TECHNISCHE HOCHSCHULE NÜRNBERG
GEORG SIMON OHM

Fakultät Elektrotechnik Feinwerktechnik Informationstechnik

Studiengang „Bachelor Elektrotechnik und Informationstechnik“

Digital Rights Management für elektronische Patientenakten

Bachelorarbeit von

Gabriel Kaufmann

Matrikelnummer: 3128129

Wintersemester 2020/2021

Abgabedatum: 11.Februar 2021

Betreuer:

Prof. Dr. Oliver Hofmann

Inhaltsverzeichnis

1 Einleitung

International hat Deutschland ein leistungsfähiges Gesundheitswesen (vgl. [BERT]), jedoch besteht ein schwerwiegendes Defizit. Bei der Kommunikation zwischen den Patienten und den verschiedenen medizinischen Sektoren gibt es bislang noch keine einheitlich normierte Schnittstelle. Informationen werden nicht genormt, ausführlich und fachspezifisch zwischen den medizinischen Instanzen kommuniziert. Hierunter leidet sowohl die Qualität als auch die Effizienz der individuellen Behandlungen, da immer wieder Schwund und Fehlinterpretationen von Patientendaten auftreten (vgl. [EHEA, S.8]). Dieses Problem ist seit längerem bekannt und es wurde als Gegenmaßnahme, zum Beispiel bereits 1998 (vgl. [EHEA, S.1]) eine Initiative der Selbstverwaltung beschlossen. Diese trägt den Namen „Aktionsforum Telematik im Gesundheitswesen“ (ATG). Erarbeitet wird das ATG von Organisationen des deutschen Gesundheitswesens. Diese haben es sich zum Ziel gemacht, das deutsche Gesundheitswesen mittels moderner IT zu optimieren und medizinische Kommunikation zukünftig ausschließlich digital stattfinden zu lassen. Bereits in vielen Ländern hat die stetig wachsende Entwicklung der Informationstechnik dazu geführt, dass Patientendaten digitalisiert und vernetzt wurden. Der deutsche Staat hat nun den Start der ersten elektronischen Patientenakte am 01.Januar 2021 durchgeführt (vgl. [DEFU]). Die Verwendung dieser ist freiwillig, da das Grundrecht auf Datenschutz (vgl. [DATNS]) in Deutschland eine verpflichtende elektrische Patientenakte nach der aktuellen Verwirklichung verbietet. Dieses sagt aus, dass jeder Mensch ein Grundrecht auf Datenschutz beziehungsweise informationelle Selbstbestimmung hat. Jeder Mensch hat das Recht, Herr über seine eigenen Daten zu sein. Mit der am Anfang 2021 veröffentlichten Version der elektronischen Patientenakte kann der Patient lediglich seine kompletten Daten an einen Arzt freigeben (vgl. [BNDEPA]). Es ist nicht gewährleistet, dass der Patient einer medizinischen Station Leserechte nur auf bestimmte Teile seiner Daten geben und diese auch zeitlich limitieren kann. Es müsste zusätzlich mehr „Digital Rights Management“ (kurz: DRM) beachtet, geplant und implementiert werden. Dies ist eine Abwandlung eines Kopierschutzes, welcher nicht die Kopie der Daten selbst verhindert, sondern die Verwendung und Transparenz von Daten kontrolliert und eine Verbreitung dessen vermeiden soll. (vgl. [DRMEXP])

1.1 Aufgabenstellung/Anforderungsanalyse

Aufgabe ist es, herauszufinden wie eine in der Einleitung geschilderte Lösung, mittels DRM aussehen könnte, um Patientenakten zukünftig digital, individuell und vor allem sicher zu verwalten, unabhängig von bereits verwendeten oder geplanten Lösungen. Wie könnte es möglich sein, dass zudem jeder Mensch über seine eigenen Daten bestimmen kann, um diese individuell freizugeben, so wie dieser es möchte? Insbesondere wird die Handhabung der Zugriffsrechte und dessen Bezug auf die abgespeicherten Patientendaten betrachtet. Hierfür werden die Funktionsweisen für die temporäre Freigabe, der Zugriff auf freigegebene, aber auch auf nicht freigegeben Daten untersucht.

1.2 Vorgehen

Es wird ein Prototyp eines solchen Konzeptes entworfen, um anschließend mithilfe dessen, mögliche Sicherheitslücken evaluieren und eventuelle Lösungen, falls vorhanden, für diese vorstellen zu können. Der Prototyp soll funktionsfähig und möglichst sicher sein. Funktionsfähig bedeutet, dass ein Beispielpatient mittels einer grafischen Oberfläche seine eigenen Daten einsehen, verwalten und einer anderen Partei temporär Zugriff auf einzelne Unterkategorien seiner Patientenakte gewähren kann. Während dieser Zeit können die Daten eingesehen, aber nicht weiterverbreitet werden. Der Zugriff auf die Daten wird über Instanzen in Form von verschiedenen beispielhaften medizinischen Ebenen, welche unterschiedliche Zuständigkeitsgebiete haben simuliert. Nach Ablauf der temporären Frist soll es der anderen Partei nicht mehr möglich sein, auf die individuellen Daten zuzugreifen.

2 Grundlagen

Die Grundlagen erklären alle wichtigen Begriffe, die einen Zusammenhang zu dem Digital Rights Managementsystem der elektronischen Patientenakte haben.

2.1 Überblick Patientenakte

Die Patientenakte wird in dem Prototyp in elektronischer Form verwendet. Der Inhalt der Patientenakte und die gesetzlichen Gegebenheiten lassen sich auf die digitale Form reflektieren und können übernommen werden.

2.1.1 Inhalt

Der Inhalt einer Patientenakte setzt sich aus allen Aufzeichnungen des Arztes oder der Ärztin zusammen. Diese bestehen aus Anamnese (Vorgeschichte einer Krankheit), Diagnosen, Notizen über Untersuchungen, Untersuchungsergebnisse, Therapiemaßnahmen, Operationen, Befunde, Aufklärungen, Einwilligungen und auch Arztbriefe. (vgl. BGB § 630f)

2.1.2 Gesetzliche Gegebenheiten

Das BGB gibt an, dass jeder Arzt oder Ärztin daran gebunden ist, alle relevanten Daten über Behandlungen und dessen Ergebnisse umfassend in einer für jeden Patienten individuell angelegten Patientenakt zu führen. Diese kann elektronisch als Dokument oder in Papierform archiviert werden und muss mindestens zehn Jahre abrufbar sein. (vgl. BGB, § 630f)

2.2 Begriffserklärung Digital Rights Management

Digital Rights Management (abgekürzt „DRM“) ist ein Ansatz zum Schutz von Urheberrechten für digitale Medien und Inhalte. Dieser Ansatz umfasst den Einsatz von Technologien, die die Nutzung von urheberrechtlich geschützten Werken und Software einschränken. In gewisser Weise ermöglicht die digitale Rechteverwaltung den Urhebern beziehungsweise den Besitzern von digitalen Inhalten zu kontrollieren, was zahlende beziehungsweise berechtigte Nutzer mit ihren Werken tun können. Für Unternehmen kann die Implementierung von Digital Rights Management-Systemen dazu beitragen, den Zugriff oder die Nutzung bestimmter Endgeräte oder den Zugriff auf gesonderte Informationen durch unbefugte Benutzer zu verhindern, wodurch das Un-

ternehmen rechtliche Probleme vermeiden kann, die aus einer nicht autorisierten Nutzung entstehen. DRM spielt heute eine wachsende Rolle bei der Datensicherheit. (vgl. [ENT, S.3])

Datendiebstal ist durch ein erhöhtes Aufkommen von Peer-to-Peer Datenaustauschdiensten wie Torrent-Sites zu einem Unheil für urheberrechtlich geschützte Daten und Anwendungen geworden. Digital Rights Management Systeme sind nicht konzeptioniert worden, um diejenigen zu fangen, die sich an dem Datendiebstal beteiligen. Stattdessen soll es diesen Technologien unmöglich machen, Inhalte zu stehlen und weiterzugeben, da alleine der Datenbesitzer bestimmt, wer die Anwendungen und Informationen verwenden darf. (vgl. [URH])

In der Regel umfasst die digitale Rechteverwaltung Architekturen, die die Zeit oder die Anzahl der Geräte begrenzen, die auf bestimmte Dateninhalte zugreifen dürfen.

Verleger, Autoren, Programmierer und andere Ersteller von Inhalten verwenden eine DRM-Anwendung die Medien, Daten, E-Books, Inhalte, Software oder anderes urheberrechtlich geschütztes Material verschlüsselt. Nur diejenigen, die über die Entschlüsselungsschlüssel verfügen, können auf das Material zugreifen. Der Entschlüsselungsschlüssel befindet sich neben den Nutzungsbedingungen in der Regel in der Lizenz. Die Nutzungsbedingungen werden von diesen Anwendungen verwendet, um zu begrenzen und einzuschränken, welche Rechte der Benutzer im Bezug zu den Materialien besitzt. (vgl. [ENT, S.3-6])

2.3 Zusammenführung DRM und Patientenakte

Werden nun die beiden Techniken, Digital Rights Management und die Patientenakte zusammengeführt, so resultiert daraus die elektronische Patientenakte. Hier kann jeder Benutzer selbst entscheiden, was mit seinen Daten passiert und wer diese einsehen, beziehungsweise bearbeiten kann. Die elektronische Patientenakte soll die Kommunikation zwischen den Ärzten ausbauen und den Datenschutz für den individuellen Patienten verbessern (vgl. [ARZTPRAX]). Da Ärzte daran gebunden sind, medizinische Aufzeichnungen in Form einer Patientenakte zu archivieren, können diese auch selbst organisatorische Vorteile aus einer elektronischen Patientenakte ziehen. Sie

müssen die Daten der Patienten nicht mehr lokal in den einzelnen medizinischen Einrichtungen lagern und administrieren, sondern können einfach die bereitgestellte Infrastruktur und Server benutzen, um so Ihre Aufzeichnungen zu den individuellen Patienten zu verwalten.

2.4 Begriffserklärungen

Folgend werden wichtige Begrifflichkeiten erklärt, welche zur Verständnis des Prototyps relevant sind. Außerdem werden die Normen und Werkzeuge geschildert, welche bei der Implementierung dessen verwendet wurden.

