Mobile Anwendungsszenarien der elektronischen Gesundheitskarte

Detlef Hühnlein[1] Torsten Eymann[2] Ulrike Korte[3] Thomas Wieland[4]

[1] secunet Security Networks AG
detlef.huehnlein@secunet.com

[2] Universität Bayreuth
torsten.eymann@uni-bayreuth.de

[3] Bundesamt für Sicherheit in der Informationstechnik
ulrike.korte@bsi.bund.de

[4] Hochschule Coburg
thomas.wieland@fh-coburg.de

Zusammenfassung

Im Rahmen der Einführung der elektronischen Gesundheitskarte (eGK) werden die Systeme der Leistungserbringer und Kostenträger im Gesundheitswesen über eine neue Telematikinfrastruktur miteinander vernetzt. Hierbei stehen bislang leider ausschließlich die ortsgebundenen Systeme der Beteiligten im Fokus der Planung und Realisierung. Da aber viele wichtige Anwendungsfälle der eGK – beispielsweise der Zugriff auf Notfalldaten durch Rettungspersonal oder das Ausstellen von elektronischen Rezepten beim Hausbesuch – typischerweise nicht in den Räumlichkeiten der Leistungserbringer erfolgen, müssen zusätzlich auch mobile Einsatzszenarien betrachtet werden. Im Fokus des vorliegenden Beitrags steht die Frage, welche Änderungen oder Ergänzungen der aktuellen Spezifikationen notwendig sind, um den Einsatz von ortsungebundenen Geschäftsprozessen und mobilen Endgeräten in der Gesundheitstelematik zu ermöglichen.

1 Einleitung

Gemäß § 291a Abs. 1 [SGB V] muss die existierende Krankenversichertenkarte zu einer elektronischen Gesundheitskarte (eGK) erweitert werden, durch die eine aktuelle Prüfung des Versicherungsstatus und die elektronische Übermittlung von Verordnungen sowie eine Reihe von für den Versicherten freiwilligen Anwendungen, wie z.B. die elektronische Patientenakte, möglich werden. Auf Basis verschiedener Vorarbeiten [b4h-RA, b4h-SO, FHG-LA] werden derzeit von der Gesellschaft für Telematikanwendungen der Gesundheitskarte GmbH (gematik) die notwendigen Spezifikationen [gemSpek] und Komponenten für die erforderliche Informations-, Kommunikations- und Sicherheitsinfrastruktur (Telematikinfrastruktur) zur Einführung und Anwendung der eGK erarbeitet. Bei der Entwicklung der Spezifikationen

P. Horster (Hrsg.) · DACH Security (2007) pp.

[gemSpek] und Komponenten der Telematikinfrastruktur durch die Gesellschaft für Telematikanwendungen der Gesundheitskarte (gematik) stehen bislang ausschließlich die ortsgebundenen Systeme der Beteiligten im Fokus der Planung und Realisierung. Da aber viele wichtige Anwendungsfälle der eGK – beispielsweise der Zugriff auf Notfalldaten durch Rettungspersonal oder das Ausstellen von elektronischen Rezepten beim Hausbesuch – typischerweise nicht in den Räumlichkeiten der Leistungserbringer erfolgen, und die Tätigkeit von Ärzten, Apothekern und anderen Heilberuflern oft nicht an feste Rechnerarbeitsplätze gebunden ist, müssen zukünftig auch Aspekte der Mobilität berücksichtigt werden, um das volle Potenzial der elektronischen Gesundheitskarte ausschöpfen zu können. In diesem Beitrag soll untersucht werden, welche Änderungen oder Ergänzungen der aktuellen Spezifikationen der gematik für eine mobile Nutzung der elektronischen Gesundheitskarte notwendig sind. Hierfür wird folgendermaßen vorgegangen: Abschnitt 2 beleuchtet einige typische mobile Anwendungsszenarien im Gesundheitswesen. Nach einer Skizze der derzeit geplanten Telematikinfrastruktur in Abschnitt 3 werden in Abschnitt 4 entsprechende Erweiterungen für eine mobile Nutzung der elektronischen Gesundheitskarte vorgeschlagen. In Abschnitt 5 werden die neuen Herausforderungen zusammengetragen, für die in Abschnitt 6 entsprechende Lösungsansätze aufgezeigt werden. In Abschnitt 7 werden schließlich die wesentlichen Erkenntnisse dieser Arbeit zusammengefasst.

2 Mobile eHealth-Anwendungsszenarien

Mobilität ist ein wesentliches Anforderungsmerkmal eines effektiven Gesundheitssystems, nicht nur im Notfall- oder Rettungswesen. Patienten und medizinisches Personal benötigen Informationen blitzartig und an einem nicht vorher bestimmbaren Zugriffsort, oder wollen solche Informationen zur weiteren Verarbeitung an eine zentrale Leitstelle senden. Die Existenz eines stationären Netzes kann hierbei für einige Teilstrecken einer solchen Datenübertragung wertvolle Dienste leisten. Mindestens an einem Ende des Kommunikationsprozesses steht jedoch ein mobiles Endgerät. Im Folgenden sollen schlaglichtartig einige Anwendungsszenarien im Gesundheitswesen beleuchtet werden, in denen die elektronische Gesundheitskarte und der Heilberufsausweis in Verbindung mit mobilen Endgeräten genutzt werden müssen:

- Mobiler Zugriff auf Notfalldaten und weitere Patientendaten
- Prüfen des Versichertenstatus und Ausstellen eines Rezeptes beim Hausbesuch
- Sicherer mobiler Zugriff auf medizinische Daten und Organisationsdaten
- „Komfortsignatur“ für Leistungserbringer im Gesundheitswesen

2.1 Mobiler Zugriff auf Notfalldaten und Patientenakten

Ein Notarzt oder Rettungssanitäter benötigt für die Erstbehandlung des Patienten dessen Notfalldaten. Hierfür führt er die eGK in sein mobiles, vertrauenswürdiges Endgerät ein, um den auf der eGK gespeicherten Notfalldatensatz angezeigt zu bekommen. Die Autorisierung für diesen Zugriff erfolgt durch eine Card-to-Card-Authentisierung zwischen der eGK und der in das mobile Endgerät integrierten Mobile Health Card. Bei Bedarf werden die in der Datei EF.NET gespeicherten Daten der SMC-Applikation (z.B. Adresse des VPN-Konzentrators) genutzt, um eine mittels VPN gesicherte Verbindung zu den zentralen Systemen der Gesund-

heitstelematik aufzubauen. Sofern der Versicherte zustimmt, kann der Arzt auf weitere Patientendaten zugreifen.

