EUROPÄISCHE UNION
Investition in unsere Zukunft
Europäischer Fonds
für regionale Entwicklung

Die Landesregierung
Nordrhein-Westfalen

eGesundheit.nrw

Whitepaper – Sicherheitsaspekte der einrichtungsübergreifenden Elektronischen Patientenakte

Projekt eBPG – Unterarbeitspaket UAP01-08 (Datenschutz- und Sicherheitsaspekte der EPA)

RUHR
UNIVERSITÄT
BOCHUM

RUB

System
Security Lab

Version 1.1

Autoren:
Thomas Hupperich, Lennart Köster, Christoph Kowalski, Hiva Mahmoodi
(Ruhr-Universität Bochum)
Ahmad-Reza Sadeghi
(Ruhr-Universität Bochum / TU-Darmstadt / Fraunhofer SIT)
Marcel Winandy
(Ruhr-Universität Bochum)

Bochum, 6. Dezember 2013 (aktualisierte Version)

Forschungsgruppe Systemsicherheit (Prof. Dr.-Ing. Ahmad-Reza Sadeghi)
Horst Görtz Institut für IT-Sicherheit
Ruhr-Universität Bochum
Universitätsstr. 150
44780 Bochum
`http://www.trust.rub.de`

Inhaltsverzeichnis

1 Einführung **4**

2 Grundlagen **5**
2.1 Gesundheitswesen 5
2.2 Bedrohungen 6
2.3 Sicherheit 7
2.4 Schwerpunkte 9

3 EPA-Architektur **10**
3.1 Ziele und Überblick 10
3.2 Arztgeführte eEPA 10
3.3 Ablauf der Verschlüsselung 11
3.4 Kernfunktionen 11
Langzeitverschlüsselung 12
Autorisierter Zugriff 12
Transportsicherheit 12
Protokollierung 12
Zugriffsberechtigung 12
Abläufe im Lebenszyklus des Systems 12

4 Anforderungen **13**

5 Arbeitsbereiche **15**
5.1 Schlüsselverwaltung 15
5.2 Datenhaltung, Datenübertragung und Vertraulichkeit 16
5.3 Autorisierungsgeheimnis 17
5.4 PKI 18
5.5 Metadaten 18
5.6 Bedrohungen 19

6 Ausblick **19**

1 Einführung

Die elektronische Speicherung und Verwaltung von persönlichen medizinischen Daten ist ein sehr sensibles Thema, da es um hochgradig sensitive personenbezogenen Informationen geht. Durch den Trend zur integrierten Versorgung im Gesundheitswesens, bei der verschiedene Leistungserbringer bei der Behandlung von Patienten zusammenarbeiten, wird auch der Datenaustausch zwischen den Leistungserbringern immer wichtiger. Diesem Trend geschuldet ist die Entwicklung von einrichtungsübergreifenden Elektronischen Patientenakten (eEPA), welche nicht mehr nur die, bei einer Organisation angefallenen, medizinischen Daten eines Patienten enthält, sondern auch die Daten anderer, ebenfalls an der Behandlung beteiligter Organisationen. Da nicht zu erwarten ist, dass jede Organisation ihre eigene IT-Infrastruktur für EPA-Systeme betreiben möchte, ist anzunehmen, dass früher oder später ausgelagerte oder zentrale Informationssysteme zum Einsatz kommen, die in Händen Dritter liegen. Was es auf der einen Seite den teilnehmenden Leistungserbringern einfacher ermöglicht, ohne großen Aufwand an einer eEPA teilzunehmen, verursacht auf der anderen Seite Fragen nach dem Datenschutz und der Kontrolle über die Daten.

Da medizinische Daten auf diese Weise die Primärsysteme von Arztpraxen und Krankenhäusern verlassen können, entstehen besondere Schutzbedarfe, welche durch die geltende Rechtslage untermauert werden. Zum Schutz der Daten müssen diese während der Übertragung besonders gesichert werden um unbefugten Dritten keinen Zugriff zu ermöglichen. Ebenso ist der Schutz der Daten während der Speicherung beim eEPA-Betreiber notwendig, da dieser nicht im Behandlungsvertrag zwischen Patient und Leistungserbringer eingeschlossen ist und entsprechend zu keiner Zeit und unter keinen Umständen Zugriff auf die Daten des Patienten erhalten darf.

Die Verwendung einer Zugriffskontrolle zum Schutz der Daten schützt diese nur gegenüber externen Zugriffen, nicht aber gegenüber dem eEPA-Betreiber selbst. Daher ist diese Sicherheitsmaßnahme zum Schutz der Daten der Patienten alleine unzureichend. Pseudonymisierung der zu schützenden Daten stellt ebenfalls nur eine unbefriedigende Lösung dar, da bereits Analysen pseudonymisierter, statistischer Datenbanken gezeigt haben, dass dieses Verfahren nicht als sicher erachtet werden kann. Die Daten der Patienten sind daher vor ihrer Speicherung in der eEPA, also vor dem verlassen des Systems der Leistungserbringers, zu verschlüsseln. Zudem muss diese Verschlüsselung unter der Kontrolle des Patienten liegen, da sämtliche Sicherheitsmaßnahmen innerhalb der eEPA-Infrastruktur, die von Dritten kontrolliert werden, im Zweifelsfall als kompromittiert anzusehen sind.

Ausgehend vom Szenario der Verschlüsselung von Patientendaten ergeben sich jedoch einige Probleme. Zum einen muss der Patient in der Lage sein, Zugriff auf seine Daten zu gewähren, zum anderen darf nur er allein in der Lage sein dies zu ermöglichen. Besonders muss hier an die Gruppe chronisch kranker und alter Menschen gedacht werden, welche möglicherweise nur eingeschränkt in der Lage sind ihre Umgebung wahrzunehmen und mit dieser zu interagieren. An das Verschlüsselungs- und Autorisierungsverfahren sind deshalb hohe Ansprüche hinsichtlich der Praktikabilität der Verfahren zu stellen. Letztlich muss allerdings auch der Arzt alleinig in der Lage sein nach Autorisierung durch den Patienten dessen eEPA zu verwalten, da nur er das nötige Fachwissen besitzt um informierte Entscheidungen zu treffen.

Ausgehend von den Anforderungen und den sich daraus ergebenden Problemen ist es das Ziel, die angesprochenen Probleme unter Berücksichtigung von Praktikabilität zu lösen und im Rahmen dieses Vorgehens etwaige, weitere auftretende Probleme der Lösungen zu analysieren und zu beseitigen. Insbesondere die Langzeitsicherheit der Daten muss dabei gewährleistet werden. Im Rahmen des Projektes *eBusiness Plattform Gesundheit (eBPG)* beschäftigt sich das Unterarbeitspaket UAP01-08 genau mit diesen Fragestellungen, welche in diesem Whitepaper übersichtsweise erläutert werden.