2.4.1 Rest API

Eine Rest API („Representational State Transfer Application Programming Interface“) ist ein Webservice, mithilfe dessen mehrere Geräte miteinander kommunizieren können. Dieser macht es möglich, Informationen und Programme auf unterschiedliche Server aufzuteilen. Diese Server können dann mithilfe eines HTTP-Request angesprochen werden, um so die gewünschten Informationen anzufordern oder um bestimmte Aufgaben von dem Server erledigen zu lassen. (vgl. [RESTAPI, S.9])

2.4.2 Hashfunktion

Eine Hashfunktion wandelt eine beliebig große Zeichenkette beziehungsweise Information zu einem Ausgabewert mit einer festgelegten Länge um. Der Ausgabewert wird als Hash oder Hashwert bezeichnet. Der Hash ist eine Folge aus einzelnen Bits und kann mit Hilfe von Codierungen als Buchstaben und Zahlen dargestellt werden. Es darf nicht möglich sein, aus dem berechneten Hash die ursprüngliche Zeichenkette bestimmen oder zurückberechnen zu können. (vgl. [CRYPTO, S.271])

Im Prototyp wird die Hashfunktion „SHA-256“ verwendet. Diese wird vom Bundesamt für Sicherheit in der Informationstechnik empfohlen und wird als technische Richtlinie repräsentiert. (vgl. [BSICRYP, S.42])

2.4.3 Symmetrische Verschlüsselung

Die symmetrische Verschlüsselung ist ein Werkzeug, um Daten zu schützen. Bei dieser Methode wird ein geheimer Schlüssel zum Verschlüsseln und zum Entschlüsseln der Daten verwendet, nur die Beteiligten der Kommunikation dürfen den Schlüssel kennen. Der Schlüssel kann zum Beispiel ein Wort oder aber auch eine zufällige Folge

von Buchstaben, Zahlen und Symbolen sein. Der Absender und der Empfänger müssen den selben Schlüssel kennen, damit sie die Daten verschlüsseln und im Nachhinein wieder entschlüsseln können. (vgl. [CRYPTO, S.179-180])

In der praktischen Umsetzung des Konzeptes wird die symmetrische Verschlüsselungsmethode „AES-256“ verwendet. Dieser Algorithmus verwendet Schlüssel mit einer Länge von 256 Bit und wird vom Bundesamt für Sicherheit in der Informationstechnik, aufgrund des langen Schlüssels bei längerer Aufbewahrung von verschlüsselten Daten empfohlen. (vgl. [BSICRYP, S.22])

2.4.4 Asymmetrische Verschlüsselung

Im Gegensatz zur symmetrischen Verschlüsselung werden bei der asymmetrischen Verschlüsselung zwei separater, aber mathematisch miteinander verbundene kryptografische Schlüssel verwendet, um Daten zu verschlüsseln und zu entschlüsseln. Die Schlüssel werden als öffentlicher Schlüssel und privater Schlüssel bezeichnet. Werden Daten mit dem öffentlichen Schlüssel verschlüsselt, kann nur der Besitzer des privaten Schlüssels diese entschlüsseln. Andersherum, kann eine Nachricht, welche mit dem privaten Schlüssel verschlüsselt wurde, nur mit dem öffentlichen Schlüssel entschlüsselt werden. Jeder Teilnehmer einer Kommunikation sollte ein Schlüsselpaar besitzen. Der öffentliche Schlüssel ist jedem Teilnehmer der Kommunikation zugänglich. Jeder Teilnehmer kann den öffentlichen Schlüssel von jemand anderem anfordern, um so zum Beispiel eine Nachricht für den Besitzer des entsprechenden privaten Schlüssels zu verschlüsseln, die nur er wieder entschlüsseln und lesen kann. Der private Schlüssel bleibt geheim und ist lediglich dem Besitzer bekannt. (vgl. [CRYPTO, S.202-203])

Der Prototyp verwendet die asymmetrische Verschlüsselungsmethode „RSA“, hier wird von dem Bundesamt für Sicherheit in der Informationstechnik eine Schlüssellänge von 2000 Bit empfohlen. (vgl. [BSICRYP, S.47])

2.4.5 Signatur

Ein mathematisches Schema, welches zum Nachweis der Authentizität von digitalen Nachrichten oder Dokumenten verwendet wird, wird als Signatur bezeichnet. Eine gültige Signatur hat die Eigenschaft, die Integrität und Authentizität der Information zu bestätigen und sicherzustellen, dass die Nachricht oder Dokument nach dem Signieren nicht mehr verändert wurde.

Das Konzept beruht darauf, dass der Absender einer Nachricht, die Nachricht selbst oder den Hashwert dessen mit dem eigenen privaten Schlüssel verschlüsselt und an die Nachricht anhängt. Der Empfänger kann nun mit dem öffentlichen Schlüssel des Absenders die angehängte Signatur entschlüsseln und feststellen, ob der Absender die Nachricht signiert hat und diese unverändert angekommen ist. Sobald jemand anderes die Nachricht signiert oder den Inhalt der Nachricht ändert, stimmt die Nachricht mit der entschlüsselten Signatur nichtmehr überein und gilt als ungültig. (vgl. [CRYPTO, S.216])

Zum Signieren von Daten wird bei dem Prototyp der RSA Algorithmus verwendet, da dieser als asymmetrische Verschlüsselungsmethode implementiert ist.

2.4.6 PKI

Bei der asymmetrischen Verschlüsselung muss sichergestellt sein, dass die öffentlichen Schlüssel unverändert und korrekt übertragen werden. Ein PKI („Public Key Infrastructure“) stellt eine vertrauenswürdige und sichere Infrastruktur dar, bei der die öffentlichen Schlüssel durch digitale Zertifikate von vertrauenswürdigen Autoritäten bestätigt und signiert werden. Durch ein PKI lässt sich schlussfolgernd die Integrität von öffentlichen Schlüsseln sicherstellen. (vgl. [CRYPTO S.370-372])

2.4.7 Smartcard

Eine Smart Card wird verwendet um den privaten Schlüssel eines Benutzers zu schützen. Der private Schlüssel kann nicht von der Smart Card gelesen werden und benötigt in der Regel zusätzlich einen PIN, um aktiviert zu werden. Dies wird durch einen privaten Token auf der Karte und dem integrierten Chip ermöglicht. Alle Verschlüsselungen mit dem privaten Schlüssel finden auf der Smartcard statt. (vgl. [CRYPTO, S.371-372])

2.4.8 Integrität

Integrität bezieht sich auf die Genauigkeit, die Vollständigkeit und die Vertrauenswürdigkeit von Daten während ihres gesamten Lebenszyklus. Sie beschreibt den Zustand von Daten, diese können entweder gültig oder ungültig sein, entsprechend ob diese genau, vollständig, unverändert und vertrauenswürdig sind. Mit Hilfe von Signaturen, lässt sich die Integrität von Daten feststellen. (vgl. [ITSEC, S.108])

2.4.9 Vertraulichkeit

Vertraulichkeit besagt, dass ausgetauschte Informationen nicht für unbefugte Teilnehmer zugänglich sind. Dies wird oft durch symmetrisch oder asymmetrische Verschlüsselung gewährleistet, indem die Informationen oder Nachrichten verschlüsselt übertragen werden. (vgl. [ITSEC, S.103])

2.4.10 Verfügbarkeit

Verfügbarkeit definiert, wie zugänglich Systeme sind, wenn sie benötigt werden. Da elektronische Systeme verwendet werden, kann die Verfügbarkeit nicht bei 100 Prozent liegen. Neben den Systemen selbst bezieht sich die Verfügbarkeit auch auf die Kommunikation zwischen den Systemen. (vgl. [ITSEC, S.110])

3 Related Work

Platz	Ranking 2016	Ranking 2018
1	Dänemark, Schweden	Dänemark
2	Estland, Finnland, Slowakei	Finnland, Schweden
3	Portugal	Estland, Spanien
4	Spanien	Schweiz
5	Österreich	Slowakei, Vereinigtes Königreich
6	Schweiz	Portugal
7	Belgien	Frankreich
8	Deutschland, Litauen, Niederlande	Niederlande, Österreich
9	Vereinigtes Königreich	Belgien, Deutschland, Litauen, Polen
10	Italien	Tschechische Republik
11	Frankreich, Slowenien	Italien, Slowenien
12	Polen	Irland
13	Tschechische Republik	
14	Irland	

Abbildung 1 – Ländervergleich, implementierung einer elektronischen Patientenakte aus [REWO]

International hat Deutschland ein leistungsfähiges Gesundheitswesen (vgl. [BERT]). Auf dem Stand der Implementierung einer funktionsfähigen elektronischen Patientenakte findet sich Deutschland auf dem neunten Platz im Ländervergleich der EU wieder (siehe Abbildung 1). Deutschland hat sich von 2016 bis 2018 um einen Platz verschlechtert. Dieses Ranking berücksichtigt noch nicht die im Jahr 2021 eingeführte erste Version der elektronischen Patientenakte. Um verwandte Arbeiten zu analysieren, ist es notwendig, dass die beteiligten Systeme schon getestet und Informationen zu den Implementierungen veröffentlicht wurden.

Beispielhaft hierfür und als Vorreiter für funktionierende Systeme zeigen sich Estland und die skandinavischen Länder Dänemark, Finnland und Schweden.

3.1 Estland

Die elektronische Patientenakte besteht in Estland seit 2008. Zusätzlich zu den gewöhnlichen USE-Cases der elektronischen Patientenakte gibt es noch weitere Funktionen wie zum Beispiel das elektronische Rezept. Realisiert wird das Konzept in Estland über die Blockchain. In Estland ist die Akte nicht verpflichtend und kann bei Bedarf deaktiviert werden. Dies wird lediglich von weniger als einem Prozent der Bevölkerung in Anspruch genommen und zeigt, wie gut sich das Verfahren etabliert hat. (vgl. [ERFA, S.8-9])

3.2 Dänemark

Seit dem Implementierungsjahr 2004 sind die Ärzte in Dänemark gesetzlich daran gebunden, eine Schnittstelle zu der elektronischen Patientenakte zu besitzen, damit Patienten diese verwenden können. Die Funktionsweise der elektronischen Patienten-

akte wird mittels einer Webanwendung realisiert. Diese verweist auf einen Cloudspeicher, um die Patientendaten abzufragen. Hier können die Patienten ihre Daten verwalten. Zum Einloggen wird ein einmaliges Passwort verlangt, welches sich ständig ändert. Zu vergleichen ist dies mit der Tan für eine Überweisung. Die elektronische Patientenakte weist viele weiter Funktionen, unter anderem das elektronische Rezept auf und wird in Dänemark immer weiter ausgebaut und mit immer mehr Daten des alltäglichen Lebens verknüpft. (vgl. [ERFA, S.11])

4 Konzeption

Das Digital Rights Management System steuert bei der Verwendung der digitalen Patientenakte, welche Parteien auf wessen individuell angelegten Patientendaten zugreifen und bearbeiten darf. Um mit dem Prototyp ein solches Schema zu simulieren, werden verschiedene statische Objekte in der Datenbank erzeugt, welche miteinander interagieren. Zudem wird durch die Einträge sichtbar, welche möglichen Unterteilungen und welche Benutzerinstanzen in dem System verwendet werden können.

4.1 Parteien

Zur Veranschaulichung und zum Testen des Prototyps werden beispielhafte Elemente in Form von Ärzten und Patienten erstellt. Zusätzlich gibt es noch die Verwaltung selbst, welche sich um die Infrastruktur und die Datenbereitstellung kümmern muss.

4.1.1 Der Patient

Der Patient selbst kann mit der Anwendung Lizenzen ausstellen und somit Rechte verteilen, die festlegen, wer auf seine Akte Zugriff bekommt und diese lesen, bearbeiten oder mitverwalten kann.

Hier gibt es zwei Patienten. Ein Patient verwaltet seine Akte selber und ein zweiter, der einer anderen Partei die Rechte stellt, um seine Akte zu verwalten, da er selbst unzurechnungsfähig ist. Der zweite Patient soll nach der Abgabe der Rechte keinen Zugriff mehr auf diese haben.

4.1.2 Der Hausarzt

Der Hausarzt ist in der Lage, für ihn freigegebene Daten einzusehen und diese abhängig von den Zugriffsrechen zu bearbeiten oder zu ergänzen.

Es gibt einen Hausarzt, der seine lokal gelagerten Einträge zu den entsprechenden Patienten virtualisieren möchte, um so die Vorteile der elektronischen Patientenakte zu nutzen.