2.2 Versichertenstatus und eRezept beim Hausbesuch

Ein weiterer Anwendungsfall ist die Prüfung des Versichertenstatus und das Ausstellen eines elektronischen Rezeptes durch den Hausarzt bei einem Hausbesuch. Hierzu führt der Arzt die eGK des Patienten in sein mobiles Endgerät ein, um die auf der Karte gespeicherten Stammdaten und den Versichertenstatus einzulesen. Bei Bedarf nutzt er eine VPN-gesicherte Verbindung zur Telematikplattform, um den Versichertenstatus beim so genannten Versichertenstammdatendienst online zu prüfen und eine mögliche Aktualisierung der Daten der Karte anzustoßen. Danach gibt er die elektronischen Verordnungsdaten an seinem mobilen Endgerät ein, erstellt für diese gemäß § 2 Abs. 1 Nr. 10 AMVV[1] unter Verwendung seines in der Praxis gesteckten Heilberufsausweises (HBA) oder der HBA-Applikation auf der Mobile Health Card eine qualifizierte elektronische Signatur und schreibt das elektronische Rezept komprimiert und verschlüsselt auf die eGK. Bei Bedarf wird das elektronische Rezept zusätzlich über eine mittels VPN gesicherte Verbindung zum so genannten Verordnungsdatendienst in der Telematikplattform übertragen.

2.3 Zugriff auf medizinische und organisatorische Daten

Mittels der VPN-Technologie des mobilen Endgerätes kann für den Arzt auch ein gesicherter Zugriff auf die in den Primärsystemen gespeicherten medizinischen Daten oder Organisationsdaten (z.B. Terminkalender) und persönlichen Nachrichten möglich sein, so dass auf diese bei Bedarf über mobile Endgeräte zugegriffen werden kann. Als Transportnetze können hierbei drahtlose Wide Area Networks (Funk-WAN), wie z.B. GSM/GPRS, UMTS oder WiMAX, und lokale Netze (WLAN) unterstützt werden, so dass der Zugriff sowohl beim Hausbesuch als auch im klinischen Umfeld ermöglicht wird. Der Betrieb eines WLAN im Krankenhaus unterliegt besonderen Anforderungen zur elektromagnetischen Verträglichkeit, die in der Norm DIN EN 60601-1-2 beschrieben werden, ist jedoch ansonsten problemlos möglich.

2.4 „Komfortsignatur“ für Leistungserbringer

Da für die Erzeugung einer qualifizierten elektronischen Signatur im Gesundheitswesen im Regelfall das jeweilige Stecken des Heilberufsausweises an einem stationären Arbeitsplatz und die Eingabe einer sechsstelligen PIN nötig ist, aber Ärzte und Apotheker typischerweise nicht an einem festen Arbeitsplatz tätig sind, wird eine starke Beeinträchtigung der Abläufe in der Praxis durch die Erstellung von qualifizierten elektronischen Signaturen für elektronische Rezepte befürchtet[2]. Abhilfe verspricht hier die so genannte „Komfortsignatur“ (vgl. [Hühn07], [KiSc06]), für die der Heilberufsausweis beispielsweise einmalig täglich für die Signaturerzeugung aktiviert wird und die Willenserklärung für das jeweilige Erstellen einer

[1] Verordnung über die Verschreibungspflicht von Arzneimitteln (Arzneimittelverschreibungsverordnung, AMVV), vom 21. Dezember 2005, BGBl. I, S. 3632, http://www.gesetze-im-internet.de/amvv/index.html

[2] Beispielsweise äußerte sich kürzlich ein Vertreter der Ärzteschaft wie folgt: "Jetzt unterschreibt ein Arzt die Rezepte schnell mal am Tresen, das geht zack-zack. In Zukunft muss er für jedes Rezept eine sechsstellige PIN eingeben. […] Wenn das bei der flächendeckenden Einführung der Karte immer noch so ist, dann ist das elektronische Rezept tot." (vgl. http://www.aerztezeitung.de/docs/2006/06/16/02ao1601.asp?cat=/computer)

qualifizierten elektronischen Signatur durch eine biometrische Authentifizierung oder über ein persönliches mobiles Endgerät des Leistungserbringers, z.B. ein RFID-Token oder eine Bluetooth-fähige Uhr, ausgelöst wird.

3 Geplante Telematikinfrastruktur

Im Rahmen der Einführung der elektronischen Gesundheitskarte ist geplant, dass die Leistungserbringer im Gesundheitswesen (Ärzte, Apotheker etc.) die zentralen Telematikdienste (Versichertenstammdatendienst zur Prüfung des Versicherungsstatus, Verordnungsdatendienst für die Verwaltung von elektronischen Rezepten etc.) über einen so genannten Konnektor nutzen können (Abbildung 1).

