

Retrospektive der bekannten sicherheitstechnischen Problematiken bei der Einführung der elektronischen Gesundheitskarte und der Telematikinfrastruktur in Deutschland.

Ali Sunyaev¹, Stefan Knippl¹, Sebastian Dünnebeil²,
Jan-Marco Leimeister³, Helmut Krcmar²

¹ Wirtschafts- und Sozialwissenschaftliche Fakultät
Universität zu Köln
Deutschland
{sunyaev, knipl}@wiso.uni-koeln.de

² Fakultät für Informatik
Technische Universität München
Deutschland
{duennebe, krcmar}@in.tum.de

³ Fakultät für Wirtschaftswissenschaften
Universität Kassel
Deutschland
leimeister@uni-kassel.de

Abstract: Die Sicherheitsmechanismen und das Sicherheitskonzept der Telematikinfrastruktur sind ein wesentlicher Bestandteil der veröffentlichten technischen Spezifikationen zur Einführung der elektronischen Gesundheitskarte in Deutschland. Für eine zuverlässige Handhabung der Gesundheitstelematik ist die Qualität der eingesetzten Sicherheitstechnik essentiell. Dieser Beitrag überprüft mögliche Sicherheitsproblematiken rund um die elektronische Gesundheitskarte, die in früheren Analysen der gematik-Spezifikationen festgestellt worden waren. Hierzu untersuchen wir ebenfalls, inwiefern und ob die Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH (gematik) diese kommunizierten Fragestellungen in den aktuellen Spezifikationen der Telematikinfrastruktur berücksichtigt hat.

1 Einleitung

Die Einführung der Telematikinfrastruktur (TI) ist eines der weltweit größten Projekte im Informationstechnik-Bereich. Die Verwaltung von sensiblen medizinischen Daten aller Bürger der Bundesrepublik hat bereits zum jetzigen Zeitpunkt reges Interesse von Seiten vieler unterschiedlicher Interessensgruppen geweckt. Viele daraus hervorgegangene

Publikationen haben sich zumindest in Teilen mit der Sicherheit der medizinischen Daten beschäftigt. In diesem Beitrag werden exemplarisch einige der in [Su09b], [Su09c], [HSK08], [Kn09], [SLK10] und [Ma08] beschriebenen Bedenken betrachtet. Außerdem wird überprüft, ob diese Kritiken sinnvoll waren und wenn ja, ob sie in den aktuellsten Spezifikationen der gematik zu Änderungen geführt haben.

2 Ergebnisse

Trotz mancher genereller Bedenken gegenüber der elektronischen Gesundheitskarte und der Telematikinfrastruktur, welche durchaus diskutabel sein können, soll es in diesem Beitrag im Wesentlichen um konkrete Bedenken bezüglich der Sicherheit der TI gehen. So befürchtet beispielsweise [Ma08] Gesetzesänderungen nach der Einführung, die die Sicherheitsvorschriften zugunsten des Staates aufweichen könnten, sowie eine schlechte Kosten-Nutzen-Bilanz. Diese müssen natürlich auch berücksichtigt werden, sind aber aufgrund der anderen Thematik nicht Gegenstand dieses Beitrags.

Im Folgenden wird mehrere Male auf die von der Projektgruppe bit4Health erarbeiteten Sicherheitsanforderungen zur Einführung der Gesundheitskarte [NBB04] hingewiesen. Dieses Konsortium bestand aus Fachleuten von SAP, IBM Deutschland, dem Fraunhofer-Institut für Arbeitswirtschaft und Organisation, der InterComponentWare AG und der Sagem Orga (damals: ORGA Kartensysteme). Es wurde von der Bundesregierung beauftragt, eine herstellerneutrale Rahmenarchitektur und Sicherheitsinfrastruktur für ein vernetztes Gesundheitswesen zu entwerfen [In06]. Die daraus entstandenen Dokumente bilden die Basis, auf der die gematik eine konkrete und detaillierte Ausarbeitung aller Einzelaspekte erstellt hat.

2.1 Lichtbild

[Kn09] sieht ein Problem in der Handhabung der Lichtbilder, die auf eGK und HBA aufgebracht werden. Diese sollen zur visuellen Identifikation der Versicherten durch das medizinische Personal dienen und auf diese Weise Missbrauchsmöglichkeiten einschränken.

