Der Versicherte kann in diesem Fall die Praxis verlassen, bevor die Speicherung abgeschlossen ist, weiß dann jedoch nicht sicher, wann der Speichervorgang abgeschlossen ist.

	Kriterium	**Ungeschützter USB-Stick (STICK)**		**USB-Stick mit Schutzmaßnahmen (STICK_S)**		**eGK mit erweitertem Speicher (eGK_M)**		**eGK mit Zusatzspeicher (eGK_M+)**	
2.D.1	*Übertragungsrate*	*Sehr schnell (>3MByte/s)*	ì	*Sehr schnell (>3MByte/s)*	ì	*Langsam (625kBit/s)*	î	*Langsam (625kBit/s), bei kontaktlos bis zu 5MBit/s*	î
2.D.2	*Zeitbedarf für Ver- und Entschlüsselung*	*Vernachlässigbarer Zeitbedarf*	ì	*Vernachlässigbarer Zeitbedarf*	ì	*Keine Ver- und Entschlüsselung erforderlich*	ì	*Je nach Implementierung des Produkts*	ì
2.D.3	*Zusätzlicher Handhabungsaufwand*	*Handling eines 2. Mediums*	î	*Handling eines 2. Mediums. zusätzliche PIN-Eingabe*	î	*Kein Zusatzaufwand*	ì	*Kein Zusatzaufwand*	ì

	Kriterium	Ungeschützter USB-Stick (STICK)		USB-Stick mit Schutzmaß-nahmen (STICK_S)		eGK mit er-weitertem Speicher (eGK_M)		eGK mit Zu-satzspeicher (eGK_M+)	
2.D.4	*Performanz des KT, Kon-nektors*	*Ausreichende Performanz*	è	*Ausreichende Performanz*	è	*Ausreichen-de Perfor-manz*	è	*Ausreichende Performanz*	è
2.D	Gesamtbe-wertung Zeit-bedarf	Vorteil der schnellen Über-tragung. Zu-satzaufwand durch Handha-bung von zwei Medien.	è	Vorteil der schnellen Übertragung. Zusatzaufwand durch Hand-habung von zwei Medien und zusätzli-cher PIN.	è	Geeignete Lösung für kleine Da-tenvolumen. Kein zweites Medium er-forderlich.	è	Geeignete Lösung für praxisgerech-te große Da-tenvolumen. Kein zweites Medium er-forderlich.	è

Tabelle 10-5 Bewertung Kriterium „Zeitbedarf des Anwendungsfalls“

2.E Unterstützung beim Schutz der Daten

Der Lösungsvorschlag der BÄK legt die Verantwortung für den Schutz der Daten und den Datenerhalt in die Hände des Versicherten, der sich für die dezentrale Speichermedien entscheidet.

2.E.1 Anwendungsspezifischer Zugriffsschutz (AK)

Der Zugriffsschutz verhindert den physikalischen Zugriff auf Daten. STICK verfügt über keinerlei Zugriffschutz. STICK_S verfügt über herstellerspezifische Zugriffschutzmechanismen, die bei den von FOKUS untersuchten Produkten nicht anwendungsspezifisch handhabbar sind. Ein anwendungsspezifischer Zugriffsschutz ist mit STICK und STICK_S deshalb nicht umsetzbar. Wie die eGK unterstützen auch eGK_M und eGK_M+ diese Schutzmaßnahme.

Das Fehlen dieser Schutzmaßnahme führt zum Ausschluss der Implementierungsvarianten STICK und STICK_S.

2.E.2 Protokollieren von Zugriffen (AK)

Das manipulationssichere Ablegen von protokollierten Zugriffsdaten ist bei der Verwendung von STICK und STICK_S nicht umsetzbar. Ein Ablegen der Daten auf der eGK ist ebenfalls nicht möglich, da keine eindeutige Bindung zwischen eGK und STICK bzw. STICK_S besteht (vgl. Bewertung 3.C).

eGK_M und eGK_M+ können diese Schutzmaßnahme unterstützen.

Das Fehlen dieser Schutzmaßnahme führt zum Ausschluss der Implementierungsvarianten STICK und STICK_S.

2.E.3 Möglichkeit zum Sperren des Mediums (AK)

Anders als die eGK und die Varianten eGK_M und eGK_M+ haben STICK und STICK_S keine eindeutige elektronische Kennung, sind dem Versicherten nicht fest zugeordnet und werden nicht von einem Herausgeber verwaltet, der z. B. auf Anfrage des Versicherten eine Sperrung durchführen kann.

Eine Sperrung von STICK und STICK_S ist nicht möglich. eGK_M und eGK_M+ können wie eine eGK gesperrt werden.

2.E.4 Erneuerung des Mediums, Update des Verschlüsselungsschutzes

Die eGK des Versicherten wird durch den Kartenherausgeber ausgetauscht, bevor die kryptografischen Mechanismen als unsicher eingestuft werden müssen. Der Versicherte muss also nicht auf das Verfallsdatum des kryptografischen Schutzes achten.

Sofern die Daten auf dem dezentralen Speichermedium mithilfe der eGK verschlüsselt wurden, müssen die Daten mit der alten eGK entschlüsselt , danach mit der neuen eGK wieder verschlüsselt und dann auf das dezentrale Speichermedium zurückgeschrieben werden. Es ist zurzeit kein Verfahren spezifiziert, wie und durch wen dies sicher umgesetzt wird. Eine Umsetzung scheint technisch möglich. Bei STICK, STICK_S und bei eGK_M+ mit ungesichertem Zusatzspeicher ist diese Verfahren anzuwenden.

Bei STICK und STICK_S liegt es in der alleinigen Verantwortung des Versicherten den Prozess rechtzeitig durchzuführen. Der Herausgeber der eGK kann nichts beitragen, da er von der Existenz des zusätzlichen dezentralen Speichermediums nichts weis. Dies wird viele Anwender überfordern und zu einem Datenverlust führen.

Bei Nutzung von eGK_M und eGK_M+ als dezentrale Speichermedien ist keine Erneuerung der Verschlüsselung nötig, da die Daten unverschlüsselt sicher gespeichert werden können. Zwar muss auch hier der Datentransfer in die neue Karte ausgeführt werden. Dies kann in Zukunft nach dem noch zu erstellenden Datenerhaltungskonzept der TI der eGK bewerkstelligt werden.

Gesamtbewertung zum Kriterium „Unterstützung beim Schutz der Daten“:

Beim Kriterium „Unterstützung beim Schutz der Daten“ sind für STICK und STICK_S bei den Unterkriterien „Anwendungsspezifischer Zugriffsschutz“ und „Protokollieren von Zugriffen“ massive Defizite identifiziert worden, die zum Ausschluss führen. Beim Unterkriterium „Erneuerung des Mediums, Update des Verschlüsselungsschutzes“ ist die Situation ähnlich. Die Varianten STICK und STICK_S sind für die Verwendung durch den Versicherten nicht geeignet, da die benötigten Hilfen zur Sicherstellung des Schutzes und der Verfügbarkeit der Daten nicht implementiert werden können.

Tabelle 10-6 bietet eine Übersicht über die Bewertung zur Unterstützung des Versicherten beim Schutz der Daten.

	Kriterium	Ungeschützter USB-Stick (STICK)		USB-Stick mit Schutzmaßnahmen (STICK_S)		eGK mit erweitertem Speicher (eGK_M)		eGK mit Zusatzspeicher (eGK_M+)	
2.E.1	*Anwendungsspezifischer Zugriffschutz*	*Nicht möglich*	*AK*	*Nicht möglich*	*AK*	*Kann wie bei eGK unterstützt werden*	*ì*	*Kann wie bei eGK unterstützt werden*	*ì*
2.E.2	*Protokollieren von Zugriffen*	*Nicht manipulationssicher*	*AK*	*Nicht manipulationssicher*	*AK*	*Kann wie bei eGK unterstützt werden*	*ì*	*Kann wie bei eGK unterstützt werden*	*ì*
2.E.3	*Sperren des Mediums*	*Nicht möglich*	*AK*	*Nicht möglich*	*AK*	*Kann wie bei eGK unter-*	*ì*	*Kann wie bei eGK unter-*	*ì*

	Kriterium	Ungeschützter USB-Stick (STICK)		USB-Stick mit Schutzmaß-nahmen (STICK_S)		eGK mit er-weitertem Speicher (eGK_M)		eGK mit Zu-satzspeicher (eGK_M+)	
						stützt werden		*stützt werden*	
2.E.4	*Erneuerung des Mediums*	*Erfordert IT-Wissen des Versicherten*	*î*	*Erfordert IT-Wissen des Versicherten*	*î*	*Kann wie bei eGK unter-stützt werden*	*ì*	*Kann wie bei eGK unter-stützt werden*	*ì*
2.E	Unterstüt-zung beim Schutz der Daten	Schutz der Da-ten kann von Versicherten nicht umgesetzt werden.	AK	Schutz der Daten kann von Versicher-ten nicht um-gesetzt wer-den.	AK	Wie bei der eGK gewähr-leistet	ì	Wie bei der eGK gewähr-leistet	ì

Tabelle 10-6 Bewertung Kriterium „Unterstützung beim Schutz der Daten“

10.2.3 Zusammenfassung der Bewertungskategorie 2

Die Zusammenfassung der Bewertung für die Kategorie „Nutzung in Fachanwendungen“ ergibt die folgenden Ergebnisse:

1. Die Speichermedien STICK und STICK_S sind ungeeignet, da ein Ausschlusskriterium, die mangelhafte Unterstützung des Versicherten beim Schutz seiner Daten, erfüllt ist. Die Ursache liegt in den fehlenden Schutzmaßnahmen dieser Implementierungsvarianten. Wesentliche Funktionen, die dem Versicherten helfen, seine personenbezogenen Daten sicher zu nutzen, stehen nicht zur Verfügung. Stattdessen ist nun der Versicherte selbst nach [Konzept] für den Schutz seiner personenbezogenen Daten verantwortlich. Dazu sind jedoch spezielle Fertigkeiten erforderlich, die der Versicherte üblicherweise nicht besitzt. Dem Versicherten wird damit eine Aufgabe auferlegt, die er nicht wahrnehmen kann. Dies führt zu gravierenden Konsequenzen: Entweder ein großer Teil der Versicherten muss von der Nutzung der dezentralen Speicherung absehen oder es entstehen –falls die dezentrale Speicherung nichtsdestoweniger genutzt wird –massive Sicherheitsprobleme für den Versicherten ohne dass ihm das notwendigerweise bewusst wird.
2. Bei realistischen Dateigrößen ist die Übertragungsgeschwindigkeit der Schnittstelle nach ISO7816-3 ausreichend. Für die in Kapitel 7.3.4 benannten Szenarien liegt die Größe einer einzelnen Datei bei 3-500kByte. Insbesondere dann, wenn der Standard mit 625kBits/s ausgeschöpft wird, liegen die zu erwartenden Transferzeiten damit üblicherweise unterhalb von 8 sec. Die USB 2.0 Schnittstelle ist zwar wesentlich schneller, allerdings müssen dann zwei Medien (eGK und STICK) gehandhabt werden. Dies macht den Geschwindigkeitsvorteil teilweise zunichte und führt zu einem vergleichbaren Zeitbedarf des Anwendungsprozesses.
3. eGK_M ist aus Sicht der anwendungsbezogenen Kriterien gut geeignet, kann aber nur bei Datenvolumen, die kleiner als 1 MByte liegen, genutzt werden. Dies ist für große Datenvolumen ein Ausschlusskriterium. Allerdings zeigen die angenommenen Einsatzszenarien, dass eine praktische Nutzung im Wirkbetrieb mit sinnvollen Anwendungen möglich ist.
4. eGK_M+ kann auch große Datenvolumen aufnehmen. Ansonsten ist die Handhabung wie bei der eGK. Die Geschwindigkeit der Schnittstelle nach ISO7816-3 ist für realistische Dateigrößen ausreichend. Optional könnte eGK_M mit einer Schnittstelle nach ISO14443 ausgestattet werden. Diese stellt heute Datenraten von 848kBit/s bereit

und wird nach der Umsetzung der in der Entwicklung befindlichen Spezifikationen zur VHDR (Very High Data Rate) Übertragungsraten bis zu 5 MBit/s erlauben.

Tabelle 10-7 stellt die Bewertungen für alle Kriterien und die abschließende Bewertung für die Kategorie „Nutzung in Fachanwendungen“ für alle Implementierungsvarianten dar.

