LDRef1 [redacted] 15. März 2005

Ablaufbeschreibung und (vorläufige) Bewertung des Use Cases „eRezept" der Gesundheitskarte Schleswig-Holstein

Basis: 1. Dok. „Implementierungsvorschlag zum Use Case `eRezept`" in Version 0.4, 02.12.2004, [redacted]

2. Auskunft von [redacted] per Email am 21.02.2005

1. Ablaufbeschreibung

Das Flensburger Modell setzt eine elektronische Gesundheitskarte voraus, auf der mit einem als sicher zertifizierten Betriebssystem eine asymmetrische (Ende-zu-Ende-)Verschlüsselung ermöglicht wird. Um alle Einsatzszenarien abzudecken, werden sowohl der Transport auf der Karte selbst als auch der über einen Server (jedoch unter Verwendung der Gesundheitskarte) umgesetzt.

Für Letzteres verwendet das Verfahren einen so genannten „netzbasierten Speicherort", der individuell eingerichtet wird und in einer normalen Email-Adresse des Karteninhabers bestehen kann. Beim Erstkontakt zwischen diesem und dem verschreibenden Leistungserbringer wird der Speicherort – der in der Karte gespeichert ist – ausgelesen und im System des Leistungserbringer abgelegt. Gibt es noch keinen Speicherort, so wird dieser bei einem Provider erzeugt. Der Erstkontakt wird darüber hinaus dazu verwendet, den öffentlichen Schlüssel der Gesundheitskarte aus dieser auszulesen und im System des Leistungserbringers zu speichern.

Der Leistungserbringer erzeugt sodann das elektronische Rezept, signiert es unter Verwendung seines Heilberufsausweises und fügt die (qualifizierte) elektronische Signatur bei. Bei der Speicherung auf der Karte erfolgt zunächst eine CVC-Authentifizierung zwischen Gesundheitskarte und Heilberufsausweis, bevor das Rezept auf die Gesundheitskarte geschrieben wird.

Bei der Übermittlung mittels Server wird das Rezept im Primärsystem des Leistungserbringers mit dem öffentlichen Schlüssel der Gesundheitskarte verschlüsselt (bzw. es erfolgt eine Hybridverschlüsselung, die aber sicherheitstechnisch identisch zu bewerten ist) und unter Verwendung einer zusätzlichen Transportverschlüsselung an den netzbasierten Speicherort versendet. Für diesen Vorgang ist – nach dem Erstkontakt – weder die Anwesenheit des Versicherten noch seiner Gesundheitskarte erforderlich.

Das Einlösen des Rezepts setzt ein so genanntes „Gesundheits-Terminal" voraus, welches in seiner Gesamtheit zertifiziert werden soll und in Bezug auf die bauliche Abschirmung einem EC-Automaten ähnelt. Das Terminal befindet sich bei einem Leistungserbringer (regelmäßig ein Apotheker). Der Einlösevorgang beginnt mit einer gegenseitigen Authentifizierung zwischen dessen Heilberufsausweis und der Gesundheitskarte. Sodann werden dem Versicherten alle für ihn gespeicherten Rezepte angezeigt.

Bei einer Speicherung auf der Karte erfolgt dies durch Auslesen, bei einer Speicherung in

seinem netzbasierten Speicherort werden die Daten von dort angefordert, unter Einsatz einer Transportverschlüsselung zum Gesundheits-Terminal verschickt, dort durch die Gesundheitskarte entschlüsselt und dem Versicherten angezeigt. Dieser wählt (z.B. mittels Touch-Screen oder Tastatur) ein oder mehrere Rezepte aus, die er einlösen möchte. Sodann wird ihm eine Liste von „berechtigten Heilberuflern" angezeigt, unter denen er einen auswählt. Das kann, muss aber nicht der Leistungserbringer sein, in dessen räumlicher Nähe er sich gerade befindet. Handelt es sich um einen anderen Leistungserbringer, ermittelt das Gesundheits-Terminal den öffentlichen Schlüssel von dessen Heilberufsausweis, verschlüsselt das Rezept damit und verschickt es. Das Rezept wird als eingelöst vermerkt und gelöscht. Der empfangende Heilberufler entschlüsselt das Rezept und gibt das Medikament ab. Dies kann auch im Versandhandel erfolgen.

