Schreier G, Hayn D, Ammenwerth E, editors. Tagungsband der eHealth2011. 26.-27.Mai 2011; Wien. OCG; 2011.

BEWEISSICHERE INFRASTRUKTUR FÜR TELEMEDIZINISCHE ANWENDUNGEN

Madiesh M[1], Paasche T[2], Hackel S[1]

Kurzfassung

Als Ergebnis der rapiden Entwicklung der Informations- und Kommunikationstechnologien ist in den letzten Jahren eine Vielzahl neuer telemedizinischer Anwendungen entstanden. Diese Anwendungen sind aber ohne IT-Sicherheitsmaßnahmen nicht betreibbar. Der Beitrag zeigt eine Lösung für die sichere Kommunikation und Archivierung von medizinischen Daten auf. In dieser Lösung werden die Erfahrungen aus dem DFG-Projekt BeLab vorgestellt. BeLab ist konzeptionell als Serviceorientierte Architektur ausgelegt. Die Public-Key-Infrastruktur kann dabei auch die der elektronische Gesundheitskarte / des Heilberufeausweises sein.

Abstract

As a result of the rapid development of information and communication technology in recent years a variety of new telemedicine applications were developed. These applications are however not able to operate without IT-security. The paper shows a solution for secure communication and archiving of medical data. In this solution, the experiences of the DFG-project BeLab are presented. BeLab is designed conceptually as a service-oriented architecture. The public key infrastructure can also be the electronic health card / electronic health professional card.

Keywords – Telemedizin, BeLab, elektronische Signatur, elektronische Gesundheitskarte, Heilberufsausweis

1. Einleitung

Der demographische Wandel in Deutschland [1] hat neue Lösungsansätze im Gesundheitswesen notwendig gemacht. Die Telemedizin ist ein Lösungsansatz, der von der rapiden Entwicklung der Informations- und Kommunikationstechnologie profitiert. Sie hat eine große Rolle bei der Kostenreduzierung und der Geschäftsprozessoptimierung im Gesundheitswesen eingenommen. Telemedizinische Anwendungen können durch die Vernetzung dazu führen, dass durch menschliche Fehler oder kriminelle Angriffe Informationen über die Patienten durch Unbefugten bekannt oder manipuliert werden. Dieser Beitrag zeigt auf, wie die IT-Sicherheit basierend auf der Technology der elektronischen Signatur bei der Übertragung und Archivierung von medizinischen Daten gewährleistet werden kann. Nach der Einleitung werden im Abschnitt 2 die grundlegenden Begriffe (z. B. eGK

1 Fachbereich Q.4 - Informationstechnologie, Physikalisch-Technische Bundesanstalt PTB, Braunschweig
2 Master-Student an der TU Braunschweig

und HBA) beschrieben. Danach wird im Abschnitt 3 die Funktionsweise des dieser Arbeit zu Grunde liegenden Systems des „Beweissicheren elektronischen Laborbuchs“ (BeLab) [8] beschrieben. Weiterhin erfolgt ein Vergleich mit medizinischen Dokumentationen. Im Abschnitt 4 wird aufgezeigt, wie sich aus dem BeLab-System der Ansatz für eine beweissichere Infrastruktur für telemedizinische Anwendungen ableiten lässt. Mit dem Fazit und Ausblick wird dieser Beitrag abgeschlossen.

2. Grundlagen

2. 1. Datensicherheitsanforderungen

Die rechtlichen, funktionalen und organisatorisch-technischen Anforderungen können in sechs Grundanforderungen zusammengefasst werden: Vollständigkeit, Lesbarkeit, Integrität Authentizität, Verkehrsfähigkeit und die Verfügbarkeit [5].