Den Autoren ist aber keine Rechtsgrundlage bekannt, welche die Versicherten zur Abgabe eines Lichtbilds verpflichten würde. Nach bisherigen Erfahrungen der Kartenherausgeber wird dies deshalb von einem hohen Prozentsatz der Versicherten auch nicht getan¹. Außerdem werden die Bilder weder von den Kostenträgern selbst, bzw. durch von Ihnen beauftragte Fotografen, angefertigt. Auch wird auf keine andere Art und Weise verifiziert, dass ein Lichtbild die Versicherte oder den Versicherten selbst zeigt. Dadurch können Kostenträger nicht sicherstellen, dass die Lichtbilder den Anforderungen genügen, welche etwa an ein Lichtbild für einen deutschen Reisepass gestellt werden. Im Allgemeinen ist hier zwar kaum Mißbrauch zu erwarten. Dennoch sollte am besten durch den Gesetzgeber eine Regelung geschaffen werden, die für Klarheit sorgt.

¹vgl. etwa [Sy07]

2.2 Verletzung der Informationshoheit der Versicherten

[Ma08, S.88f.] sieht in [NBB04] die Informationshoheit der Versicherten verletzt. Einerseits wird deutlich gemacht, dass Versicherte selbst entscheiden können müssen, wer Einblick in ihre Daten nehmen kann [NBB04, S.19], andererseits wird die Möglichkeit eingeräumt, Versichertendaten “in Ausnahmefällen” direkt den Gesetzlichen Krankenkassen zur Verfügung zu stellen [NBB04, S.19]. Hier wird weder gefordert, dass die Versicherten darüber informiert werden müssen, noch werden die Umstände, die dazu vorliegen müssen (“Schadensersatzansprüche gegenüber Dritten”) genauer definiert. Ebenso wird die Anforderung aufgestellt, dass es eine Möglichkeit geben muss, pseudonymisierte Daten der Versicherten periodenübergreifend auszuwerten [NBB04, S.38]. Es steht zu befürchten, dass bei Vorliegen größerer Datenmengen über eine Versicherte oder einen Versicherten mit verhältnismäßig geringem Aufwand eine Depseudonymisierung durchgeführt werden kann.

In den Dokumenten der gematik wird die Datenhoheit der Versicherten betont. Es gibt keine Ausnahmefälle, in denen von diesem Prinzip abgewichen werden kann. Auch in [oV88] wird ausdrücklich betont, dass der Zugriff auf die Daten nur mit dem Einverständnis der Versicherten durchgeführt werden darf. Wird dieses nicht erteilt, so darf keine Benachteiligung erfolgen [oV88, 291a, Abs. 5 und 8]. Aufgrund der Pseudonymisierung gilt, dass für eine periodenübergreifende Auswertung die Mitwirkung der Kartenherausgeber nötig wäre, welche die Pseudonyme vergeben. Für eine über mehr als ein Pseudonym hinausgehende Begutachtung (also mehr als eine eGK, in der Regel dementsprechend 5 Jahre) müssten diese Daten von ihnen herausgegeben werden.

Da der Kartenherausgeber keinerlei Zugriff auf die in der TI gespeicherten Daten haben wird, kann er eine solche Auswertung keinesfalls selbst durchführen. Selbst dann könnten jedoch keine umfassenden Erkenntnisse gewonnen werden. Alle Datenobjekte sind mit dem Schlüssel der oder des Versicherten verschlüsselt sind und können nur von ihnen selbst entschlüsselt werden. Dies ändert sich nur dann, wenn Schlüsseltreuhänder eingeschaltet würden. Zum Einen erscheint der Aufwand dafür enorm hoch und zum Anderen erscheint es fraglich, ob dies den Vorgaben von [oV90] entspräche. Diese Kritik hat damit ihren Widerhall bei der Entstehung der durch die gematik aufgestellten Rahmenbedingungen gefunden.

2.3 Zusammenführung von administrativen und medizinischen Daten

[HSK08] fanden den Widerspruch, dass einerseits bei jedem Fachdienst zuständige Datenschutzbeauftragte einen Schlüssel zur Zusammenführung administrativer und medizinischer Daten besitzen sollen [NBB04, S.20]. Andererseits darf die Sicherheit nicht auf dem Vertrauen in einzelne Personen beruhen [NBB04, S.30]. Dies soll effektiv verhindern, dass etwa Erpressung oder Bestechung zu einer ernsthaften Gefährdung der medizinischen Daten führen könnten. Diese beiden Vorgaben widersprechen sich gegenseitig.