2 Grundlagen

Ausgangspunkt unserer Betrachtung ist die geplante Telematik-Infrastruktur des Gesundheitswesens in Deutschland. Dieser Abschnitt gibt eine Übersicht der Strukturen dieser Infrastruktur und einen Einblick in die grundlegenden Begriffe der Kryptographie.

2.1 Gesundheitswesen

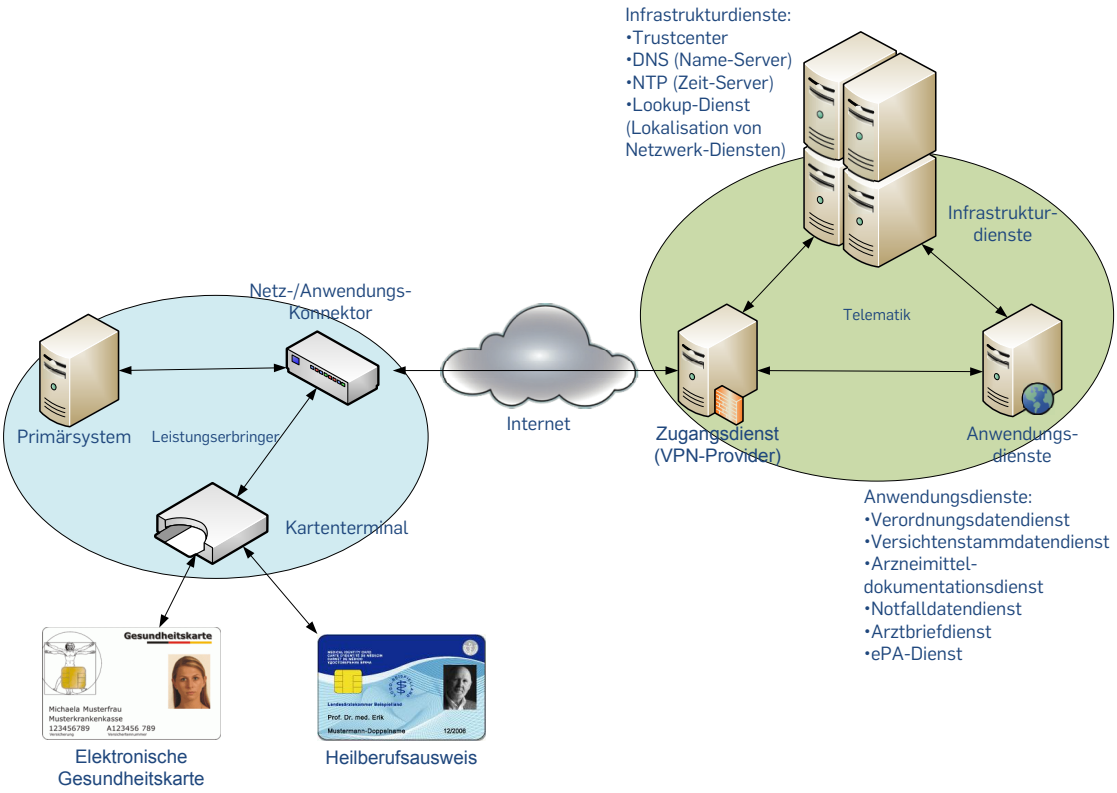

Abbildung 1: Telematik-Intrastruktur im Gesundheitswesen

Die Grundstrukturen für den Datenaustausch zwischen Leistungserbringern bilden die jeweiligen Primärsysteme und das Internet. Im Falle von Krankenhäusern sind die Pri-

märsysteme Krankenhausinformationssysteme, in Arztpraxen Patientenverwaltungssysteme. Die jeweiligen Systeme dienen zur Speicherung von medizinischen Daten welche für die Behandlung von Patienten nötig sind oder während dieser anfallen. Als Akteure lassen sich sowohl der Patient als auch der Leistungserbringer identifizieren. Leistungserbringer sind Personen welche Leistungen für die Krankenversicherten erbringen, beispielsweise Ärzte. Ausgehend von immer komplexeren Behandlungsfällen und der damit verbundenen Nachsorge kommen immer mehr Patienten in den Kontakt mit mehreren Leistungserbringern während nur eines Krankheitsfalles. Aus diesem Szenario ergibt sich das Erfordernis nach vermehrtem Datenaustausch zwischen den Leistungserbringern. Da die aktuelle Generation von Primärsystemen und damit verbundenen Patientenakten nicht in der Lage ist, einrichtungsübergreifenden Datenaustausch hinreichend zu ermöglichen geht der Trend zu einer neuen Generation von einrichtungsübergreifenden Elektronischen Patientenakten. Zudem bieten immer mehr Unternehmen sogenannte Cloud-Services an, welche die Speicherung von Daten bei dritten Anbietern ermöglichen, so dass Kunden auf eine eigene Datenhaltung verzichten können. Es bietet sich daher für Leistungserbringer an, die Datenhaltung für die neue Generation von EPAs an Dritte auszulagern. Entscheidend für ein solches Vorgehen ist dabei die Sicherheit der Daten beim Anbieter des Cloud-Services.

2.2 Bedrohungen

Aus der Struktur der Telematik-Infrastruktur ergeben sich verschiedene Punkte für Angriffe, dargestellt in Abbildung 2.

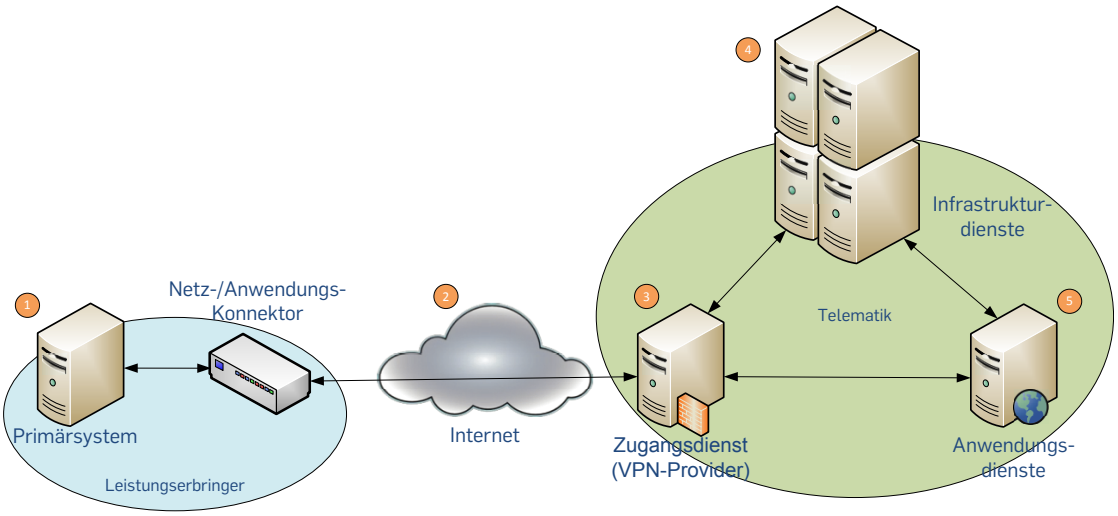

Abbildung 2: Bedrohungen der Telematik-Intrastruktur

1. Die Umgebung des Leistungserbringers ist einer der Angriffspunkte um unberechtigt Daten zu erlangen. Neben Social Engineering sind hier besonders Malware-Angriffe zu erwarten.