2. 2. Einsatz von elektronischen Signaturen

2.2. 1. Fortgeschrittene und qualifizierte Signatur

Eine elektronische Signatur basiert auf der Anwendung eines Schlüsselpaars, welches aus einem privaten und einem öffentlichen Schlüssel besteht (asymmetrische Kryptographie). Fortgeschrittene elektronische Signaturen müssen nach § 2 Nr. 2 Signaturgesetz (SigG) [4] eindeutig dem Signaturschlüssel-Inhaber zugeordnet sein, wodurch die Authentifizierung des Zertifikatinhabers gewährleistet ist und die Integrität der Daten überprüft werden kann. Eine qualifizierte elektronische Signatur ist nach § 2 Nr. 3 SigG eine fortgeschrittene elektronische Signatur, die auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat basiert und mit einer sicheren Signaturerstellungseinheit erzeugt wurde.

2.2. 2. Zusammenspiel der elektronischen Gesundheitskarte und des Heilberufsausweises

Die beiden Karten wurden entworfen, um eine Infrastruktur für die Telemedizin zu schaffen. Die elektronische Gesundheitskarte (eGK) ist mit einer Prozessorchipkarte ausgestattet, auf der die digitale Identität für die Telematikinfrastruktur gespeichert ist. Analog zur elektronischen Gesundheitskarte hat auch der Heilberufsausweis (HBA) einen Mikrochip und dient als Ausweis im Arzt- und Apothekenbereich. Beide Karten bieten verschiedene Funktionen wie Signatur-, Authentifizierungs- und Verschlüsselungsfunktionen, die als Basis für die Datensicherheit verwendet werden könnten. eGK und HBA werden zum Authentifizieren und zum Datenzugriff auf die eGK gemeinsam benötigt. Nach PIN-Eingabe durch den Arzt wird der Zugriff mittels Client-zu-Client-Authentifizierung auf nur ungeschützten Versichertenstammdaten und Notfalldatensatz erfolgt. Der Zugriff auf andere Daten erfordert die PIN-Eingabe der Patienten [6].

3. Das BeLab-Projekt und die Telemedizin

BeLab [8] ist ein von der DFG gefördertes Projekt, welches sich mit der Beweiswerterhaltung von elektronischen Laborbüchern auseinander setzt. Das Laborbuch ist eng mit der Arbeit von Wissenschaftlern verbunden. Es ist eine Art Tagebuch, in dem der Wissenschaftler in einer über den Tag hinausreichenden Form seine tägliche Arbeit und seine Forschungsergebnisse für die spätere Auswertung dokumentiert [3]. Im Laborbuch werden im Prinzip alle Informationen zu den Forschungs-

projekten festgehalten. Es enthält Informationen über Methoden, Geräte, Messungen und daraus abgeleitete Ergebnisse, Literaturrecherchen, Beteiligung von Forschern etc. Über die Forschung hinaus werden Laborbücher auch in der Analytik, z. B. in medizinischen Laboren, der Lebensmittelkontrolle und anderen Anwendungsbereichen (z. B. staatliche Zulassungsverfahren) verwendet.

Der Ansatz ist, die Ähnlichkeiten der Arbeitsweisen von Naturwissenschaftlern mit ihren elektronischen Laborbüchern mit der von Medizinern mit ihren sensorerweiterten elektronischen Patientendokumenten zu vergleichen und nach Synergien zu schauen.

3. 1. Komponenten des BeLab-Systems

Die in *Abbildung 1* dargestellten Komponenten des BeLab-Systems werden in diesem Abschnitt erörtert. Ausgehend von dem Import der beweissicher zu archivierenden Daten aus elektronischen Laborbüchern zeigt die Abbildung den Verlauf von deren Verarbeitung bis hin zur Langzeitarchivierung.