In den aktuellen Dokumenten der gematik wird diese Möglichkeit nicht mehr genannt. So wird definiert, dass “eine Zusammenführung der Metadaten von zwei Fachdiensten (...)

NICHT möglich sein [darf]” [ge08b, S.172]. Das schließt zwar die Zusammenführung bei nur einem einzelnen Fachdienst nicht aus, weist aber doch konzeptionell in die entgegengesetzte Richtung.

Das Treuhänderkonzept [ge09a, S.60] stellt sicher, dass Daten, die mit dem Schlüssel der oder des Versicherten chiffriert sind, auch nur von dieser oder diesem selbst oder unter Einbeziehung mehrerer Personen entschlüsselt werden können. Damit ist die Prämisse, dass Sicherheit nicht von einzelnen Personen abhängen darf, wieder weitgehend hergestellt. Könnte eine Zusammenführung von administrativen und medizinischen Daten stattfinden, so wäre es möglich, daraus Rückschlüsse zu ziehen. So könnten etwa Schätzungen über die Häufigkeit der Inanspruchnahme medizinischer Leistungen aufgestellt werden. Die eigentlichen medizinischen Daten könnten aber zunächst ohne Hinzuziehen der Treuhänder nicht entschlüsselt bzw. ausgewertet werden. Die ursprünglichen Bedenken können somit als geklärt bezeichnet werden.

2.4 Falsche Annahmen im Zonenkonzept

Durch [HSK08] wird eine zentrale Prämisse des von der gematik aufgestellten Zonenkonzepts in Frage gestellt, welche besagt, dass sich Bedrohungen nicht über die Zonen Grenzen hinweg ausbreiten können, da hier die nötigen Vorkehrungen getroffen würden, um dies zu verhindern². [HSK08] konstruieren einen Angriff, in dem eine Innentäterin oder ein Innentäter sich mittels eines HBAs von Zone 1 aus einen unbefugten Zugang zur TI verschafft. Dort wird der HBA erfolgreich authentifiziert. Auf dieser Basis kann nun ein Angriff auf die inneren Zonen durchgeführt werden. Damit wird dies als falsche Annahme dargestellt.

Tatsächlich wird die Bedrohungsquelle nicht wie proklamiert innerhalb der Grenzen von Zone 1 gehalten. Man sollte sich jedoch bewusst sein, dass in diesem Fall nicht von einer isolierten Bedrohung, sondern von zwei sich gegenseitig bedingenden gesprochen werden muss. Zum Einen muss eine Verletzung der Sicherheitsbedingungen in Zone 1 auftreten, also etwa das Entwenden eines HBAs und der zugehörigen PINs durch Innentäter³. Zum Anderen kann dann ausgehend auf dieser Basis in einem weiteren Schritt ein Angriff in den dadurch erreichten inneren Zonen durchgeführt werden.

Da unter bestimmten Umständen an den Zonengrenzen unbefugt eine erfolgreiche Authentifizierung erreicht werden kann, ist die durch die gematik angestellte Annahme tatsächlich etwas zu vollmundig. Im Kern kann sie dennoch als gültig angesehen werden. Eine Bedrohungsquelle, die ihren Ursprung in einer anderen Zone hat, hat weitaus eingeschränktere Möglichkeiten für darauf aufbauende Angriffe, als dies für Bedrohungsquellen in der gleichen Zone gilt.

²vgl. [ge08b, S.32]

³vgl. z.B. [Su08b] für verschiedene Angreiferprofile

2.5 Zeitabstände zwischen Anpassungen der Sicherheitsstandards

Die gematik erlegt sich selbst die Aufgabe auf, regelmäßig die Mindeststandards des Sicherheitskonzepts zu überprüfen, ob diese der jeweils gültigen Bedrohungslage weiterhin entsprechen. [SLK10] kritisieren hierbei lediglich, dass die Standards nur einmal jährlich überprüft und angepasst werden müssen⁴. Jährlich werden eine große Anzahl an Schwachstellen in Protokollen, Diensten und Chiffrierungsverfahren bekannt. Dies betrifft damit auch Komponenten und Bestandteile der TI. Unter diesem Gesichtspunkt und angesichts der zu schützenden Daten mutet die Mindestbefüllung der Empfehlungen der IT-Grundschutzkataloge des BSI von nur einer Überprüfung pro Jahr [Bs09, S.1] zumindest befremdlich an.