2. Das Internet bietet zahlreiche Angriffsmöglichkeiten. Neben dem Abhören der Kommunikation kann sich ein Angreifer als ein Teil der Telematik ausgeben und so vertrauliche Daten erlangen.

3. Durch die Kompromittierung der Zugangsdienste können Dritte die Kommunikation mitlesen, Zugang zu den Diensten der Telematik erhalten und diese angreifen.

4. Durch die Kompromittierung der Infrastrukturdienste können Dritte wertvolle Daten erlangen, die Kommunikation über ihre eigenen Server leiten und die stattfindende Kommunikation mitlesen. Zudem besteht die Möglichkeit der Denial-of-Service-Angriffe (DoS), bei denen an den Zugangspunkten der Infrastruktur so viel Last erzeugt wird, dass diese zusammenbrechen und die geschützten Dienste nicht mehr erreichbar sind.

5. Dritte könnten durch Angriffe auf die Anwendungsdienste in den Besitz medizinischer Daten gelangen. Zudem besteht die Gefahr dass Insider Daten entwenden oder Teile der Infrastruktur durch Diebe gestohlen werden, was wiederum in einer weiteren Möglichkeit des Datenverlustes resultiert.

Ausgehend von der Bedrohungslage ist besonders die Bedrohung durch Insider nicht zu unterschätzen. Sollten die zu etablierenden Sicherheitsmaßnahmen lediglich auf der Zugriffsbeschränkung durch eine Zugriffskontrolle auf Applikationsebene beruhen, können Insider diese einfach durch einen direkten Zugriff auf die Speicher des EPA-Servers umgehen. Somit wäre Insidern der Zugriff auf die im Klartext vorliegenden Daten der Patienten möglich.

2.3 Sicherheit

Grundsätzlich wichtig für die Sicherheit der medizinischen Informationen sind kryptographische Schlüssel, die Verschlüsselung von Daten mittels dieser Schlüssel sowie elektronische Signaturen und Zertifikate.

Kryptographische Schlüssel dienen dazu Informationen zu verschlüsseln und diese so vor dem Zugriff Unbefugter zu schützen. Es gibt zwei grundlegende Formen von Schlüsseln, symmetrische und asymmetrische. Ein symmetrischer Schlüssel wird sowohl zum verals auch entschlüsseln von Dokumenten genutzt und ist auch für große Datenmengen effizient. Asymmetrische Schlüsselpaare bestehen aus einem öffentlichen und einem privaten Schlüssel. Ein mit einem öffentlichen Schlüssel verschlüsseltes Dokument kann nur mit dem entsprechenden privaten Schlüssel des Schlüsselpaars entschlüsselt werden. Die Verschlüsselungsvorgänge bei asymmetrischen Schlüsseln sind allerdings rechenintensiv und daher langsam, sie eignen sich nicht um große Datenmengen effizient zu verschlüsseln.

Elektronische Signaturen bestätigen die Authentizität eines signierten Dokumentes, da Signaturen nur mit dem jeweiligen privaten Schlüssel eines Signaturschlüssels erstellt werden können, welcher sich ausschließlich im Besitz des Signierenden befindet.

Zertifikate wiederum sind signierte Daten welche bestimmte Eigenschaften beschreiben und durch die Signatur Authentizität und Integrität vermitteln. Grundlage hierfür ist ein

entsprechendes Netzwerk von Vertrauen, bei dem der das Zertifikate ausstellenden Stelle grundlegendes Vertrauen entgegengebracht wird.

Um die im Klartext vorliegenden Daten der Patienten zu schützen gibt es die Möglichkeit diese zu pseudonymisieren und den Besitzer der Daten hierdurch unkenntlich zu machen. Pseudonymisierung ist ein Verfahren bei dem identifizierende Merkmale eines Patienten ersetzt oder entfernt werden um dessen Identität zu verschleiern. Durch dieses Verfahren soll es unmöglich gemacht werden Patienten anhand ihrer, in Klarform vorliegenden, Daten identifizieren zu können.

Eine naive Anwendung der Pseudonymisierung hat jedoch Schwachstellen: z.B. ist die Auflösung der Pseudonymisierung bereits unter Zuhilfenahme der Merkmale Geburtstag, Geschlecht und Postleitzahl möglich. Neuere Pseudonymisierungsverfahren sind gegen diese Art Angriffe resistent, es ist jedoch unbewiesen ob verbleibende, vermeintlich unkritische Identifikationsmerkmale nicht doch eine De-Pseudonymisierung ermöglichen.

Es zeigt sicher daher dass die Beschränkung von Zugriff oder die Pseudonymisierung von Daten keinen ausreichenden Schutz bieten und die Daten zu verschlüsseln sind um ihre Sicherheit zu gewährleisten. Es bedarf hierbei besonderer Abwägungen hinsichtlich des zu verwendenden Verschlüsselungsverfahrens mit denen die Daten auf dem EPA-Server geschützt werden sollen.

Hier sind insbesondere Verfahren unzureichend, welche die Verschlüsselung der medizinischen Daten auf dem EPA-Server selbst oder gar nur eine Transportverschlüsselung der Daten vorsehen. Dokumente werden hierbei zwar bei der Übertragung zum Server durch eine Verschlüsselung geschützt, erreichen den EPA-Server jedoch letzten Endes wieder im Klartext. Erst auf dem Server geschieht eine Verschlüsselung des Dokuments unter einem Langzeitschlüssel, wodurch keine Ende-zu-Ende-Verschlüsselung vorliegt. Der EPA-Server ist somit zu jeder Zeit in der Lage, jegliche Dokumente ohne das Zutun des Patienten entschlüsseln zu können. Dies ist insbesondere kritisch, wenn der Betreiber den Standort des EPA-Servers verlagert (z.B. ins Ausland) oder wenn unbefugte Personen Zugang zum Server gelangen (dies schließt auch Administratoren ein).