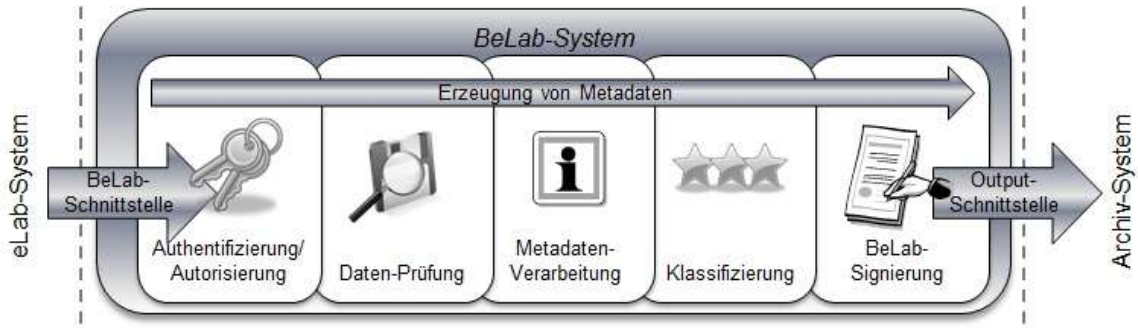

Abbildung 1: Komponenten des BeLab-Systems

3.1. 1. Anbindung elektronischer Laborbücher

An das BeLab-System lassen sich unterschiedliche elektronische Laborbücher (eLabs) anbinden. Die elektronischen Laborbücher übermitteln hierfür z. B. zu archivierende Labor-, Mess- oder Forschungsdaten an die BeLab-Schnittstelle. Die Daten müssen hierfür vom eLab entsprechend aufbereitet werden. Im Idealfall handelt es sich bereits um XML-Daten. Die BeLab-Schnittstelle akzeptiert aber auch zusätzlich Dateien in unterschiedlichen Formaten.

3.1. 2. Die BeLab-Schnittstelle

Die BeLab-Schnittstelle wurde als Web Service realisiert. Über Simple Objekt Access Protocol [11] (SOAP)-Nachrichten können die Laborbücher zu archivierende Daten an das BeLab-System übermitteln. Die BeLab-Schnittstelle fordert, dass in den Anfragen ein sog. BeLab-Container angegeben wird. Dieser Container umfasst einen eindeutigen Identifier (ID) des eLab (SystemID genannt) und ermöglicht eine Strukturierung der vom eLab abgelegten Daten. Nach erfolgreicher Archivierung liefert die BeLab Schnittstelle dem Benutzer eine eindeutige ID zurück.

3.1. 3. Automatische Erzeugung von Metadaten

Während der gesamten Verarbeitung der vom eLab übermittelten Daten werden zusätzliche Metadaten erzeugt. Im Metadaten-Container wird der Status der Verarbeitung durch die Komponenten

des BeLab-Systems gespeichert. Der Metadaten-Container kann somit als zusätzliche Protokollierung (Logfile) der BeLab-Verarbeitung angesehen werden.

3.1. 4. Authentifizierung, Autorisierung und Datenprüfung

Die Kommunikation mit dem BeLab-System wird über HTTPS realisiert. Für die Übermittlung von Anfragen an die BeLab-Schnittstelle müssen die angebundenen elektronischen Laborbücher Client-Zertifikate (im BeLab-System ist X.509 festgelegt) verwenden. Anhand dieser Client-Zertifikate erfolgt die Authentifizierung des jeweiligen eLabs. Anhand der eindeutigen ID des Zertifikats erfolgt eine anschließende Autorisierung, die z. B. den Zugriff bestimmter Benutzer für einzelne System-, Projekt- oder ContainerIDs erlauben oder verweigern kann.

Das BeLab-System kann eine Konsistenzprüfung der von den elektronischen Laborbüchern übermittelten Daten durchführen (z.B. Gewährleistung fortlaufender Zeitstempel oder Sequenznummern). Diese Validierung der Eingabedaten kann von den Betreibern angepasst werden. Im Rahmen der Datenprüfung können auch die eingehenden Datenformate geprüft werden. Handelt es sich um bereits digital signierte Dateien, kann diese Signatur für die Konsistenzprüfung (Integrität und Authentizität der übermittelten Daten) verwendet werden.