	Kriterium	**Ungeschützter USB-Stick (STICK)**		**USB-Stick mit Schutzmaß-nahmen (STICK_S)**		**eGK mit er-weitertem Speicher (eGK_M)**		**eGK mit Zu-satzspeicher (eGK_M+)**	
2.A	Datenvolu-men	Sehr große Speicherkapa-zität	ì	Sehr große Speicherkapa-zität	ì	Nur für Da-tenvolumen bis zu 2MByte. Für große Datenvolu-men nicht geeignet (AK).	AK	Für alle er-warteten Einsatzsze-narien geeig-net.	è
2.B	Datenerhalt	bedingt geeig-net	è	bedingt geeig-net	è	Geeignet	ì	Geeignet	ì
2.C	Gesamtbe-wertung der Handhabbar-keit	Zweites Medi-um erforderlich	è	Zweites Medi-um erforder-lich, zusätzli-che PIN-Eingabe	î	Gleicher Pro-zess wie bei eGK. Kein Zusatzauf-wand.	ì	Gleicher Pro-zess wie bei eGK. Kein Zusatzauf-wand.	ì
2.D	Gesamtbe-wertung Zeit-bedarf	Vorteil der schnellen Über-tragung. Zu-satzaufwand durch Handha-bung von zwei Medien.	è	Vorteil der schnellen Übertragung. Zusatzaufwand durch Hand-habung von zwei Medien und zusätzli-cher PIN.	è	Geeignete Lösung für kleine Da-tenvolumen. Kein zweites Medium er-forderlich.	è	Geeignete Lösung für praxisgerech-te große Da-tenvolumen. Kein zweites Medium er-forderlich.	è
2.E	Unterstüt-zung beim Schutz der Daten	Schutz der Da-ten kann von Versicherten nicht umgesetzt werden.	AK	Schutz der Daten kann von Versicher-ten nicht um-gesetzt wer-den.	AK	Wie bei der eGK gewähr-leistet	ì	Wie bei der eGK gewähr-leistet	ì
KAT2	Bewertung Kategorie 2: Nutzung in Fachanwen-dungen	Ungeeignet, da Ausschlusskri-terien erfüllt.	AK	Ungeeignet, da Ausschlusskri-terien erfüllt.	AK	Gute Eig-nung für kleine Da-tenvolumen. Für große Datenvolu-men nicht geeignet	ì AK	Für alle er-warteten Einsatzsze-narien geeig-net.	ì

Tabelle 10-7 Bewertung Kategorie 2 „Nutzung in Fachanwendungen“

10.3 Bewertungskategorie 3 “Integration in die TI”

Anschluss / Zugriff aus der TI

3.A Schnittstelle des Mediums zur TI

Die aktuelle Implementierung der Kartenterminals ist für die Nutzung der eGK ausgelegt und unterstützt Speichermedien in Kartenform mit einer Schnittstelle nach ISO7816-3. Terminals, die die Komfortsignatur unterstützen, werden darüber hinaus mit einer Schnittstelle nach ISO/IEC14443 ausgestattet.

Die USB-Schnittstelle und auch die Implementierung nach ISO7816-12 (USB-Protokoll über die physikalische ISO7816-Schnittstelle) werden durch die aktuelle Spezifikation der Kartenterminals nicht unterstützt. Eine stichprobenartige Umfrage bei den Herstellern ergab, dass nicht davon ausgegangen werden kann, dass diese Schnittstellen nachgerüstet werden können.

Der Konnektor unterstützt je nach Bauart USB-Schnittstellen. Allerdings ist ein direkter Anschluss des dezentralen Speichermediums an den Konnektor für den Leistungserbringer in den meisten Fällen nicht praktikabel, da nur ein Konnektor in der Praxis, im Krankenhaus oder der Apotheke vorhanden ist. Die eGK und das dezentrales Speichermedium müssen jedoch an den Arbeitsplätzen, die mit KT und Primärsystemzugang ausgestattet sind, kombiniert und in einem definierten Ablauf eingesetzt werden können. Die Option des Anschlusses an den Konnektor wird deshalb verworfen.

Für die Bewertung der Implementierungsvarianten ergibt sich folgende Situation:

- STICK und STICK_S können nicht an die aktuell spezifizierten KT angeschlossen werden. Eine Erweiterung der Terminal-Hardware und/oder Software wäre je nach Gerät erforderlich, um diese Varianten zu unterstützen. Dies erfordert Neuentwicklungen durch die Hersteller und neue Zulassungen der Geräte. Bei STICK_S kommt hinzu, dass über die KT die zusätzliche PIN-Eingabe abgewickelt werden müsste. Dies würde Modifikationen der KT und des Konnektors erfordern.
- eGK_M benötigt keine Anpassung der existierenden Kartenterminals (ggf. sind Firmwareaktualisierungen zur Takt-/Geschwindigkeitsverbesserung möglich).
- eGK_M+ benötigt keine Anpassung der existierenden Kartenterminals sofern die Schnittstelle nach ISO7816-3 verwendet wird. Dies ist für begrenzte Datenmengen ausreichend.

  Für größere Datenmengen könnten Komfortsignatur-KT genutzt und auf deren Schnittstelle nach ISO14443 zurückgegriffen werden. Die Medien müssten dann als Dual-Interface-Karten ausgeführt werden. Alternativ könnte die KT um die Schnittstelle ISO7816-12 erweitert werden. Dies würde zumindest keine Gehäuseänderung erfordern und dadurch den Aufwand gegenüber einer Implementierung zusätzlicher USB-Schnittstellen an dieser Stelle begrenzen.

3.B Umsetzung der geforderten Funktionen in der TI

Die Steuerung der speziellen Anwendungsfälle - wie z.B. zur Auswahl zwischen Nutzung dezentraler Medien und Speicherung im Fachdienst - muss im System zusätzlich abgebildet werden. Dies gilt grundsätzlich für alle Varianten des Speichermediums.

Für die Nutzung von STICK und STICK_S ist die Ver- und Entschlüsselung der Daten erforderlich. Dies muss durch den Konnektor geleistet werden. Diese Funktion steht im Prinzip bereits zur Verfügung. Bei STICK_S kommt hinzu, dass über die KT die zusätzliche PIN-Eingabe abgewickelt werden müsste. Dies würde Modifikationen der KT und des Konnektors erfordern.

eGK_M+ benötigt ebenfalls die Ver- und Entschlüsselung von Daten falls der Zusatzspeicher nicht sicher implementiert ist. Dies kann aber je nach Herstellerimplementierung durch die Karte selbst geleistet werden.

eGK_M und – sofern der Zusatzspeicher sicher ist auch eGK_M+ – benötigen keine Ver- und Entschlüsselung der Daten durch den Konnektor.

3.C Erkennung des dezentralen Datenspeichers in der TI (AK)

Je nach Einsatzumgebung der dezentralen Komponenten bei den Leistungserbringern können an einem Konnektor mehrere Kartenterminals betrieben werden. Der Anschluss des dezentralen Speichermediums darf daher prinzipiell nicht direkt am Konnektor erfolgen, sondern am Kartenterminal oder für die Varianten STICK und STICK_S an einem speziellen Terminal, dass auch die hierfür erforderlichen Schnittstellen physikalisch bereitstellt.

In der TI haben alle Komponenten, auch die dezentralen Komponenten Konnektor, Kartenterminal und die eingesetzten Karten (eGK, HBA, SMC), digitale Identitäten, die eine sichere und eindeutige Kommunikation zwischen den Komponenten sicherstellen.

Speziell für die dezentralen Speichermedien gilt, dass eine Erkennung und ggf. Zuordnung von zusammengehörigen Speichermedien (z.B. USB-Stick und eGK) erforderlich ist, um auch in Einsatzumgebungen, wo mehrere Geräte gleichzeitig im Zugriff sind, sichergestellt ist, dass stets auf das zum Versicherten gehörige Medium zugegriffen wird. Neben der optischen Personalisierung ist somit eine elektronische nicht manipulierbare Identität des dezentralen Speichermediums erforderlich.

Die eGK und damit auch eGK_M und eGK_M+ erfüllen dieses Kriterium, da beim Kartenherausgeber die elektronische Identität der Karte festegelegt wird.

STICK und STICK_S verfügen derzeit über keine einheitliche technische Möglichkeit eine elektronische Personalisierung vorzunehmen, bei der eine Manipulation durch den Nutzer ausgeschlossen werden kann. Im Hinblick auf die Protokollierung kann somit auch eine Zuordnung der Protokolleinträge zu einem bestimmten Speichermedium nicht erfolgen. Verwechslungen von Speichermedien z. B. in größeren Praxen oder Krankenhäusern wären nicht auszuschließen.

3.D Gefährdungen durch das Medium (AK)

Das wesentliche Risiko besteht im Eintrag von Schadsoftware in die TI. Dazu wurden folgende Annahmen getroffen:

- Bei der Definition von STICK wurde vorausgesetzt, dass keine Treiber installiert werden müssen.
- Bei der Definition von STICK_S in Kapitel 8.1.2 wurde zusätzlich vereinbart, dass eine spezielle Variante für die Nutzung in der TI der eGK spezifiziert wird, die eine fest vorgegebene Treibersoftware aufweist. Diese Software könnte geprüft, freigegeben und dann im Konnektor und in den KT generell verfügbar gemacht werden. Eine herstellerspezifische Installation wäre dann überflüssig und die damit verbundenen Gefahren wären abgewendet.

Dies führt zu folgende Bewertungen der verschiedenen Implementierungsvarianten des dezentralen Mediums:

- Unter diesen Voraussetzungen ist eine Installation von Software auch zur Nutzung von STICK, STICK_S nicht erforderlich und wird demzufolge auch nicht unterstützt. In diesem Fall gibt es kein Risiko für die TI durch Nutzung der Implementierungsvarianten STICK und STICK_S. Anders ist die Situation, wenn STICK und STICK_S an einem normalen PC oder z.B. direkt am Primärsystem angeschlossen werden.
- Bei eGK_M und eGK_M+ besteht kein Risiko für die TI durch den Eintrag von Schadsoftware.

Speziell in letzter Zeit sind Sicherheitsvorfälle bekannt geworden, die gegen den Einsatz von USB-Schnittstellen für Daten mit hohem Schutzniveau sprechen[15].

3.E Gefährdungen durch Dateninhalte

Das Risiko besteht im Eintrag von Schadsoftware über bestimmte Datenformate in die TI. Dazu wurden folgende Annahmen getroffen:

- Es gibt eine fest vereinbarte Datenstruktur auf dem dezentralen Speichermedium.
- Datenformate, die für die einzelnen Anwendungen verwendet werden sollen, werden auf Sicherheitsrisiken geprüft. Die Verwendung dieser Datenformate wird verbindlich festgelegt.

Unter diesen Voraussetzungen ist die Nutzung aller vier Implementierungsvarianten unkritisch.

3.F Kosten durch neue Schnittstellen und Funktionen der TI

Bei der Bewertung der Kriterien „Schnittstelle des Mediums zur TI“ und „Umsetzung der geforderten Funktionen in der TI“ ist beschrieben worden, welche Erweiterungen der TI generell bei der Einführung der optionalen dezentralen Speicherung nötig werden und welche Erweiterungen in Abhängigkeit von der Implementierungsvariante des dezentralen Mediums umgesetzt werden müssten. Alle Erweiterungen der Komponenten und Dienste und auch die Einführung neuer Prozesse verursachen Kosten für die Erarbeitung der Konzepte, die Spezifikation, ggf. die Zulassung und Einführung neuer Komponenten.

Wichtig für die Ermittlung der Kosten ist, dass die Unterstützung einer dezentralen Speicherung von freiwilligen Anwendungen grundsätzlich erfolgen müsste. Der Versicherte wird erwarten, dass jeder Leistungserbringer diese Funktion unterstützen kann. Änderungen der TI und insbesondere der dezentralen Komponenten würden also flächendeckend eingeführt werden müssen.

(1) <u>Potentielle generelle Kostenwirkung bei Einführung der optionalen dezentralen Speicherung:</u>

Sofern die jeweilige Anwendung dies zulässt, soll es wahlweise möglich sein, die Daten im Fachdienst oder in einem dezentralen Medium des Versicherten zu speichern. Dazu sind bei der Implementierung der Anwendung in der TI, im Fachdienst und im Primärsystem Vorkehrungen (insbesondere die Optionswahl) zu berücksichtigen, die von der Variante des Mediums unabhängig sind. Die Kosten von potentiell nötigen Anpassungen der KT-Schnittstellen oder neuer Speichermedien werden

[15] todo

hier nicht betrachtet. Eine quantitative Aufwands- und Kostenschätzung ist auf Basis der jetzt verfügbaren Informationen nicht möglich. Nach aktueller Einschätzung sollten sich die Gesamtkosten der Implementierung einer Anwendung in der TI durch die generisch benötigten Funktionen zur optionalen dezentralen Speicherung nicht signifikant erhöhen.