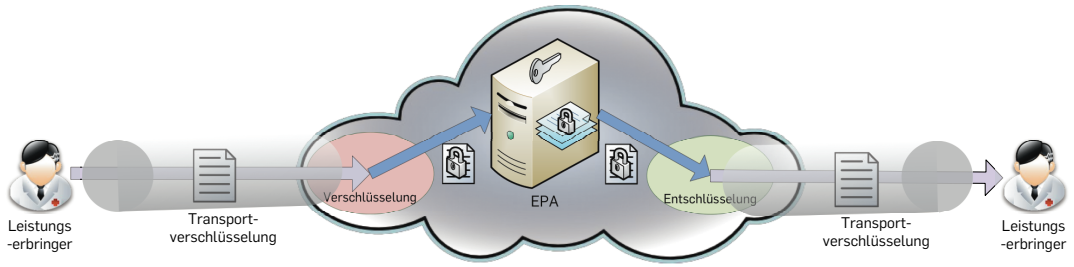

Abbildung 3: Zentrale Ver- und Entschlüsselung beim EPA-Provider

2.4 Schwerpunkte

In einem speziellen Unterarbeitspaket des Projektes *eBusiness Plattform Gesundheit (eBPG)* beschäftigen sich Forscher der Ruhr-Universität Bochum mit der Sicherheit der gespeicherten medizinischen Daten von Patienten in einrichtungsübergreifenden Elektronischen Patientenakten. Hier gilt es, dass nicht nur beim Transfer der Daten von einem System zum anderen die Vertraulichkeit und der Datenschutz personenbezogener medizinischer Daten gewährleistet werden, sondern auch bei deren Speicherung. Dieser Schutz soll durch geeignete kryptographische Verfahren umgesetzt werden. Eine Besonderheit dabei ist, dass im gesamten Behandlungsverlauf (und damit verbundenen Datenverarbeitungsprozessen) die Kontrolle über die Verschlüsselung einzig beim Patienten liegt, und nicht etwa bei Systemkomponenten, die ggf. unter Kontrolle Dritter (z.B. allgemeine IT-Provider) liegen.

Abbildung 4 stellt die Schwerpunkte der Betrachtungen blau dar, orange ausgeführt sind grundsätzliche Sicherheitstechniken, die zum Einsatz kommen werden, die aber nicht Schwerpunkt des Unterarbeitspaketes sind.

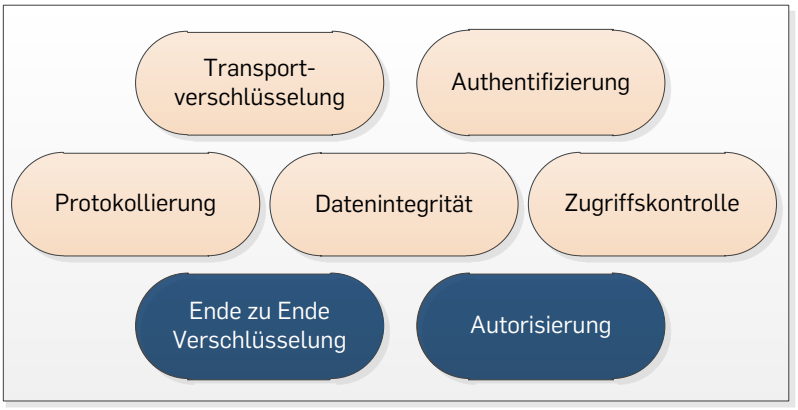

Abbildung 4: Schwerpunkte der Betrachtungen

Die Hauptschwerpunkte sind:

- **Ende-zu-Ende Verschlüsselung**: Dies bedeutet, dass medizinische Daten eines Patienten von einem Ende (Leistungserbringer) zum anderen Ende (anderer Leistungserbringer) ohne Unterbrechung durchverschlüsselt werden. Weder bei der Übertragung noch bei der (zwischenzeitlichen) Speicherung auf Infrastrukturen Dritter werden die Daten unverschlüsselt verarbeitet.
- **Autorisierung**: Hiermit ist die grundlegende Autorisierung des Datenzugriffs durch den Patienten gemeint. Das heißt, der Patient ermöglicht durch technische Vorgänge eine explizite Einverständniserklärung, dass (a) ein Leistungserbringer auf seine Daten zugreifen darf und dass (b) seine Daten an weitere Leistungserbringer übertragen werden dürfen. Hiermit sind jedoch nicht feingranulare Zugriffsrechte auf Do-

kumente z.B. innerhalb einer Organisation gemeint. Letzteres fällt unter den Punkt Zugriffskontrolle und liegt außerhalb des Fokus des Unterarbeitspaketes.

Nicht betrachtet werden dagegen der Schutz der Verfügbarkeit (z.B. gegen Denial-of-Service Angriffe) sowie der Schutz der Infrastruktur- und Zugangsdienste an sich. Dies liegt außerhalb des Fokus des Unterarbeitspakets. Ebenso wird die Sicherheit der Primärsysteme (z.B. Client-Rechner beim Arzt) in diesem Projekt als gegeben angenommen.[1]

3 EPA-Architektur

3.1 Ziele und Überblick

Durch die Entwicklung einer praktikablen und einrichtungsübergreifenden EPA-Architektur sollen die Sicherheit des Systems und die Vertraulichkeit der Daten der Patienten im System gewährleistet werden. Das darf aber die Verwendbarkeit des Systems für die Benutzer auf keinen Fall gefährden. Die Leistungserbringer und die Patienten sollen nichts vom Verfahren mitbekommen, das zur Sicherstellung der Architektur und Bewahrung der Vertraulichkeit der Patienten durchgeführt wird. Die Fehlertoleranz muss im System gegeben sein. Alle Betrachtungen gehen dabei von einer generischen EPA-Architektur aus, in die sich das System einfügen lässt. Entsprechend sind die zu beachtenden Vorgaben zur Umsetzung dieses Systems gering, um keine zu großen Anpassungen zu erfordern.

Das Ziel dieses Systems ist es, die Patientendaten überall verschlüsselt zu halten und damit Ende-zu-Ende Verschlüsselung umzusetzen. Das umfasst sowohl die Speicherung als auch die Übertragung der EPA des Patienten. Die Verschlüsselung und Entschlüsselung erfolgen ausschließlich durch die explizite und aktive Erlaubnis des Patienten.

3.2 Arztgeführte eEPA

Die Daten der eEPA sollen durch die Ärzte des Patienten verwaltet werden, da nur diese das nötige medizinische Fachwissen besitzen um entscheiden zu können, welche Informationen andere Ärzte für ihre behandlungsrelevanten Entscheidungen benötigen werden. Sollte beispielsweise ein Patient selbstständig entscheiden bestimmte, für eine Diagnose relevante, Dokumente einem Leistungserbringer vorzuenthalten kann dies zu einer falschen Diagnose führen. Da dies haftungsrechtlich äußerst problematisch ist, soll der Patient seine Rechte wie das Löschen und Sperren von Dokumenten nur über einen sogenannten Aktenmoderator wahrnehmen können. Ein Aktenmoderator ist ein Leistungserbringer, welcher das besondere Vertrauen des Patienten genießt und durch diesen bestimmt wurde. Der Aktenmoderator setzt auch die Zugriffsberechtigungen für die Akte eines Patienten.