4.1.3 Der IT-Beauftragte

Der Beauftrage registriert neue Benutzer und kümmert sich darum, dass diese Ihren privaten Schlüssel und Daten, welche zum Einloggen benötigt werden, erhalten. Er fungiert als Administrator und kann zusätzlich neue Klassen als Unterkategorien von Patientenakten anlegen, um diese genauer zu kategorisieren.

Er benötigt ein administratorberechtigtes Benutzerkonto.

4.2 Rechte

Ein Patient kann einer anderen Partei verschiedene Rechte zu seiner Patientenakte geben.

4.2.1 Lesen

Besitzt eine Partei der Infrastruktur das Recht eine spezifische Patientenakte zu lesen, kann sie die zugeteilten Aktenteile einsehen.

4.2.2 Schreiben

Hat ein Benutzer das Recht „Schreiben“ kann er die Patientenakte bearbeiten und nach Belieben verändern. Um das Recht „Schreiben“ zu besitzen, benötigt der Benutzer zusätzlich das Recht „Lesen“, da er sehen muss, welche Daten er verändert.

4.2.3 Lizenz

Mit dem Recht „Lizenz“, darf der Benutzer neue Lizenzen im Zusammenhang mit der referenzierten Patientenakte ausstellen. Dieses Recht trägt in der Regel der Besitzer der Patientenakte selbst. Er kann dies aber weitergeben und sein eigenes Recht „Lizenz“ behalten oder abgeben.

4.3 Aktenteile

Da die Zugriffe und Rechte nicht auf die komplette Patientenakte eines Benutzers geschehen und vergeben werden sollen, muss diese in verschiedene Aktenteile aufgegliedert werden. Zu diesem Zweck werden zwei beispielhafte Instanzen verwendet.

4.3.1 Impfpass

Im Impfpass werden Einträge der einzelnen Impfungen des Patienten gesammelt.

4.3.2 Akute Erkrankungen

In dieser Unterkategorie werden akute Erkrankungen des Benutzers gespeichert.

5 Implementierung

5.1 Entwurf

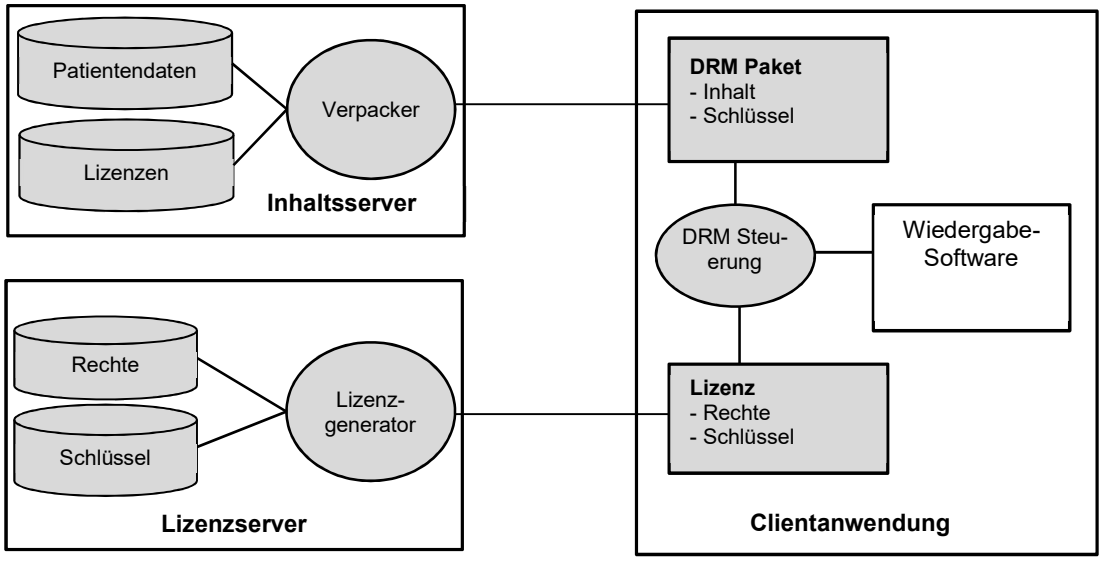

Abbildung 2 - Architektur eines DRMS nach Rosenblatt, Trippe und Mooney

Der Entwurf für den Prototyp orientiert sich an der Architektur eines Digital Right Management Systems nach Rosenblatt, Trippe und Mooney (vgl. [ROSEN]). Dieses Besteht aus drei Hauptbestandteilen, den Inhaltsserver, die Clientanwendung und dem Lizenzserver (siehe Abbildung 2), welche alle über eine Telematik Infrastruktur kommunizieren.

Die Idee dieser Zugriffssteuerung wird mit Hilfe verschiedener kryptografischer Verfahren realisiert. So ist der Inhalt aus dem Inhaltsserver, welcher die Daten in einer Datenbank lagert, verschlüsselt und somit unlesbar ohne weitere Mittel. Die Daten können ohne Bedenken herausgegeben werden, ohne dass sich die Person, welche die gewünschten Daten anfordert, verifizieren muss. Da dieser nur die Daten verwerten kann, wenn er den Schlüssel besitzt, der die Daten entschlüsseln kann. Dieser wird von dem Lizenzserver bei richtiger Identität und Rechten bereitgestellt.

Der Prototyp bringt noch weitere Eigenschaften mit sich. Es sind neben dem Lesen noch weitere Funktionen verfügbar. Das Digital Rights Management System bietet die Möglichkeit, befugten Nutzern Daten zu verändern. Somit können andere Instanzen, welche ebenso befugt sind, auf die individuelle Akte zuzugreifen und indirekt Ergebnisse untereinander auszutauschen. Ein befugter Arzt kann also in die Akte eines Patienten Notizen eintragen, welche von den anderen befugten Ärzten auch gesehen werden können.

Ein anderes Benutzerrecht, welches vom Urheber der Daten vergeben werden kann, ist die Befugnis, weitere Befugnisse an Dritte auszustellen. Somit kann der Dritte die Akte des Patienten entweder komplett selbst verwalten, zum Beispiel im Falle von Unzurechnungsfähigkeit oder es kann auch der Patient zusammen mit dem Dritten über die Patientenakte bestimmen. Dies hängt davon ab, ob der Patient die Rechte behalten kann oder darf.

Des Weiteren sind alle Rechte die Patientenakte zu nutzen, zeitlich limitiert, sodass eine Person, welche Zugriffsrechte hat, nach Ablauf einer Frist nicht mehr neue und aktualisierte Einträge in die Patientenakte einsehen, bearbeiten oder weitere Rechte an diese ausstellen kann.

Diese Funktionen unterscheiden den zu Zwecken dieser Arbeit erstellten Prototyp von dem Digital Right Management System nach Rosenblatt, Trippe und Mooney. In den Prototypen wird die selbe Architektur verwendet wie in Abbildung 2. Es werden von dem Lizenzserver Lizenz verwaltet und sogenannte Lizenzzertifikate ausgestellt, welche alle wichtigen Informationen beinhalten, um sich bei dem Inhaltsserver auszuweisen. Jedes Lizenzzertifikat ist einzigartig und an den Besitzer der Patientenakte und den wünschten potentiellen Leser oder Schreiber der Akte gebunden. Dieses enthält außerdem einen Schlüssel (im Folgenden auch als Gesamtschlüssel bezeichnet), welcher nötig ist, um die Akte das erste Mal zu entschlüsseln.

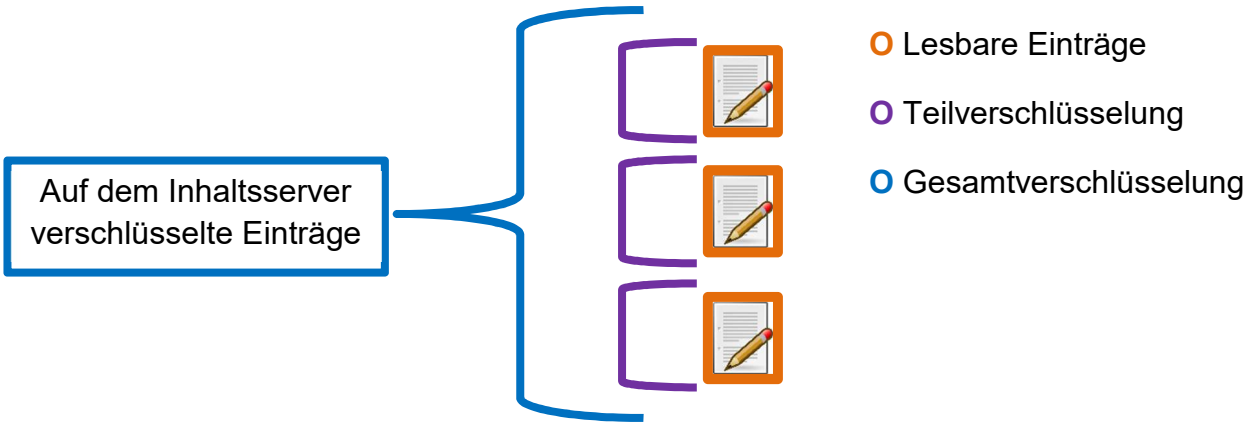

Abbildung 3 - Verschlüsselte Einträge einer Patientenakte auf dem Inhaltsserver

Erklärt der Inhaltsserver das Lizenzzertifikat für gültig, bearbeitet er im Vorfeld die verschlüsselten Daten (siehe Abbildung 3) mithilfe des Lizenzzertifikates und kann mit

dessen Hilfe die Gesamtverschlüsselung entschlüsseln, um die Aktenteile anschließend als einzelne Teilverschlüsselungen an den Benutzer zu senden. Nur der Benutzer selbst, kann dann die Daten lesen, da er mit Hilfe seines privaten Schlüssels die Teilverschlüsselungen entschlüsseln kann, um schlussfolgernd die lesbaren Einträge zu erhalten.

Die Gruppierung der Ärzte, aber auch die der Patienten teilen sich eine gemeinsame grafische Oberfläche in Form einer Webanwendung. Die Ärzte besitzen genauso wie die Patienten ein Benutzerkonto in der Infrastruktur. Somit kann man als Patient nicht nur Ärzten Rechte auf die eigene Akte geben, sondern auch anderen Patienten.

Im Folgenden wird auf den Aufbau der einzelnen Komponenten eingegangen. Dies umfasst den Lizenzserver, den Inhaltsserver und die Clientwebanwendung (im Folgenden auch als Patientenakten-Verwaltungssystem bezeichnet). Es wird die Programmstruktur und die Datenstrukturen deren Datenbanken, mit dessen zusammenhängen erläutert.