Auch in der aktuellsten Version des gematik-Sicherheitskonzeptes wurde dieser Zeitraum nicht verändert [ge08b, S.43ff.]. Eine Verringerung dieses Zeitraums müsste nicht zwingend zu einer Verbesserung der Sicherheit führen. Eine Aktualisierung des Sicherheitskonzeptes darf auch außerhalb dieser regelmäßigen Überprüfung jederzeit stattfinden, wenn Probleme entdeckt werden. Eine häufigere Überprüfung dieses Konzeptes würde jedoch zu einer regelmäßigen Auseinandersetzung mit neuen Bedrohungsquellen und Sicherheitsproblemen zwingen und erscheint damit dennoch empfehlenswert.

2.6 Fehlende Server-Authentifizierung

In ihrer Arbeit fanden [SLK10] eine fragwürdige Einschränkung der gegenseitigen Authentifizierung der Komponenten der TI. So wird prinzipiell durch den Konnektor keine Authentifizierung der Server des Zeitdiensts durchgeführt, "da die Systeme im VPN der Telematikinfrastruktur als sicher angesehen werden" [ge06, S.60]. Tatsächlich sind die inneren Zonen der TI aufgrund ihrer verhältnismäßig großen Zentralität deutlich einfacher zu kontrollieren, als dies für die dezentralen Systeme in Zone 1 gilt. Darüber hinaus gibt es speziell bei den Zeitservern eine große Redundanz, [ge08b, S.139] so dass für einen erfolgreichen, verwertbaren Angriff die Kompromittierung eines einzigen Servers nicht ausreicht [ge08b, S.139f.]. Dies sollte allerdings nicht darüber hinwegtäuschen, dass die aufgestellte Prämisse deutlich weitgehender ist, als angemessen wäre. Des Weiteren wäre eine Authentifizierung an dieser Stelle mit keinerlei großen Nachteilen verbunden, wie erhöhter Prozesslaufzeit oder erhöhtem Datentransfervolumen, und mit nur geringem Aufwand realisierbar. Insofern ist es nicht nachzuvollziehen, warum diese These auch in den aktuellen Dokumenten der gematik aufrecht erhalten wird [ge09b, S.122]. Sinnvollerweise sollte auch hier zukünftig eine zumindest einseitige Authentifizierung des Servers durchgeführt werden.

⁴vgl. auch [Su09c]

2.7 Keine Verwendung quelloffener Software

Die gematik beteuert, dass “Security by Obscurity [...] nicht als zielführend [...] angesehen” wird [ge08d, S.80]. [HSK08] argumentieren, dass eben dieses Prinzip eingesetzt wird, indem erklärt wird, dass der Großteil der verwendeten Software einen hohen Schutzbedarf genießt, da es sich bei ihr um Firmengeheimnisse handeln würde. Etwas abgeschwächt wird dies dadurch, dass die Quellen den Mitarbeitern des BSI und der gematik zugänglich sein werden und darüber hinaus durch diese geprüft werden müssen. Dies verhindert dennoch, dass freie Sicherheitsexperten den Quellcode auf potentielle Probleme überprüfen. Diese Regelung besteht nach wie vor in den aktuellen Dokumenten der gematik. Rein rechtlich sollte es durchaus möglich sein, die Zulassung einer neuen Komponente an die Offenlegung des Quellcodes der Software zu koppeln. Eine Offenlegung brächte zwar das Problem mit sich, dass Bedrohungsquellen ohne Aufwand an Material kommen. Sie könnten daher gezielt nach Schwachstellen suchen und diese anschließend möglicherweise ausnutzen. Basierend auf dem Prinzip von Kerckhoff [Ke83] muss aber immer davon ausgegangen werden, dass das System einem ernsthaften Angreifer bis ins Detail bekannt ist. Die Vorteile der Offenlegung übertreffen aus sicherheitstechnischer Sicht damit mit großer Wahrscheinlichkeit die möglichen Nachteile [MN03].

2.8 Unzureichende Definition der Sperrlistenverwaltung

[SLK10] kritisieren, dass zwar das notwendige Vorhandensein von Sperrinformationen durch die gematik vorgeschrieben wurde, nicht jedoch näher definiert worden ist, wie diese bereitzustellen sind. Auch ist nicht klar, ob Authentifizierung zum Zugriff erfolgen muss, wo die zuständigen Server angesiedelt werden und welche Funktionalitäten sie bieten.