Werden während der Konsistenz-, Format- oder Signaturprüfung von der Prüfkomponente Fehler ermittelt, so wird die weitere Verarbeitung im BeLab-System abgebrochen und dem Benutzer bzw. dem eLab eine Fehlermeldung zurückgeliefert. Der Wissenschaftler muss dann entscheiden, ob er die Daten trotzdem sichern will oder nicht. Das Ergebnis der Prüfungen wird im Metadaten-Container vermerkt und somit für eine spätere Verwendung archiviert.

3.1. 5. Metadaten-Verarbeitung

Bereits in den übermittelten Daten vorhandene Metadaten (Zeitstempel, Namen und Bezeichnungen, Parameter der Messapparatur usw.) werden in der Komponente „Metadaten-Verarbeitung“ in den zuvor von der BeLab-Schnittstelle angelegten Metadaten-Container übernommen.

3.1. 6. Klassifizierung

Das BeLab-Projekt definiert unterschiedliche Güteklassen für die Beweissicherheit und die Langzeitarchivierung. Die durchgeführte Klassifizierung der Daten ermöglicht eine Bewertung der übermittelten Daten bezüglich der Qualität der langfristigen Beweissicherheit.

3.1. 7. BeLab-Signierung

Die übermittelten Daten, im Rahmen des BeLab-Systems erzeugte Metadaten sowie die durch die Klassifizierung ermittelte Güte werden durch das BeLab-System mit einer digitalen Signatur bestätigt. Diese Signatur gewährleistet bei nachfolgenden Prüfungen der Daten im Archiv die korrekte Verarbeitung durch das BeLab-System sowie die Integrität der erzeugten Metadaten.

3.1. 8. Output-Schnittstelle

Für die Anbindung eines Archivsystems stellt das BeLab-System eine generische Schnittstelle zur Verfügung. Im BeLab-Projekt wird ein Archivsystem eingestellt werden, welches die Kriterien der

technischen Richtlinie TR03125 des Bundesamts für Sicherheit in der Informationstechnik (BSI)[2] erfüllt.

3. 2. Wie kann man das BeLab-Konzept auf den Bereich der Telemedizin anwenden?

Dazu wurde eine Bachelorarbeit angefertigt, die Parallelen in der Datenrepräsentation zwischen Laborbüchern und sensorerweiterten elektronischen Patientendokumenten analysiert hat. Sie wurde an der TU-Braunschweig in Kooperation mit dem BeLab-Projekt betreut [12]. In dieser Bachelorarbeit wurde gezeigt, dass zwischen den Laborbuch-Dokumenten (als Beispiel das Laborbuch für die Bauartzulassung von Waagen) und den sensorerweiterten elektronischen Patientendokumenten, die im Bereich Telemedizin verwendet werden können, auf aggregierter Ebene deutliche Parallelen bestehen, die sich in ähnlichen, teils identischen Datenkategorien ausdrücken. *Tabelle 1* stellt den Datenvergleich zwischen den beiden Dokumenten dar.

Tabelle 1: Datenvergleich zw. Laborbuch-Dokumenten und Patientendokumenten

Dokumente der elektronischen Laborbücher	Sensorerweiterte elektronische Patientendokumente
Kundendaten	Patientendaten
Herstellerangaben	Stammdaten des Patienten
Verantwortlicher Wissenschaftler	Verantwortlicher Arzt
Computergenerierte Daten	Computergenerierte Daten
Rechnungsdaten	Rechnungsdaten
Messdaten / Kalibrierdaten	Allgemeine Untersuchungsergebnisse
Messdaten / Kalibrierdaten	Sensorische Untersuchungsergebnisse
Solldaten	Normwerte
Experimentalverlauf	Behandlungsverlauf
Prüfungsergebnis	Diagnose

3. 3. Vergleichbare Arbeiten im Bereich der Telemedizin

Eine Arbeit [10] hat ebenfalls den SOA-Ansatz benutzt. Die an medizinischen Monitoren anfallenden Daten von Neugeborenen wurden in Form von XML-Datenpaketen versandt und gespeichert. In dieser Arbeit wurde aber die Sicherheit bei der Datenübertragung und –Speicherung nicht diskutiert.