5.1.1 Der Lizenzserver

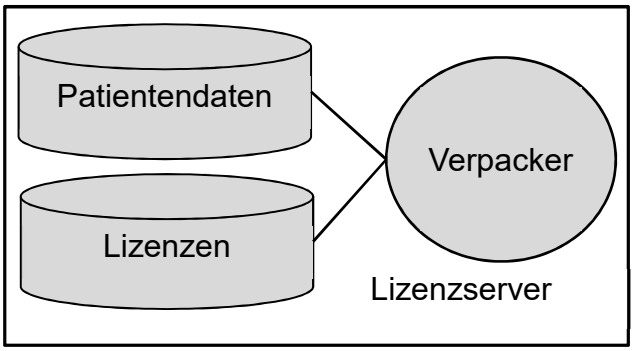

Abbildung 4 - Übersicht Lizenzserver

Der Lizenzserver ist ein Webserver, welcher die Clientwebanwendung in Form einer Website zur Verfügung stellt. Mit Hilfe von dem Django Framework werden so die Daten der Datenbank verarbeitet, verwaltet und dynamisch an den Endbenutzer über HTTP weitergegeben. Auf dem Lizenzserver werden die Profile der Patienten und Ärzte erstellt und in der Datenbank eingepflegt. Der Verpacker kümmert sich um die Datenbank und setzt die Website über HTML dynamisch zusammen, um dem Benutzer die Verwaltung seiner Patientenakte zu ermöglichen. Die Patientendaten und die Lizenzen (siehe Abbildung 4) werden von der Datenbank separat betrachtet. Diese beiden Objekte Verweisen in einzelnen Attributen aufeinander.

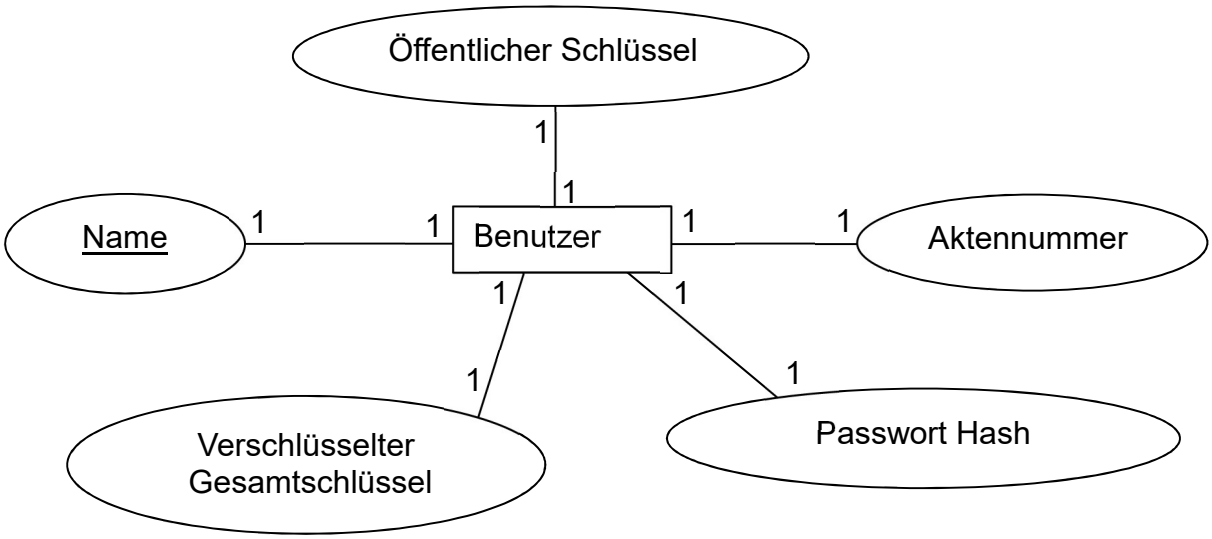

Abbildung 5 - ERM Model eines Benutzers

Das Model eines Benutzers (siehe Abbildung 5) kann sowohl einen medizinischen Sektor oder einen Patienten repräsentieren, hier gibt es keinen Unterschied. Beide haben dieselben Funktionen. Die Objekte lassen sich mit dem Namen des Benutzers

identifizieren. Der Name fungiert als Primärschlüssel und muss somit eindeutig sein, um das Objekt zuzuordnen zu können. Mit dem Erstellen eines Benutzers wird automatisch ein Schlüsselpaar in Form von einem privaten und einem öffentlichen Schlüssel erstellt. Der öffentliche Schlüssel wird mit dem eigentlichen Benutzerprofil in der Datenbank in den Daten des Benutzers (siehe Abbildung 4) abgespeichert und hinterlegt. Der private Schlüssel wird in einer separaten Textdatei zusammen mit dem öffentlichen Schlüssel geschrieben. Diese Textdatei muss dann an den Benutzer gesendet werden, damit er seinen privaten und öffentlichen Schlüssel kennt und somit die Infrastruktur verwenden kann. Dieser muss beide Schlüssel bei dem Login angeben, sodass einige JavaScript Funktionen im Browser eine Smartcard simulieren können.

Der verschlüsselte Gesamtschlüssel wird bei der ersten Erstellung der ersten Lizenz generiert und kann die Gesamtverschlüsselung (siehe Abbildung 3) der Patientendaten entschlüsseln. Er ist ein verschlüsselter symmetrischer Schlüssel, welcher mit dem öffentlichen Schlüssel des Inhaltsservers verschlüsselt wurde. Der Schlüssel ist in der Lage die Gesamtverschlüsselung der gesamten Mappe zu entschlüsseln, er begrenzt sich also nicht nur auf den referenzierten Aktenteil. Somit ist es nicht nötig, den Schlüssel an die Lizenz zu binden, sondern kann direkt mit den Patientendaten des Besitzers der Akte gelagert werden. Eine Patientenakte hat also einen Gesamtschlüssel, welcher für alle Lizenzen in Bezug auf diese Akte gilt.

Das Passwort für das Benutzerkonto wird zufällig bei der Erstellung des Kontos generiert und sollte dann möglichst sicher an den Eigentümer übermittelt werden. Dieses kann der Benutzer nach erstmaliger Anmeldung beliebig ändern. Es wird lediglich der Hash des Passwortes gespeichert. Bei der Anmeldung des Benutzers erzeugt die Clientwebanwendung den Hash aus dem Passwort und sendet diesen zum Server, um dort mit dem gespeicherten Hash des Passwortes des Benutzerkontos verglichen zu werden.

Die Aktennummer ist eindeutig und kann nur einem Benutzer gehören, diese verweist auf die eigentliche elektronische Patientenakte mit den verschlüsselten Inhalten. Die Aktennummer wird durch die Identifikationsnummer des Benutzers repräsentiert und ist somit eindeutig.

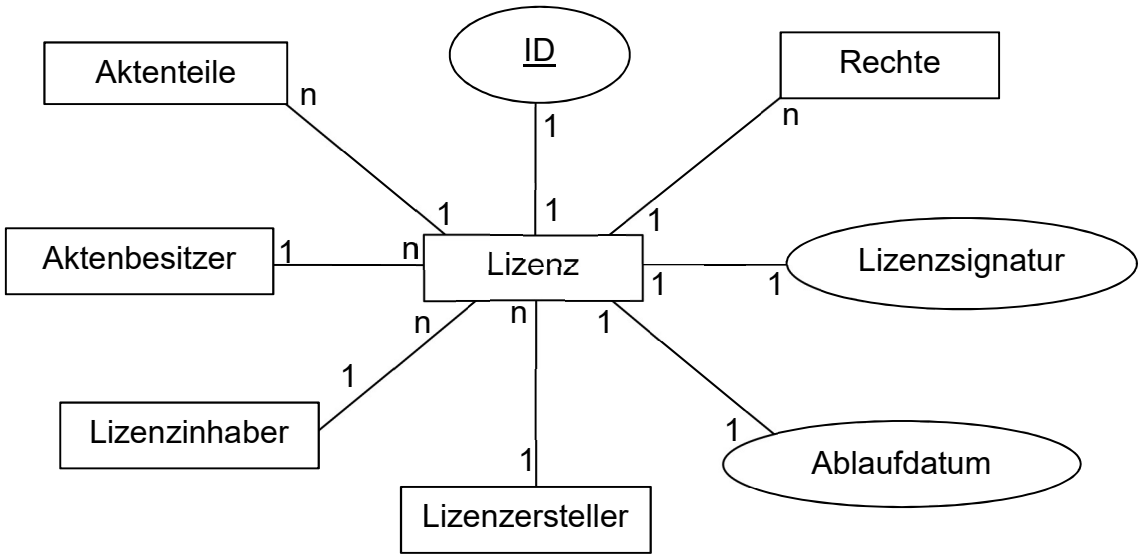

Abbildung 6 - ERM Lizenz

Eine Lizenz beinhaltet alle variablen Parameter, die für die Interpretation der Lizenz notwendig sind (im Folgenden auch als Lizenzattribute bezeichnet). Zusätzlich beinhaltet die Lizenz die Signatur des Lizenzerstellers von den Lizenzattributen. Die Lizenzattribute sind Aktenbesitzer, Lizenzinhaber, Lizenzersteller, Ablaufdatum, Aktenteile und Rechte. Um die Integrität der Lizenzattribute zu sichern, muss der Lizenzersteller diese zusätzlich mit seinem privaten Schlüssel signieren. Das in Abbildung 6 gezeigte Modell stellt die Lizenz dar, sie enthält die Lizenzattribute und die Signatur des Lizenzerstellers. Eine Lizenz kann aber in verschiedenen Formen auftreten. Sie kann sowohl als Objekt vorkommen, welches alle Lizenzattribute und die Signatur beinhaltet, aber auch in anderen Formen, aus denen die einzelnen Teile der Lizenz entnommen und interpretiert werden können, solange die Signatur des Erstellers und die Lizenzattribute gültig sind.

Das Datenbankmodel der Lizenz (siehe Abbildung 6) identifiziert sich eindeutig durch ihre ID. Dies vereinfacht die Handhabung der Lizenzen in der Datenbank.

Der Aktenbesitzer ist ein Benutzer (siehe Abbildung 5) und referenziert den Besitzer der Patientenakte, für die diese Lizenz gültig ist.

Der Lizenzinhaber kann ein Arzt aber auch ein anderer Beteiligter sein und wird durch den Namen des Benutzerobjektes (siehe Abbildung 5) bestimmt. Der Lizenzinhaber ist der Benutzer für den die Lizenz ausgestellt wurde. Er kann die Lizenz verwenden. Der

Aktenbesitzer kann mit demselben Lizenzinhaber in der Datenbank mehrmals vorkommen, da jemand gegebenenfalls derselben Person unterschiedliche Rechte beziehungsweise Ablaufzeiten auf verschiedene Teile seiner Akte gewähren möchte.

Zusätzlich zu dem Lizenzinhaber und dem Aktenbesitzer, gibt es noch den Lizenzersteller, welcher immer der Benutzer ist, der die Lizenz erstellt und signiert hat. Die Lizenzsignatur wird mit öffentlichen Schlüssel des Lizenzerstellers überprüft.

Der Bezug zwischen dem Benutzer (siehe Abbildung 5) und der Lizenz (siehe Abbildung 6) besteht über die Lizenzattribute Aktenbesitzer, Lizenzersteller und Lizenzbesitzer. Diese sind alle Benutzerobjekte und können, jeweils beliebig variieren. Jeder Benutzer kann beliebig viele Lizenzen besitzen, ebenso kann er beliebig viele Lizenzen ausstellen oder selbst der Aktenbesitzer sein.

Der Ablaufzeitpunkt bestimmt, wie lange die Lizenz gültig ist. Sie setzt sich aus dem Datum des Tages und der Uhrzeit des Ablauftermins zusammen.

Die Aktenteile beschreiben, für welche Teile der Patientenakte die Lizenz gültig ist. Dieses hat Attribute wie zum Beispiel „Impfpass“ oder „Akute Erkrankungen“. Die Aktenteile können je nach Belieben erweitert werden, um so die Akte des Patienten weiter zu gestalten. Hierfür ist ein extra Objekt angelegt, welches lediglich den Namen des Aktenteiles enthält. Somit können diese Objekte den Lizenzen mehrfach und einheitlich zugeordnet werden.