Hier wurde seitens der gematik in einigen Punkten nachgebessert. So ist nun klar, dass die Integrität der Sperrlisten sicher gestellt werden muss und für den Anwender jederzeit nachprüfbar sein werden [ge08c, S.77]. Ist dies nicht gewährleistet, werden diese nicht genutzt, um die Gültigkeit eines Zertifikats zu überprüfen [ge08c, S.78]. Damit wird verhindert, dass ein unbefugter Schreibzugriff auf die Sperrliste die beliebige Sperrung und Entsperrung von Zertifikaten ermöglicht.

Darüber hinaus wird nur noch in geringen Umfang mit Sperrlisten gearbeitet. Diese können zwar (“in Ausnahmefällen” [ge09a, S.145]) eingesetzt werden, üblicherweise wird aber OCSP (Online Certificate Status Protocol) benutzt, um die Gültigkeit von Zertifikaten zu überprüfen; diese Möglichkeit muss immer gegeben sein [ge09a, S.45]. Alles Weitere zur Funktionsweise der Gültigkeitsprüfung wird durch die Server-Betreiber (Trusted Service Provider, TSP) festgeschrieben.⁵ Damit können die ursprünglich aufgestellten Kritikpunkte als im Wesentlichen geklärt gelten.

⁵vgl. [ge08a, S.39f.]

2.9 Unzureichende Spezifikation des Trusted Viewers

[HSK08] sind der Meinung in der Spezifikation der vertrauenswürdigen Anzeigekomponente, dem Trusted Viewer (mittlerweile extended Trusted Viewer, xTV), eine Inkonsistenz und eine Sicherheitslücke entdeckt zu haben. Der Trusted Viewer stellt sicher, dass tatsächlich nur Inhalte signiert werden, von denen die Versicherten und Leistungserbringer glauben, sie zu signieren. In den Konnektorspezifikationen wurde nur ungenau darauf eingegangen, wie und in welcher Form der Trusted Viewer realisiert werden sollte. So konnte dieser Service als direkter Bestandteil des Konnektors oder als eigene Hardwarekomponente oder gar als Funktionalität der angeschlossenen Clients realisiert werden. Darüber hinaus musste der Konnektor eine Schnittstelle zum Trusted Viewer enthalten, auch wenn der Trusted Viewer Teil des Konnektor selbst sein sollte. Außerdem war es aus Sicherheitsicht als kritisch einzustufen, dass der Trusted Viewer keine eigene Identität erhalten sollte, also nicht durch den Konnektor oder die Primärsysteme authentifiziert werden konnte.

In diesen Punkten wurden mittlerweile durch die gematik mehrere Änderungen durchgeführt. Die Wahlfreiheit, wie der Trusted Viewer realisiert werden kann, wurde eingeschränkt⁶. Damit wird der xTV in zwei Bestandteile zerfallen: einen, welcher im Konnektor beheimatet sein wird und eine Komponente für das Primärsystem [ge09b, S.93]. Bei letzterer ist wie bisher nicht vorgeschrieben, ob dies in Form einer Softwarelösung auf dem Primärsystem durchgeführt werden soll oder in Form einer angeschlossenen Hardwarekomponente geschieht, jedoch ist immerhin die konkrete Ausgestaltung der Schnittstelle zwischen diesen beiden Komponenten definiert [ge09b, S.307].

Dies ist eine Verbesserung gegenüber dem Zustand, den [HSK08] kritisiert haben, da es somit weitestgehend möglich ist, den xTV-Dienst aus dem Praxisverwaltungssystem (PVS) heraus über eine fest definierte Schnittstelle zu nutzen. Eine Festlegung darauf, die Komponente des Primärsystems entweder als Softwarelösung oder als Hardwarelösung zu fordern, hätte jedoch verhindert, dass nun jeder Anbieter eines PVS für jeden zertifizierten Konnektor beide Möglichkeiten unterstützen muss. Dies erhöht die Komplexität und damit auch die Fehleranfälligkeit deutlich. Diese hätte damit ohne jeglichen Sicherheitsverlust des Systems reduziert werden können. Letztlich hätte dies zu weniger Problemen bei Inbetriebnahme und laufendem Betrieb geführt und wäre damit der generellen Akzeptanz der eGK zuträglich gewesen. Dennoch ist diese Präzisierung gegenüber der von [HSK08] betrachteten Version zu begrüßen. Positiv muss insbesondere erwähnt werden, dass mittlerweile auch der xTV-Komponente im Konnektor eine eigene Identität zugeordnet wird [ge09a, S.173]. Damit können Man-in-the-Middle-Angriffe und Spoofing-Attacken weitgehend ausgeschlossen werden, da dadurch alle Gegenstellen die Integrität des xTVs überprüfen können.

