STANDARDORIENTIERTE SPEICHERUNG VON VERSCHLÜSSELTEN DOKUMENTEN IN EINEM XDS-REPOSITORY

Köster L[1], Korkmaz F[1], Winandy M[1]

Zusammenfassung

Medizinische Daten von Patienten verlassen beim elektronischen Datenaustausch über einrichtungsübergreifende Patientenakten (EPA) die Primärsysteme der Leistungserbringer. Die Daten sind daher besonders zu schützen. Eine rein auf einer Zugriffskontrolle basierende Lösung bietet keinen Schutz gegen Insider, die Daten müssen daher verschlüsselt gespeichert werden. Dieser Artikel beschreibt einen CDA-Wrapper für das XDS-Profil der IHE Initiative, so dass in der vorgesehenen Dokumentenstruktur die eigentlichen medizinischen Daten verschlüsselt abgelegt werden.

Abstract

During data exchange between health professionals via Electronic Health Records (EHR) systems, medical data of patients' are leaving the health professionals' premises. Hence, the data have to be protected against unauthorized access. An approach based solely on access control does not provide protection against insiders, therefore data needs to be encrypted. This article describes a CDA Wrapper for the XDS Profile of the IHE initiative. The CDA-Wrapper enables to store encrypted medical information within an interoperable format.

Keywords – IHE, XDS, DEN, Verschlüsselung, Ende-zu-Ende-Vertraulichkeit

1. Einleitung

Die steigende Verbreitung von elektronischen Patientenakten (EPA) führt dazu, dass diese Akten immer größere Mengen an vertraulichen Daten enthalten [2]. Zeitgleich bietet sich Leistungserbringer die Möglichkeit, ihre EPA bei einem Drittanbieter zu outsourcen, letzten Endes in die Cloud, wo sie nicht mehr der direkten Kontrolle des Leistungserbringers unterliegen [7]. Da die Daten der Patienten in einem solchen Falle die Primärsysteme der Leistungserbringer verlassen, sind sie besonders zu schützen. Ein Ziel des Schutzes der medizinischen Dokumente ist Ende-zu-Ende-Vertraulichkeit. Diese schützt Informationen am Startpunkt des Transportvorgangs derart, dass Inhalte der Transaktion nur an ihrem Endpunkt wieder verfügbar werden. Alle Intermediäre der Transaktion erhalten keinen Einblick in den Inhalt der Transaktion, lediglich Sender und Empfänger kennen diesen. Im medizinischen Kontext sind Sender und Empfänger ausschließlich autorisierte Leistungserbringer, d.h. behandelnde Ärzte und medizinisches Personal, sowie der Patient selbst.

[1] Systemsicherheit, Horst Görtz Institut für IT-Sicherheit, Ruhr-Universität Bochum

Eine Ende-zu-Ende-Vertraulichkeit ist grundsätzlich durch Verschlüsselung realisierbar: Die Daten werden beim einstellenden Arzt verschlüsselt und erst wieder beim nächsten abrufenden Arzt entschlüsselt. Im Sinne des Datenschutzes und der Persönlichkeitsrechte des Patienten, darf nur dieser selbst die Möglichkeit zur Entschlüsselung autorisieren. Bezogen auf die EPA bedeutet dies, dass nicht nur der Transport (d.h. die elektronische Übermittlung) der medizinischen Daten, sondern auch die persistente Speicherung der Dokumente in der EPA bis zu ihrem Abruf verschlüsselt bleiben muss [1]. Insbesondere dürfen IT-Dienstleister wie der EPA-Provider oder dessen Personal (z.B. Administratoren) keine Möglichkeit zur Entschlüsselung der medizinischen Daten von Patienten haben. Zu den schutzwürdigen Daten zählen hierbei nicht nur die Dokumente selbst (z.B. ein Laborbefund), sondern auch deren Metadaten, da diese Informationen über den Inhalt des Dokumentes bereitstellen (z.B. Name des Patienten und behandelnden Arztes). Eine patienten-kontrollierte Autorisierung der Ver- und Entschlüsselung kann z.B. durch Speicherung der kryptographischen Schlüssel auf einer im Besitz des Patienten befindlichen Smartcard (z.B. elektronische Gesundheitskarte) realisiert werden. Alternative Verfahren, wie z.B. Attributbasierte Verschlüsselung unter Einsatz von vertrauenswürdigen Schlüsselservern, sind ebenso denkbar [4].