Das Soarian Health Archive der Firma Siemens dient als zentrale Ablage für anfallende medizinische Daten und Dokumente. Dieses Archiv verwendet eigene kryptografische Verfahren für die nach Angaben des Herstellers revisionssichere Ablage und kann in verschiedene KIS-Systeme integriert werden.

4. Ergebnisse

Es konnte gezeigt werden, dass es sich im Falle der elektronischen Laborbücher auf aggregierter Ebene um ähnliche Datenformen handelt wie bei sensorerweiterten elektronischen Patientendokumenten. Durch die Verwendung der eGK/HBA als PKI kommen qualifizierte digitale Signaturen zum Einsatz. Somit gibt es Gemeinsamkeiten zwischen qualifiziert digital signierten elektronischen Laborbuchdokumenten und mit der eGK/HBA signierten elektronischen sensorerweiterten Patientendokumenten, die wiederum als Input für die BeLab-Middleware dienen können. Diese Gemein-

samkeiten werden noch verstärkt durch die Tatsache, dass die verwendeten Daten gleichartige Datenformate verwenden, was zu Datenspeicherungsverfahren auf der Basis von XML führt.

Beim BeLab-System handelt es sich um eine Middleware, die den Inhalt von elektronischen Laborbüchern / sensorerweiterten Patientendokumenten elektronischen Langzeitspeichersystemen zuführen kann, die die rechtssichere Langzeitspeicherung der Daten gewährleistet, wenn gilt:

- Die Daten aus den elektronischen sensorerweiterten Patientendokumenten / Laborbüchern sind mit einer qualifizierten digitalen Signatur versehen,
- die Daten bestehen die von der BeLab-Middleware geforderten Bedingungen,
- das elektronische Langzeitspeichersystem ist nach dem BSI- CC-PP-0049-2008 [9]: Protection Profile gemäß Common Criteria für ArchiSafe [7] vom BSI zertifiziert und
- die Technische Richtlinie 03125 des BSI [2] erfüllt.

Wenn dies für elektronische sensorweite Patientendokumente gilt, so gilt dies auch für Patientendokumente und dann prinzipiell auch für sämtliche Patientenakten, die die obigen Bedingungen erfüllen. Das eLab entspricht einem Telemedizin-Client. Die Patientendaten und die verschiedenen Untersuchungsergebnisse, die durch den Arzt während der Untersuchung des Patienten erstellt wurden, werden durch diesen Telemedizin-Client aufgenommen und durch eine qualifizierte digitale Signatur signiert und verschlüsselt und als SOAP-Nachricht zum Server gesendet. Der Server kommuniziert mit der BeLab-Schnittstelle, die via einer SOAP-Nachricht versendet wird. Danach werden die verschiedenen BeLab-Funktionen von der Authentifizierung bis der sicher Archivierung durchgeführt.

Somit kann diese Middleware komplett im Gesundheitssektor eingesetzt werden. Weil die Middleware den Anschluss an mittlerweile1 auf dem Markt existierende Komponenten ermöglicht, ist somit auch die Überführung in die Praxis gewährleistet.

5. Fazit und Ausblick

Es wird eine beweissichere Infrastruktur für die telemedizinischen Anwendungen vorgeschlagen. Mit Hilfe der kryptografischen Verfahren, die als Basis für die Datensicherheit innerhalb dieser Infrastruktur verwendet werden, ist es möglich, die im Medizinbereich anfallenden Daten von ihrer Entstehung bis zur Ablage im elektronischen Langzeitspeicher für die Dauer der Aufbewahrungsfrist rechtssicher zu verarbeiten und zu archivieren.