Die Rechte beschreiben die Nutzerbefugnisse des Lizenzinhabers und können einen oder mehrere der Attribute „Schreiben“, „Lesen“ oder „Lizenzen“ beinhalten. Die Rechte sind wie die Aktenteile als ein separates Objekt angelegt, damit diese nach Belieben erweitert und den einzelnen Lizenzen mehrfach und einheitlich zugeordnet werden können.

Die Lizenzsignatur setzt sich aus der Signatur von allen Lizenzattributen der Lizenz zusammen. Diese hat den Zweck, die Integrität der Lizenz sicherzustellen. Signiert wird ein String zusammengesetzt aus allen Lizenzattributen der Lizenz. Die beiden Attribute Aktenteile und Rechte werden in der Lizenz ausgeschrieben und jeweils dessen Attribute mit einem Komma getrennt. So wird zum Beispiel bei einer Lizenz, wel-

che die Rechte Lesen und Schreiben beinhalten soll, die Zeichenkette „Lesen,Schreiben“ verwendet. Damit die verschiedenen Lizenzattribute der Lizenz klar unterschieden werden können, werden diese mit einem „&“-Zeichen getrennt. So lassen sich die einzelnen Attribute der Lizenz leicht herausfiltern, indem die Server den String in verschiedene Segmente unterteilt, welche dem Lizenzobjekt nach einer festgelegten Reihenfolge zugeordnet werden können.

Ein gültiger Signaturstring kann wie folgt aussehen:

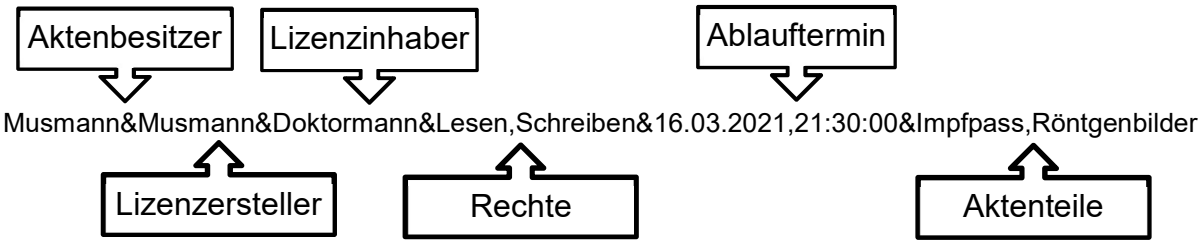

Abbildung 7 - Gültige Lizenzzeichenkette mit Beschreibung

Mit der Lizenzzeichenkette (siehe Abbildung 7) und einer gültigen Signatur (zusammen entspricht dies einer Lizenz) kann Herr Doktormann auf Wunsch des Lizenzerstellers den Impfpass und die Röntgenbilder der vom Patienten Herrn Musmann bis zum 16.03.2021 21:30 Uhr lesen und bearbeiten. Jedes Lizenzattribut und die Signatur des Erstellers werden einzeln in der Datenbank aufgeführt. Bei der Überprüfung der Signatur wird der Signaturstring zusammensetzt. Es ist zu beachten, dass bei der Zusammensetzung der Zeichenkette immer dieselbe festgelegte Reihenfolge und Schreibweise verwendet wird, damit die Überprüfung der Signaturen richtig und genormt ablaufen kann. Wird die Zeichenkette nicht richtig zusammengesetzt, wird die Gültigkeit der Lizenz bei der Überprüfung der Signatur für nichtig erklärt, selbst wenn die Attribute zu der Signatur passen.

Jedes Objekt, aus denen alle Lizenzattribute entnommen und eine Lizenzzeichenkette erstellt werden kann, gilt zusammen mit einer gültigen Signatur von dem Lizenzersteller als Lizenz. Auch die Lizenzzeichenkette selbst zusammen mit der passenden Signatur wird als Lizenz bezeichnet.

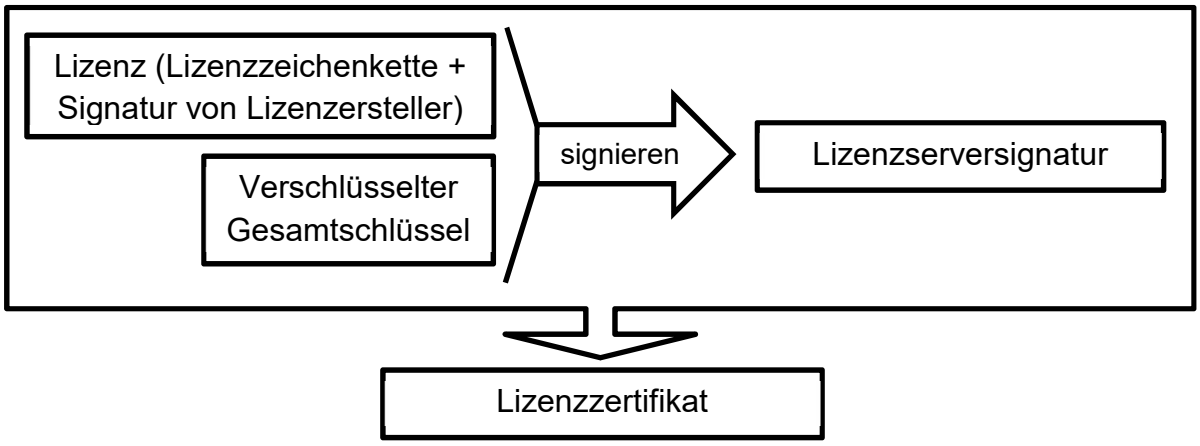

Abbildung 8 - Aufbau Lizenzzertifikat

Die Lizenz muss zu einem Lizenzzertifikat (siehe Abbildung 8) ergänzt werden, damit der Benutzer dieses bei dem Inhaltsserver verwenden kann. Die aus Abbildung 7 gezeigte Zeichenkette ist zusammen mit der Signatur des Lizenzerstellers eine gültige Lizenz, muss aber zusätzlich von dem Lizenzserver bestätigt werden. Die Tatsache, dass die Lizenz von dem Lizenzserver überprüft wurde, wird durch das Lizenzzertifikat bestätigt. Das Lizenzzertifikat setzt sich zusammen aus der Lizenz in Kombination mit dem entsprechenden verschlüsselten Gesamtschlüssel. Zusätzlich muss der Lizenzserver den Lizenzstring bilden, den verschlüsselten Gesamtschlüssel anhängen, das Resultat mit seinem privaten Schlüssel signieren und die Signatur anhängen. Die Lizenz zusammen mit dem verschlüsselten Gesamtschlüssel und der Signatur des Lizenzservers bilden das Lizenzzertifikat (siehe Abbildung 8). Auch bei dem Lizenzzertifikat ist das Format irrelevant, solange die Server die Attribute des Objektes so zusammensetzen können, dass am Ende eine gültige Signatur überprüft werden kann.

5.1.2 Der Inhaltsserver

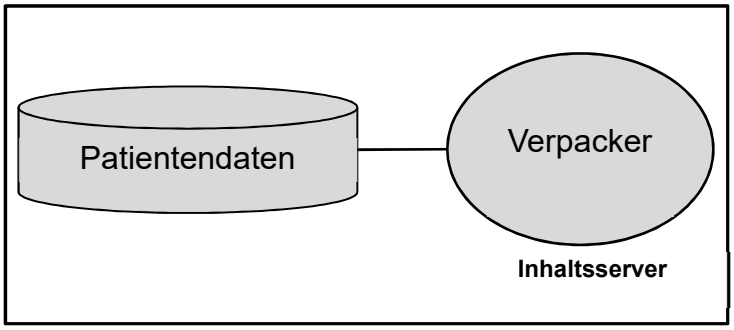

Abbildung 9 - Aufbau Inhaltsserver

Der Inhaltsserver beinhaltet den Inhalt der Akten von den Patienten in verschlüsselter Form, wie in Abbildung 3 beschrieben, kann diesen aber selbst nicht lesen. Er ist ein Django REST API Server und kann verschiedene Aufgaben, welche zum Lesen oder Bearbeiten der Akte relevant sind, erfüllen.

Der Rest API Server ist ein eigener Server getrennt von dem Lizenzserver. Diese können miteinander kommunizieren. Durch die getrennte und unabhängige Betrachtung des Layouts können auf analytischer Ebene mehr Informationen aus der Infrastruktur des Prototyps bezogen werden. Ebenso sollen die Aufgaben klar strukturiert sein. Der Inhaltsserver soll lediglich die eintreffenden Lizenzzertifikate überprüfen und insofern diese gültig sind, die entsprechenden Daten ausgeben oder einspeichern.

Diese Funktionen lassen sich mithilfe von POST oder GET HTTP Anfragen ansprechen. Es wird bei dem Inhaltsserver keine Authentifikation mittels Login benötigt und somit können die Funktionen der REST API direkt genutzt werden. Der Benutzer der Webanwendung muss sich lediglich bei dem Lizenzserver anmelden. Wie in Abbildung 9 visualisiert, besteht der Server aus dem Verpacker und der Datenbank. Der Verpacker kümmert sich darum, eingehende Anfragen zu bearbeiten, mit der Datenbank zu interagieren und entsprechende Rückmeldung an den Anfragenden zu senden. Bei dem Inhaltsserver müssen alle Benutzer registriert und dessen öffentliche Schlüssel in die Datenbank eingetragen werden, die auch in dem Lizenzserver aufgeführt werden. Dies wird manuell über die von Django bereitgestellte Administrationsoberfläche getätigt. Hier wird der Benutzer mit dem dazugehörigen öffentlichen Schlüssel eingetragen und gespeichert.