⁶vgl. [ge09b, S.38]

2.10 Keine kryptographische Identität der Primärsysteme

[SLK10] kritisieren, dass kein eigenes Identitätszertifikat für die mit dem Konnektor verbundenen Primärsysteme vorgesehen ist. Dies führt dazu, dass zwar die Primärsysteme den Konnektor einseitig authentifizieren können. Sie können aber nicht sicherstellen, dass kein Man-in-the-Middle-Angriff stattfinden kann. Der Konnektor kann zur Zeit nicht überprüfen, ob eine Verbindung mit einem Primärsystem direkt aufgebaut wurde oder unter Einbeziehung eines Dritten. Dieser könnte sich dabei dem Konnektor gegenüber als Primärsystem und dem Primärsystem gegenüber als Konnektor ausgeben. Daher könnten Anfragen des Primärsystems an den Konnektor verändert oder abgehört werden⁷.

Hieran hat sich auch in den aktuellen Spezifikationen nichts geändert. Dieses Problem ließe sich auch nur durch das Hinzufügen kryptographischer Identitäten für die Primärsysteme lösen. Hier wäre zu überlegen, ob dies hardwaretechnisch gelöst werden könnte. Denkbar wäre der Einsatz eines Dongles, eines Kopierschutzsteckers, der die Identität enthält und meist an den USB-Port eines Clients angesteckt wird. Da ansonsten die kryptographischen Identitäten manuell auf jedem Client eingerichtet werden müssten, wäre dies eine einfach umzusetzende Lösung, die auch ohne größeres technisches Verständnis durchgeführt werden kann. Da jedoch der Schutz vor Diebstahl eines Dongles in einer Arzt-Praxis vermutlich nicht ausreichend gewährleistet werden kann, ist dies keine wirklich praktikable Lösung.

Der größte Teil der ablaufenden Kommunikation zwischen Primärsystemen und Konnektor wird bereits mit den geheimen Schlüsseln von HBA und eGKs verschlüsselt. Daher können auch ohne kryptographische Identität der Primärsysteme zunächst nur wenige konkrete Daten abgehört werden. Gefälschte Anfragen an den Konnektor sind zwar in der Lage, das Ziel der Verfügbarkeit zu gefährden, können aber nicht die Integrität oder Authentizität des Datenaustauschs mit der TI verletzen. Eine eigene Identität der Clients ist damit wünschenswert, jedoch nur mit hohem Aufwand realisierbar.

2.11 Ungenügende Vorgaben und Richtlinien für Primärsysteme

[HSK08] beklagen, dass gerade im Hinblick auf die Primärsystemen keine Vorgaben oder zumindest Richtlinien seitens der gematik gibt. Speziell, da dort alle medizinischen Daten erstellt und zum großen Teil gespeichert werden, geht damit eigentlich ein sehr hoher Schutzbedarf einher. Derartige Vorschriften oder Richtlinien findet man auch in den aktuellen Versionen der Spezifikationen nicht. Gerade die Primärsysteme in der Zone 1 stellen die am unmittelbarsten angreifbaren Systeme dar. Zugleich besitzen die hier vertretenen Akteure die geringste Fachkompetenz im Bereich der IT-Sicherheit. Dennoch wurden bisher lediglich von Dritten Vorschläge zur Verbesserung der IT-Sicherheit erarbeitet⁸. Da jedoch Richtlinien und besonders Vorschriften von offizieller Seite eine deutlich höhere Beachtung und Umsetzung finden, sollte in diesem Bereich auch noch eine offizielle Veröffentlichung durch die gematik erfolgen.

⁷vgl. auch [Su09b] und [Su09a]

⁸vgl. z.B. [Su08a], [Ka10]

3 Ausblick

Die vorgestellten Bedenken können rechtzeitig vor der flächendeckenden Einführung der eGK in Deutschland behoben werden, bzw. wurden bereits größtenteils behoben. Bei weiteren, hier nicht näher aufgeführten, Bedenken⁹ sehen die Autoren von einer expliziten Behauptung ab.