Diese Arbeit beschreibt eine SOA-basierte generische Schnittstelle, die für die Beweissicherheit und die Langzeitarchivierung von medizinischen Daten bedeutsam sein kann. Diese Schnittstelle kann von verschiedenen telemedizinischen Clients und Krankenhaus-Information-Systeme (KIS) verwendet werden.

6. Literatur

[1] Alterung der Weltbevölkerung: 1950-2050. Zusammenfassung. Vereinte Nationen, New York 2001. http://www.un.org/esa/population/publications/worldageing19502050/pdf/german_execsum.pdf, (gesehen am 21.01.11)

1 Zum Zeitpunkt der Tagung sollte das BSI das Zertifikat an den Hersteller vergeben haben.

Schreier G, Hayn D, Ammenwerth E, editors. Tagungsband der eHealth2011. 26.-27.Mai 2011; Wien. OCG; 2011.

[2] BSI Technische Richtlinie TR-03125 Vers. 1.0 : Vertrauenswürdige elektronische Langzeitspeicherung, https://www.bsi.bund.de/cln_156/ContentBSI/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html, 2009., und deren Nachfolgefassung 1.1 mit verändertem Titel: „Beweiswerterhaltung kryptographisch signierter Dokumente“: https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03125/index_htm.html, 2011

[3] EBEL, H.F., BLIEFERT, C., Bachelor-, Master- und Doktorarbeit: Anleitungen für den naturwissenschaftlich-technischen Nachwuchs (4. Aufl.). Weinheim : Wiley-VCH, 2009.

[4] Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften, vom 16.05.2001. BGBl. 2001 Teil I Nr. 22, S. 876 ff, geändert durch Art. 1 G v. 4. 1.2005 I 2. http://bundesrecht.juris.de/bundesrecht/sigg_2001/, 2001.

[5] HACKEL, S., ROßNAGEL, A., Langfristige Aufbewahrung elektronischer Dokumente, in. D. Klumpp, H. Kubicek,
A. Roßnagel und W. Schulz (Hrsg.), Informationelles Vertrauen für die Informationsgesellschaft, Springer-Verlag Berlin Heidelberg 2008.

[6] HÄBER, A., WERNER, D., Einführung der elektronischen Gesundheitskarte in Krankenhäusern, in R. Koschke, O. Herzog, K. Rödiger, M. Ronthaler (Hrsg.), Informatik 2007 – Beiträge der 37. Jahrestagung der Gesellschaft für Informatik e.V.(GI), Band P-110 von Lecture Notes in Informatics, 444-449, Bremen, Germany, September 2007. Gesellschaft für Informatik.

[7] http://www.archisafe.de/

[8] http://www.belab-forschung.de/

[9] https://www.bsi.bund.de/ContentBSI/Themen/ZertifizierungundAnerkennung/ZertifierungnachCCundITSEC/SchutzprofileProtectionProfile/schutzprofile.html#PP0049

[10] MCGREGOR, C:, HEATH, J., WEI, M.,"A Web Services Based Framework for the Transmission of Physiological Data for Local and Remote Neonatal Intensive Care," eee, pp.496-501, 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'05), 2005

[11] SNELL, J., TIDWELL, D., KULCHENKO, P., Introducing SOAP, Kap. 2, in J. Snell, D. Tidwell und P. Kulchenko (Hrsg), Programming Web Services with SOAP, O'Reilly Media 2001.

[12] PAASCHE, T, Parallelen in der Datenrepräsentation zwischen Laborbüchern und sensorerweiterten elektronischen Patientendokumenten, Bachelorarbeit, TU Braunschweig, September 2010.

Corresponding Author

Moaaz Madiesh
Physikalisch-Technische Bundesansalt PTB, IT Abteilung
Bundesallee 100, DE-38116 Braunschweig
Email: moazmadiesh@hotmail.com

Schreier G, Hayn D, Ammenwerth E, editors. Tagungsband der eHealth2011. 26.-27.Mai 2011; Wien. OCG; 2011.