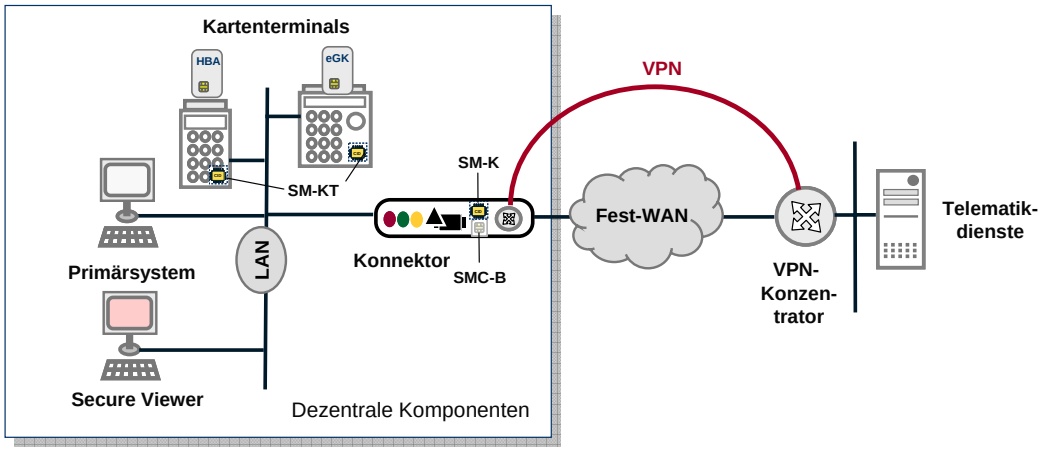

Abbildung 1: Geplante Telematikinfrastruktur zur Einführung der eGK

Hierbei verbindet der Konnektor die lokalen Netze der Leistungserbringer über ein IPSec-basiertes [RFC2401] virtuelles privates Netz (VPN) mit der Telematikplattform. Die Hardware dieses Konnektors besitzt eine kryptographische Identität (SM-K), die für die Prüfung der Integrität des Konnektors und für den Aufbau des VPN genutzt wird. Daneben existiert eine als PlugIn-Karte im ID-000-Format vorgesehene Secure Module Card (SMC) Typ B [SMCSpek], die der Institution des Leistungserbringers zugeordnet ist und für die Authentifizierung auf Transport- [RFC2246] und Anwendungsebene [WSSec] genutzt wird. Außerdem fungiert der Konnektor als Applikations-Proxy zwischen den Primärsystemen (Praxisverwaltungssystem, Krankenhausinformationssystem, Apothekenverwaltungssystem etc.) der Leistungserbringer und den zentralen Telematikdiensten. Schließlich realisiert er mittels der Kartenterminals, die ihrerseits mindestens mit einer hardware-basierten kryptographischen Identität (SM-KT) und ggf. einer SMC-A[3] ausgestattet sind, die Ansteuerung der involvierten Chipkarten (eGK und Heilberufsausweis (HBA)). Der Konnektor besitzt selbst keine Anzeigekomponente, sondern überträgt bei Bedarf die darzustellenden Daten an das möglicherweise unsichere Primärsystem oder eine vertrauenswürdige Anzeigeeinheit (Secure Viewer).

[3] Der Zugriff auf die eGK kann statt mit einem HBA (vgl. [HBASpek]) oder einer SMC-B auch mit einer SMC-A (vgl. jeweils [SMCSpek]) realisiert werden. Diese SMC-A kann auch für Zwecke des Secure Messaging (vgl. [ISO7816-8]) zur sicheren Übermittlung der PIN zu einem entfernt gesteckten HBA (vgl. [VerSA]) oder ein Komfortsignaturverfahren (vgl. [KiSc06]) genutzt werden. Da es nicht ausgeschlossen scheint, die SM-KT und SMC-A auf einer einzigen Chipkarte zu realisieren soll hier nicht näher auf die SMC-A eingegangen werden.

Durch diese Telematikinfrastruktur wird gemäß § 291a Abs. 2 und 3 [SGB V] zumindest das elektronische Rezept, der elektronische Versicherungsnachweis, der Notfallausweis, der elektronische Arztbrief, die Anwendungen zur Arzneimitteltherapiesicherheit, die elektronische Patientenakte, das Patientenfach und die Patientenquittung ermöglicht. Darüber hinaus ist die Telematikinfrastruktur offen für weitere Mehrwertdienste.

4 Mobile Telematikinfrastruktur

Für die mobile Nutzung der elektronischen Gesundheitskarte muss die Funktionalität der verschiedenen dezentralen Komponenten (vgl. Abbildung 1) auf möglichst einem einzigen mobilen Endgerät – dem „mobilen Konnektor“ – realisiert werden. Dieses mobile Endgerät ist über VPN-gesicherte drahtlose Kommunikationsnetze mit der Telematikinfrastruktur oder einem stationären Konnektor gekoppelt (vgl. Abbildung 2).

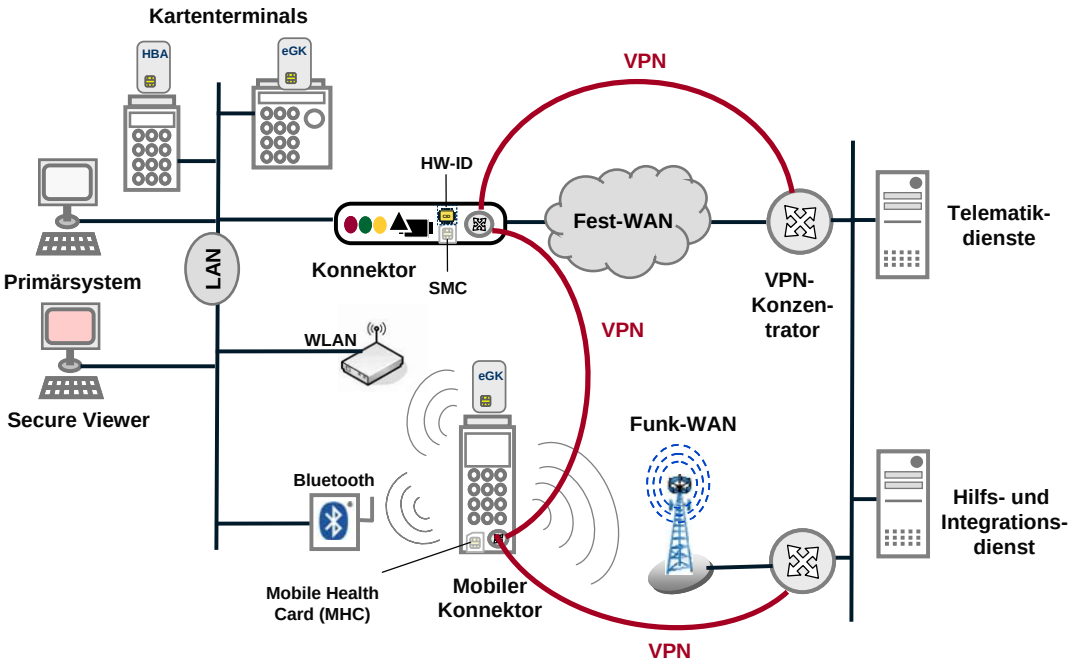

Abbildung 2: Erweiterte Systemarchitektur für die mobile Nutzung der eGK

Da mit UMTS, WLAN, Bluetooth etc. drahtlose Kommunikationstechnologien für vielfältige Einsatzumgebungen grundsätzlich zur Verfügung stehen, muss in Abschnitt 5 vor allem die Realisierung des „mobilen Konnektors“ näher betrachtet werden.