(2) Potentielle Kostenwirkung in Abhängigkeit der Implementierungsvariante des Speichermediums:

Hier werden die Kosten von potentiell nötigen Anpassungen der KT-Schnittstellen und der Funktion der TI für die verschiedenen Varianten der Speichermedien betrachtet. Eine quantitative Aufwands- und Kostenschätzung ist auf Basis der jetzt verfügbaren Informationen nicht für alle Varianten möglich. Die Betrachtung fokussiert deshalb auf den Vergleich der Varianten.

- Die Einführung von STICK und STICK_S würde erhebliche Kosten verursachen. Es müssten z.B. die erforderliche Erweiterung der KT entwickelt und zugelassen, Verfahren zum Datenerhalt spezifiziert und implementiert werden, etc. Insbesondere müsste zumindest ein Teil der KT ausgetauscht werden.
- Die Einführung von eGK_M+ mit unsicherem Zusatzspeicher würde moderate Kosten verursachen. Bei Verwendung der Schnittstelle nach ISO7816 oder ISO14443 könnten die aktuell vorhandenen oder geplanten KT verwendet werden. Nur wenn eine Verwendung einer alternativen Schnittstelle gewünscht wird, wäre ggf. ein Tausch der KT erforderlich.
- Die Einführung von eGK_M und eGK_M+ mit sicherem Zusatzspeicher und Nutzung der Schnittstellen ISO7816-3 und ISO14443 würde keine nennenswerten Aufwende und Kosten im System verursachen, da bestehende Verfahren und Schnittstellen verwendet werden.

3.G Kosten durch zusätzlichen Arbeitsaufwand

Der zusätzliche zeitliche Aufwand, den der Leistungserbringer bei Nutzung der Option zur dezentralen Speicherung zu erbringen, ist bereits bei der Betrachtung des Kriteriums „Zeitbedarf des Anwendungsfalls“ bewertet worden. Da der Zeitbedarf der entscheidende Faktor bei der Ermittlung der Kosten durch zusätzlichen Arbeitsaufwand ist, kann diese Bewertung für die Varianten des Speichermediums direkt übernommen.

Hier kann nur ein qualitativer Vergleich der Implementierungsformen geleistet werden. Eine quantitative Abschätzung der Kosten erfordert eine detaillierte Ausarbeitung der Konzepte.

Vergleich zur Speicherung in einem Fachdienst:

Bei normalen Dateigrößen sollte der Zeitbedarf einer Speicherung im Fachdienst und im dezentralen Speichermedium ungefähr gleich sein. Die Speicherung im Fachdienst hat gegenüber der Speicherung in einem dezentralen Medium den Vorteil, dass dieser Prozess der Datenspeicherung im Hintergrund abgeschlossen werden kann. Der Leistungserbringer muss nicht abwarten, bis die Speicherung komplett erfolgt ist, sondern kann den Anwendungsfall abschließen und parallel zur Komplettierung der Speicherung im Fachdienst neue Arbeiten aufnehmen. Die Dauer der Behandlung oder des Beratungsvorgangs wird also nicht durch die Speicherdauer vorgegeben.

3.H Risiken und Kosten durch Nichtverfügbarkeit von Daten

Die dezentrale Speicherung birgt die Gefahr des Datenverlustes, wenn das dezentrale Medium verloren geht, gestohlen wird oder aufgrund eines Defekts nicht mehr ausgelesen wer-

den kann. Weiterhin kann es vorkommen, dass die Daten dem Leistungserbringer nicht zur Verfügung stehen, weil der Versicherte das Speichermedium vergessen hat.

(1) Generelle Bewertung der ausschließlich dezentralen Speicherung

Bei Speicherung im Fachdienst kann von einer professionellen Datensicherung ausgegangen werden. Ein kompletter Datenverlust ist sehr unwahrscheinlich. Dies ist bei der ausschließlichen Speicherung in einem dezentralen Medium anders. Das Medium kann abhanden kommen oder funktionsunfähig werden. Die gespeicherten Daten sind dann verloren. Um die Daten wiederzubeschaffen, müssen alle Leistungserbringer, die Daten abgelegt haben, die Daten erneut bereit stellen. Dies ist theoretisch möglich, da Leistungserbringer verpflichtet sind, medizinische Daten selbst zu archivieren. Allerdings wäre die Wiederbeschaffung der Daten mit einem erheblichen Aufwand des Versicherten und der Leistungserbringer verbunden. Alternativ müssten die entsprechenden Untersuchungen ggf. wiederholt werden.

Die Speicherung auf einem dezentralen Medium hat bei der Sicherstellung der Verfügbarkeit der Daten gravierende Nachteile gegenüber der Speicherung im Fachdienst. Auch [Konzept] räumt ein, dass die Verfügbarkeit nicht sichergestellt werden kann. Datenverlust ist möglich und führt zu erheblichen Aufwand und Kosten für Leistungserbringer und ggf. Kostenträger bei der Wiederbeschaffung. Weiterhin kann die Nichtverfügbarkeit von Daten zu Nachteilen für den Versicherten bei der Behandlung führen. Der Versicherte muss, bevor er die Wahl für eine dezentrale Speicherung trifft, über diese Nachteile und Gefahren aufgeklärt werden.

Die Wiederbeschaffung von verlorengegangenen Daten kann abhängig vom jeweiligen Fall erhebliche Kosten für Leistungserbringer, Kostenträger und den Versicherten verursachen.

(2) <u>Bewertung in Abhängigkeit der Implementierungsvariante des Speichermediums:</u>

Das vorstehend beschriebene Risiko eines Verlusts der Daten gilt für allen Implementierungsvarianten und ist der dominierende Faktor bei der Bewertung. Allerdings gibt es Unterschiede in der Handhabbarkeit der Lösung (siehe Kriterium „Handhabbarkeit“) die sich in untergeordnetem Maß auf die Verfügbarkeit auswirken können.

STICK und STICK_S müssen zusätzlich zur eGK mitgeführt werden. Die Wahrscheinlichkeit, dass beide Medien ständig mitgeführt werden, ist gering. Dies vergrößert das Risiko für die Verfügbarkeit der Daten. Die Nutzung von eGK_M und eGK_M+ hat hier Vorteile. Es wird nur ein Medium benötigt, das überdies bequem ständig mitgeführt werden kann.

10.3.1 Zusammenfassung der Bewertungskategorie 3

In der Bewertungskategorie „Integration in die TI“ wird die Erfüllung des Ziels der Verfügbarkeit der Daten zur Bewertung aller Varianten herangezogen. Die Verfügbarkeit kann bei dezentraler Speicherung nicht sichergestellt werden. Daraus ergibt sich ein generelles, signifikantes Risiko für die Speicherung von Daten auf dezentralen Medien.

Die Bewertung der verschiedenen Implementierungsvarianten zeigt, dass alle Implementierungsformen genutzt werden könnten, die Varianten der eGK jedoch einfacher und kostengünstiger in die TI der eGK zu integrieren sind. Allerdings zeigen sich erhebliche Unterschiede in der Bewertung zwischen den Varianten eGK_M, eGK_M+ und den beiden STICK-Implementierungen.

eGK_M und eGK_M+ können genau wie die eGK in der TI verwendet werden. Die KT und alle anderen Komponenten können unverändert bleiben. Lediglich wenn schnellere Schnittstellen gewünscht werden, müssten die Kartenterminals ggf. angepasst werden. In jedem Fall bleibt aber die Rückwärtskompatibilität gesichert. Die Kosten einer potentiellen Einführung in den Wirkbetrieb sind dementsprechend gering. Insbesondere kann der Leistungserbringer aufgrund der Rückwärtskompatibilität selbst entscheiden, ob er in neue, ggf. schnellere Terminals investieren möchte. Ein Zwang besteht dazu nicht. Alle Sicherheitsfunktionen werden wie bei der eGK unterstützt. Hier entstehen bei eGK_M und eGK_M+ weder neue Kosten noch neue Gefahren.

Für die Nutzung von STICK und STICK_S sind Spezifikationsänderungen an den KT und weitere Anpassungen der TI erforderlich. Eine Nutzung mit existierenden Komponenten kann nicht zugesichert werden. Eine Rückwärtskompatibilität ist dadurch nicht gegeben. Die kosten einer potentiellen Einführung sind demzufolge höher als bei eGK_M und eGK_M+.

Sicherheitsrisiken für die TI durch die Nutzung der verschiedenen Implementierungsvarianten des dezentralen Speichermediums sind nicht identifiziert worden. Dies gilt jedoch nur unter den angenommenen Voraussetzungen:

- STICK und STICK_S benötigen keine Installation von Treibern. Diese sind in den Komponenten der TI vorhanden.
- Dateistrukturen und Verwaltungsinformationen des Mediums sind korrekt und nicht manipulierbar.
- Dateiformate sind vorgegeben und enthalten keine Schadsoftware.

Sollte eine dieser Randbedingungen nicht eingehalten werden, können gerade bei STICK und STICK_S massive Risiken für die TI auftreten.

Tabelle 10-8 zeigt die Ergebnisse der Bewertungskategorie 3 „Integration in die TI“.

	Kriterium	**Ungeschützter USB-Stick (STICK)**		**USB-Stick mit Schutzmaßnahmen (STICK_S)**		**eGK mit erweitertem Speicher (eGK_M)**		**eGK mit Zusatzspeicher (eGK_M+)**	
3.A	Schnittstelle des Mediums zur TI	Erweiterung der KT erforderlich	î	Erweiterung der KT erforderlich. Zusatzaufwand für PIN-Eingabe	î	Schnittstelle vorhanden. Rückwärtskompatibilität gesichert.	ì	ISO7816-3-Schnittstelle vorhanden. Rückwärtskompatibilität gesichert. 14443-Schnittstelle bei Komfort-KT	ì
3.B	Umsetzung der geforderten Funktionen in der TI	Genereller Implementierungsaufwand, Aufwand für Ver- und Entschlüsselung	è	Genereller Implementierungsaufwand, Aufwand für Ver- und Entschlüsselung Zusatzaufwand für PIN-Eingabe	î	Genereller Implementierungsaufwand	è	Genereller Implementierungsaufwand. Ggf. Aufwand für Ver- und Entschlüsselung	è

	Kriterium	**Ungeschützter USB-Stick (STICK)**		**USB-Stick mit Schutzmaßnahmen (STICK_S)**		**eGK mit erweitertem Speicher (eGK_M)**		**eGK mit Zusatzspeicher (eGK_M+)**	
3.C	Erkennung des dezentralen Datenspeichers	Verwechslungen des Mediums möglich	AK	Verwechslungen des Mediums möglich	AK	Gegeben	ì	Gegeben	ì
3.D	Gefährdungen durch das Medium	Keine Gefährdungen bei Einhaltung der Randbedingungen	ì	Keine Gefährdungen bei Einhaltung der Randbedingungen	ì	Keine Gefährdung gegeben	ì	Keine Gefährdung gegeben	ì
3.E	Gefährdungen durch Dateninhalte	Keine Gefährdungen bei Einhaltung der definierten Randbedingungen	ì	Keine Gefährdungen bei Einhaltung der definierten Randbedingungen	ì	Keine Gefährdungen bei Einhaltung der definierten Randbedingungen	ì	Keine Gefährdungen bei Einhaltung der definierten Randbedingungen	ì
3.F	Kosten durch neue Schnittstellen und Funktionen der TI	Erhebliche Kosten durch neue KT und Verfahren in der TI	î	Erhebliche Kosten durch neue KT und Verfahren in der TI	î	Moderate Kosten	ì	Moderate Kosten bei Verwendung der vorhandenen Schnittstellen der TI (ISO7816-3, ISO14443)	ì
3.G	Kosten durch zusätzlichen Arbeitsaufwand[16]	Vorteil der schnellen Übertragung. Zusatzaufwand durch Handhabung von zwei Medien.	è	Vorteil der schnellen Übertragung. Zusatzaufwand durch Handhabung von zwei Medien und zusätzlicher PIN.	è	Geeignete Lösung für kleine Datenvolumen. Kein zweites Medium erforderlich.	è	Geeignete Lösung für praxisgerechte große Datenvolumen. Kein zweites Medium erforderlich.	è
3.H	Risiken und Kosten durch Nichtverfügbarkeit von Daten	Risiko des Verlusts und der Nichtverfügbarkeit. Hoher Aufwand und Kosten für Wiederbeschaffung	î	Risiko des Verlusts und der Nichtverfügbarkeit. Hoher Aufwand und Kosten für Wiederbeschaffung	î	Risiko des Verlusts und der Nichtverfügbarkeit. Hoher Aufwand und Kosten für Wiederbeschaffung	î	Risiko des Verlusts und der Nichtverfügbarkeit. Hoher Aufwand und Kosten für Wiederbeschaffung	î
KAT3	Bewertung Kategorie 3: Integration in die TI	Erweiterungen der KT durch zusätzliche Schnittstelle erforderlich.	è	Erweiterungen der KT durch zusätzliche Schnittstelle und Funktio-	î	Integration in die TI einfach und kostengünstig möglich. Rück-	ì	Integration in die TI einfach und kostengünstig möglich. Rück-	ì

[16] Bei der Verwendung der dezentralen Speicherung kann sich für den Leistungserbringer ein signifikanter Mehraufwand gegenüber der Speicherung im Fachdienst ergeben.