[1] Die genauere Betrachtung der Sicherheit von Endsystemen ist Bestandteil eines anderen Projektes. Siehe dazu auch: `http://www.rubtrust-meditrust.de`

3.3 Ablauf der Verschlüsselung

Abbildung 5 beschreibt den Ablauf der Ver- und Entschlüsselung sowie den Ablauf der für beiden Vorgänge benötigten Autorisierung. Die Autorisierung erfolgt dabei über das Aushändigen eines Autorisierungsgeheimnisses durch den Patienten an den Leistungserbringer. Die Autorisierung soll dabei beispielsweise über die dargestellten Medien mögich sein, beispielsweise Fax, Telefon, Email oder SmartCard. Nach Erhalt des Autorisierungsgeheimnisses gibt der Leistungserbringer dieses in seinen Computer ein und verschlüsselt das zu verschlüsselnde Dokument unter Zuhilfenahme des Autorisierungsgeheimnisses derart, dass die Entschlüsselung nur mithilfe eines weiteren Autorisierungsgeheimnis des Patienten möglich ist. Anschließend stellt der Leistungserbringer das verschlüsselte Dokument über einen sicheren Kanal, und nach vorausgegangener Berechtigungsprüfung, in die EPA des Patienten ein.

Will der Patient es einem anderen Leistungserbringer ermöglichen dieses Dokument abzurufen so händigt er dem Leistungserbringer ein neues Autorisierungsgeheimnis aus. Der Leistungserbringer weist seine Berechtigung am EPA-Server nach und erhält daraufhin das verschlüsselte Dokument. Er entschlüsselt abschließend das Dokument durch die Informationen des Autorisierungsgeheimnisses und kann das Dokument nun einsehen.

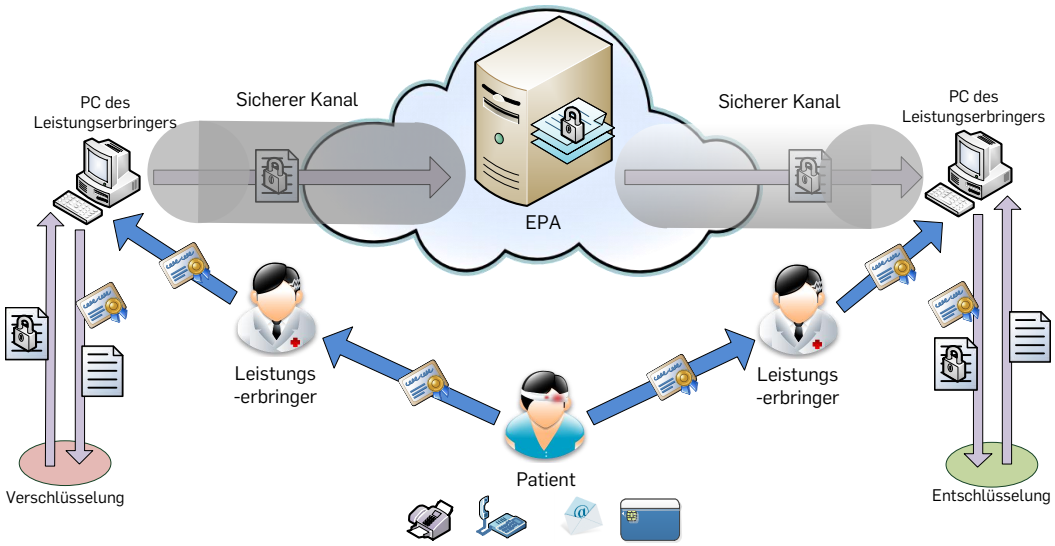

Abbildung 5: Ablauf des Autorierungsvorgangs und der Ver- sowie Entschlüsselung

3.4 Kernfunktionen

Dieser Abschnitt beschreibt die wichtigsten Funktionen des zu entwickelnden Systems: Langzeitverschlüsselung, Autorisierter Zugriff, Transportsicherheit, Protokollierung, Zugriffsberechtigung, und die Abläufe im Lebenszyklus des Systems.

Langzeitverschlüsselung

Aufgrund der langen Aufbewahrungsfristen der medizinischen Dokumente müssen die zu verwendenden Schlüssel eine entsprechende Sicherheit gewähren und das zu verwendende Verschlüsselungsverfahren muss sich einfach austauschen lassen. Daher bietet die Sicherheitsarchitektur die Möglichkeit der Umschlüsselung und der doppelten Verschlüsselung, sollte das gewählte Verfahren gebrochen werden. Die jeweilige Länge des verwendeten Schlüssels lässt sich aufgrund der Austauschbarkeit des gesamten Schlüsselverfahrens den Bedürfnissen entsprechend anpassen.

Autorisierter Zugriff

Jeder Zugriff von jedem Akteur des Systems muss autorisiert werden. Die Leistungserbringer benötigen eine aktive Einwilligung des Patienten bei jeglicher Art des Zugriffs auf die EPA des Patienten. Es gibt keine Partei in diesem System, die ohne Autorisierung den Inhalt einer EPA einsehen kann. Jeder Akteur verfügt über ein sogenanntes Autorisierungsgeheimnis, welches er bei Bedarf zur Verfügung stellt, um den Akt des Zugriffes zu autorisieren. Die Autorisierung gilt ausschließlich für den Zugriff innerhalb eines bestimmten Zeitraums. Hierfür soll es Mechanismen geben, welche die Wiederverwendung eines Autorisierungsgeheimnisses bzw. zeitlich unbegrenzte Autorisierungen verhindern. Außerdem sollen Leistungserbringer innerhalb eines durch den Autorisierungsmechanismus bestimmten Zeitfensters auf die EPA eines Patienten zugreifen können, ohne bei jedem Zugriff erneut autorisiert werden zu müssen.

Transportsicherheit

Die Übertragung aller Daten muss deren Vertraulichkeit gewährleisten. Daher werden Daten immer nur verschlüsselt übertragen.

Protokollierung

Alle sicherheitskritischen Anfragen, Zugriffe und Aktivitäten während des gesamten Systemablaufs müssen protokolliert werden.

Zugriffsberechtigung

Die Patientenakten müssen durch Definition der Zugriffsrechte vor unberechtigtem Zugriff geschützt werden. Verschlüsselung alleine reicht nicht aus. Ein Leistungserbringer kann erst nach der Überprüfung seiner Zugriffsberechtigungen auf eine verschlüsselte eEPA zugreifen.

Abläufe im Lebenszyklus des Systems

Das sind die Kernfunktionen, die während des Lebenszykluses des Systems auftreten. Die Kernfunktionen sind in vier Kategorien zu betrachten:

- *Initialisierung*: Vertragsschluss, Aktivierung der Benutzerkonten, Initialisierung und Konfigurierung der Teilkomponenten.
- *Betrieb*: Die wichtigsten Systemfunktionen fallen in diese Kategorie. Hierzu sind u.a. folgende Funktionen aufzuzählen: EPA lesen/schreiben/ändern, Einsichtnahme in die EPA, Festlegung von Zugriffsberechtigungen, Erstellung neuer Autorisierungsgeheimnisse, usw.
- *Störungsbehebung*: Es soll Mechanismen geben, durch die Störungen behoben werden können, welche während des Betriebes auftreten. Verlust des Autorisierungsgeheimnises, Ausfall der Teilkomponenten, Sperrung des Zugriffs im Notfall und Einwilligungsunfähigkeit/Tod des Patienten sind einige Störungsbeispiele.
- *Terminierung*: Es muss für jeden Teilnehmer die Möglichkeit bestehen, aus dem System auszuscheiden. Die entsprechenden Mechanismen zur Terminierung sind als ein bedeutungsvoller Teil des Systems zu berücksichtigen.