Darüber hinaus ist es als weitere Zukunftsvision denkbar, die elektronische Gesundheitskarte nicht in Form einer eigenständigen Chipkarte im ID1-Format zu realisieren, sondern als „virtuelle Gesundheitskarte“ in Form einer zusätzlichen Chipkartenapplikationen auf einer Multiapplikationskarte. In diesem Fall kann die eGK-Applikation beispielsweise wie in [KrMR07] vorgeschlagen auf einer USIM-Karte aufgebracht werden, so dass mittels des mobilen Endgerätes des Versicherten über NFC-Protokolle [NFC07] drahtlos auf die (virtuelle) elektronische Gesundheitskarte zugegriffen werden kann.

5 Herausforderungen für den mobilen Konnektor

Während die mindestens[4] drei unterschiedlichen Hardwarekomponenten (Primärsystemrechner, Kartenterminal und Konnektor) und bis zu fünf kryptographischen Hardwaremodule (eGK, HBA, SMC-B, SM-K und SM-KT) für den stationären Einsatz aus technischer[5] Sicht vergleichsweise unproblematisch sind, müssen hier für die mobile Nutzung entsprechende Anpassungen vorgenommen werden. Die erstrebenswerte Lösung des „mobilen Konnektors", bei der alle dezentralen Komponenten auf einem einzigen mobilen Endgerät integriert sind, führt zu folgenden Problemen:

1. Viele Chipkartenslots notwendig

   Für die Unterstützung der vorgesehenen kryptographischen Hardwaremodule sind zwei Chipkartenslots im ID1-Format (für eGK und HBA), ein Chipkarten-Slot im ID000-Format (für SMC-B) sowie alternativ Trusted Platform Modules (TPM) für Konnektor und Kartenterminal bzw. zusätzliche Chipkartenslots im ID000-Format (für SM-K und SM-KT) nötig. Darüber hinaus wird für die Nutzung von UMTS ein weiterer Chipkartenslot im ID000-Format für die USIM-Karte benötigt. Gängige mobile Endgeräte besitzen aber nicht ausreichend viele der benötigten Chipkartenslots im ID000- und ID1-Format, so dass eine kostenintensive Spezialentwicklung für die Realisierung des „mobilen Konnektors" notwendig werden würde.

2. Sicherheit von Betriebssystemen für mobile Endgeräte

   Während im stationären Fall die unterschiedlichen Komponenten (Primärsystem, Netz- und Anwendungskonnektor, Kartenterminal) physikalisch oder durch entsprechend sichere Virtualisierungstechniken zumindest logisch voneinander getrennt sind, muss die informationstechnische Trennung auf dem mobilen Endgerät anderweitig erfolgen. Hierbei muss beispielsweise sichergestellt werden, dass möglicherweise existierende Schadsoftware im Primärsystem des mobilen Endgeräts keine Kenntnis von eingegebenen PINs erhalten kann. Deshalb kommt der Sicherheit von Betriebssystemen für mobile Endgeräte eine besondere Bedeutung zu.

3. Beschränkte Rechenleistung mobiler Endgeräte

   Durch den Einsatz von Webservices, die Konsolidierung der verschiedenen Funktionen auf einer Hardware und zusätzlich notwendige Sicherheitsmechanismen gelangt man möglicherweise an die Grenzen der Rechenkapazität heute verfügbarer mobiler Endgeräte. Deshalb sind möglicherweise weitere Optimierungen für die Nutzung mobiler Endgeräte nötig.

[4] Im Rahmen der aktuellen Spezifikationen der Telematikinfrastruktur ist es insbesondere möglich, den Konnektor in Netz- und Anwendungskonnektor aufzuteilen und unterschiedliche Kartenterminals für eGK und HBA zu nutzen.

[5] Vor dem Hintergrund aktueller Meldungen zu den vermeintlichen Kosten der eGK-Einführung (vgl. http://www.heise.de/newsticker/meldung/78348/) könnte eine kritische Überprüfung der aktuellen Spezifikationen im Hinblick auf Kosten-Nutzen-Aspekte sinnvoll erscheinen.

6 Skizze möglicher Lösungsansätze

In diesem Abschnitt sollen jeweils mögliche Lösungsansätze für die in Abschnitt 5 zusammengetragenen Probleme aufgezeigt werden.

6.1 Konsolidierung der kryptographischen Identitäten

Während die unterschiedlichen, dem Leistungserbringer zugeordneten kryptographischen Identitäten (HBA, SMC-B, SM-K und SM-KT) zwar unterschiedlichen Zwecken dienen und voraussichtlich von unterschiedlichen Institutionen herausgegeben und verwaltet werden, so existieren keine zwingenden technischen Gründe, wieso die jeweiligen Schlüsselinformationen auf physikalisch getrennten Chipkarten aufgebracht sein müssen. Betrachtet man die Spezifikationen des HBA[6] und der SMC[7] (Typ B), so wird deutlich, dass sich die Strukturen im Wurzelverzeichnis und der DF.ESIGN-Anwendung lediglich darin unterscheiden, dass die jeweiligen CV-Zertifikate möglicherweise von unterschiedlichen Zertifizierungsinstanzen ausgestellt werden und die X.509-Zertifikate beim HBA auf die natürliche Person des Leistungserbringers selbst, aber bei der SMC (Typ B) auf die Institution des Leistungserbringers (z.B. Arztpraxis Dr. Müller) ausgestellt werden. Während die detaillierte Personalisierung der SM-K und SM-KT den Herstellern überlassen ist, so ist festgelegt, dass sie ein asymmetrisches Schlüsselpaar (angedeutet durch EF.PrK_K und EF.PuK_K) und Referenzwerte zur Prüfung der Software-Identität (EF.INT) besitzen müssen.