2. (Vorläufige) Bewertung

Der konzeptionelle Ansatz des Flensburger Modells ist datenschutzrechtlich und ablauftechnisch positiv zu bewerten. Eine Reihe von technischen und insbesondere auch finanzierungsrelevanten Fragen bleibt aber offen.

Die vorgeschlagene Ende-zu-Ende-Verschlüsselung setzt – datenschutzrechtlich vorbildlich – die Verwendung der elektronischen Gesundheitskarte bei jedem Zugriff auf das Rezept voraus. Hierdurch wird die selbstbestimmte Entscheidung des Versicherten über die Offenbarung der Rezeptdaten ermöglicht. Dies ist vor allem deshalb wichtig, weil aus diesen Daten unmittelbar auf Gesundheitszustand und Behandlungen des Betroffenen zurückgeschlossen werden kann und es sich deshalb – im Unterschied zu den Versicherungsstammdaten – nicht „nur" um administrative Daten handelt.

Zur Aktivierung des geheimen Schlüssels der Gesundheitskarte ist nach dem Konzept keine technische Autorisierung durch den Inhaber (z.B. durch eine PIN) erforderlich. Das entspricht der gesetzlichen Regelung in § 291a Abs. 5 SGB V. Die Freischaltung ohne PIN ist datenschutzrechtlich auch akzeptabel, weil der Schutz durch den Besitz der elektronischen Gesundheitskarte dem bisherigen Schutz durch den Besitz des Rezepts entspricht und sogar dadurch verbessert wird, dass im Verlustfall ein Zugriff nur unter Verwendung eines elektronischen Heilberufsausweises möglich ist.

Die beschriebene Transportverschlüsselung sorgt – die Sicherheit der verwendeten kryptographischen Algorithmen und Parameter unterstellt – dafür, dass jeglicher Zugriff auf die Daten auf dem Transportweg zuverlässig ausgeschlossen wird. Der Versicherte muss nicht auf die Zuverlässigkeit der übermittelnden und speichernden Stellen (bei denen es sich im Vollbetrieb regelmäßig um externe Dienstleister handeln wird) vertrauen, weil seine Daten auf technischem Wege geschützt werden. Weder diese Stellen noch sonstige Beteiligte im Gesundheitswesen (Krankenversicherungen, andere Leistungserbringer) können die Daten einsehen.

Integrität und Authentizität der Rezeptdaten werden durch die qualifizierte elektronische Signatur des Leistungserbringers gewährleistet. Die nach § 291a Abs. 6 Satz 2 SGB V erforderliche Protokollierung der letzten 50 Lese- und Schreibzugriffe auf die Gesundheitskarte wird in einem zyklischen Speicher der Karte realisiert. Es ist jedoch unklar, in welcher Granularität die Zugriffe protokolliert werden.

Konzipiert – nicht jedoch umgesetzt – ist die Frage des Key Recovery bei einem Verlust der Gesundheitskarte. Die datenschutzrechtlich wünschenswerte absolute Bindung des Datenzugriffs an den Einsatz des kartenspezifischen geheimen Schlüssels führt dazu, dass bei Verlust oder Diebstahl die mit diesem Schlüssel verschlüsselten Daten unwiederbringlich

verloren sind, wenn kein Key Recovery eingesetzt wird. Der Idee nach soll der geheime Schlüssel geteilt und bei zwei organisatorisch getrennten vertrauenswürdigen Stellen aufbewahrt werden. Dies stellt eine denkbare Lösung dar. Das Problem des Key Recovery ist bei der Rezeptanwendung aber kein entscheidendes Problem, da im Verlustfall – wie bisher – ein Ersatzrezept ausgestellt werden kann. Eine Notwendigkeit entsteht erst bei komplexeren und umfänglichen Anwendungen, insbesondere bei der elektronischen Patientenakte.