Die gematik hat vorwiegend widerspruchssarme Konzepte zum Schutz der Sicherheitsziele entworfen. Diese Dokumente sind öffentlich einsehbar und stellen damit eine Einladung an alle interessierten Parteien dar, an der Weiterentwicklung der Konzepte teilzunehmen. Nur so kann ein bestmöglicher Schutz gegen Bedrohungsquellen angestrebt werden. Dass sich dies auch in einem gewissen Rahmen auszahlt, lässt sich am Beispiel dieser Arbeit beobachten.

Literatur

- [Bs09] BSI (2009): IT-Grundschutzkataloge - 11. Ergänzungslieferung. M 2.199 Aufrechterhaltung der Informationssicherheit. In: <https://www.bsi.bund.de/cae/servlet/contentblob/478422/publicationFile/55552/massnahmen.zip>, zugegriffen am 10. März 2010.
- [ge06] gematik (2006): Konnektorspezifikation. Teil 1 - Allgemeine Funktionen und Schnittstellen des Konnektors. Version 0.6.0. o.O., 2006.
- [ge08a] gematik (2008a): Certificate Policy. Gemeinsame Zertifizierungs-Richtlinie für Teilnehmer der gematik-TSL zur Herausgabe von X.509-ENC/AUTH/OSIG-Zertifikaten. Version 1.3.0, o.O., 2008.
- [ge08b] gematik (2008b): Übergreifendes Sicherheitskonzept der Telematikinfrastruktur. Version 2.4.0, o.O., 2008.
- [ge08c] gematik (2008c): Übergreifendes Sicherheitskonzept der Telematikinfrastruktur - Anhang B - Sicherheitsanforderungen. Version 2.4.0, o.O., 2008.
- [ge08d] gematik (2008d): Übergreifendes Sicherheitskonzept der Telematikinfrastruktur - Anhang C - Schutzbedarfsanalyse. Version 2.4.0, o.O., 2008.
- [ge09a] gematik (2009a): Gesamtarchitektur. Version 1.7.0, o.O., 2009.
- [ge09b] gematik (2009b): Konnektorspezifikation. Version 3.0.0, o.O., 2009.
- [HSK08] Huber, M.; Sunyaev, A.; Krcmar, H. (2008): Security Analysis of the Health Care Telematics Infrastructure in Germany. In: ICEIS 2008 - Proceedings of the Tenth International Conference on Enterprise Information Systems, Vol. ISAS-2, pp. 144-153. Barcelona, Spain.
- [In06] Initiative D21 (2006): Die neue Gesundheitskarte - ein Themenservice. 03/06. In: http://www.old.initiated21.de/fileadmin/files/themenservice/themenservice_3/NEU_Themenservice_03_06.pdf, zugegriffen am 22. März 2010.

⁹z.B. bei der an sich nicht schädlichen Möglichkeit, den Konnektor zum Signieren und Verschlüsseln zu missbrauchen, vgl. [Su10] oder der Frage der langfristigen Vertraulichkeit verschlüsselter medizinischer Daten, vgl. [SLK09]