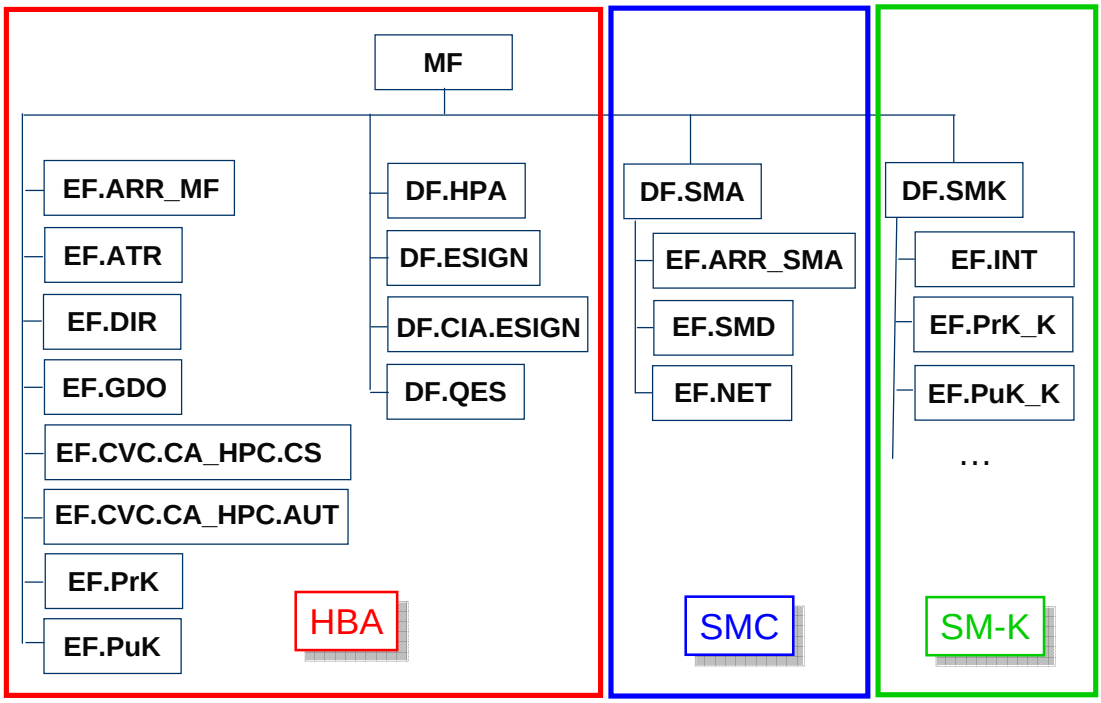

Abbildung 3: Dateistruktur einer möglichen „Mobile Health Card“

Da es keinen zwingenden technischen Grund gibt, dass die unterschiedlichen Schlüssel auch im mobilen Einsatzszenario auf unterschiedlichen Chipkarten aufgebracht sein müssen, kann,

[6] Vgl. [HBASpek], Abbildung 1 (Dateistruktur des HBA), Seite 18.

[7] Vgl. [SMCSpek], Abbildung 4 (Strukturübersicht für SMC Typ B), Seite 31.

wie in Abbildung 3 angedeutet, die Funktionalität des HBA, der SMC (Typ B) und der SM-K des „mobilen Konnektors“ auf einer einzigen Chipkarte – der so genannten Mobile Health Card (MHC) – zusammengefasst werden, sofern diese während des Betriebs fest mit dem persönlichen mobilen Endgerät des entsprechenden Leistungserbringers verbunden ist.

6.2 Sicherheitsaspekte bei mobilen Endgeräten

Mobile Endgeräte stellen sich technisch durchaus heterogen dar. Es ist auf dem Markt eine große Bandbreite an Geräten mit unterschiedlicher Ressourcenausstattung und daraus resultierenden divergenten Sicherheitsmerkmalen verfügbar. Die wichtigsten Klassen aus Sicht der Nutzung im Gesundheitswesen sind:

1. Notebook, d.h. tragbarer PC
2. PDA, Smartphone oder entsprechendes, aber spezialisiertes Endgerät
3. Mobiltelefon

Viele der oben genannten Einsatzszenarien sind mit allen drei Kategorien realisierbar. Dabei stellt das Notebook jedoch einen Sonderfall dar. Durch integrierte Kartenleser, eine gleichartige Softwareausstattung und entsprechende Netzanbindung kann es ähnlich wie ein stationärer PC behandelt werden. Zunächst stellt lediglich die ggf. nicht permanent verfügbare Verbindung ins Internet und damit zur Telematikplattform einen Unterschied dar, der jedoch für die vorgesehenen Anwendungen nicht kritisch ist. Hier wie dort ist eine kontinuierliche Wartung der Softwareplattform auf den Geräten, einschließlich der regelmäßigen Aktualisierung von Anti-Viren-Programmen, persönlichen Firewalls und des zugrunde liegenden Betriebssystems, ohnehin unverzichtbar. Auch weitere Aspekte der „Betriebssystemhärtung“ wie das Abschalten von nicht benötigten Server-Diensten, eine gezielte Verwaltung der Berechtigungen sowie der Verzicht auf Admin-Rechte sind generell zu empfehlen. Idealer Weise sind die minimalisierte Systemplattform und die Anwendungen mit einem unterschiedlichen Bedarf an Sicherheit und Flexibilität mittels vertrauenswürdiger Virtualisierungstechniken voneinander separiert (vgl. [SINA-VW]).

Außerdem ist bei Notebooks die Tatsache von besonderer Bedeutung, dass derartige Geräte grundsätzlich tragbar sind und daher an jeden beliebigen Ort gebracht und dort benutzt werden können. Insbesondere können sie auch von ihrem Benutzer dort vergessen und zurückgelassen oder aber ihm entwendet werden. Auf diese Weise kann einem Unbefugten u.U. ein Rechner mit sensiblen medizinischen Daten – und schlimmstenfalls einem steckenden HBA – in die Hände fallen. Daher ist neben der vertrauenswürdigen Systemplattform auch die sichere Verschlüsselung der Daten und der relevanten Programme bzw. der gesamten entsprechenden Speicherbereiche bei einem Einsatz im Gesundheitswesen zwingend erforderlich.