Eine wichtige Anforderung bei der Entwicklung von Verschlüsselungsverfahren für EPAs ist die Möglichkeit der Integration des Verfahrens in bestehende Systeme [3]. Diese Systeme können auf den Frameworks der Initiative „Integrating the Healthcare Enterprise“ (IHE) basieren. So bietet IHE für den Austausch und die Speicherung von medizinischen Dokumenten das Cross-Enterprise Document Sharing (XDS) Profil an [5]. Dieses Profil definiert Akteure, die die Dokumente erzeugen (*Document Source*), verarbeiten (*Document Consumer*) oder speichern (*Document Repository* und *Document Registry*), und Transaktionen zur Kommunikation zwischen den Akteuren. IHE bietet auch das Document Encryption (DEN) Profil an, welches sich mit verschiedenen Varianten zur Verschlüsselung beschäftigt [6]. Das DEN Profil beschreibt jedoch nicht die Ablage und dauerhafte, CDA-konforme Speicherung von verschlüsselten Dokumenten in einem XDS Repository. Die Standardisierung der Schnittstellen zur verschlüsselten Speicherung ist erforderlich, da der IHE-Grundgedanke der Interoperabilität ansonsten nicht mehr gewährleistet ist und Kompatibilität mit den Systemen anderer Nutzer nicht zugesichert werden kann. Es ist daher notwendig, eine Dokumentenstruktur zu etablieren, welche es ermöglicht, verschlüsselte Dokumente weitestgehend standardkonform in einem XDS Repository zu speichern.

Dieser Artikel beschreibt eine Realisierung einer solchen Dokumentenstruktur und belegt die Machbarkeit des erarbeiteten Konzeptes durch eine Implementierung und den Test dieser Implementierung gegen OpenXDS, eine OpenSource XDS-Implementierung [8]. Diese Arbeit entstand im Rahmen des Projektes eBPG – eBusiness Plattform Gesundheitswesen[2], welches vom Bundesland Nordrhein-Westfalen und der EU (Europäischer Fonds für regionale Entwicklung) gefördert wird.

2. Bisherige EPA-Infrastruktur

Die Rahmenarchitektur einer XDS-basierten EPA, *Abb.1*, besteht aus einem Document Repository und einer Document Registry. Dokumente lassen sich mittels der Transaktion "ITI-41 Provide and Register Document Set" im Repository ablegen. Übertragen werden neben dem Dokument selbst zusätzlich dessen Metadaten. Das Repository registriert das Dokument nach Eingang und Speicherung mit den Metadaten in der Registry. Die Registry speichert die Metadaten und ermöglicht Anfragen hinsichtlich der zu einem Patienten verfügbaren Dokumente. Die Transaktion

[2] eBPG Webseite: http://www.ebpg-nrw.de

"ITI-43 Retrieve Document Set" ermöglicht den Abruf von Dokumenten aus dem Repository anhand ihres eindeutigen Identifiers, den man zuvor mittels einer Anfrage („Registry Stored Query“) bei der Registry anhand von Metadaten (z.B. der Patienten-ID) ermittelt hat. Dokumente und Metadaten werden dabei unverschlüsselt in Repository und Registry abgelegt. Benutzern mit entsprechenden Rechten oder technischen Fähigkeiten ist es daher nach Erlangung (illegitimen) Zugangs zur Infrastruktur möglich, jegliche Dokumente einzusehen. Entsprechend sollten Dokumente nicht unverschlüsselt in die Systeme des Drittanbieters gelangen sondern bereits beim Verlassen der Client-Systeme durch Ende-zu-Ende-Vertraulichkeit geschützt werden. Wichtig ist hierbei zu verstehen, dass die Ende-zu-Ende-Vertraulichkeit nicht mit der Transaktion zum Document Repository enden darf, sondern erst beim autorisierten Leistungserbringer, d.h. demjenigen Document Consumer, dem der Patient die Entschlüsselung seiner Daten erlaubt.