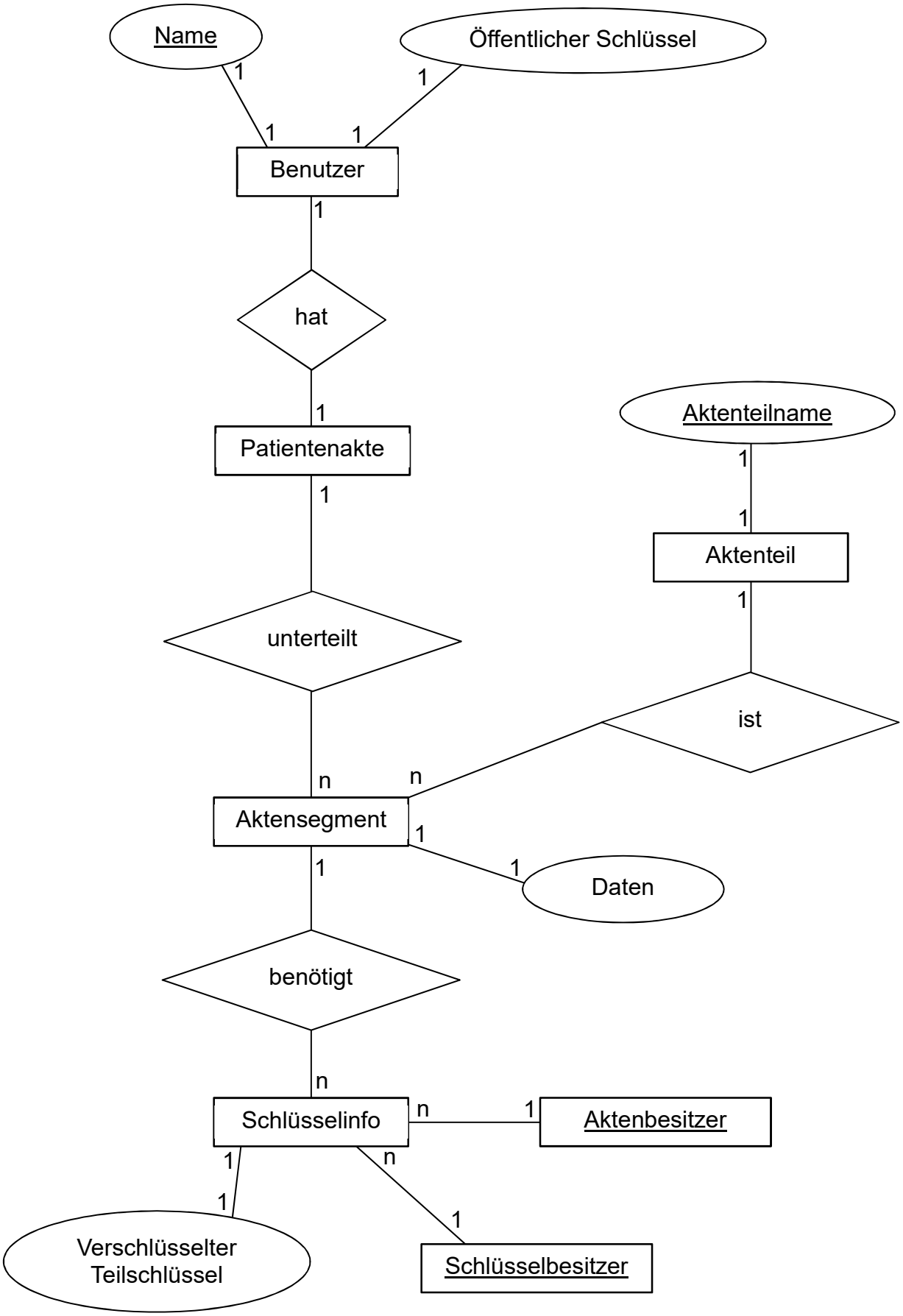

Abbildung 10 - ERM Patientendaten des Inhaltsservers

In der Datenbank des Inhaltsservers (siehe Abbildung 10) wird von dem einzelnen Benutzer lediglich der öffentliche Schlüssel und dessen Name gespeichert. Dies ist ausreichend, um später die Lizenzen zu verifizieren.

Im Prototyp ist der Benutzer an seine Patientenakte gebunden und ist dessen primärer Schlüssel. Ein Benutzer besitzt genau eine Patientenakte. Diese wird über den Benutzernamen identifiziert und kann hierrüber selektiert werden.

Die Patientenakte unterteilt sich nun in verschiedene Sektoren. Dies ermöglicht es, dem Urheber nur einzelne Teile seiner Akte freizugeben. In dem Prototyp sind zum Beispiel Teile wie „Impfpass“ oder „Akute Erkrankungen“ freigeschalten. Es ist aber auch möglich, auf diese Weise einzelne Dateien oder Dokumente aufzubewahren, indem der IT-Beauftragte diese als Aktenteile einträgt. Das Aktenteil ist ein Modelobjekt, welches lediglich den Namen von dem Aktensegment selbst enthält. Dies ist gleichzustellen mit dem Aktenteil Objekt von dem Lizenzserver, diese müssen immer auf beiden Servern gleich sein, damit keine Lizenzen ausgestellt werden, die bei dem Inhaltsserver keinen Inhalt finden. Das Aktensegment beinhaltete alle Informationen, die für das Nutzen der Patientenakte relevant sind. Sie unterteilen die Akte in verschiedene Teile und können für jedes existierende Aktenteil einmal für einen Patienten angelegt werden. Die verschlüsselten Daten selbst (siehe Abbildung 3) sind nun in dem Attribut mit dem Namen Daten in dem Aktensegment gespeichert. Hier werden die Nutzinformationen für das Segment gespeichert. Diese sind mehrfach verschlüsselt und können nur von befugten Nutzern entschlüsselt werden.

Damit ein befugter Nutzer die Daten entschlüsseln kann, benötigt er zusätzlich die Schlüsselinfo. Sie setzt sich aus dem Schlüsselbesitzer und dem verschlüsselten Teilschlüssel zusammen, mit dessen Hilfe der Lizenzinhaber die Teilverschlüsselung (siehe Abbildung 3) entschlüsseln kann. Der Schlüsselbesitzer ist ein Benutzer, für den es für diesen spezifischen Aktenteil des Aktenbesitzers eine gültige Lizenz (er ist somit der Lizenzinhaber) im Lizenzserver existiert. Ein Aktensegment kann zudem beliebig viele Schlüsselinfos besitzen, da es für die Akte beliebig viele Lizenzträger geben kann. Jeder Lizenzträger kann maximal für einen Aktenteil der Patientenakte eines Patienten eine Schlüsselinfo besitzen. Diese Schlüsselinfo referenziert sich auf einen

Lizenzinhaber und kann nicht von jemand anderem verwendet werden. Der verschlüsselte Teilschlüssel kann nur mit dem privaten Schlüssel des Lizenzinhabers (welcher immer der Schlüsselbesitzer ist) entschlüsselt werden.

5.1.3 Die Clientwebanwendung

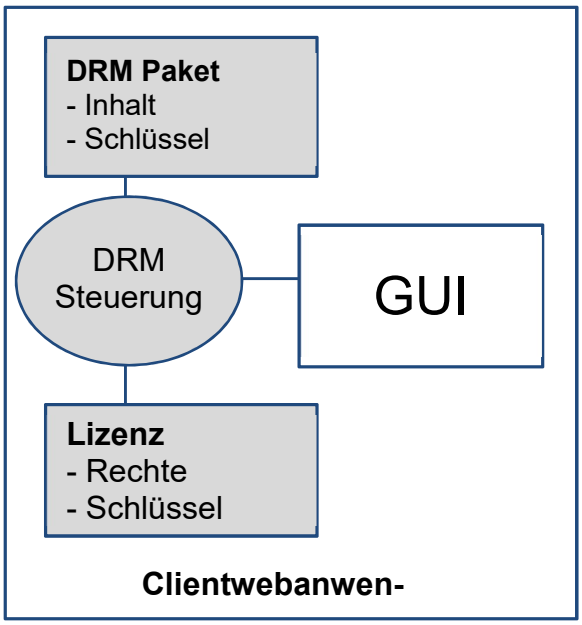

Abbildung 11 - Übersicht Clientwebanwendung

Die Clientwebanwendung ist eine Website, welche von dem Lizenzserver gestellt wird. Sie wird im Folgenden auch als Patientenakten-Verwaltungssystem bezeichnet werden. Sie besteht aus der grafischen Benutzeroberfläche und im Hintergrund verknüpfte JavaScript Funktionen, welche die DRM Steuerung darstellen (siehe Abbildung 11). Die JavaScript Funktionen realisieren die Kommunikation mit dem Inhaltsserver und ermöglichen das Verschlüsseln und Entschlüsseln von Patientendaten, um diese anschließend zu visualisieren oder bei Bedarf an den Inhaltsserver zu senden.

Bei dem Login wird neben dem Loginnamen und dem Passwort der private und der öffentliche Schlüssel des Benutzers verlangt. Um Lizenzen und somit die Anwendung zu nutzen, müssen diese Schlüssel richtig eingegeben werden. Beide Schlüssel werden in dem Session-Storage der Anwendung gespeichert. Diese werden verwendet, um die Smartcard zu simulieren, welche zum Entschlüsseln, Verschlüsseln und signieren von Daten und somit zum Erstellen von Lizenzen relevant sind. Das Patientenakten-Verwaltungssystem ist das Bindeglied zwischen Lizenzserver und Inhaltsserver. Sie erstellt die Lizenzen und fordert die Lizenzzertifikate bei dem Lizenzserver an. Hat

sie die Lizenz, werden die Daten von dem Inhaltsserver angefragt und mithilfe des Lizenzzertifikates entschlüsselt.

6 Evaluation

6.1 Funktionsanalyse der Use-Cases

Nun werden die verschiedenen Anwenderfälle geschildert und veranschaulicht. Hier wird auf die Einzelheiten der verschiedenen Server und der Clientwebanwendung eingegangen, um die Funktionalität des Digital Rights Management Systems zu erklären.

6.1.1 Einloggen in das Patientenakten-Verwaltungssystem

Möchte sich der Benutzer in das Patientenakten-Verwaltungssystem einloggen, muss er zunächst ein Benutzerkonto beantragen.

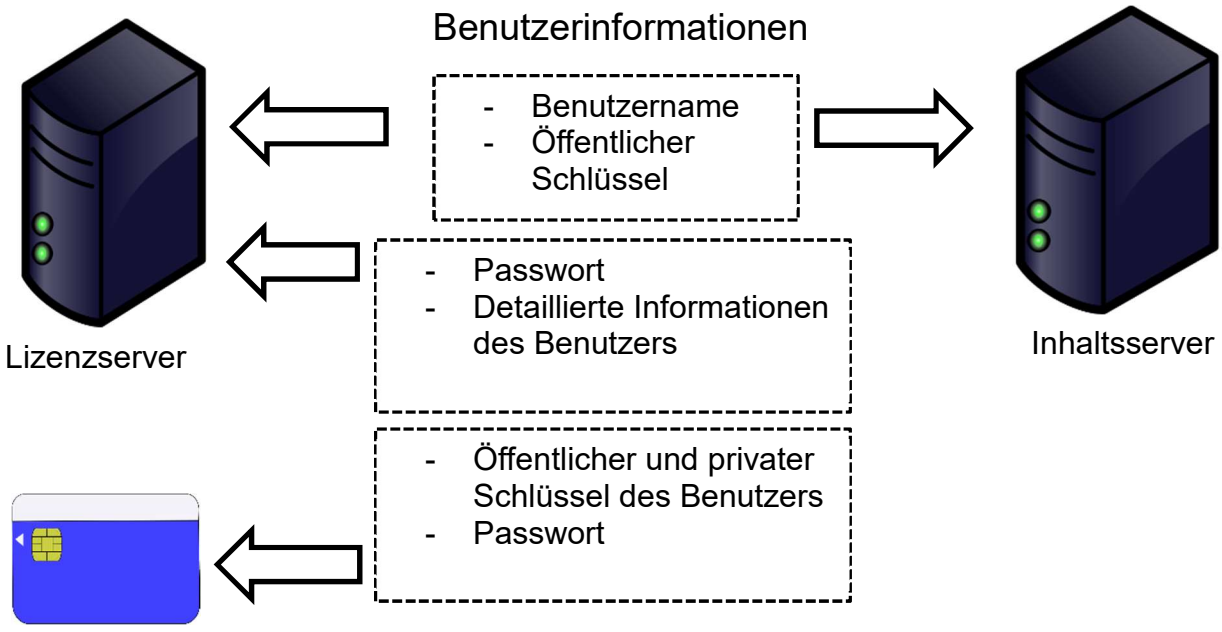

Abbildung 12 - Speicherorte der benutzerbezogenen Informationen

Dieser muss dem Betreiber der Infrastruktur seinen gewünschten Benutzernamen mitteilen. Daraufhin generiert der Lizenzserver alle weitere nötigen Benutzerinformationen. Die Pfeile in Abbildung 12 weisen auf den Speicherort der Benutzerinformationen hin. Bei der Erstellung des Benutzerkontos wird ein öffentlicher und ein privater Schlüssel generiert. In der Praxis würden diese in eine Smartcard integriert werden. Der Prototyp speichert diese in eine Textdatei ab. Der öffentliche Schlüssel wird zusammen mit dem Benutzernamen in dem Inhaltsserver und dem Lizenzserver jeweils in einem

neuen Benutzerobjekt gespeichert. Das zufällig generierte Passwort zusammen mit detaillierten Informationen wie zum Beispiel der E-Mail-Adresse des Benutzers wird in dem Lizenzserver gespeichert. Nach Abschluss dieses Prozesses muss der Betreiber der Infrastruktur dem Benutzer die Smartcard beziehungsweise die Textdatei und den Benutzernamen mit dem Passwort zukommen lassen.