Daneben sind die drahtlosen Netzwerkverbindungen (Bluetooth, WLAN etc.) über entsprechend sichere Virtuelle Private Netze zu schützen. Da die protokollspezifischen Sicherheitsmaßnahmen hier keinen ausreichenden Schutz bieten (vgl. [JaWe01], [TWP07]), müssen zusätzliche Sicherheitsmaßnahmen auf höheren Schichten (z.B. [RFC2401], [RIM07]) vorgesehen werden.

Während die angeführten grundlegenden Sicherheitsaspekte auch für PDAs und Smartphones gelten, so scheint das Thema Trusted Computing für diese Plattformen jedoch weniger weit entwickelt als beispielsweise für Desktop-Betriebssysteme (vgl. [PRR05], [MuRo05]). Ob hierbei aktuelle Betriebssysteme wie Windows Mobile 5.0 und entsprechende sicherheitsspe-

zifische Ergänzungen, wie das Messaging and Security Feature Pack (MSFP), für eine signifikante Verbesserung sorgen, ist näher zu untersuchen.

Bei Standardgeräten wie marktüblichen PDAs und Smartphones kommt zudem hinzu, dass sie oft über keine Schnittstellen zu einem Kartenleser für Chipkarten verfügen. Einige bieten einen USB-Port an, über den ein Kartenleser angeschlossen werden kann. Bei anderen sind jedoch nur proprietäre Schnittstellen vorhanden. Einen Ausweg bietet hier der Bluetooth-Funkstandard, der inzwischen von den meisten derartigen Geräten unterstützt wird. Hersteller wie Research In Motion (RIM) bieten separate Chipkartenleser mit Bluetooth-Anbindung[8] an, wobei zusätzliche Sicherheitsmaßnahmen auf höheren Ebenen vorgesehen sind. Wie in [RIM07] erläutert, wird die Kommunikation zwischen dem mobilen Endgerät und dem Kartenterminal zusätzlich verschlüsselt, wobei die hierfür verwendeten Schlüssel nicht statisch in den Geräten hinterlegt werden, sondern unter Verwendung eines Passwort-basierten Schlüsselaustausch-Verfahrens auf Basis elliptischer Kurven ausgehandelt werden.

Auch wenn das Abhören von Bluetooth-Verbindungen durch das häufige[9] Wechseln der Sendefrequenz nicht trivial ist, stellt dies für Angreifer mit hohem Angriffspotenzial kein unüberwindbares Hindernis dar (vgl. [Mos07]). Deshalb sind beim Einsatz von Bluetooth – insbesondere für sensible Anwendungen im Gesundheitswesen – wie in [RIM07] zusätzliche Sicherheitsmaßnahmen notwendig.

Für den Einsatz im Gesundheitswesen kommen aus diesen Gründen vor allem spezialisierte Geräte in Frage, die bereits alle notwendigen Kartenleser integriert haben. Für diese ist auch ein angepasster Formfaktor sowie spezielle Software-Umgebung möglich. Erste derartige Geräte sind bereits in einigen Kliniken und bei Pflegediensten im Einsatz.

Bei Mobiltelefonen sind die Möglichkeiten im Allgemeinen noch stärker eingeschränkt. Aufgrund geringer Speicherkapazität, kleinem Display und unzureichenden Eingabemöglichkeiten ist ein direkter Einsatz von Mobiltelefonen als Endgerät bei Anwendungen der eGK eher unwahrscheinlich. Aus Sicht der Systemsicherheit scheinen Mobiltelefone jedoch gewisse Vorteile zu bieten, da eine Code-Signierung auf Anwendungsebene erfolgt und Applikationen gegenüber den anderen Komponenten in einer logisch getrennten Umgebung ablaufen können. Allerdings kann auch hier die Bluetooth-Schnittstelle bei einigen Geräten missbraucht werden, weshalb zusätzliche Sicherheitsmaßnahmen in höheren Protokollschichten angezeigt sind.

Allerdings bedeutet die Interaktion mit dem HBA eine technische Herausforderung für Mobiltelefone. Hier ist die oben genannte Lösung mit einem Bluetooth-fähigen Chipkartenleser oft die einzige Zugriffsmöglichkeit. Weitere bereits genannte Aspekte, wie die Absicherung bei Verlust des Geräts, gelten hier analog.

Aufgrund der Komplexität der Algorithmen beim Einsatz der eGK stellt sich jedoch die Frage, ob Mobiltelefone angesichts der beschränkten Rechenleistung und Speicherausstattung überhaupt dazu in der Lage sind, als Endgeräte zu fungieren.

Zusammenfassend lässt sich festhalten, dass eine Realisierung des mobilen Konnektors auf Basis einer Notebook-artigen Plattform bereits mit heute verfügbaren Mitteln in sehr sicherer

[8] http://www.blackberry.com/products/accessories/smartcard.shtml

[9] Typischer Weise 1600 mal pro Sekunde.

Art und Weise möglich ist aber für weniger leistungsfähigere mobile Endgeräte (PDA, Smartphone, Mobiltelefon etc.) in diesem Bereich noch etwas Forschungsbedarf existiert.

6.3 Optionen für die Verteilung der Anwendungslogik

6.3.1 Server-Unterstützung

Sofern ein ausreichend leistungsfähiges Kommunikationsnetz (z.B. WLAN im Krankenhaus) zur Verfügung steht, kann eine Ultra-Thin–Client-Architektur zum Einsatz kommen, so dass das mobile Endgerät lediglich für die Ein- und Ausgabe von Daten genutzt werden muss. Die gesamte Anwendungslogik befindet sich dabei auf dem Server und muss nur dort installiert und gepflegt werden. Das Endgerät übernimmt lediglich die unmittelbare Benutzerschnittstelle.

Hierbei bietet sich vor allem die AJAX-Technologie an. Dabei werden nicht wie klassischerweise stets vollständige Webseiten übertragen, sondern nur einzelne Elemente gezielt aktualisiert. Eine Absicherung der Verbindung ist entweder über eine VPN-Verbindung oder mittels TLS möglich. Die Anwendung auf dem mobilen Endgerät stellt sich dem Benutzer dann wie ein bekannter Web-Browser dar, so dass eine rasche Vertrautheit mit der Nutzung des mobilen Geräts erreicht werden kann.