In ablauftechnischer Sicht ermöglicht die Bereitstellung des doppelten Übermittlungswegs (Karte und Server) einerseits mehr Einsatzszenarien als eine alternative Lösung, andererseits stellt sie ein Backup-Verfahren (vor allem für den Ausfall eines Servers) dar. Bei einer reinen Kartenlösung wäre beispielsweise eine Rezeptbestellung per Telefon nicht möglich, die jedoch (nach dem Erstkontakt) über einen Server realisiert werden kann. Eine reine Serverlösung würde die Rezeptausstellung bei Hausbesuchen und zumindest auf absehbare Zukunft (d.h. bis zur Einrichtung eines zumindest europaweiten Gesundheitsnetzes) das Einlösen des Rezepts im Ausland unmöglich machen.

Schwachpunkt des Konzepts ist bislang die Umsetzung der Rezepteinlösung.[1] Es wird explizit davon ausgegangen, dass das "Gesundheits-Terminal" in seiner Gesamtheit eine „Black Box" ist, die komplett im Rahmen der Sicherheitszertifizierung überprüft wird. Zwar bestehen konkrete Anforderungen, etwa das Löschen temporärer Daten und Dateien im Terminal bei einem Benutzerwechsel. Die konkrete Realisierung – etwa in der Apotheke – bleibt aber völlig offen. Aus datenschutzrechtlicher Sicht wäre insbesondere zu fordern:

- Eine vollständige Abschottung von der EDV des Apothekers mit Ausnahme der CVC-Authentifizierung und dem Empfang des Rezepts, wenn der Versicherte den Apotheker, bei dem er sich befindet, als Empfänger bestimmt. Es ist unbedingt – technisch – zu verhindern, dass der Apotheker die Daten, die im Terminal (das sich wiederum in seiner Einflusssphäre befindet) im Klartext vorliegen, gegen den Willen des Patienten einsehen kann.

- Eine bauliche Gestaltung, die eine visuelle Kenntnisnahme sowohl des Apothekenpersonals also auch anderer Kunden zuverlässig ausschließt. Diese an sich harmlos klingende Anforderung könnte in der Praxis zu nahezu unüberwindlichen Problemen führen. Im Prinzip benötigt jeder Kundenplatz jeder Apotheke in Deutschland ein entsprechendes Terminal, weil im Vollbetrieb das papierne Rezept vollständig ersetzt werden soll und an jedem Kundenplatz eine Bedienung erfolgen können muss. Inwieweit dies zu platztechnischen und ablauforganisatorisch Problemen führt, ist unklar.

- Eine einfache und übersichtliche Handhabung des Systems, die auch technisch nicht versierte Versicherte nicht überfordert. Wenn dies nicht gewährleistet wird, besteht die Gefahr, dass die Einführung der Gesundheitskarte zu einer Spaltung der Gruppe der Versicherten führt: Karteninhaber, die mit dem Zugriffssystem umgehen können, würden durch die technischen Schutzmechanismen geschützt, während die informationelle Selbstbestimmung der übrigen Betroffenen durch die Notwendigkeit, fremde Hilfe in Anspruch nehmen zu müssen, gefährdet wäre.

  Sofern der Patient allerdings keine Bedenken hat, den Gesamtbestand seiner Rezeptdaten dem Apotheker gegenüber zu offenbaren, kann er auf die Nutzung des Gesundheitsterminals verzichten und dem Apotheker seine Gesundheitskarte direkt aushändigen. Aufgrund der Zugriffsrechtematrix kann der Apotheker mit der Karte

[1] Das ist nicht als Kritik an den Verfassern des Konzepts misszuverstehen, bei dessen Erstellung einige Umsetzungsprobleme bewusst ausgeklammert wurden.

des Patienten ausschließlich Rezeptdaten erschließen.