Nachdem der Benutzer diese erhalten hat, kann er sich bei dem Patientenakten-Verwaltungssystem anmelden. Im Login gibt er seinen Benutzernamen, Passwort und öffentlichen und privaten Schlüssel an. Hier erstellt die Clientwebanwendung ein Login-Cookie, mit dessen Hilfe sich die Anwendung bei dem Lizenzserver verifizieren kann.

Bei jeder Verbindung zu dem Lizenzserver ist vorausgesetzt, dass der Benutzer eingeloggt ist. Dies bedeutet, es wurde ein Login-Cookie mit den entsprechenden Daten erstellt und im Webbrowser gespeichert, um sich bei wiederholten Anfragen zu authentifizieren. Möchte der Webclient Funktionen des Lizenzservers nutzen, wird jedes Mal dieses Cookie zu dem Server mitgeschickt und überprüft. Bei dem Inhaltsserver ist keine Überprüfung des Logins notwendig, da hier andere Sicherheitsmechanismen greifen, um die Daten der Patienten zu schützen.

In allen anderen Use-Cases ist der Benutzer eingeloggt und die Anwendung kann sich über das erstellte Login-Cookie bei jeder Anfrage an den Lizenzserver authentifizieren. Es wird nicht mehr explizit erwähnt oder in den Grafiken gezeigt.

6.1.2 Erstellung der Akte

Bei dem erstmaligen Einloggen des Benutzers in das Patientenakten-Verwaltungssystem muss er zunächst seine eigene Patientenakte anlegen und erstellen. Er besitzt zwar schon ein Benutzerkonto, hat aber noch keine Patientenakte. Zu diesem Zeitpunkt sind lediglich die Benutzerdaten auf dem Lizenzserver und auf dem Inhaltsserver zusammen mit seinem öffentlichen Schlüssel vorhanden.

Um eine Akte zu erstellen, muss eine initiale Lizenz von dem eingeloggten Benutzer (der Lizenzersteller) erzeugt werden. Diese wird an den Lizenzserver gesendet. Hier wird bei einer gültigen Lizenz ein Gesamtschlüssel generiert, mit dem öffentlichen Schlüssel des Inhaltsservers verschlüsselt und zusammen mit der initialen Lizenz signiert. Es entsteht das Lizenzzertifikat (siehe Abbildung 8). Das Lizenzzertifikat wird anschließend zurückgesendet. Daraufhin generiert die Clientwebanwendung für jeden

Aktenteil, den es geben soll, einen neuen Teilschlüssel und pseudo Daten, welche mit den Teilschlüsseln verschlüsselt werden. Die Teilschlüssel werden mit dem eigenen öffentlichen Schlüssel verschlüsselt und zusammen mit den verschlüsselten Pseudodaten und dem Lizenzzertifikat an den Inhaltsserver gesendet. Dieser validiert das Lizenzzertifikat und legt bei Gültigkeit die Patientenakte auf dem Inhaltsserver an.

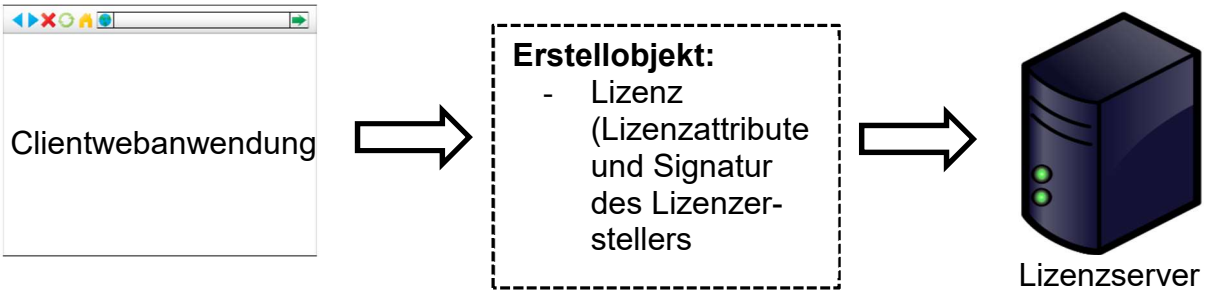

Abbildung 13 - Übersicht der ersten Anfrage zu der Erstellung einer Patientenakte

Der erste Schritt, um sich seine Akte zu erstellen, ist, dass der eingeloggte Benutzer eine Initiale Lizenz generiert. In dieser Lizenz kann der Benutzer die Lizenzattribute frei wählen. Er kann mit dem Lizenzattribut „Lizenzinhaber“ festlegen, wer vollen Zugriff auf seine Patientenakte haben soll. Selektiert er sich selbst, kann er weiterhin mit seiner Akte arbeiten. Wählt er jemand anderen, kann er solange nicht auf seine Akte zugreifen, bis die gewählte Person dem Patienten selbst eine Lizenz mit vollen Rechten ausstellt. Dies wäre zum Beispiel im Falle einer Vormundschaft nötig, damit der Vormund vollen Zugriff über die Patientenakte besitzt. Sind alle Lizenzattribute der Lizenz ausgewählt, werden diese mit dem privaten Schlüssel des Benutzers (dem Lizenzersteller) signiert und an den Lizenzserver gesendet (siehe Abbildung 13).

Auf dem Lizenzserver selbst wird nun die Lizenz mit dessen Signatur verifiziert, ob diese von dem eingeloggten Benutzer signiert wurde und überprüft, ob es sich bei der Erstellung der Lizenz um das erste Mal handelt. Gibt es bei beiden Abfragen ein positives Resultat, kann die Lizenz im Lizenzserver gespeichert werden.

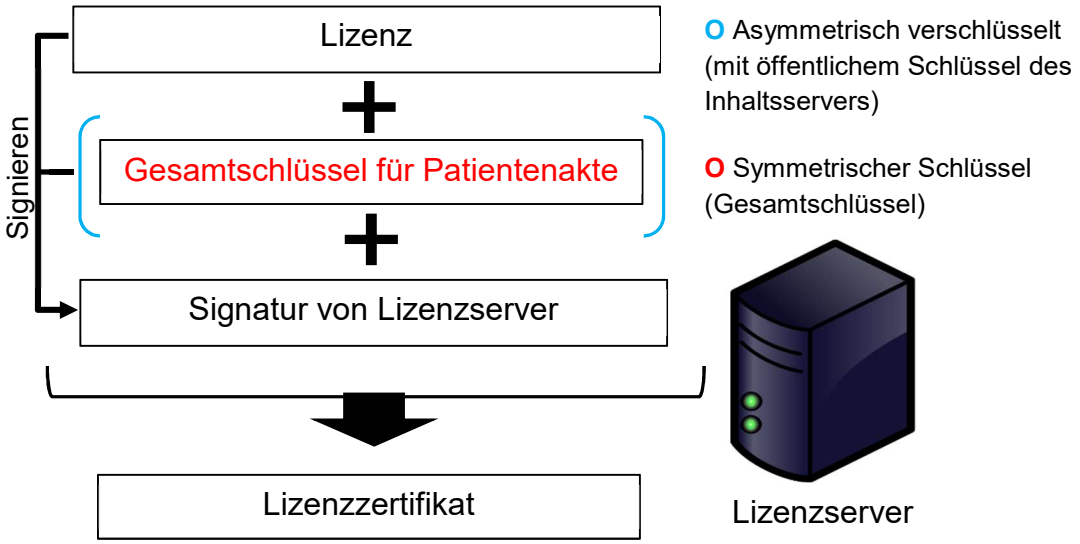

Abbildung 14- Zusammensetzung eines Lizenzzertifikates

Der Lizenzserver speichert gültige Lizenzen und sendet bei dessen Abfragen gültige Lizenzzertifikate zurück an den Benutzer. Auch bei der Erstellung der Patientenakte wird nach der Validierung der initialen Lizenz, die Lizenz in der Datenbank hinterlegt. Damit der Lizenzserver das Lizenzzertifikat erstellen kann, muss er zunächst den Gesamtschlüssel (symmetrischer Schlüssel) für die Patientenakte generieren. Den Gesamtschlüssel zu generieren, um ein Lizenzzertifikat auszustellen, wird lediglich im Erstellprozess der Akte benötigt, da es noch keinen Gesamtschlüssel für die Patientenakte des Benutzers gibt. Der Gesamtschlüssel wird zusätzlich mit dem öffentlichen Schlüssel des Inhaltsservers verschlüsselt und zusammen mit der initialen Lizenz signiert, um anschließend an den Benutzer als gültiges Lizenzzertifikat (siehe Abbildung 14) gesendet werden zu können.

Der Gesamtschlüssel gilt für die gesamte Patientenakte (siehe Abbildung 3). Es gibt somit immer nur einen gültigen verschlüsselten Gesamtschlüssel für die Patientenakte, dieser wird an das Objekt des Benutzers (der Aktenbesitzer) in der Datenbank referenziert. Die Lizenzzertifikate werden nicht in der Datenbank gespeichert, sondern werden bei jeder Anfrage dynamisch aus der entsprechenden Lizenz, dem verschlüsseltem Gesamtschlüssel und der Signatur des Lizenzservers erstellt.

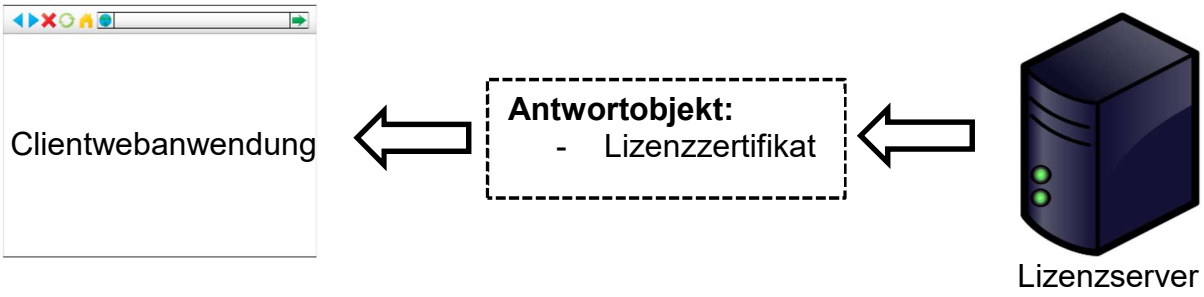

Abbildung 16 - Übersicht von der Antwort des Lizenzservers

Nach dem Erhalt des Datenpaketes (siehe Abbildung 15) bestehend aus dem gültigen Lizenzzertifikat, wird es temporär in der Webanwendung gespeichert. Um nun die eigentliche Patientenakte zu erstellen, muss die Anwendung alle verfügbaren Aktenteile kennen. Hierfür fragt die Clientwebanwendung bei dem Inhaltsserver und dessen REST API nach allen verfügbaren Aktenteilen. Diese stehen bei dem Inhaltsserver öffentlich zur Verfügung und kann von jedem abgefragt werden.