4 Anforderungen

Das zu entwickelnde Sicherheitskonzept soll sich in die Telematik-Infrastruktur des Gesundheitswesens einfügen. An das zu entwickelnde Sicherheitskonzept der eEPA stellen sich hinsichtlich Funktionalität und aufgrund der notwendigen Beachtung der Rahmenbedingungen bestimmte Anforderungen. Besonders im Vordergrund steht hierbei die Praktikabilität aller zu entwickelnder Verfahren. Zentraler Punkt ist dabei ein, alleinig dem Patienten zur Verfügung stehendes, Autorisierungsgeheimnis, mit welchem er den Zugriff auf seine eEPA ermöglichen kann. Der Zugriff soll dabei nur Zeit begrenzt erfolgen um einen behandlungsbezogenen Abruf von Informationen zu gewährleisten und eine pauschale, nicht mehr rückgängig machbare Autorisierung zu vermeiden. Das Autorisierungsgeheimnis dient nicht nur zur Autorisierung, es muss auch die Adressierung der EPA des Patienten gewährleisten und Teil des Ver-/Entschlüsselungsprozesses von EPA-Daten sein.

Das Autorisierungsgeheimnis muss zudem neu generiert werden können, da es an die Leistungserbringer übergeben wird und daher nur einmal zu einem Zugriff autorisieren soll. Es soll also alle Informationen enthalten, die für den Zugriff auf eine eEPA benötigt werden, und diesen Zugriff gleichzeitig auch autorisieren. Zudem soll die Autorisierung zeit- und ortsunabhängig erteilt werden können, da dies durch die mögliche Abwesenheit des Patienten während der Dokumentenerstellung und des damit verbundenen Einbringens in die eEPA bedingt ist.

Die Autorisierung muss auf verschiedenen Wegen erfolgen können. Beispiele sind fernmündliche Wege (Telefon), externe Speichermedien, oder einfach ausgedruckt auf Papier. Dies bedingt in allen Fällen eine Menschenlesbarkeit und eine nicht zu große Länge des Geheimnisses selbst. Eine Darstellung als Barcode sollte ebenfalls möglich sein, um die Eingabe in ein IT-System zu vereinfachen. Die Skalierbarkeit der Lösung über verschiedene technische Umsetzungen und Medien hinweg ist eine zentrale Anforderungen an die Verwenderbarkeit der zu entwickelnden Lösung. Verfahren welche an ein Medium gebunden

sind und sich nur schwer oder etwa gar nicht auf anderen Medien einsetzen lassen sind möglicherweise nicht mehr einsetzbar wenn sich die Rahmenbedingungen und damit die Anforderungen an das Verfahren ändern. Die Forderung der Skalierbarkeit ist daher neben der Sicherstellung der Verwendbarkeit auch als Anforderung an die Zukunftssicherheit des Verfahrens zu betrachten.

Ziel dieser Vorgaben ist ein einfacher Umgang mit dem Autorisierungsgeheimnis, um auch älteren und behinderten Menschen die Nutzung zu ermöglichen. Diese Personen sind neben chronisch Kranken die Hauptzielgruppe einer EPA, da sie konstante Betreuung benötigen, entsprechend oft bei Leistungserbringern vorstellig werden und daher auch am meisten von einem Überblick aller behandlungsrelevanter Informationen einer EPA profitieren.

Neben den funktionalen Anforderungen an das Autorisierungsgeheimnis spielen die Sicherheitsanforderungen eine gewichtige Rolle. Da die Daten der Patienten verschlüsselt gespeichert werden sollen, muss das zu wählende Verschlüsselungsverfahren aufgrund der gesetzlich festgelegten Dokumentationsfristen, beispielsweise 30 Jahre im Falle von Aufzeichnungen von Röntgenbehandlungen, eine hohe Langzeitsicherheit bieten und einfach austauschbar sein, falls das gewählte Verfahren als nicht mehr sicher angesehen wird. Verstärkt wird diese Anforderung zudem durch die Tatsache, dass medizinische Daten auch generationsübergreifende Informationen (z.B. Erbkrankheiten) liefern und somit auch nachfolgende Generationen die Vertraulichkeit der Daten gewährleistet werden muss.

Es muss für das zu verwendende Verschlüsselungsverfahren ein Key-Recovery-Verfahren geben mit dem ein, aufgrund der langen Laufzeit der EPA, zu rechnender Schlüsselverlust abgefangen werden kann. Die Verschlüsselung muss dabei auch ungerichtet erfolgen, d.h. dass der Empfänger des zu verschlüsselnden Dokumentes im Voraus nicht bekannt ist und dies entsprechend keinen Einfluss auf die Verschlüsselung haben darf. Die Verschlüsselung von Informationen muss auch auf Client-Seite erfolgen, da sie müßig wäre, wenn der Server das unverschlüsselte Dokument erhalten und dieses erst bei Empfang verschlüsseln würde.

Als zusätzlicher Schutzmechanismus neben der Verschlüsselung der EPA-Daten müssen die verschlüsselten Informationen durch eine Zugriffskontrolle geschützt werden. Diese Zugriffskontrolle muss anhand von Rollen- und Identitätsinformationen entscheiden können auf welche Informationen ein Leistungserbringer zugreifen kann. Dies bedingt im gleichen Schritt eine Authentifizierung aller Teilnehmer und eine Protokollierung ihrer Zugriffsversuche um schadhaftes Verhalten erkennen zu können.

Die Authentifizierung bei allen Teilsystemen muss dabei automatisch erfolgen um zu viele Benutzereingaben zu vermeiden. Geeignete Single-Sign-On Verfahren sollten daher zum Einsatz kommen. Um die Authentizität und Integrität aller in der EPA gespeicherten Informationen zusichern zu können, müssen diese Informationen durch den einstellenden Leistungserbringer mit einer elektronischen Signatur versehen werden.

Die Sicherheitsanforderungen, welche den Bedrohungen geschuldet sind, wirken dabei oft entgegengesetzt der Anforderungen an die Praktikabilität. Die Verschlüsselung und die erforderliche Autorisierung komplizieren die Abläufe aller zur Verfügung zu stellender Funktionalitäten, sind aber zwingend notwendig. Entsprechend müssen hier Kompromisse getroffen werden, welche die Sicherheit jedoch nicht gefährden dürfen.

Die Versuche zur Sicherung des Systems würden höchstwahrscheinlich scheitern, wenn

diese darin resultieren, dass die Verwendbarkeitskriterien vernachlässigt werden. Alle Sicherheitsmerkmale des Systems sind erst dann wertvoll, wenn das Endprodukt, welches den Patienten und Leistungserbringern zur Verfügung gestellt wird, gewisse Verwendbarkeitsanforderungen erfüllt. Benutzerfreundlichkeit, Verfügbarkeit für verschiedenste Benutzergruppen, einfache(s) Verständnis, Navigation und Dateneingabe, Unabhängigkeit vom verwendeten Endgerät und eine Hilfefunktion sind unvermeidbare Verwendbarkeitsmerkmale, welche das Endprodukt bieten sollte.