	Kriterium	Ungeschützter USB-Stick (STICK)		USB-Stick mit Schutzmaß-nahmen (STICK_S)		eGK mit er-weitertem Speicher (eGK_M)		eGK mit Zu-satzspeicher (eGK_M+)	
		Keine Rück-wärtskompatibi-lität: Nutzung mit existieren-den KT kann nicht zugesi-chert werden.		nen erforder-lich. Keine Rückwärts-kompatibilität: Nutzung mit existierenden KT kann nicht zugesichert werden.		wärtskompa-tibilität gege-ben.		wärtskompa-tibilität gege-ben.	

Tabelle 10-8 Ergebnisse Bewertungskategorie 3 „Integration in die TI“

10.4 Bewertungskategorie 4 “Eignung für den Wirkbetrieb”

4.A Marktverfügbarkeit der Speichermedien

Die Bewertung der Marktverfügbarkeit bezieht sich nicht nur auf den heutigen Stand an verfügbaren Produkten, sondern betrachtet insbesondere auch die künftige technische Entwicklung.

Ein entscheidender Punkt für die Marktverfügbarkeit ist die Nachfrage, die von der Umsetzung der dezentralen Speicherung ausgehen würde. Dazu folgende Abschätzung: Es wird angenommen, das nur jene Versicherte Medien zur dezentralen Speicherung besitzen werden, die diese auch wirklich nutzen möchten. Wenn 10% der Versicherten sich für diese Option entscheiden (siehe Beratungsvorlage der BÄK in Kapitel 2), ergibt sich aus Sicht der Hersteller ein Marktpotential von ca. 6-8 Mio Stück. Dies stellt einen ausreichenden Business Case dar, um begrenzte Anpassungen (z.B. der Software oder des Gehäuses) bei existierenden Chipprodukten, Sticks und Karten durchzuführen.

Für die verschiedenen Varianten der Speichermedien ergibt sich folgende Situation der Verfügbarkeit.

1. STICK ist verfügbar. Es gibt eine große Zahl von Herstellern und einen lebhaften Markt.
2. STICK_S ist in der geforderten einheitlichen Variante mit spezifischer Software / Funktionalität zurzeit nicht verfügbar. Es erscheint als wahrscheinlich, dass die geforderten Anpassungen vom Markt geliefert werden. Es erscheint darüber hinaus möglich, dass funktionale Anpassungen des STICK_S, die die Funktion des STICK_S der eGK weiter annähern, vom Markt geliefert werden könnten.
3. Die Chiplösung für die eGK_M ist von einzelnen Herstellern bereits lieferbar. Bei allen namhaften Chipherstellern ist eine erhebliche Erweiterung des sicheren Speichers Bestandteil der Roadmap. Die Entwicklung geeigneter Chips muss also nicht durch die Einführung dezentraler Speichermedien für die TI der eGK getragen werden. Kartenhersteller können diese neuen Chips wie bisher in Karten verarbeiten und müssen die existierende Software für die eGK_M gar nicht oder nur geringfügig anpassen.
4. Die Chiplösung für die eGK_M+ ist von wenigen Herstellern bereits lieferbar (z.B. Atmel). Andere Chiphersteller haben öffentlich derartige Produkte angekündigt (z.B. Infineon, Samsung). Weitere Entwicklungen sind zu erwarten. Auch hier muss die Entwicklung ge-

eigneter Chips also nicht durch dieses Projekt getragen werden. Kartenhersteller können diese neuen Chips wie bisher in Karten verarbeiten.

Eine Belieferung und ein aktives Marktgeschehen scheinen bei entsprechender Nachfrage im Laufe der nächsten Jahre für alle Varianten wahrscheinlich. Für STICK und STICK_S ist nicht absehbar ob, und wie eine Zertifizierung erreicht werden könnte und durch die Marktteilnehmer in der Produktion umgesetzt würde. STICK und eGK_M wären mit großer Wahrscheinlichkeit bereits für die Tests RVO R3 verfügbar.

4.B Referenzen im Einsatzgebiet eIdentity

Falls Referenzen für das Einsatzgebiet eIdentity vorliegen, kann von einem geringem Risiko bei der Einführung in den Wirkbetrieb ausgegangen werden. Deshalb geht das Vorhandensein von Referenzen in die Bewertung ein.

(1) Generelle Bewertung der ausschließlich dezentralen Speicherung

Die dezentrale Speicherung wird z. B. auch bei eID- und Reisedokumenten angewendet. So sind die Fingerabdrücke beim ePass nur im Pass selbst gespeichert. Für diese Implementierung gibt es eine große Zahl von namhaften Referenzen. Allerdings geht es hier um statische Daten, die vor der Ausgabe des Dokuments gespeichert und niemals verändert werden. Die Aufgabe des Datenerhalts besteht nicht. Bei Verlust des Mediums trägt allein der Bürger die Aufwände und Kosten für die Wiederbeschaffung. Die letzten Punkte auf die TI der eGK und das dezentrale Speichermedium nicht anwendbar.

Alle bekannten europäischen eHealth-Projekte arbeiten ausschließlich mit serverbasierter Speicherung. Das gilt auch für jene, die Chipkarten als Medium der Versicherten verwenden. Beispiele hierfür sind die österreichische eCard oder die französische Sesam Vitale Card.

Es gibt daher keine komplette Referenz für die dezentrale Speicherung in der hier benötigten Ausprägung mit vergrößertem Speicher. Es gibt jedoch viele Referenzen dafür, dass chipkartenbasierte Implementierungen und insbesondere Chipkarten in Händen des Bürgers, Patienten, etc über Jahre sicher und zuverlässig funktionieren (vgl. Anhang A.1.2 Auswertung von Marktstudien).

(2) Bewertung in Abhängigkeit der Implementierungsvariante des Speichermediums

Unter (1) wurde dargelegt, dass es keine vollständige Referenz für eine dezentrale Speicherung im Einsatzgebiet eIdentity gibt. Es gibt dort allerdings viele Referenzen für den erfolgreichen Einsatz von Chipkarten oder anderen elektronischen Dokumenten, die Chips verwenden, die auch in der eGK eingesetzt werden.

Die sichere Chipkarte wurde in den 1990er Jahren für Einsatzgebiete mit hohem Sicherheitsbedarf und industriellen Anforderungen an Zuverlässigkeit eingeführt. Die sichere Chipkarte hat sich in diesen Einsatzgebieten als Medium des Anwenders zur Identifizierung, Authentifizierung und Speicherung durchgesetzt.

Die USB-Schnittstelle wurde im Jahr 1996 von Intel in den PC-Markt eingeführt. USB-Sticks gibt es seit Ende der 90er Jahre. Der USB-Stick hat sich als mobiles Speichermedium im Konsumentenmarkt durchgesetzt. Es gibt für den USB-Stick keine Referenzen als Medium des Versicherten im Einsatzgebiet eHealth**.** Es gibt dagegen eine Reihe von schweren Sicherheitsverletzungen, die durch die Verwendung von USB-Sticks begünstigt wurden. Seither ist in vielen Behörden und Firmen die Nut-

zung von USB-Sticks verboten. Bisher sind lediglich kleinere Umsetzungen im Bereich eIdentity bekannt. Bespiele für die Implementierung von STICK_S sind firmenspezifische Sticks, die Daten transportieren und zur Authentifizierung dienen.

4.C Marktoffenheit (AK)

Marktoffenheit ist eine wesentliche Voraussetzung für die Implementierung von Lösungen der TI der eGK. Die Forderung nach offenen Spezifikationen kann prinzipiell für alle vier Implementierungsvarianten umgesetzt werden.

Die folgende Tabelle gibt eine Übersicht über die bereits verfügbaren Spezifikationen für die Varianten STICK, STICK_S einerseits und eGK_M, eGK_M+ andererseits:

Spezifikationsbereich	STICK, STICK_S	eGK_M, eGK_M+ mit Schnittstelle ISO7816-3	Option: eGK_M+ mit zusätzlicher Schnittstelle ISO14443
Physikalischer Aufbau	Nicht normiert und nicht einheitlich	ISO/IEC 7810 gematik eGK Spezifikation Teil 3 V2.2.0	
Schnittstelle (Phys. Eigenschaften)	USB Stecker Typ A	ISO7816-1 gematik eGK Spezifikation Teil 3 V2.2.0	ISO 10373-6 gematik eGK Spezifikation Teil 3 V2.2.0 muss erweitert werden.
Schnittstelle (Protokollebene)	USB 2.0 (Mass Storage Class)	ISO7816-3	ISO14443, ISO7816
Anwendungsebene	Dateisystem ohne anwendungsspezifische Ausprägung	gematik eGK Spezifikation Teil 1 und Teil 2 (Erweiterung erforderlich)	gematik eGK Spezifikation Teil 1 und Teil 2 (Erweiterung erforderlich)

Tabelle 10-9 Verfügbarkeit offener Spezifikationen

Die Tabelle 10-9 zeigt, dass für die Implementierungsvariante eGK_M und eGK_M+ mit Kontaktschnittstelle die existierenden Spezifikationen der eGK weitgehend verwendet werden können. Für eGK_M+ sind eventuell Erweiterungen vorzunehmen.

Für STICK_S müssten Spezifikationen für die Schutzfunktion (PIN) erstellt werden.

4.D Zuverlässigkeit

Die Zuverlässigkeit ist ein entscheidendes Kriterium für die Eignung des dezentralen Datenspeichers zum Wirkbetrieb. Die Zuverlässigkeit muss für einen definierten Zeitraum und ein realitätsnahes Nutzungsszenario (z.B. das ständige Mitführen des Mediums in der Geldbörse) gewährleistet sein. Bei Chipkarten ist durch geeignete Referenzen nachgewiesen, dass die erforderliche Zuverlässigkeit erreicht werden kann. Bei STICK und STICK_S erscheint dies bei geeigneter Bauform auch möglich. Referenzen konnten dafür jedoch nicht gefunden werden.

Für den Wirkbetrieb reichen Referenzen aus anderen Projekten nicht aus. Vielmehr muss durch geeignete Prüfungen der Nachweis geführt werden, dass die produzierten Produkte den Anforderungen genügen. Dies lässt sich nur über geeignete Prüfverfahren erreichen, die bei Zulassung der Komponenten und produktionsbegleitend eingesetzt werden.