Neben diesen datenschutzrechtlichen Anforderungen erscheint die Einführung eines Terminals, der den Betroffenen „alle berechtigten Heilberufler" anzeigt, aus anderen Gründen wenig durchdacht. Im Pilotbetrieb in Flensburg werden dies regelmäßig nur wenige Apotheker oder andere Leistungserbringer sein. Im Echtbetrieb wird jedoch jeder Heilberufler, d.h. beispielsweise jeder Apotheker – und das gilt seit DocMorris europaweit – „berechtigt" sein. Das führt zu folgenden Problemen:

- Handhabbarkeit: Es ist bislang in Flensburg noch kein Modell für den Umgang mit der Datenmasse entwickelt worden. Allein in Deutschland gibt es ca. 20.000 Apotheken. Es dürfte einerseits kaum sinnvoll sein, diese alle listen- oder ordnermäßig aufzuführen, weil der Versicherte daran regelmäßig kein Interesse haben wird und die allermeisten Apotheken keinen bundesweiten Versand anbieten. Andererseits kann das auch nicht ausgeschlossen werden. Jedenfalls müssten Internet- und Versandapotheken aufgeführt werden. Auch der Umfang der Informationen muss bedacht werden (nur Namen der Apotheke? Versand- und Abrechnungsmodalitäten? Besondere Angebote?)

- Wettbewerbsrecht: Im Rahmen dieses Vermerks bleibt die Frage ausgeklammert, inwieweit Leistungserbringer dazu verpflichtet werden können, in ihren Räumen ein Terminal bereitzustellen, über das die Versicherten geschäftliche Kontakte mit Dritten anbahnen. Diese Frage bedarf aber unbedingt eingehender Prüfung. Wenn man davon ausgeht, dass die Entwicklung im Gesundheitswesen hin zu mehr Wettbewerb geht und mehr und mehr Tätigkeiten der Apotheken zu Dienstleistungen werden, für die der Versicherte selbst aufkommen muss, dürfte es zumindest im nicht-preisgebundenen Bereich überaus zweifelhaft sein, ob ein Terminal mit weitreichenden Zugangsmöglichkeiten zu Konkurrenten verpflichtend zulässig wäre.

- Finanzierung: Der Aspekt der Finanzierung hängt eng mit dem Wettbewerb zusammen. Eine Überwälzung der Kosten für die Terminals auf die Apotheker mag solange noch vertretbar sein, wie die nachfolgenden Geschäfte mit diesen abgeschlossen werden (auch andere Leistungserbringer werden ihre EDV im Zuge der Einführung der Gesundheitskarte modernisieren müssen). Wenn sich der Versicherte am Terminal jedoch – beispielsweise aus Kostengründen – für die Beauftragung einer Versandapotheke entscheidet, so muss ein Geschäftsmodell entwickelt werden, das die nicht ortsgebundenen Anbieter angemessen an den Anschaffungs- und laufenden Kosten der Terminals beteiligt.

Es ist verständlich, dass diese weitreichenden Probleme beim Flensburger Modell ausgeklammert wurden, weil sie erst bei einer Projektgröße auftreten, die über den bisherigen Piloten hinausgeht. Es bestehen selbstverständlich auch keine Einwände dagegen, den technischen Ablauf des Rezepts als Modul für die Gesamtarchitektur zu erproben und weitere Aspekte, die ohnehin mehr die Gesamtarchitektur betreffen, zunächst auszublenden. Es ist aber zu betonen, dass die angesprochenen offenen Fragen beim Abruf des Rezepts nicht lediglich wirtschaftliche und wettbewerbsrechtliche, also den Versicherten nicht direkt berührende, Probleme aufwerfen, sondern ihn sowohl in seiner informationellen Selbstbestimmung (Abruf der Rezeptdaten) als auch seiner wirtschaftlichen Vertragsfreiheit (Auswahl eines Leistungserbringers) unmittelbar betreffen.