- [Ka10] Kassenärztliche Bundesvereinigung (2010): Anforderungen an Hard- und Software in der Praxis. Hinweise zum Datenschutz. Ein Leitfaden für Ärzte und Psychotherapeuten. In: <http://daris.kbv.de/daris/link.asp?ID=1003760425>, Berlin 2010, zugegriffen am 02. März 2010.
- [Ke83] Kerckhoffs A. (1883): La cryptographie militaire. In: *Journal des sciences militaires*, vol. IX, S. 5-38, Januar 1883, S. 161-191, Februar 1883.
- [Kn09] Knüttel, A. (2009): Probleme und Lösungsansätze zur eGK/HBA aus der Sicht eines Testkrankenhauses und der NKG. In: *conhIT 2009 - Satellitenveranstaltung GMDS/BVMI, Workshop 2: GMDS-Projektgruppe "Einführung von eGK und HBA in Krankenhäusern"*.
- [Ma08] Maus, T. (2008): Risiken + Nebenwirkungen. Der Beipackzettel zur Gesundheitskarte. In: <http://www.medi-deutschland.de/datei.php?id=1080>, zugegriffen am 03. Februar 2010.
- [MN03] Mercuri, R.T.; Neumann, P.G.(2003): Security by Obscurity. In: *Communications of the ACM*, Vol.46, No. 11, S.160.
- [NBB04] Neeb, J.; Bunz, H.; Biltzinger, P. (2004): Erarbeitung einer Strategie zur Einführung der Gesundheitskarte. Sicherheitsanforderungen. In: Projektgruppe bit4Health, http://www.inso.tuwien.ac.at/uploads/media/b4h_sicherheitsanforderungen_v1-1.pdf, zugegriffen am 01. Februar 2010.
- [oV88] o.V. (1988): Sozialgesetzbuch (SGB) Fünftes Buch (V) - Gesetzliche Krankenversicherung -(Artikel 1 des Gesetzes v. 20. Dezember 1988, BGBl. I S. 2477). In: http://bundesrecht.juris.de/sgb_5/BJNR024820988.html, zugegriffen am 08. Februar 2010.
- [oV90] o.V. (1990): Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Artikel 1 des Gesetzes vom 14. August 2009 (BGBl. I S. 2814) geändert worden ist. In: http://www.gesetze-im-internet.de/bdsg_1990/BJNR029550990.html, zugegriffen am 18. Februar 2010.
- [Su08a] Sunyaev, A.; von Beck, J.; Jedamzik, S.; Krcmar, H. (2008): IT-Sicherheitsrichtlinien für eine sichere Arztpraxis. 1. Auflage, Shaker Verlag, Aachen 2008.
- [Su08b] Sunyaev, A.; Huber M.J.; Mauro, C.; Leimeister J.M.; Krcmar, H. (2008): Bewertung und Klassifikation von Bedrohungen im Umfeld der elektronischen Gesundheitskarte. In: *Proceedings of Informatik 2008 - Beherrschbare Systeme - dank Informatik*, Band 1, Hrsg: GI - Gesellschaft für Informatik, GI Lecture Notes in Informatics, München, S.65-70.
- [Su09a] Sunyaev, A.; Dünnebeil, S.; Mauro, C.; Leimeister, J.M.; Krcmar, H. (2009): Sicherheitsbetrachtung der Primärsysteme in der Deutschen Gesundheitstelematik. In: *Proceedings of 54. Jahrestagung der Deutschen Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie (GMDS)*. Essen, 07.-10.09.2009.
- [Su09b] Sunyaev, A.; Kaletsch, A.; Mauro, C.; Krcmar, H. (2009): Security Analysis of the German electronic Health Card's Peripheral Parts. In: *ICEIS 2009 - Proceedings of the 11th International Conference on Enterprise Information Systems*. Milan, Italy, 6-10 May 2009. Volume ISAS, pp. 19-26.
- [Su09c] Sunyaev, A.; Leimeister, J.M.; Krcmar, H. (2009): Security Analysis of the German Healthcare Telematics. In: *AMCIS 2009 - Proceedings of the 15th Americas Conference on Information Systems*. San Francisco, California, 6-9 August 2009. Paper 232.
- [Su10] Sunyaev, A.; Kaletsch, A.; Duennebeil, S.; Krcmar, H. (2010): Attack Scenarios for possible Misuse of Peripheral Parts in the German Health Information Infrastructure. In: *Proceedings of the 12th International Conference on Enterprise Information Systems (ICEIS 2010)*. Funchal, Madeira - Portugal, 8 - 12 June, 2010. Volume DISI, pp. 229-235.

- [SLK09] Sunyaev, A.; Leimeister, J.M.; Krcmar, H. (2009): Telematik im Gesundheitswesen: Sichere Autobahn mit unsicheren Auffahrten? In: Krankenhaus-IT Journal, Nr. 2/2009, S. 46-47, 2009.
- [SLK10] Sunyaev, A.; Leimeister, J.M.; Krcmar, H. (2010): Open Security Issues in German Healthcare Telematics. In: Proceedings of the Third International Conference on Health Informatics (HealthInf 2010), January 20-23, 2010, Valencia, Spain, pp. 187-194.
- [Sy07] systemform Media Card GmbH (2007): Einführung der elektronischen Gesundheitskarte (eGK) - Erste Erfahrungen aus der Praxis. In: ECM Tag Fokus Gesundheit 2007, http://www.pentadoc.de/fileadmin/_temp_/documents/ecmtag/20070612_rheingau/Einfuehrung_der_elektronischen_Gesundheitskarte_-_Erste_Erfahrungen_aus_der_Praxis.pdf, zugegriffen am 16. Juli 2010.