Die folgende Tabelle gibt eine Übersicht über die bereits verfügbaren Prüfspezifikationen für die spezifizierten Eigenschaften für die Varianten STICK, STICK_S einerseits und eGK_M, eGK_M+ andererseits:

Spezifikationsbereich	STICK, STICK_S	eGK_M, eGK_M+ mit Schnittstelle ISO7816-3	Option: eGK_M+ mit zusätzlicher Schnittstelle ISO14443
Physikalischer Aufbau und physikalische Belastbarkeit	Nicht normiert und nicht einheitlich	ISO/IEC 10373-1: Card size ID-1 Card Thickness Corners Edges Card construction Card materials Bending stiffness Flammability Toxicity Resistance to chemicals Card dimensional stability and warp age with temperature and humidity Light Durability Peel strength Adhesion or blocking Opacity Overall Card warpage Resistance to heat Surface distortions Contamination and interaction of card components ISO/IEC 10373-1 ISO 12757-1 / -2 Biegefestigkeit Torsionsfestigkeit Weichmacherstabilität Beschreibbarkeit und Wischfestigkeit Haftfestigkeit Chipmodul	ISO/IEC 10373-1: Card size ID-1 Card Thickness Corners Edges Card construction Card materials Bending stiffness Flammability Toxicity Resistance to chemicals Card dimensional stability and warp age with temperature and humidity Light Durability Peel strength Adhesion or blocking Opacity Overall Card warpage Resistance to heat Surface distortions Contamination and interaction of card components ISO/IEC 10373-1 ISO 12757-1 / -2 Biegefestigkeit Torsionsfestigkeit Weichmacherstabilität Beschreibbarkeit und Wischfestigkeit Haftfestigkeit Chipmodul

Spezifikationsbereich	STICK, STICK_S	eGK_M, eGK_M+ mit Schnittstelle ISO7816-3	Option: eGK_M+ mit zusätzlicher Schnittstelle ISO14443
		Abriebfestigkeit der Personalisierung Beständigkeit gegen Schweiß- und Speichelsimulanz ISO/IEC 10373-3: Dimensions of contacts Number and location of contacts Assignment of contacts UV-Light X-rays Surface Profile of contacts Mechanical Strength of contacts Static electricity	Abriebfestigkeit der Personalisierung Beständigkeit gegen Schweiß- und Speichelsimulanz ISO/IEC 10373-3: UV-Light X-rays Surface Profile of contacts Mechanical Strength of contacts Static electricity
Interoperabilität Schnittstelle (El. Eigenschaften)	USB 2.0	ISO/IEC 10373-3	BSI TR-3105
Interoperabilität Schnittstelle (Protokollebene)	USB 2.0	ISO/IEC 10373-3	BSI TR-3105
Interoperabilität Anwendungsebene	Dateisystem ohne anwendungsspezifische Ausprägung	gematik eGK Spezifikation Teil 1 und Teil 2 (Erweiterung erforderlich)	gematik eGK Spezifikation Teil 1 und Teil 2 (Erweiterung erforderlich)

Tabelle 10-10 Verfügbarkeit von Prüfspezifikationen

Die Tabelle 10-10 zeigt, dass für die Implementierungsvariante eGK_M und eGK_M+ mit Kontaktschnittstelle die existierenden Prüfspezifikationen der eGK für Zuverlässigkeitstests in vollem Umfang verwendet werden können. Prüfinstitute, die Kartentest nach den o. g. Vorschriften durchführen, sind vorhanden (z.B. Fogra, Cetecom-ICT).

Für STICK und STICK_S müssten Prüfspezifikationen komplett neu erstellt werden. Dies ist ein erhebliches Hemmnis für die Feldeinführung und damit auch für die Forderung nach einem Test.

4.E Nachweis der Sicherheit

Die Gewährleistung des Datenschutzes und der IT-Sicherheit ist eine wesentliche Voraussetzung für die Implementierung von Lösungen der TI der eGK. Deshalb implementiert die TI der eGK offene Sicherheitskonzepte und Schutzprofile.

Die Umsetzung der darin enthaltenen Sicherheitsanforderungen für die dezentralen Komponenten wir durch unabhängige Prüfinstitute evaluiert und durch das BSI zertifiziert.

Die folgende Tabelle gibt eine Übersicht über die bereits verfügbaren Sicherheitsvorgaben (Schutzprofile) für die Varianten STICK, STICK_S einerseits und eGK_M, eGK_M+ andererseits:

Spezifikationsbereich	STICK, STICK_S	eGK_M, eGK_M+ mit Schnittstelle ISO7816-3	Option: eGK_M+ mit zusätzlicher Schnittstelle ISO14443
Schutzprofile	STICK_S: PP-0025b (CC EAL2+) FIPS 140-2	Chip: PP-0002, PP-0036 (CC EAL5+) eGK: PP-0020 (CC EAL4+)	Chip: PP-0002, PP-0036 (CC EAL5+) eGK: PP-0020 (CC EAL4+)-> Erweiterung erforderlich

Tabelle 10-11 Verfügbarkeit offener Spezifikationen

Die Tabelle 10-9 zeigt, dass für die Implementierungsvariante eGK_M und eGK_M+ mit Kontaktschnittstelle die existierenden Schutzprofile der eGK weitgehend verwendet werden können. Für eGK_M+ sind eventuell Erweiterungen vorzunehmen.

Für STICK und STICK_S müssten Schutzprofile, die die spezifischen Anwendungsprozesse integrieren, erstellt werden. Dies hätte wahrscheinlich auch eine Anpassung der Schutzprofile für den Konnektor und die KT zur Folge. Das Schutzprofil PP-0025, das für STICK anwendbar wäre, erreicht lediglich EAL2+. Dies reicht für die sichere Speicherung von Daten mit sehr hohem Schutzbedarf nicht aus. Eine FIPS-Zertifizierung liegt nur in Ausnahmefällen für proprietäre Lösungen vor.

4.F Kosten des Speichermediums

Die geschätzten Kosten der einzelnen dezentralen Speichermedien sind in Kapitel 8 benannt.

eGK_M und eGK_M+ ersetzen die eGK des Versicherten komplett. Dieser braucht nicht mehr mit einer eGK ausgestattet werden. Der genannte Preis enthält also die eGK-Funktionalität und die Kosten für das dezentrale Speichermedium. Für einen bereinigten Vergleich mit STICK, STICK_S müssten die Kosten für eGK_M, eGK_M+ noch um den Preis der eGK (ca. 1,50€) reduziert werden. Die Kosten für die Speichermedien STICK, STICK_S sind demnach der aktuellen Schätzung also deutlich höher als für eGK_M und eGK_M+ (ca. Faktor 2).

4.G Migrationsunterstützung.

Die Migration bei den Varianten STICK und STICK_S ist auf folgendem Weg denkbar:

Der Leistungserbringer hält in seiner Umgebung eine Software zur Migration vor und der Versicherte kann auf Nachfrage und Zustimmung die Migration beim Leistungserbringer durchführen lassen. Bei dieser Lösung ist zu beachten, dass gerade bei langlebigen Daten die Wahrscheinlichkeit sehr groß ist, dass notwendige Migrationsschritte ausgelassen werden und der Datenverlust droht.

Die Varianten eGK_M und eGK_M+ bieten dagegen den Vorteil, dass sie automatisch beim Arztbesuch eine Prüfung beim Leistungserbringer erfolgen kann. Der Leistungserbringer kann dann den Versicherten die Migration anbieten und diese nach Zustimmung durchführen.

4.H Kontrollierter Austausch von dezentralen Speichermedien (AK)

Für die Varianten STICK und STICK_S ist es ohne ein eindeutiges und über die Lebensdauer des STICK unveränderbares Identifikationsmerkmal kaum möglich das geforderte Kriterium zu erfüllen. Weiterhin ist zu beachten, dass dieses Merkmal in der TI auch verwendet werden können muss, um einen Ausschluss vom Betrieb vorzunehmen. Ohne Identifikationsmerkmal ist das Kriterium nicht erfüllt.

Die Varianten eGK_M und eGK_M+ bieten dagegen, als Weiterentwicklung der eGK, diese Möglichkeit und können bei Verwendung erkannt und auch gesperrt werden.

10.4.1 Zusammenfassung der Bewertungskategorie 4

STICK ist im Markt verfügbar. Das Marktgeschehen funktioniert. STICK_S, eGK_M und eGK_M+ sind als Plattformprodukte ebenfalls verfügbar, allerdings sind die Anpassungen an die geforderten Funktionen der TI der eGK bisher nicht erfolgt. Bei dem möglichen Marktbedarf von mehreren Millionen Stück kann es aber insbesondere bei eGK_M als gesetzt angesehen werden, dass bei entsprechender Nachfrage kurzfristig ein funktionierender Markt entstehen wird. Dies gilt in 1-2 Jahren auch für eGK_M+.

Für die Varianten der eGK gibt es durch die eGK und langjährige Erfahrungen mit Chipkarten alle erforderlichen Spezifikationen, Schutzprofile, Prüfvorschriften und Prüflabore um die Interoperabilität, Sicherheit und insbesondere die Zuverlässigkeit der Mediums für die vorgesehene Lebensdauer zu gewährleisten. Gerade Prüfvorschriften und bewährte Tests für die Zuverlässigkeit und Lebensdauer, gibt es für STICK und STICK_S nicht. Dies erhöht signifikant das ohnehin schon vorhandene Risiko des Datenverlustes.

Die Kosten des Mediums können nur geschätzt werden. Die Varianten der eGK sind grundsätzlich im Vorteil, da sie die klassische eGK ersetzen können, während die Varianten des USB-Stick zusätzlich zur eGK verwendet werden. Außerdem sollten die Preise für die Varianten der eGK unterhalb der Preise für STICK_S liegen.

Tabelle 10-12 zeigt die Ergebnisse der Bewertungskategorie 4 “Eignung für den Wirkbetrieb”.

	Kriterium	Ungeschützter USB-Stick (STICK)		USB-Stick mit Schutzmaßnahmen (STICK_S)		eGK mit erweitertem Speicher (eGK_M)		eGK mit Zusatzspeicher (eGK_M+)	
4.A	Marktverfügbarkeit der Speichermedien	Bereits verfügbar	ì	Anpassung steht noch aus. Verfügbarkeit sehr wahrscheinlich	è	Chip bereits verfügbar von einzelnen Herstellern. Weitere Hersteller folgen. eGK-Anpassung steht aus.	è	Chip bereits verfügbar von einem Hersteller. Weitere Hersteller folgen. eGK-Anpassung steht aus.	è
4.B	Referenzen im Einsatzgebiet eIdentity	Keine Referenzen im Sicherheitsbereich. Mehrere schwere Sicherheitsverletzungen.	î	Keine Referenzen als sicheres Speichermedium im Einsatzgebiet. Sicherheitsverletzun-	è	Referenzen als sicheres Speichermedium durch existierende Chipkartenprojekte	ì	Referenzen als sicheres Speichermedium durch existierende Chipkartenprojekte	ì

	Kriterium	**Ungeschützter USB-Stick (STICK)**		**USB-Stick mit Schutzmaß-nahmen (STICK_S)**		**eGK mit er-weitertem Speicher (eGK_M)**		**eGK mit Zu-satzspeicher (eGK_M+)**	
				gen bekannt.					
4.C	Marktoffen-heit	Markoffenheit ist gegeben.	ì	Marktoffene Implementie-rung möglich. Spezifikations-aufwand für Schutzfunktion erforderlich.	è	Markoffen-heit ist wie bei eGK ge-geben.	ì	Markoffenheit ist wie bei eGK gege-ben. [17].	ì
4.D	Zuverlässig-keit	Keine ausrei-chenden Prüf-standards vor-handen	î	Keine ausrei-chenden Prüf-standards vor-handen	î	Prüfstan-dards und Prüflabore vorhanden	ì	Prüfstan-dards und Prüflabore vorhanden	ì
4.E	Nachweis der Sicherheit	Nicht bewertet, da keine Si-cherheitsfunkti-on spezifiziert		Keine ausrei-chenden-Schutzprofile vorhanden	î	Schutzprofile und Prüflabo-re vorhanden	ì	Schutzprofile und Prüflabo-re vorhanden	ì
4.F	Kosten des Speicherme-diums (ge-schätzt)	< 2,50€ exklu-sive Kosten eGK.	è	< 5€ exklusive Kosten eGK.	î	< 2,50€ in-klusive Kos-ten eGK	ì	< 4€ inklusive Kosten eGK	ì
4.G	Migrationsun-terstützung.	Prüfung auf durchzuführen-de Migration nur möglich, wenn der Ver-sicherte das Speichermedi-um mitführt. In diesem Fall Migration mög-lich.	è	Prüfung auf durchzufüh-rende Migrati-on nur mög-lich, wenn der Versicherte das Speicher-medium mit-führt. In die-sem Fall Mig-ration möglich.	è	Automati-sche Prüfung für die Not-wendigkeit einer Migra-tion beim LE, danach Mig-ration mög-lich	ì	Automatische Prüfung für die Notwen-digkeit einer Migration beim LE, da-nach Migrati-on möglich	ì
4.H	Kontrollierter Austausch von dezentra-len Spei-chermedien	Nicht bewertet, da keine Si-cherheitsfunkti-on spezifiziert		Keine sichere Identifikation des Speicher-mediums als unsicheres Speichermedi-um möglich.	è	Aufgrund der Identifikati-ons- und Sperrmecha-nismen mög-lich	ì	Aufgrund der Identifikati-ons- und Sperrmecha-nismen mög-lich	ì
KAT4	Bewertung Kategorie 4: Eignung für den Wirkbe-trieb	Verfügbar, Funktionieren-der Markt. Keine Referen-zen im Anwen-dungsbereich, keine ausrei-chenden Prüf-standards für Lebensdauer,	î	Keine Refe-renzen im An-wendungsbe-reich, keine ausreichenden Prüfstandards für Lebens-dauer, etc, Kein geeigne-tes Schutzpro-	î	Kurzfristig bei entspre-chendem Bedarf ver-fügbar. Viele Referenzen. Sicherheit und Zuver-lässigkeit kann für ge-	ì	Mittelfristig bei entspre-chendem Bedarf ver-fügbar. Viele Refe-renzen. Si-cherheit und Zuverlässig-keit kann für	ì

[17] Mäßiger Spezifikationsaufwand bei Verwendung der Option einer kontaktlosen Schnittstelle nach ISO14443.