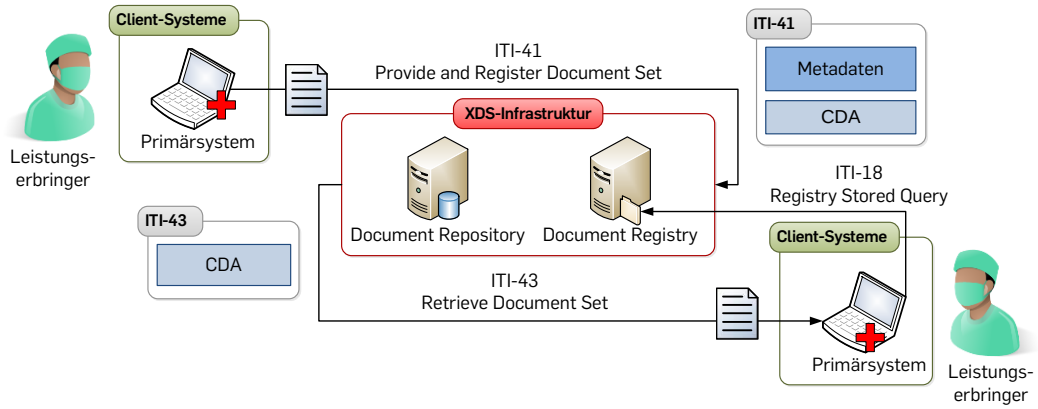

Abbildung 1: Speichern und Abrufen von Dokumenten nach XDS

3. Infrastruktur mit Ende-zu-Ende-Vertraulichkeit

Der Integration von Verschlüsselung in die Rahmenarchitektur, *Abb. 2*, ging eine Analyse der existierenden Transaktionen voraus. Um eine echte Ende-zu-Ende-Vertraulichkeit zu gewährleisten, müssen die Dokumente bereits auf der Clientseite (d.h. beim Leistungserbringer bzw. Document Source) verschlüsselt werden. Hierfür wurde von uns ein Krypto-Modul konzipiert, welches die Verschlüsselung übernimmt. Dieses Krypto-Modul kann entweder als Software-Plugin oder als eigenständiges Hardware-Modul im Primärsystem realisiert werden. Für die Verschlüsselung ist der Input des Patienten zwingend notwendig, da nur er die Ver-/Entschlüsselung seiner Dokumente autorisieren kann [1]. Das Primärsystem sendet alle für die Transaktion erforderlichen Daten an das Krypto-Modul, und der Patient ermöglicht dem Krypto-Modul die Verschlüsselung unter Zuhilfenahme seines Schlüssels (z.B. Eingabe über eine Smartcard). Anschließend erzeugt das Krpyto-Modul ein Wrapper-CDA, in welches das verschlüsselte CDA eingebracht wird.

Neben der Verschlüsselung der eigentlichen Daten werden auch die von IHE vorgegebenen Metadaten durch unser Krypto-Modul nach Datenschutz-Kriterien gefiltert. Wenn Metadaten datenschutzkritisch sind (z.B. Patientenname enthalten), werden diese nicht als Metadaten an die Registry übertragen und auch nicht in den Header des Wrapper-CDA übernommen. Zur Erkennung datenschutzkritischer Metadaten haben wir die nach IHE vorgegebenen Metadaten analysiert und nach personenbezogenen Informationen klassifiziert. Die als kritisch klassifizierten Metadaten werden durch das Krypto-Modul herausgefiltert und mit in den verschlüsselten Teil des Wrapper-CDA übernommen. Da das Wrapper-CDA dem CDA-Schema folgt, lässt es sich ohne Konflikte im Repository ablegen und kann durch die Transaktion ITI-43 abgerufen werden. Ebenso wie zur

Verschlüsselung ist auch im Falle der Entschlüsselung der Input des Patienten und seine damit einhergehende Autorisierung notwendig. Ver- und Entschlüsselung finden in der sicheren Umgebung der Clientsysteme statt.