Die Pflicht der elektronischen Signatur von EPA-Daten ist dabei der medizinischen Dokumentationspflicht geschuldet, welche Teil der gesetzlichen Rahmenbedingungen ist. Die gesetzlichen Rahmenbedingungen betreffen unter anderem die Vertraulichkeit der medizinischen Daten, diese müssen gegenüber allen Teilnehmern des Systems vertraulich gehandhabt werden, und der Zugriff für Dritte muss untersagt sein. Die Datenhoheit des Patienten muss erhalten bleiben, er muss der Verarbeitung und dem Abruf seiner Daten explizit zustimmen. Das gesetzlich festgelegte Auskunftsrecht des Patienten muss berücksichtigt werden, dieses kann auch nicht durch Vertrag aufgegeben werden.

5 Arbeitsbereiche

5.1 Schlüsselverwaltung

Die Ver- und Entschlüsselng der eEPA des Patienten ist ein essentieller Teil dieses Systems. Ein praktikables Verschlüsselungsverfahren muss folgende Anforderungen erfüllen:

1. In einem Verschlüsselungsverfahren im EPA-System kennt die verschlüsselnde Partei die entschlüsselnde Partei nicht, obwohl dies bei kryptographischen Verfahren normalerweise eine Voraussetzung ist. Deshalb muss die Abwesenheit dieser Voraussetzung beim Entwurf des Verschlüsselungsmechanismus des EPA-Systems berücksichtigt werden.

2. Es soll einen Mechanismus geben, durch den das Verschlüsselungsverfahren mit dem Autorisierungsgeheimnis des Patienten autorisiert wird.

3. Die Speicherung des zur Ver- und Entschlüsselung erforderlichen Schlüsselmaterials auf einer dem Patienten zugehörigen Smartcard (z.B. eGK) ist keine Lösung für dieses Problem, weil es die folgenden Voraussetzungen erfüllt sein müssen, welche im eEPA-System nicht gegeben sind:
   - Der Patient muss bei jedem Zugriff auf seine EPA körperlich anwesend sein, um sich mit einer PIN zu authentifizieren und dadurch das Verschlüsselungsverfahren zu autorisieren.
   - Der Patient muss sowohl körperlich als auch geistig in der Lage, sich die PIN zur Authentifizierung gegenüber seiner Smartcard zu merken und diese in einer EPA-Zugriffssituation in einen Kartenleser einzugeben.

- In einer EPA-Zugriffssituation muss es eine räumlich Nähe zwischen Leistungserbringer, Patient, Kartenlesegerät und einer entsprechenden E/A-Einheit eines IT-Systems geben.

Noch dazu muss man den Umstand berücksichtigen, wenn die Smartcard verloren geht oder unbrauchbar wird. Ein Backup von Smartcard-Daten bei einer Dritten Partei ist sehr fraglich, weil es die Sicherheit der eEPA-Daten extrem gefährdet.

4. Die Informationen zu Ver- und Entschlüsselung müssen auf eine solche Art und Weise gehalten bzw. verwaltet werden, dass
   - die Sicherheit des vom Patienten autorisierten Verschlüsselungsverfahrens garantiert ist;
   - die Stelle, welche diese Informationen speichert, zu keiner Schwachstelle des Systems wird, d.h. Überlastung und Ausfall müssen verhindert werden; und
   - beim Ausfall dieser Teilkomponente alle im System stattfindenden Vorgänge weiter durchführbar sind und keine Informationen verloren gehen, d.h. es muss für geeignete Wiederherstellungsmechanismen gesorgt werden.

5. Bei der Verwendung eines Schlüssels für die Verschlüsslung der Informationen der eEPA eines Patienten ist zu beachten, dass die Stärke des Schlüssels im Laufe der Zeit abnimmt. Dies ist bedingt durch die stetig steigende Rechenkapazität im Mikroprozessorbereich. Zudem könnte das gewählte Verfahren gebrochen werden, dies würde eine erhebliche Abnahme der, um ein Dokument durch einen Brute-Force-Angriff zu entschlüsseln, nötigen Berechnungen bedeuten. In einem solchen Falle muss das verwendete Schlüsselverfahren ausgetauscht werden. Je nach Form des Mediums auf dem sich der Schlüssel befindet und wie dezentral dieser gehalten wird ergeben sich hier große organisatorische und logistische Probleme.

6. Sollte die Langzeitsicherheit der verwendeten Schlüssel gefährdet sein, wird eine Umschlüsselung nötig. Dies würde das Entschlüsseln aller Dokumente und deren erneute Verschlüsselung mit einem neuen Verfahren bedeuten. Fraglich ist hierbei, wer die Umschlüsselung vornimmt und wie diese vonstatten geht, da hierfür aufgrund der zu erwartenden Datenmengen ein erheblicher Rechenaufwand zu bewältigen sein wird. Die Alternative zur Umschlüsselung wäre die kaskadierende Verschlüsselung, das bereits verschlüsselte Dokument einfach erneut zu verschlüsseln. Dies würde den Aufwand bei allen stattfindenden Entschlüsselungen jedoch erhöhen. Hier ist es entsprechend notwendig, einen Plan zu entwickeln der später problemlos mit der existierenden Infrastruktur bewältigt werden kann.

5.2 Datenhaltung, Datenübertragung und Vertraulichkeit

Die Daten des Patienten müssen vor unberechtigtem Zugriff geschützt werden. Bei der Übertragung sowie auch bei der persistenten Speicherung medizinischer Daten von Patienten muss das Prinzip der Vertraulichkeit gewahrt bleiben. Zugriffskontrolle allein an

den IT-Systemschnittstellen kann hier keinen ausreichenden Schutz bieten. Die elektronischen Patientenakten der Patienten sollen daher so verschlüsselt gespeichert werden, dass die Kontrolle über die Entschlüsselung alleine beim jeweiligen Patienten selbst liegt.

Eines der sicherheitskritischsten Probleme im eEPA-System ist das Verbot einer möglichen Zuordnung zwischen dem Patienten und seiner EPA. Das ist auf Grund der hohen Datenschutzmaßnahmen in Deutschland von besonderer Bedeutung. Technisch macht diese Anforderung das Design des EPA-Systems schwierig, da eine Patient-EPA-Zuweisung an keiner Stelle im gesamten System, vor allem in keiner Teilkomponente, möglich sein darf. Beim Entwurf des Systems müssen für alle Komponenten alle möglichen Szenarien berücksichtigt werden, um sicherzustellen, dass keine Komponente die Identität der Patienten ermitteln kann. Die Anonymität der Patienten ist hinsichtlich des Systementwurfes ein komplexes Thema. Die einzige Stelle, welcher die Zuordnung eines Patienten zu einer eEPA möglich sein darf, ist der behandelnde Leistungserbringer. Die Bekanntgabe der Identität des Patienten ist an anderen Stellen unter keinen Umständen zulässig. Es gilt zu untersuchen, inwiefern die Anonymität der Patienten durch geeignete Pseudonymisierung erreicht werden kann.