	Kriterium	Ungeschützter USB-Stick (STICK)		USB-Stick mit Schutzmaß-nahmen (STICK_S)		eGK mit er-weitertem Speicher (eGK_M)		eGK mit Zu-satzspeicher (eGK_M+)	
		etc		fil. Teuerste Variante.		plante Le-bensdauer überprüft werden. Kos-tengünstigste Variante.		geplante Le-bensdauer überprüft werden.	

Tabelle 10-12 Ergebnisse Bewertungskategorie 4 „Eignung für den Wirkbetrieb“

10.5 Zusammenfassung der Bewertungen

10.5.1 Einführung

Die 20. Gesellschafterversammlung hat der gematik den Auftrag erteilt, die Forderung nach einem Test dezentraler Speichermedien zu bewerten (siehe Auftragsbeschreibung in Kapitel 2).

Auftragsgemäß wurde von der gematik eine Bewertung erstellt, die auf definierten Bewertungskriterien und der Nutzung des Wissens unabhängiger Experten beruht. Das konzeptionelle Vorgehen wurde mit dem Fachausschuss abgestimmt.

Die vier Bewertungskategorien und die zugeordneten Kriterien wurden ausgewählt, um beurteilen zu können, ob die potentiell zu testende Lösung alle wesentlichen Bedingungen für einen erfolgreichen Einsatz im Wirkbetrieb erfüllen kann. Nur wenn dies bestätigt ist, kann der Forderung nach einem Test stattgegeben werden.

Die Antwort soll in den beiden folgenden Schritten gegeben werden:

1. Ist die Speicherung von anwendungsspezifischen Daten in dezentralen Speichermedien der Versicherten im Wirkbetrieb generell einsetzbar?
2. Ist die Speicherung von anwendungsspezifischen Daten in dezentralen Speichermedien der Versicherten nach [Konzept] mit ungeschützten USB-Sticks einsetzbar? Gibt es alternative Implementierungsvarianten des dezentralen Mediums, die besser geeignet sind?

Natürlich ist eine positive Antwort im zweiten Schritt nur möglich, wenn die generelle Eignung im ersten Schritt gegeben ist.

10.5.2 Bewertung der generellen Eignung

Das Angebot der Nutzung von dezentralen Speichermedien in Versichertenhand als Alternative zur Speicherung der anwendungsspezifischen Daten im Fachdienst führt nach Meinung der BÄK zu einer Erhöhung der Akzeptanz der Systemlösung der TI der eGK bei den künftigen Anwendern. Fraunhofer FOKUS und gematik teilen diese Einschätzung.

Diesem Akzeptanzgewinn stehen jedoch Argumente entgegen, die im Folgenden aufgeführt sind:

1. Die Verfügbarkeit der Daten kann bei der dezentralen Speicherung nicht gewährleistet werden. Dies ist in [Konzept Kapitel 1.1] und bei der Bewertung des Kriteriums „Risiken und Kosten durch Nichtverfügbarkeit von Daten“ dargelegt. Ein Verlust des Mediums

oder ein technischer Defekt können zu einem dauerhaften Datenverlust führen. Die Wiederbeschaffung ist möglich, aber ggf. mit erheblichen Aufwänden der Leistungserbringer, Versicherten und Kostenträger verbunden. Das Fehlen der Daten kann die Behandlung des Versicherten beeinträchtigen.

2. Die Lebensdauer von Speichermedien und die Schutzwirkung von kryptografischen Verfahren sind zeitlich begrenzt. Die Daten müssen vor Ablauf dieser Zeitspannen, die mit ca. 5-10 Jahre angesetzt werden können, auf ein neues Medium transferiert bzw. mit neuen Verfahren vor Zugriff geschützt, verschlüsselt und ggf. signiert werden. Anderenfalls drohen Datenverlust oder der Verlust des Datenschutzes und der Informationssicherheit.
3. Es gibt international keine aussagekräftige Referenz für die Nutzung der dezentralen Speicherung. Alle eHealth-Vorhaben innerhalb der EU arbeiten derzeit mit serverbasierten Konzepten. Dies gilt auch für jene mit einer Chipkarte. Die Projekt ePass und ePA sind nur begrenzt als Referenz verwendbar. Ein Datenverlust hat hier lediglich eine etwas aufwändigere Grenzabfertigung zur Folge, die Wiederbeschaffung der Daten ist einfach und mit überschaubaren Kosten möglich, die überdies noch vom Bürger getragen werden.

Nichtsdestoweniger steht keiner dieser Gründe einem Einsatz der dezentralen Speicherung im Wirkbetrieb grundsätzlich entgegen. Es ist letztlich von den Prioritäten der Anwender abhängig, ob die Vorteile oder die Nachteile der dezentralen Speicherung höher gewichtet werden.

10.5.3 Bewertung der Eignung der definierten Implementierungsvarianten

In der ersten Stufe der Bewertung wurde festgestellt, dass die TI der eGK die dezentrale Speicherung von Daten ermöglichen kann. Nun ist zu bewerten, welche Implementierungsvarianten dezentraler Speichermedien geeignet sind.

Das Ergebnis der Bewertung der Implementierungsvarianten in den vier Bewertungskategorien ist in der folgenden Tabelle dargestellt.

	Bewertungskategorie	**Ungeschützter USB-Stick (STICK)**		**USB-Stick mit Schutzmaßnahmen (STICK_S)**		**eGK mit erweitertem Speicher (eGK_M)**		**eGK mit Zusatzspeicher (eGK_M+)**	
KAT1	Bewertung Kategorie 1: Konformität mit dem gesetzlichen Rahmen	Ungeeignet, da Ausschlusskriterien erfüllt.	AK	Ungeeignet, da Ausschlusskriterien erfüllt.	AK	In vollem Umfang wie bei eGK erfüllt.	ì	In vollem Umfang wie bei eGK erfüllt.	ì
KAT2	Bewertung Kategorie 2: Nutzung in Fachanwendungen	Ungeeignet, da Ausschlusskriterien erfüllt.	AK	Ungeeignet, da Ausschlusskriterien erfüllt.	AK	Gute Eignung für kleine Datenvolumen. Für große Datenvolumen nicht geeignet	ì AK	Für alle erwarteten Einsatzszenarien geeignet.	è
KAT3	Bewertung Kategorie 3:	Erweiterungen der KT durch	è	Erweiterungen der KT durch	î	Integration in die TI einfach	ì	Integration in die TI einfach	ì

	Bewertungskategorie	Ungeschützter USB-Stick (STICK)		USB-Stick mit Schutzmaßnahmen (STICK_S)		eGK mit erweitertem Speicher (eGK_M)		eGK mit Zusatzspeicher (eGK_M+)	
	Integration in die TI	zusätzliche Schnittstelle erforderlich. Keine Rückwärtskompatibilität: Nutzung mit existierenden KT kann nicht zugesichert werden.		zusätzliche Schnittstelle und Funktionen erforderlich. Keine Rückwärtskompatibilität: Nutzung mit existierenden KT kann nicht zugesichert werden.		und kostengünstig möglich. Rückwärtskompatibilität gegeben.		und kostengünstig möglich. Rückwärtskompatibilität gegeben.	
KAT4	Bewertung Kategorie 4: Eignung für den Wirkbetrieb	Verfügbar, Funktionierender Markt. Keine Referenzen im Anwendungsbereich, keine ausreichenden Prüfstandards für Lebensdauer, etc	î	Keine Referenzen im Anwendungsbereich, keine ausreichenden Prüfstandards für Lebensdauer, etc, Kein geeignetes Schutzprofil. Teuerste Variante.	î	Kurzfristig bei entsprechendem Bedarf verfügbar. Viele Referenzen. Sicherheit und Zuverlässigkeit kann für geplante Lebensdauer überprüft werden. Kostengünstigste Variante.	ì	Mittelfristig bei entsprechendem Bedarf verfügbar. Viele Referenzen. Sicherheit und Zuverlässigkeit kann für geplante Lebensdauer überprüft werden.	ì

Tabelle 10-13 Ergebnisse der Bewertungskategorien

Die Varianten des USB-Stick können nicht verwendet werden, da Ausschlusskriterien in den Kategorien 1 und 2 erfüllt sind und zusätzlich schwerwiegende Hemmnisse dem Einsatz im Wirkbetrieb entgegenstehen.

Die Varianten der eGK sind als dezentrale Speichermedien für den Einsatz in der TI der eGK geeignet. Es ist allerdings zu beachten, dass eGK_M nur für begrenzte Datenmengen von ca. 1 MByte eingesetzt werden kann. eGK_M+ unterliegt hier keinen relevanten Beschränkungen. Die zugehörigen detaillierten Begründungen finden sich in den Kapiteln zur jeweiligen Bewertungskategorie.

10.5.4 Ergebnis der Bewertung

Das Konzept der Bundesärztekammer fokussiert auf die Implementierungsvariante STICK, einem ungeschützten, unpersonalisierten USB-Speichermedium, die sich in der Bewertung in Kapitel 10.5.3 als ungeeignet erwiesen hat. Das Konzept versucht, die fehlenden Sicherheitsmechanismen durch spezielle Maßnahmen zu kompensieren. Die Experten der BÄK haben eine sehr professionelle Arbeit vorgelegt und alle wesentlichen Themen zu lösen versucht. Es verbleiben jedoch aufgrund der Verwendung eines unsicheren Speichermediums Lücken.

Das Ergebnis *der konzeptionellen Bewertung der Forderung zur Durchführung technik- und ergebnisoffener Tests von Speichermedien in der Hand von Versicherten als Alternative zu serverbasierter Speicherung* zeigt, dass ein ungeschütztes, unpersonalisiertes USB-Medium bei mehreren Kriterien aus verschiedenen Bewertungskategorien entweder als ungeeignet oder schlecht geeignet eingestuft werden muss.

Zum Beispiel sind folgende Sachverhalte kritisch zu bewerten:

§ Die Anwendungen der TI der eGK müssen allen Versicherten und Leistungserbringern diskriminierungsfrei zugänglich sein. Dazu gehört insbesondere auch, das Versicherte, die keine Fertigkeiten in den Bereichen IT und Datenschutz besitzen, die eGK und die Anwendungen sicher und unter Wahrung des Schutzes ihrer persönlichen medizinischen Daten und ihrer Rechte als Versicherte nutzen können.

  Das Konzept sieht vor, die alleinige Verantwortung für das dezentrale Speichermedium und die darauf gespeicherten medizinischen Daten an den Versicherten zu übertragen. Es stellt jedoch nicht die erforderlichen Funktionen bereit, um den Versicherten und Leistungserbringer mit durchschnittlichen IT-Kenntnissen bei der Wahrnehmung dieser Verantwortung zu unterstützen. Einige Beispiele:

  - STICK bietet keinen Zugriffsschutz. Es können an einem USB-Port - z. B. eines beliebigen PC - alle Daten vom Medium gelesen und kopiert werden. Nach Ablauf der Lebensdauer des Verschlüsselungsmechanismus (üblicherweise 6-10 Jahre) ist die Vertraulichkeit der Daten nicht mehr sichergestellt.
  - Die Daten sind kryptografisch geschützt. Das Entschlüsseln der gespeicherten Daten kann der Versicherte mit seiner eGK, der PIN und einfachen Hilfsmitteln selbst durchführen. Dies kann Datenschutzlücken zur Folge haben und den Versicherten in schwierige Situationen bringen (Arbeitgeberszenario).
  - Die Protokollierung von Zugriffen auf STICK ist zwar technisch möglich. Die Protokolldaten können jedoch manipuliert werden. Die Protokollierung auf der eGK wäre nur möglich, wenn eine eindeutige Bindung zwischen STICK und eGK bestehen würde.
  - Anders als bei der eGK muss der Versicherte selbst darauf achten, dass die Lebensdauer des Mediums und der Verschlüsselungsmechanismen der Daten nicht überschritten wird und die notwendigen Maßnahmen zum Datenerhalt einleiten.
  - Der Versicherte hätte die Verantwortung für die Verwaltung aller Daten auf dem STICK.