Eine weitere Möglichkeit ist ein Terminal-Server, bei dem die gesamte Sitzung für Anwendung serverseitig abläuft und der Client ebenfalls nur für Ein- und Ausgabe zuständig ist.

Diese Optionen erleichtern die Verteilung und Wartung der Software, könnten bei der Umsetzung jedoch auf Schwierigkeiten aufgrund des notwendigen lokalen Zugriffs auf den HBA stoßen.

6.3.2 Service-orientierte Realisierungen

Wenn mehr Logik als eine reine Thin-Client-Lösung auf das mobile Endgerät übertragen werden soll, bspw. weil das Gerät auch in Umgebungen mit schlechterer Netzanbindung eingesetzt werden soll, so können rechenintensive Operationen auf einen Server verlagert werden. Beispielsweise kann die vergleichsweise aufwändige Bildung und Prüfung von Zertifikatspfaden unter Verwendung des Server-based Certificate Validation Protocol (SCVP) [SCVP-ID] vom mobilen Endgerät auf einen stationären Konnektor oder einen spezialisierten Dienst in der Telematikinfrastruktur ausgelagert werden.

Doch die Möglichkeiten der Verteilung der Gesamtanwendung gehen weit über die reine Umschichtung von Rechenaufgaben hinaus. Wie in vielen Unternehmensanwendungen geht man auch in der Gesundheitstelematik dazu über, die Software-Architekturen nach den Prinzipien der Service-Orientierung (SOA) zu gestalten [DJMZ05]. Da sich die einzelnen Applikationen in der Telematikplattform der gematik aus Web Services zusammen setzen, ist es naheliegend diesen dienstorientierten Ansatz auch für mobile Anwendungsszenarien der eGK zu verfolgen.

Da es sich bei Web Services um eine sehr einfache und textbasierte Form der Kommunikation handelt, sind diese grundsätzlich auch mit wenig leistungsfähigen Endgeräten wie Mobiltelefonen nutzbar [ElYo04]. Das zugrunde liegende SOAP-Protokoll wird dabei meist über HTTP übertragen. Daher bietet sich zur Absicherung TLS [RFC2246] an. Dies ist jedoch nur dann sinnvoll, wenn eine reine Punkt-zu-Punkt-Verbindung zwischen Nutzer und Anbieter des Web Service möglich ist. Sind dagegen noch Vermittler oder andere Zwischenstationen (z.B.

der Broker) an der Übertragung beteiligt, so besteht bei der TLS-Verschlüsselung nur auf jeder Teilstrecke eine sichere Verbindung, jedoch nicht von Ende zu Ende. Hierfür sind weitere Technologien wie WS-Security [LaKa06] vonnöten. In dieser Spezifikation wird SOAP um Aspekte wie Signatur, Verschlüsselung, PKI etc. erweitert. Für eine Realisierung auf mobilen Endgeräten existieren hierfür auch bereits entsprechende Entwicklungswerkzeuge (vgl. [IBM07], [Nokia07]), so dass selbst mit Mobiltelefonen sichere und signierte Verbindungen über Web Services realisierbar sein dürften. Durch eine Kompression der XML-Dokumente, wie sie auch bei einem Verschlüsselungsverfahren integriert werden kann, lässt sich die zu übertragende Datenmenge und damit die Reaktionszeit reduzieren [TVNRS03]. Analoges gilt für PDAs und spezialisierte, Windows Mobile-basierte Endgeräte.

Insgesamt stellt eine verteilte, service-orientierte Architektur einen sehr vielversprechenden Ansatz dar. Aufgrund der Beschränkungen in der Bandbreite bei Datenverbindungen über Mobilfunk und der damit verbundenen Kosten sollten für mobile Anwendungen der eGK Client-Applikationen geschaffen werden, die weitgehend in sich geschlossen arbeiten und den Kommunikationsaufwand gering halten. Die Ende-zu-Ende-Sicherheit bei der Übertragung sensibler Daten mit Web Services kann durch Technologien wie WS-Security aber in jedem Fall gewährleistet werden.

7 Zusammenfassung

In diesem Beitrag wurde untersucht, in welcher Art und Weise die Spezifikationen der Telematikinfrastruktur für die Einführung der eGK ergänzt werden müssen, damit auch eine mobile Nutzung ermöglicht wird. Hierbei sollte insbesondere die Konsolidierung der notwendigen kryptographischen Identitäten auf einem Sicherheitsmodul – der so genannten Mobile Health Card – ermöglicht werden. Während eine spezifikationskonforme Umsetzung auf leistungsfähigen mobilen Endgeräten (z.B. Notebooks) bereits heute möglich ist, scheinen für weniger leistungsfähige Endgeräte (z.B. PDAs und Mobiltelefone) weitere Untersuchungen notwendig, um eine gleichsam sichere und effiziente Nutzung der Gesundheitstelematik zu ermöglichen.

Literatur

[b4h-RA] Projektgruppe bIT4health: *Rahmenarchitektur der Telematikplattform im Gesundheitswesen*, 2004, via http://www.dimdi.de/static/de/ehealth/karte/kartetechnik/rahmenarchitektur/index.html

[b4h-SO] Projektgruppe bIT4health: *Solution Outline - Skizzierung der Lösungsarchitektur und Planung der Umsetzung*, 2004, via http://www.dimdi.de/static/de/ehealth/karte/kartetechnik/solutionoutline/index.html

[DJMZ05] W. Dostal, M. Jeckle, I. Melzer, B. Zengler: *Service-orientierte Architekturen mit Web Services*. Spektrum Akademischer Verlag, Heidelberg, 2005

[eCard-2] BSI: *eCard-API-Framework – Teil 2 – eCard-Interface*, Technische Richtlinie des BSI Nr. 03112-2, in Vorbereitung

[ElYo04] J. Ellis, M. Young: *J2ME Web Services 1.0 (JSR 172)*, via http://sdlc-esd.sun.com/ESD8/JSCDL/j2me_web_services/1.0-fr/j2me_web_services-1_0-fr-spec.pdf