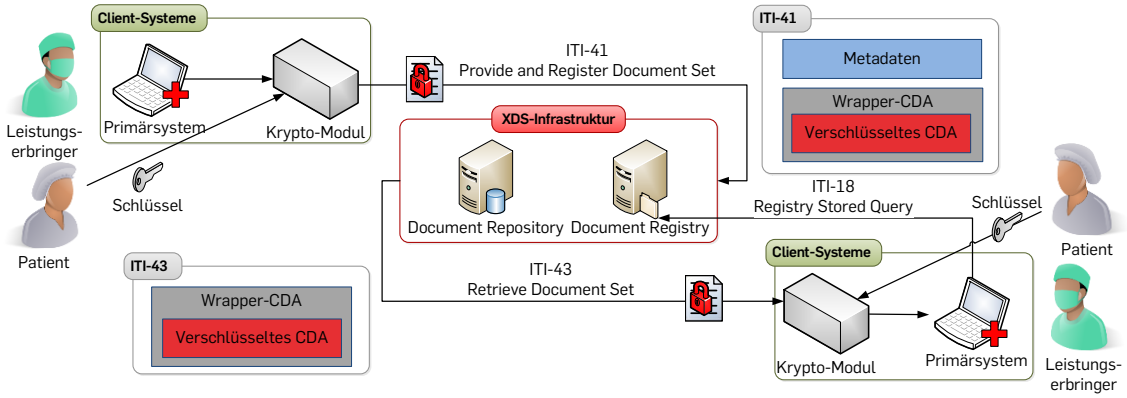

Abbildung 2: Speichern und Abrufen von verschlüsselten Dokumenten

4. Implementierung der XDS-konformen Dokumentenverschlüsselung

Das Wrapper-CDA folgt dem Aufbau eines auf XML-basierenden Standard-CDA Dokumentes und besteht aus Header und Body in welchen die im CDA-Standard definierten Elemente als Container für Informationen dienen. Die Verwendung von CDA ist der angestrebten Standardkonformität der Lösung geschuldet. Wrapper-CDA und Krypto-Modul wurden prototypisch implementiert, *Abb. 3*. Für unsere Implementierung wurden Primärsystem und Krypto-Modul in einem Webservice integriert, welcher auf einem Tomcat-Applikationsserver ausgeführt wird. Pro Patient kann eine Liste der verfügbaren Dokumente eingesehen werden. Der Webservice ermöglicht die Anzeige von einigen Werten eines CDA-Dokumentes und bietet die Möglichkeit, neue Dokumente zu erstellen und verschlüsselt in OpenXDS abzulegen. Ebenso können bereits existierende Dokumente abgerufen, entschlüsselt, editiert und erneut verschlüsselt im Document Repository abgelegt werden. Die SOAP-Nachrichten zwischen Webservice und OpenXDS werden durch eine Axis2-Schnittstelle übermittelt und entsprechen den OpenXDS-beiliegenden Nachrichten. Auf Seiten der XDS-Infrastruktur wurde gegen die XDS-Implementierung OpenXDS getestet. Die Implementierung konnte ohne Konflikte für die Speicherung genutzt werden.

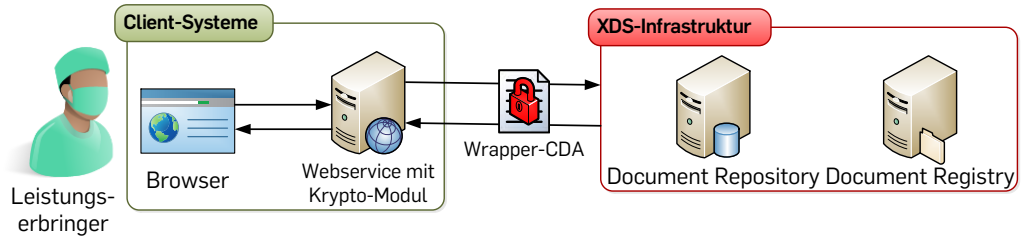

Abbildung 3: Darstellung der prototypischen Implementierung

Das Wrapper-CDA, *Abb. 4*, dient der möglichst standardkonformen Speicherung von verschlüsselten Dokumenten innerhalb eines XDS-Repositories. Das Originaldokument wird vor der eigentlichen Verschlüsselung Base64 encodiert, um die eigentlichen Daten unabhängig von XML verschlüsseln zu können. Das verschlüsselte Dokument wird anschließend in ein *nonXMLBody*-Element eines weiteren CDAs geschrieben. Dieses zweite CDA enthält neben einem auf unbedenkliche Daten reduzierten Header auch Informationen über das gewählte