  Hier werden dem Versicherten besondere Fertigkeiten abverlangt. Die Verantwortung für den Schutz der eigenen Daten kann deshalb von vielen Versicherten nicht wahrgenommen werden. Dies hat wesentlich zum Ausschluss der Lösungen STICK und STICK_S in den Bewertungskategorien 1 und 2 geführt und führt deshalb auch zur negativen Bewertung der Forderung nach Tests, die auf dem Konzept der BÄK basieren.

- § STICK und STICK_S zeigen auch in den Bewertungskategorien 3 und 4 erhebliche Schwächen, die einem Einsatz im Wirkbetrieb entgegenstehen. Hier muss insbesondere hervorgehoben werden, dass es derzeit keine hinreichenden Prüfverfahren zur Sicherstellung der Wirkbetriebstauglichkeit bzgl. Lebensdauer und Robustheit und keine Referenzen für die Verwendung von USB-Sticks in ähnlichen Projekten gibt. Gerade vor dem Hintergrund, dass die gespeicherten Daten bei einem Defekt verloren sind, muss die Zuverlässigkeit des Speichermediums für die vorgegebene Lebensdauer abgesichert sein.
- § Die erforderliche Handhabung von mehreren Medien (eGK und STICK für den Versicherten, eGK, STICK und ggf. HBA für den Leistungserbringer) ist wenig anwenderfreundlich.

Allerdings hat die Bewertung auch ergeben, dass die TI der eGK die Möglichkeit bietet, die dezentrale Speicherung von Daten sicher und anwenderfreundlich zu unterstützen. Hier gibt es offenbar ein Alleinstellungsmerkmal der TI der eGK.

Die Betrachtungen der verschiedenen Implementierungsvarianten haben neue Möglichkeiten aufgezeigt. Bei entsprechendem Marktbedarf werden perspektivisch mit eGK_M und eGK_M+ neue Typen von dezentralen Medien zur Verfügung stehen, die die Funktionalität und die Sicherheit der eGK aufweisen, unter Wahrung der Rückwärtskompatibilität und Sicherheitsziele in die existierende Infrastruktur der eGK integriert werden können und zusätzlich die dezentrale Speicherung sinnvoll unterstützen. Der Versicherte braucht dabei nach wie vor nur ein Medium. eGK_M und eGK_M+ ersetzen die heutige eGK für Versicherte, die die dezentrale Speicherung nutzen möchten.

eGK_M+ hat ca. 1 MByte Speicher, also ca. das Zehnfache der eGK, eGK_M+ wird mehr als 100 MByte Speicher aufweisen. Auf den ersten Blick scheint dies ein Nachteil gegenüber USB-Sticks zu sein, die über bis zu 64GByte Speicher verfügen. Die Betrachtung der Anwendungssituation zeigt jedoch, dass die Speichergrößen von eGK_M und eGK_M+ für die heute vorhersehbaren Einsatzszenarien des Versicherten ausreichend sind.

Auch bei Kosten einer potentiellen Einführung haben die künftigen Varianten der eGK Vorteile gegenüber den Varianten eines USB-Stick. Dies gilt sowohl für die Kosten des Mediums selbst – insbesondere weil es die klassische eGK ablösen kann - als auch für die Kosten einer Anpassung der Infrastruktur. Letztere sind vernachlässigbar, da die existierenden Schnittstellen weiterhin verwendet werden können.

Der Leistungserbringer ist nicht gezwungen, neue Geräte einzuführen. eGK_M und eGK_M+ können mit den KT des Basis-Rollout verwendet werden. Dagegen sind USB-Schnittstellen für die aktuellen Geräte nicht spezifiziert.

Empfehlung zum weiteren Vorgehen

Wie in der Bewertung in Kapitel 10.5.4 beschrieben, kann der Forderung nach Tests auf Basis des Konzepts der BÄK nicht entsprochen werden.

Gleichwohl hat die Untersuchung und Bewertung gezeigt, dass die TI der eGK die Möglichkeit zur alternativen dezentralen Speicherung ohne Einbussen beim Schutz der personenbezogenen Daten sehr gut unterstützen kann, sofern geeignete Medien wie die eGK_M und eGK_M+ verwendet werden.

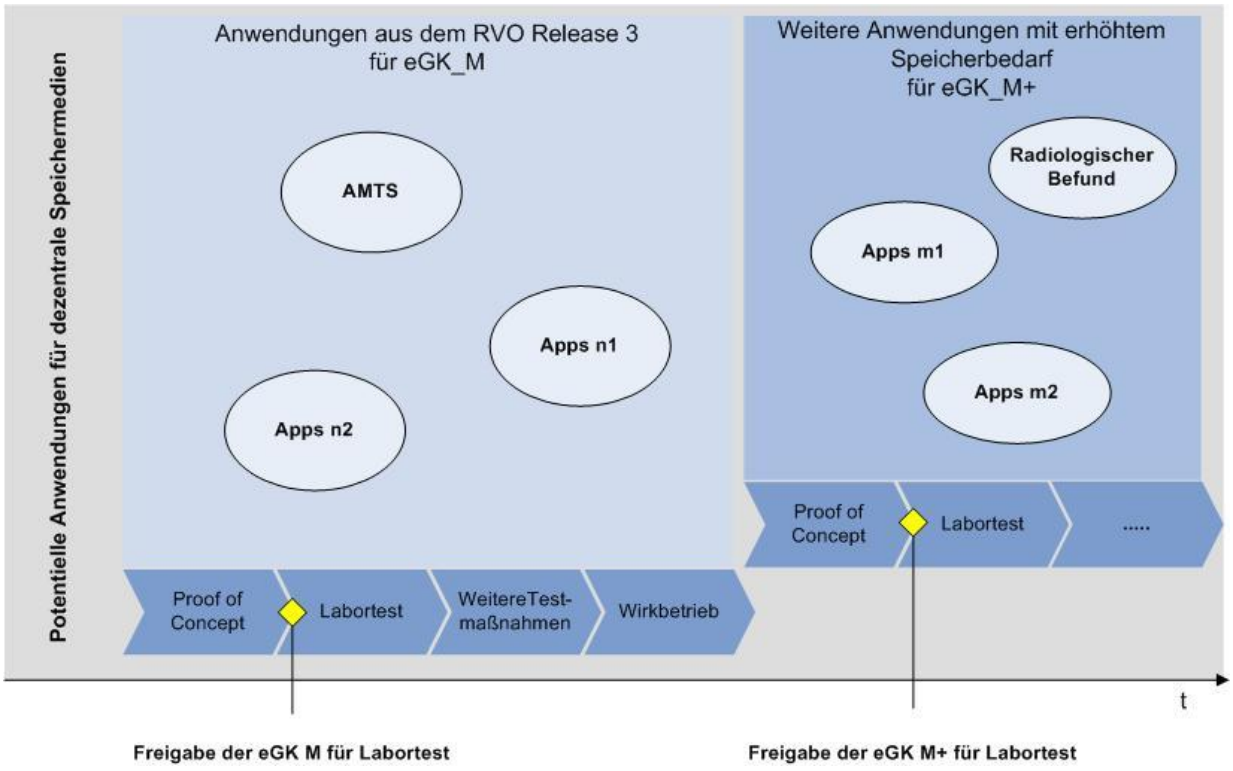
Fraunhofer FOKUS und gematik sind der Auffassung, dass das Angebot einer dezentralen Speicherung von Daten, die alternativ und optional zur Speicherung in einem Fachdienstes angeboten wird, die Akzeptanz der TI der eGK erhöhen könnte.

Fraunhofer FOKUS und gematik halten es deshalb für sinnvoll, das Thema der dezentralen Speicherung zu vertiefen. Zunächst könnte für potentiell geeignete Fachanwendungen geprüft werden, inwieweit die dezentrale Speicherung in die Fachkonzepte eingebracht werden kann Hierzu wären ca. 4 Monate erforderlich. In einem nächsten Schritt könnte die Planung von Tests vorgenommen werden. Dies würde ca. 3 Monate dauern. Eine Kooperation zwischen der gematik, interessierten Gesellschaftern (insbesondere der BÄK) und Fraunhofer FOKUS wäre zu begrüßen. Diese Arbeiten könnten nach dem erfolgreichen Abschluss der Konzeptphase des Online-Rollout starten und die Ergebnisse können dann in das die Entwicklung der eGK Generation 2 einfließen.

Die Entscheidung, ob diese Arbeiten aufgenommen werden sollten, muss von den Gesellschaftern der gematik getroffen werden. Es ist dabei zu beachten, dass der potentielle zeitliche Verlauf der Tests an den Ausbau der TI der eGK und die Einführung geeigneter freiwilliger Anwendungen gekoppelt ist. Dies entspricht auch der Intention der Beratungsvorlage und dem Konzept der BÄK.

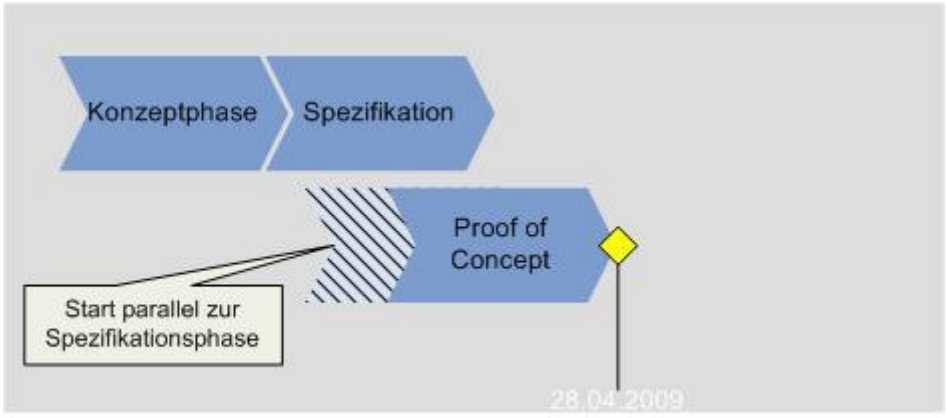
Grundsätzlich können Fraunhofer FOKUS und gematik sich aktuell folgendes Szenario zur Umsetzung von Test im Rahmen der aktuell vorhersehbaren Entwicklung der TI und potentiell geeigneter Anwendungen vorstellen.

Die nachfolgende Grafik verdeutlicht exemplarisch das mögliche Testvorgehen. Im Rahmen der Konzeptphase werden die Anforderungen für die Verwendung des dezentralen Speichermediums formuliert und finden damit Einzug in die anschließende Spezifikationsphase. Mit einem Zeitversatz wird auf Basis der ersten Spezifikationsergebnisse eine so genannte Proof-of-Concept Phase begonnen, mit der zwei Ziele verfolgt werden. Zum einen wird zum frühesten Zeitpunkt die Umsetzbarkeit der Anwendung geprüft, zum anderen muss das im Zusammenhang mit der gewählten Anwendung erprobte dezentrale Speichermedium eine Freigabe für den Einsatz in den weiteren Testmaßnahmen erhalten. Das letztgenannte Ziel entscheidet über die Verwendbarkeit des dezentralen Speichermediums für den Wirkbetrieb und wird über die weiteren Schritte, wie z.B. Labortest, in den Wirkbetrieb überführt und kann dann durch den Versicherten genutzt werden.



11 Generische Aufwandsabschätzung

Die potentielle Kostenwirkung des vorgeschlagenen Projekts „Dezentrale Speicherung“ kann aktuell auf Basis der Varianten eGK_M und eGK_M+ nur grob eingeschätzt werden, da sie von den Anforderungen der fachlichen Spezifikationen und dem Verlauf der weiteren Arbeiten zu den freiwilligen Anwendungen abhängen.



Freigabe der eGK M oder eGK_M+ für Labortest

Zu betrachten ist die Phase bis zur Freigabe einer eGK_M oder eGK_M+ für den Labortest, gemäß der Handlungsempfehlung im vorhergehenden Kapitel. Aus den Ergebnissen dieser Phase lassen sich dann nach dem Vorgehen der gematik die weiteren Schritte zur Einführung planen.

1. Aufwand für Änderungen an Fachspezifikationen und Facharchitekturen

Im Rahmen der Arbeiten zur Spezifikation von Fachanwendungen werden nur geringe Änderungen und Ergänzungen erwartet, die durch die Berücksichtigung der alternativen Speicherung auf dem dezentralen Medium eGK_M erforderlich werden. Die Erhöhung des Aufwands wird mit ca. 5% abgeschätzt.