5.3 Autorisierungsgeheimnis

Jeder Patient verfügt über eine Liste von Autorisierungsgeheimnissen, die er jeweils für die Autorisierung eines Zugriffs auf seine EPA verwendet. Das Autorisierungsgeheimnis muss ausschließlich dem Patienten bekannt sein. Selbst Leistungserbringer, die als grundsätzlich vertrauenswürdig erachtet werden, dürfen die Liste der Autorisierungsgeheimnisse des Patienten nicht erhalten.

Das Autorisierungsgeheimnis muss folgende Voraussetzungen erfüllen:

- Es muss menschenlesbar sein.
- Es muss auf verschiedenen Speichermedien speicherbar, insbesondere auf Papier druckbar sein.
- Es sollte nicht zu lang sein.
- Es sollte auch mündlich bzw. fernmündlich oder via diverser Kommunikationsmittel (z.B. Telefon) übermittelbar sein.
- Es muss einfach über die Tastatur in ein IT-System eingegeben werden können und sollte deshalb keine Sonderzeichen enthalten.
- Es sollte ausgedruckt auch als Barcode darstellbar sein.
- Der Umgang mit dem Token muss einfach sein, so dass auch ältere und behinderte Menschen damit zurecht kommen.
- Nur mit Kenntnis des Autorisierungsgeheimnises ist eine Ver- und Entschlüsselung von EPA-Informationen möglich.

- Es dient der Adressierung der EPA, d.h. ohne dessen Kenntnis ist ein Zugriff auf die EPA eines Patienten nicht möglich.
- Es eröffnet dem autorisierten Arzt ein Zeitfenster, innerhalb dessen er auf die EPA eines Patienten zugreifen kann, ohne bei jedem Zugriff erneut autorisiert werden zu müssen.

Einige Teilsysteme müssen Wissen über die Autorisierungsgeheimnisse besitzen, um diese bei Eingabe im Laufe eines Zugriffsverfahrens überprüfen zu können. Die Autorisierungsgeheimnisse müssen aus diesem Grund nach der Generation in Teilsystemen gespeichert werden, ohne anderen Teilsystemen zu ermöglichen, sich mit Hilfe der Autorisierungsgeheimnisse als Patient auszugeben. Dies stellt hohe Anforderungen an das gesamte eEPA-System. Es ergeben sich hieraus folgende Fragen:

1. Wo wird die Liste der Autorisierungsgeheimnisse generiert? Wie wird die Sicherheit der Stelle gewährleistet, bei der die Liste erzeugt wird? Sind dazu besondere Hardware und Software nötig? Wie hoch sind die Kosten solcher Hard-/Software?
2. Wer generiert bzw. lässt die Liste der Autorisierungsgeheimnisse generieren?
3. Wie wird sichergestellt, dass keiner außer dem Patienten selbst die generierte Liste erhält? Dies ist von besonderer Relevanz, sollte die Liste von einer anderen Identität als der Patient selbst erstellt werden.
4. Wie kann die Liste der Autorisierungsgeheimnisse gesperrt werden?
5. Wie kann man eine alte Liste durch eine neue Liste ersetzen? Wie kann man die Erzeugung wiederholter Autorisierungsgeheimnisse verhindern, die es z.B. in älteren Listen gegeben hat?
6. Wie kann man die Autorisierungsgeheimnisse an einen Gültigkeitszeitraum binden? Die Existenz eines Verfallszeitpunktes ist eine extrem notwendige Eigenschaft der Autorisierungsgeheimnisse.

5.4 PKI

Zum Zeitpunkt der Verschlüsselung ist der Empfänger unklar. Die EPA-Einträge müssen so gespeichert werden, dass jeder Leistungserbringer als Empfänger möglich ist. Lediglich der Patient ist als einzige Person zu jeder Zeit fest involviert. Von daher ist allein die Verwendung einer herkömmlichen Public Key Infrastruktur in diesem System nicht ausreichend. Es muss zur Behebung der oben erwähnten Einschränkung angepasst werden.

5.5 Metadaten

Die an die Patientendokumente gebundenen Metadaten reflektieren einige Informationen über den Inhalt der Dokumente und die Identität deren Besitzers. Es ist daher notwendig,

die Metadaten zu pseudonymisieren. Sonst wird die Anonymität des Patienten durch die Metadaten gefährdet.

5.6 Bedrohungen

Wir betrachten Bedrohungen des EPA-Systems durch die folgenden Entitäten:

- Insider: Legitime Benutzer des EPA-Projektes, welche versuchen, aus den ihnen zugänglichen Informationen unlautere Vorteile zu ziehen.
- Hacker: Personen welche sich darauf spezialisiert haben, elektronische Systeme im Hinblick auf Schwachstellen zu analysieren und diese auszunutzen.
- Diebe: Personen welche sich Zugang zum physischen Standort des EPA-Systems verschaffen und so elektronische Schutzmechanismen umgehen wollen.
- Malware: Bösartige Software, beispielsweise Trojaner, welche die Client- und Backend-Systeme des EPA-Systems zum Ziel haben, um über diese an die zu schützenden Informationen des EPA-Systems zu gelangen.

6 Ausblick

Medizinische Daten unterliegen besonderen Schutzbedarfen. Gleichzeitig sollen diese jedoch im Kontext einrichtungsübergreifender Elektronischer Patientenakten (eEPA) über ein potentiell unsicheres Netz ausgetauscht werden. Dadurch entstehen neue Sicherheitsanforderungen, die bei der alleinigen Datenhaltung innerhalb von Primärsysteme sonst nicht beachtet werden müssten. Diese Sicherheitsanforderungen müssen jedoch auch in Einklang mit den funktionalen Anforderungen der Anwender gebracht werden, entsprechende Lösungen müssen praktikabel sein.

Die Forschungsgruppe Systemsicherheit der Ruhr-Universität Bochum erarbeitet und analysiert innerhalb des Projektes *eBusiness Plattform Gesundheit (eBPG)* daher die hier dargestellten Anforderungen an die zu entwickelnde Sicherheitsarchitektur. Aufbauend auf diesen Ergebnissen werden Kernfunktionalitäten identifiziert, ausgearbeitet und in einer Implementierung umgesetzt. Für die Analyse der Anforderungen und Kernfunktionen werden existierende Ansätze betrachtet und auf ihre Schwachstellen und Praktikabilität analysiert. Anhand der Kernfunktionen und Anforderungen ergeben sich neue Problembereiche, für die innovative Lösungen erarbeitet werden müssen. Das Projekt eBPG hat eine Laufzeit von drei Jahren und endet im Dezember 2013.