[FHG-LA] Fraunhofer-Gesellschaft: *Spezifikation der Lösungsarchitektur zur Umsetzung der Anwendungen der elektronischen Gesundheitskarte*, 2005, http://www.dimdi.de/static/de/ehealth/karte/kartetechnik/loesungsarchitektur/ergebnisse/index.html

[gemSpek] gematik: *Spezifikationen zur Telematikinfrastruktur für die Einführung und Anwendung der elektronischen Gesundheitskarte*, via http://www.gematik.de/(S(wf12d1mqulfss355k4wd3zf0))/Standards__Spezifikationen___Normen.Gematik

[HBASpek] *Heilberufs-Ausweis und Security Module Card, Teil 2: HBA - Anwendungen und Funktionen*, Version: 2.1.0, via http://www.bmg.bund.de/cln_041/nn_667298/SharedDocs/Gesetzestexte/Gesundheitskarte/HBA-D2,templateId=raw,property=publicationFile.pdf/HBA-D2.pdf

[Hühn07] D. Hühnlein: *Rechtliche Rahmenbedingungen der „Komfortsignatur“*, im vorliegenden Tagungsband

[IBM07] IBM: *Web Services Tool Kit for Mobile Devices*, via http://www.alphaworks.ibm.com/tech/wstkmd/

[ISO7816-8] *Identification cards — Integrated circuit(s) cards with contacts — Part 8: Security related interindustry commands*, ISO/IEC 7816-8, 1999

[JaWe01] M. Jakobsson, S. Wetzel: *Security Weaknesses in Bluetooth*, in D. Naccache (Hrsg.), Progress in Cryptology - RSA Conference 2001, LNCS 2020, Springer-Verlag, 2001, S. 176-191

[KiSc06] W. Killmann, V. Schenk: *Konzept für die Komfortsignatur mit dem Heilberufsausweis*, Version 0.6, Stand 06.07.2006

[KrMR07] M. Kröber, W. Mohrs, C. Reiß: *SubscriberIdentification-Karten*, in B. Struif (Hrsg.) Personal Identity – Documents & Cards in Lifetime, 2007, S. 97-106

[LaKa06] K. Lawrence, C. Kaler: *Web Service Security: SOAP Message Security 1.1*, OASIS Open 2006, via http://www.oasis-open.org/committees/download.php/21255/wss-v1.1-spec-errata-os-SOAPMessageSecurity.pdf

[MuRo05] T. Murmann, H. Rossnagel: *How Secure Are Current Mobile Operating Systems?* in D. Chadwick and B. Preneel (Hrsg.): Communications and Multimedia Security, New York, Springer, S. 47-58, via http://sec.cs.kent.ac.uk/cms2004/Program/CMS2004final/p2a2.pdf

[Mos07] M. Moser: *Busting the Bluetooth Security Myth – Getting RAW Access*, via http://www.remote-exploit.org/research/busting_bluetooth_myth.pdf

[Nokia07] Nokia: *Nokia Mobile Web Services Framework, Architecture, APIs, SDK*, via http://forum.nokia.com/main/resources/technologies/web_services/index.html

[NFC07] NFC-Forum: *The Near Field Communication (NFC) Forum - homepage*, via http://www.nfc-forum.org/home

[PRR05] E. Pisko, K. Rannenberg, H. Roßnagel: *Trusted Computing in Mobile Platforms - Players, Usage Scenarios, and Interests*, DuD, 29, 2005, S. 526-530, via http://www.wiiw.de/publikationen/TrustedComputinginMobilePlatfo1479.pdf

[RFC2246] T. Dierks, C. Allen: *The TLS Protocol - Version 1.0*, RFC2246, via http://www.ietf.org/rfc/rfc2246.txt

[RIM07] Research in Motion: *BlackBerry Smart Card Reader Security Version 1.5 Technical Overview* , via http://www.blackberry.com/knowledgecenterpublic/'livelink.exe?func=ll&objid=1273847&objaction=open

[RFC2401] S. Kent, R. Atkinson: *Security Architecture for the Internet Protocol*, RFC2401via http://www.ietf.org/rfc/rfc2401.txt

[SCVP-ID] T. Freeman, R. Housley, A. Malpani, D. Cooper, T. Polk: *Server-based Certificate Validation Protocol (SCVP)*, Internet-Draft via http://www.ietf.org/internet-drafts/draft-ietf-pkix-scvp-27.txt

[SGB V] *Sozialgesetzbuch – Fünftes Buch (V) – Gesetzliche Krankenversicherung* (Artikel 1 des Gesetzes v. 20. Dezember 1988, BGBl. I S. 2477), zuletzt geändert durch Art. 3a G. v. 20.7.2006 I 1706, via http://bundesrecht.juris.de/bundesrecht/sgb_5/

[SINA-VW] secunet: *Die SINA Virtual Workstation 2.1*, via http://www.secunet.de/fileadmin/Downloads/sina-vw_d.pdf

[SMCSpek] *Heilberufs-Ausweis und Security Module Card, Teil 3: SMC - Anwendungen und Funktionen*, Version: 2.1.0, via http://www.bmg.bund.de/cln_041/nn_667298/SharedDocs/Gesetzestexte/Gesundheitskarte/HBA-D3,templateId=raw,property=publicationFile.pdf/HBA-D3.pdf

[TVNRS03] M. Tian, T. Voigt, T. Naumowicz, H. Ritter, J. Schiller. *Performance Considerations for Mobile Web Services*. Workshop on Applications and Services in Wiresless Networks, Bern, Switzerland, July 2003

[TWP07] E. Tews, R.-P. Weinmann, A. Pyshkin: *Breaking 104 bit WEP in less than 60 seconds*, via http://eprint.iacr.org/2007/120.pdf

[VerSA] Werbe- und Vertriebsgesellschaft Deutscher Apotheker mbH: *VERSA – Verteilte Signatur Arbeitsplätze*, via www.wuv-gmbh.de/media/versa_abstract.pdf

[WSSec] OASIS: *Web Services Security v1.0*, via http://www.oasis-open.org/specs/index.php#wssv1.0