Verschlüsselungsverfahren. Diese Informationen werden benötigt, um zum einen das während der Verschlüsselung genutzte Verfahren eindeutig identifizieren zu können, zum anderen um dem jeweils gewählten Verfahren die Möglichkeit zu geben, zusätzliche Informationen, welche im Rahmen der Entschlüsselung benötigt werden, zusammen mit dem Dokument zu speichern. Bei den zusätzlichen Informationen darf es sich aber natürlich in keinem Fall um den Schlüssel im Klarformat handeln. Ebenso muss beachtet werden, dass Dokumente nicht mehr zu entschlüsseln sein könnten, wenn hier falsche Angaben gespeichert werden.

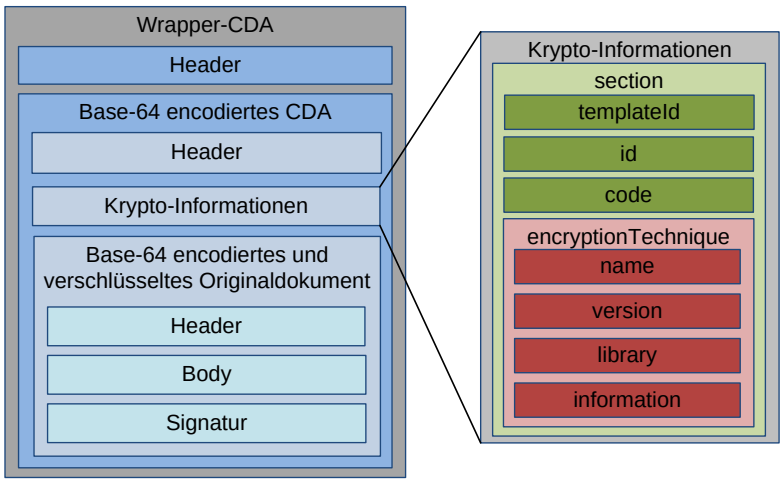

Abbildung 4: Wrapper-CDA mit Aufschlüsselung der Krytpo-Informationen

Da die zur Entschlüsselung wichtigen Krypto-Informationen zwar in einem *section*-Element gespeichert werden, *Abb. 4*, aber dennoch nicht zum CDA-Schema gehören und damit nicht standardkonform sind, wird das CDA erneut base64-encodiert in einem nonXMLBody eines weiteren CDAs gespeichert. Dieses CDA enthält dabei die gleichen Header-Informationen wie das CDA welches das verschlüsselte Dokument beinhaltet, entspricht dem CDA-Schema, abgesehen von nicht-präsenten Headerdaten, und kann somit standardkonform abgelegt werden. Die *section* der Krypto-Informationen, enthält die Elemente *templateId*, *id*, und *code* gemäß CDA-Spezifikation. Das Element *encryptionTechnique* enthält Informationen zum gewählten Verschlüsselungsverfahren. Zwingend notwendig sind hierbei der Name des Verfahrens sowie dessen Versionsnummer. Das *library*-Element soll es ermöglichen auf eine Programmbibliothek zu verweisen und so die automatisierte Verarbeitung zu erleichtern. Das *information*-Element enthält spezifische Informationen zum Verschlüsselungsverfahren. Die Inhalte dieses Elementes sind frei wählbar um künftige Verfahren problemlos integrieren zu können.

5. Diskussion

Die Entwicklung des Wrapper-CDA hat gezeigt, dass es möglich ist, verschlüsselte Dokumente und zugehörige Krypto-Informationen weitgehend standardkonform in einem XDS-Repository zu speichern. Die hier dargestellte Lösung kann als Ansatz für eine Integration von standardkonformer Verschlüsselung in das XDS Profil verstanden werden. Neben der Orientierung an bereits etablierten Standards bietet die präsentierte Lösung den Vorteil der Ende-zu-Ende-Vertraulichkeit. Darüber hinaus ermöglicht der generische Aufbau der Elemente zur Speicherung der Krypto-Informationen, dass auch künftige Verfahren verwendet werden können, um die Zukunftsfähigkeit zu sichern. Um häufige Änderungen an ausgerollten Systemen zu minimieren, werden die Krypto-Informationen im Wrapper-CDA gespeichert und nicht in den Metadaten.