2. Aufwand für Änderungen an Spezifikationen für dezentrale Komponenten

Die Anforderungen an die Spezifikationen für die eGK Generation 2 müssten angepasst werden. Die zu betrachtenden Aspekte sind die Übertragungsgeschwindigkeit, Datenverwaltung, Speicherstrukturen und Zugriffsberechtigungen. Da ohnehin Spezifikationen zu neuen Funktionen für die nächste eGK-Generation erstellt werden müssen, beschränkt sich auch hier der Aufwand auf ca. 5%.

3. Aufwand Proof-of-Concept

Es ist im Rahmen der Proof-of-Concept Phase die Erweiterungen zur eGK Generation 2 als Zusatzaufwand zu berücksichtigen. Es wird eine Aufwandserhöhung in Höhe von ca. 10% erwartet. Für diese Phase sind Musterkarten zu beschaffen, die den Freigabeprozess unterstützen. Im Rahmen dieses Prozesses auftretende Änderungsanforderungen an die für den Labortest erforderlichen Karten können eine erneute Musterkartenversion zur Folge haben. Dieses Risiko ist für alle Kartengenerationen gleich und erzeugt keinen zusätzlichen Aufwand.

12 Literaturverzeichnis

Titel	Kurzname	Erstellungsdatum / Version	Autor
Die elektronische Gesundheitskarte	[Gesundheitskarte_Rechtskommentare]	2007	Bales, Dierks, Holland, Müller
Speichermedien in der Hand des Versicherten	[eHealth_Medien]	Mai 2009	Fraunhofer FOKUS
eHealth-Infrastrukturen. Sichere Service-orientierte Strukturen im Gesundheitswesen.	[eHealth_Infrastrukturen]	Mai 2008	Fraunhofer FOKUS

Tabelle 12-1 Literaturverzeichnis

13 Anlagen

Titel	Kurzname	Erstellungsdatum / Version	Autor
Eckpunkte für ein Konzept zur dezentralen Speicherung medizinischer Daten in der Telematikinfrastruktur	[Konzept]	Version 1.0.0, 25.09.2008	Bundesärztekammer

Tabelle 13-1 Anlagen

14 Abkürzungsverzeichnis

Abkürzung	Bedeutung
BÄK	Bundesärztekammer
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik.
eGK	Elektronische Gesundheitskarte
KT	Kartenterminal
KTR	Kostenträger

Abkürzung	Bedeutung
KVK	Krankenversichertenkarte
LE	Leistungserbringer
PKI	Public Key Infrastruktur
SGB	Sozialgesetzbuch
TI	Telematikinfrastruktur

Tabelle 14-1 Abkürzungsverzeichnis

15 Glossar

Schlagwort	Bedeutung
Evaluator	Prüfinstitut, das die Konformität von Komponenten mit den Vorgaben eines Schutzprofils untersucht. Erstellt Evaluation Technical Report (ETR), der bei Common Criteria Grundlage der Zertifizierung ist.
Pilotierung	Durch den Begriff Pilotierung soll künftig die Parallelität von Test- und Wirkbetrieb gekennzeichnet werden.
Sektor	Ein Sektor umfasst einen abgrenzbaren Bereich der Leistungserbringer, für den eine Spitzenorganisation zuständig ist.

Tabelle 15-1 Glossar

A Anhang

A.1 Markterhebung: Auswertung von Marktstudien

Einleitung

Für die Einordnung der SmartCard-Technologie in Bezug auf die aktuelle Verwendung und die absehbare Entwicklung, wurden zwei Studien ausgewertet:

1. „World Government Smart Card Markets“, herausgegeben von Frost&Sullivan, N544-33, Feb 2009.

   Diese Studie erlaubt einen global ausgerichteten Einblick in den Weltmarkt für Smart Cards, der in vier geographische Regionen unterteilt wird: Europa, Mittlerer Osten und Afrika (EMEA), asiatisch-pazifischer Raum (APAC), Nordamerika, Lateinamerika. Für alle Regionen wird eine Prognose über die Entwicklung des Marktes gemacht bezüglich Verbreitungszahlen, Markttreiber und Einschränkungen. Ausgangsbasis ist das Jahr 2008.

2. „Government eID Projects Need Private Sector Initiative and Support for Broader Success“, Author Bill Nagel, herausgegeben von Forrester Research, Apr 2008.

   Bis heute haben 12 europäische Länder elektronische Identitätsausweise (eID), die sich einer öffentlichen PKI bedienen, entweder entwickelt oder setzen sie bereits ein. Nationale Regierungen möchten solche Ausweise nicht nur als sicheren Identitätsnachweis nutzen, sondern dem Bürger auch einen gesicherten Zugang zu einer Reihe von behördlichen und kommerziellen Diensten anbieten. Die Anwendung solcher Ausweise ist in Schweden weiter verbreitet als in jedem anderen Land, dies kann als Modell für zukünftige eID-Implementierungen genutzt werden.

Im Folgenden werden die aus diesen Studien gewonnen Erkenntnisse zusammengefasst und die Bedeutung für das deutsche Gesundheitswesen erläutert:

Erkennbare Entwicklung und Einordnung des Gesundheitswesens

Betrachtet werden in beiden Studien SmartCards, deren Chip Identifikationsdaten, auf der Karte auch in Klartext sichtbar, und Schlüssel / Zertifikate trägt.

Die weltweit eingesetzte Stückzahl von SmartCards, die die Identifikation und den Zugang des Bürgers zu verschieden behördlichen Diensten ermöglichen, beläuft sich gegenwärtig auf 590 Millionen. Bis zum Jahre 2014 wird sie voraussichtlich 1245 Millionen erreichen, das entspricht einer durchschnittlichen jährlichen Wachstumsrate von 13,4%[18].

Den größten Einsatz finden SmartCards zurzeit als elektronische Ausweise, die zur Identifikation dienen. Im Jahre 2008 wurden weltweit 403 Millionen solcher Ausweise ausgeliefert, bis 2014 wächst diese Zahl voraussichtlich auf 730 Millionen an. Sie werden gefolgt von SmardCards in den Bereichen ePassport (voraussichtlicher Zuwachs bis 2014 von 50 auf 180 Millionen), eHealthcare (voraussichtlicher Zuwachs bis 2014 von 58 auf 158 Millionen) und eDriversLicence (voraussichtlicher Zuwachs bis 2014 von 75 auf 175 Millionen).

Somit bilden eHealthcare-Karten einen der vier größten Einsatzbereiche für SmartCards weltweit. Eine solch hohe Verbreitung bringt den Vorteil einer breiten Datenbasis zur statistischen Auswertung und wirkt sich günstig auf den Stückpreis aus.

Faktoren, die die weite Verbreitung begünstigen:

§ Die Akzeptanz einer solchen Karte hängt von der Häufigkeit der Nutzung ab. Werden auch Dienste aus dem privaten Bereich miteinbezogen, wird sie viel häufiger eingesetzt als bei sporadischen Interaktionen mit z.B. Behörden. Mit der Erweiterung der Dienste,

18 „World Government Smart Card Markets“, herausgegeben von Frost&Sullivan, N544-33, Feb 2009, vgl. Anlage A

zu denen die Karte einen Zugang ermöglicht, erreicht man eine größere Anzahl an Nutzern und erhält statistisch besser verwertbare Daten (bzgl. Produktqualität, Akzeptanz, Benutzerverhalten, Use Cases etc.). Es werden z. Z. Erfahrungen mit dem Einsatz von SmartCards im Passengers Transportation Market intensiv verwertet (27 Länder nehmen am Visa Waiver Program teil).

§ Schweden belegt als Beispiel die Tendenz, dass eine eID-Karte als Authentifizierung und Zugangsberechtigung zu immer mehr Diensten sehr gut angenommen wird, hier handelt es sich um den Zugang zu behördlichen Diensten und eBanking[19]. Übertragen auf die eGK ist eine solche Funktionalität im Sektor Gesundheitswesen also ein Möglichkeit zur Verbesserung der Akzeptanz.

§ Ein wichtiger Faktor ist die Unterstützung von Smart Cards durch Standards (z.B. neu in USA ist GSC-IS2.1 mit ISO/IEC 7816-4).

In Sektoren wie eHealth, eGovernment, ePassport sind Rollouts einer neuen Technologie generell langsam, bedingt zum einen durch strikte Regulatorien und zum anderen durch die hohen Kosten der großen Stückzahlen und der unterstützenden Infrastruktur.

Vor diesem Hintergrund wird in den untersuchten Studien dem Faktor Speichergröße auf der Karte bisher keine Beachtung geschenkt, so dass dazu noch keine Aussagen gemacht werden können. Viel mehr werden Faktoren als entscheidend analysiert wie

- die Akzeptanz einer Technologie durch den Nutzer,
- die Performanz des Gesamtsystems,
- Verbreitung von Standards für die Unterstützung der Schnittstelle
- Interoperabilität und Kompatibilität mit Legacy-Systemen

Bezüglich dieser Faktoren liegt eine beachtliche Menge an Daten für SmartCards vor. Die Entwicklung der weltweiten Stückzahlen, insbesondere im eHealth-Bereich belegt, dass diese Technologie im Moment unter Betrachtung aller obigen Kriterien effektiv und erfolgreich ist.

A.2 Kurzbeschreibung Patienten-Kurzakte (Patient Summary)

Im grenzübergreifenden Zusammenhang spielt das sog. Patient Summary eine wichtige Rolle. Im Kontext von z.B. beruflichen oder urlaubsbedingten Aufenthalten im Ausland ist bei Erkrankungen die Verfügbarkeit von medizinischen Informationen für einen Versicherten/Patienten von Vorteil, damit möglichst unabhängig von sprachlichen Hindernissen eine medizinisch optimale Behandlung vorgenommen werden kann und auch eine geeignete Medikation erfolgen kann. Somit werden Informationen benötigt, die über die Inhalte des in Deutschland zur Anwendung gelangenden Notfalldatensatzes hinausgehen, keine vollständige Patientenakte darstellen, aber genügend aktuelle Informationen zum Gesundheitszustand des Patienten enthalten.

Auf europäischer Ebene kristallisiert sich für den Begriff des Patient Summary eine Sammlung der wichtigsten medizinischen Daten heraus. Im Gegensatz zur reinen Notfallversorgung sollen auch Daten für die akute Behandlung von nicht lebensbedrohlichen Krankheiten enthalten sein, zum Allgemeinzustand des Versicherten (z.B. zu Allergien, Unverträglichkeiten von Wirkstoffen), zu bereits verordneten und in Anwendung befindlichen Medikamenten und zu weiteren für den Arzt wichtigen Informationen (z.B. wichtige Hinweise zu evtl. vorhandenen Organschäden) .

19 „Government eID Projects Need Private Sector Initiative and Support for Broader Success“, Author Bill Nagel, herausgegeben von Forrester Research, Apr 2008, vgl. Anlage B

Eine allgemeingültige Definition der Inhalte und des Datenformats des Patient Summary ist noch nicht vorhanden. Durch eine Initiative der EU ist ein Projekt („epSOS“) unter deutscher Beteiligung[20] damit beschäftigt, ein Pilotsystem zur Nutzung von Patient Summaries und zur grenzübergreifenden eVerordnung in Europa zu spezifizieren. Mit ersten Ergebnissen kann 2009/2010 gerechnet werden.

Derzeit ist bereits abzusehen, dass im europäischen Umfeld die Speicherung und der Transport von personenbezogenen medizinischen Daten nicht dezentral umgesetzt werden wird. In vielen europäischen Ländern wird für den Zugriff auf zentral (online) gespeicherte Daten für eHealth-Anwendungen eine Chipkarte in der Hand des Versicherten als Authentifizierungswerkzeug genutzt, einige Länder verzichten sogar ganz auf die Ausgabe von Chipkarten. Aus Sicht der Interoperabilität im schon für die nahe Zukunft relevanten grenzübergreifenden Kontext ist eine Nutzung eines dezentralen Speichermediums für med. Daten als ein weiteres Hindernis in der Anwendung einzuordnen.

Eine Festlegung des Speicherformats der Inhalte (Format, Kodierung, Struktur) erfolgt erst nach der fachlichen Definition, die im Sommer 2009 abgeschlossen sein soll. Eine Ableitung der Größe und des Speicherplatzbedarfs ist somit noch nicht möglich. Da jeweils national verschiedene Informationsquellen verwendet werden, kann vermutlich nicht in allen Fällen der komplette mögliche Umfang genutzt werden. Es ist von einer Größe von wenige kByte, wenn z.B. nur „Notfalldaten“ genutzt werden, bis zu 200-300 kByte für eine umfangreiche PS auszugehen.

[20] Vgl. http://www.epsos.eu/participants/participating-countries.html