Ebenso wie die eigentlichen Dokumente müssen auch die Metadaten einer Sicherheitsanalyse unterzogen werden. Metadaten können aus Gründen der Verwendbarkeit nicht verschlüsselt werden, da sie die Basis für die Entscheidung zum Abruf eines Dokumentes bilden. Daher dürfen keine Metadaten in die Registry eingestellt werden, welche die zu schützenden Inhalte der verschlüsselten Dokumente gefährden. Die Metadaten des IHE-Standards wurden analysiert und kritische Informationen werden automatisch aus den Transaktionen entfernt. Eine detaillierte Angabe der kritischen Metadaten würde jedoch den Rahmen dieses Artikels sprengen. Ein Nachteil der Realisierung von Ende-zu-Ende-Vertraulichkeit ist der Verlust der Möglichkeit der Weiterverarbeitung von Informationen in den Infrastruktur-Systemen. Aufgrund der Verschlüsselung kann dies nicht mehr erfolgen. Es besteht jedoch weiterhin die Möglichkeit, alle Dokumente eines Patienten aus dessen EPA herunterzuladen und diese lokal weiter zu verarbeiten. Dieser Ansatz ist für einzelne Patienten umsetzbar, für mehrere Patienten ohne deren Einwilligung ohnehin aus Datenschutzgründen verboten.

Die Realisierung von Ende-zu-Ende-Vertraulichkeit beruht in diesem Konzept auf einem Krypto-Modul, welches auf der Clientseite in den Primärsystemen eingebunden wird. Um an allen Endpunkten, d.h. bei autorisierten Leistungserbringern, die Entschlüsselung garantieren zu können, muss auch dieses Modul standardisiert sein. Zusätzlich sollten alle an der EPA teilnehmenden Organisationen eine gemeinsame Strategie zur Absicherung der EPA-Daten in den Primärsystemen verfolgen, um die Sicherheit der Patientendaten garantieren zu können. Es sind daher weitere Arbeiten erforderlich um Ende-zu-Ende-Vertraulichkeit für elektronische Patientenakten zu realisieren.

6. Referenzen

[1] Engels J. Technische und organisatorische Anforderungen an sichere EPA-Systeme. Projektdokument EPA.nrw, 2008. [Online], Verfügbar: www.egesundheit.nrw.de [Abgerufen: 04-2013]

[2] Ford EW, Menachemi N, Phillips MT. Predicting the Adoption of Electronic Health Records by Physicians: When Will Health Care be Paperless? J Am Med Inform Assoc 2006;13:106-112.

[3] Gawlik A, Köster L, Mahmoodi H, Winandy M. Requirements for Integrating End-to-End Security into Large-Scale EHR Systems. In: Proceedings of the Amsterdam Privacy Conference (APC 2012), 1st International Workshop on Engineering EHR Solutions (WEES), 2012.

[4] Hupperich T, Löhr H, Sadeghi A-R, Winandy M. Flexible Patient-Controlled Security for Electronic Health Records. IHI 2012: Proceedings of the 2nd ACM SIGHIT International Symposium on Health Informatics, ACM, 2012.

[5] IHE International, IT Infrastructure (ITI) Technical Framework, Volume 1, Integration Profiles, Kap. 10 Cross-Enterprise Document Sharing, 2012.

[6] IHE International, IT Infrastructure (ITI) Technical Framework, Technical Framework Supplement, Document Encryption, 2011.

[7] Klein, C. Cloudy confidentiality: Clinical and legal implications of cloud computing in health care. J Am Acad Psychiatry Law, 2011;39(4):571–578.

[8] OpenHealthTools Inc., "OpenHealthTools", 2012. [Online], Verfügbar: www.openhealthtools.org [Abgerufen: 01-2013]

Corresponding Author
Lennart Köster
Systemsicherheit, Horst Görtz Institut für IT-Sicherheit, Ruhr-Universität Bochum
Universitätsstraße 150, D-44780 Bochum
Email: lennart.koester@trust.rub.de