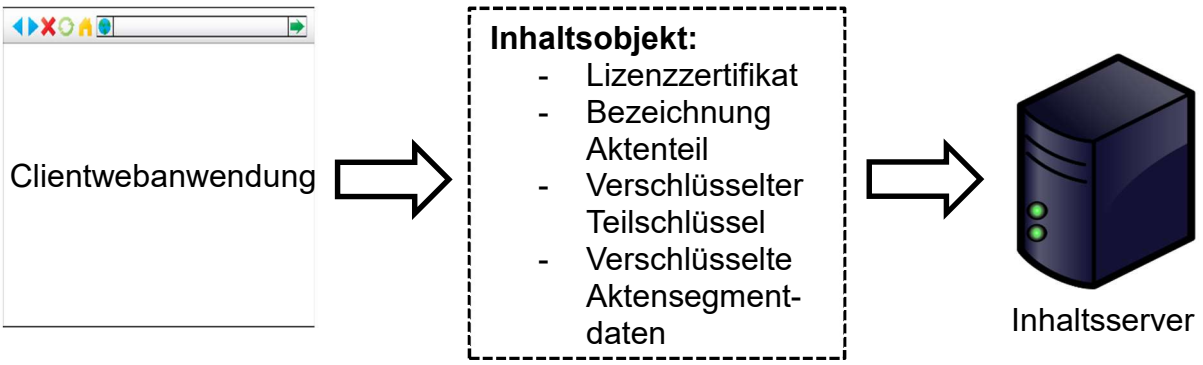

Abbildung 15 - Übersicht des Zyklus um ein Aktenteil am Inhaltsserver anzulegen

Kennt die Clientwebanwendung die Namen aller möglichen Aktenteile, wird für jeden einzelnen Aktenteil ein eigenes Anfrageobjekt erstellt. Damit der Inhaltsserver die Informationen in den Aktensegmenten nicht lesen kann, müssen die einzelnen Daten der Aktensegmente verschlüsselt werden. Hierfür wird die symmetrische Verschlüsselung verwendet. Die symmetrischen Schlüssel werden zufällig generiert. Diese Schlüssel werden im Folgenden als Teilschlüssel bezeichnet und können die Teilverschlüsselung (siehe Abbildung 3) entschlüsseln. Des Weiteren wird die Bezeichnung des Aktensegmentes als Zeichenkette mit dem Teilschlüssel verschlüsselt. Dies dient dem Zweck, um einen Pseudoeintrag in der Akte zu generieren, damit diese nicht leer ist. Nur wer den Teilschlüssel für das Aktensegment kennt, kann die Daten entschlüsseln.

Damit die Teilschlüssel nicht im Klartext auf dem Inhaltsserver gespeichert werden, ist es notwendig, diese einzeln zu verschlüsseln. Dies geschieht über asymmetrische

Verschlüsselung mit dem öffentlichen Schlüssel des Benutzers (dem Lizenzersteller). Folgernd kann nur der Ersteller selbst, welcher den privaten Schlüssel besitzt, den verschlüsselten Teilschlüssel entschlüsseln, um ihn zu nutzen. Für jeden Aktenteil wird ein solches individuelle Anfrageobjekt (siehe Abbildung 16) erstellt und an den Inhaltsserver gesendet.

Der Inhaltsserver empfängt jede Anfrage einzeln. Zunächst überprüft und verifiziert er das Lizenzzertifikat (Abbildung 14). Er kontrolliert die Signaturen von dem Lizenzersteller und von dem Lizenzserver. Die öffentlichen Schlüssel aller Benutzer sind in der Datenbank hinterlegt und der Name des Lizenzerstellers ist in dem Lizenzzertifikat aufgeführt und kann somit zugeordnet werden. Stimmen die Signaturen, werden die Rechte des Lizenzträgers mit den Rechten, welche für die Durchführung der aktuellen Funktion, das Erstellen der Akte nötig sind, verglichen. Um eine Akte zu erstellen muss der Lizenzträger alle verfügbaren Rechte besitzen. Außerdem wird der Ablaufzeitpunkt überprüft und bestimmt, ob das Lizenzzertifikat noch gültig ist. Zusätzlich muss auch der Aktenteil, welcher in der Anfrage aufgeführt und erstellt werden soll, in dem Lizenzzertifikat aufgelistet sein.

Erfüllt das Lizenzzertifikat des Inhaltsobjektes alle Kriterien, kann des spezifische Aktensegment (siehe Abbildung 10) im Inhaltsserver erstellt werden. Dieses wird an die Patientenakte des Patienten angehängt. Das Aktensegment besteht aus dem Namen des Aktenteils und den verschlüsselten Daten, welche von dem Benutzer mitgesendet wurden.

Die verschlüsselten Daten sind die verschlüsselten Aktensegmentdaten (siehe Abbildung 16), welche von dem Inhaltsserver ein zweites Mal verschlüsselt wurden. Hierfür benötigt der Inhaltsserver den Gesamtschlüssel der Akte. Dieser ist verschlüsselt in dem Lizenzzertifikat eingebunden. Der Inhaltsserver kann diesen mit seinem privaten Schlüssel entschlüsseln und benutzen. Bevor der Server die verschlüsselten Daten ein zweites Mal verschlüsselt, hängt er den Namen des Aktenteils vor den eigentlichen teilverschlüsselten Daten. Der Aktenteilname und die verschlüsselten Datenteilinhalte werden dann mit dem entschlüsselten Gesamtschlüssel symmetrisch verschlüsselt. Das Davorhängen eines Strings, welcher dem Inhaltsserver bekannt ist, hat den Zweck zu überprüfen, ob bei der nächsten Anfrage der mitgelieferte Gesamtschlüssel der

richtige ist. Somit muss bei der Gesamtentschlüsselung der Daten, bei einem korrekten Gesamtschlüssel wieder der Name des Aktenteiles als erster Bestandteil Zeichenkette vorliegen.

Damit der Lizenzträger zu einem späteren Zeitpunkt wieder auf seinen verschlüsselten Teilschlüssel zugreifen kann, wird eine Schlüsselinfo (siehe Abbildung 10) von dem Inhaltsserver erstellt, welche auf das Aktensegment verweist. Die Schlüsselinfo beinhaltet den Aktenteilnamen, den Schlüsselbesitzer, welcher als Lizenzträger in dem Lizenzzertifikat herauszulesen ist und den verschlüsselten Teilschlüssel.

Die Clientanwendung sendet so viele Anfragen (siehe „Inhaltsobjekte“ der Abbildung 16), bis alle Aktensegmente erstellt wurden. Resultierend sollten in dem Inhaltsserver für jedes verfügbare Aktenteil ein Aktensegment und jeweils eine Schlüsselinfo vorliegen. Ist dieser Vorgang abgeschlossen, ist die Patientenakte verfügbar und bereit zur Verwendung. Die Erstellung der Akte ist somit abgeschlossen.

6.1.3 Ausstellen von Lizenzen

In diesem Use-Case möchte nun der Benutzer eine Lizenz an jemand anderen ausstellen, wie zum Beispiel an seinen Hausarzt, damit dieser die Akte lesen und bearbeiten kann.

Vorausgesetzt ist, dass der Benutzer in das Patientenakten-Verwaltungssystem eingeloggt ist und bereits seine Patientenakte erstellt hat. Zudem muss der Arzt auch in dem System registriert sein.

Im Allgemeinen werden Lizenzen ausgestellt, indem der Benutzer eine Lizenz ausfüllt, erstellt und diese dem Lizenzserver präsentiert. Dieser entscheidet, ob er das Recht besitzt, Lizenzen für die Patientenakte des eingetragenen Aktenbesitzers zu erstellen. Ist dies der Fall, speichert er die gültige Lizenz und der Benutzer erhält ein gültiges Lizenzzertifikat als Antwort. Hiermit kann er Anfragen an den Inhaltsserver senden, um so die verschlüsselten Teilschlüssel zu erhalten, welche er entschlüsseln und wieder mit dem öffentlichen Schlüssel des neuen Lizenzinhabers verschlüsseln kann. Diese werden zurück an den Inhaltsserver gesendet und als neue Schlüsselinfo für den neuen Lizenzinhaber gespeichert. Mit dem Lizenzzertifikat und den Schlüsselinfos kann dann der neue Lizenzinhaber alle nötigen Daten von dem Inhaltsserver abfragen und entschlüsseln.

Der erste Schritt um Lizenzen auszustellen, verlangt, dass der eingeloggte Benutzer das Recht „Lizenz“ für die Patientenakte des potentiellen Aktenbesitzers hat. Der Benutzer bekommt von dem Lizenzserver, welcher als Webserver fungiert, alle möglichen Lizenzattribute in Form von einem Formular aufgeführt, welche er auswählen kann, um eine gültige Lizenz zu erstellen. So kann er zum Beispiel bei der Erstellung der Lizenz in der Dropdown-Liste des Patientenfeldes sehen, für welche Benutzer er die Rechte hat, Lizenzen zu vergeben. In dem Formular kann der Ersteller nun alle gewünschten Optionen auswählen. Sind alle Felder ausgefüllt, muss der Lizenzersteller (der Benutzer) die Lizenzattribute signieren und die fertige Lizenz an den Lizenzserver senden. In Abbildung 13 wird die Anfrage bereits visualisiert und unterscheidet sich in diesem Schritt nicht von dem Verfahren, um eine Akte zu erstellen.

Der Lizenzserver muss nun validieren, ob der Lizenzersteller (der Benutzer) der Anfrage die nötigen Befugnisse besitzt, um eine Lizenz für den spezifischen Patienten zu erstellen. Hierfür werden in der Datenbank nach Lizenzen gesucht, bei denen der anfragende Benutzer als Lizenzträger und der Patient, für dessen Akte die Lizenz erstellt werden soll, als Aktenbesitzer eigetragen ist. Werden solche Lizenzen gefunden, wird überprüft, ob in einer Lizenz das Recht „Lizenz“ vorliegt. Dieses Lizenzzertifikat wird daraufhin selektiert. Es wird überprüft, ob die Signatur des Lizenzerstellers korrekt ist. Ist der Ablaufzeitpunkt noch nicht eingetreten, lässt sich daraus folgern, dass der anfragende Benutzer befugt ist, neue Lizenzen zu erstellen.

Die eingesendete Lizenz muss nun verifiziert werden. Hier wird bestimmt, ob alle Variablen der Lizenzattribute richtig ausgefüllt wurden und ob die Signatur des Lizenzerstellers richtig ist. Daraufhin erweitert der Lizenzserver die Lizenz zu einem Lizenzzertifikat (siehe Abbildung 14), indem der Lizenzserver die Lizenz zusammen mit dem entsprechenden verschlüsselten Gesamtschlüssel signiert.

Die gültige Lizenz wird in dem Lizenzserver gespeichert und das neue Lizenzzertifikat wird daraufhin wieder zurück an die Clientwebanwendung gesendet.

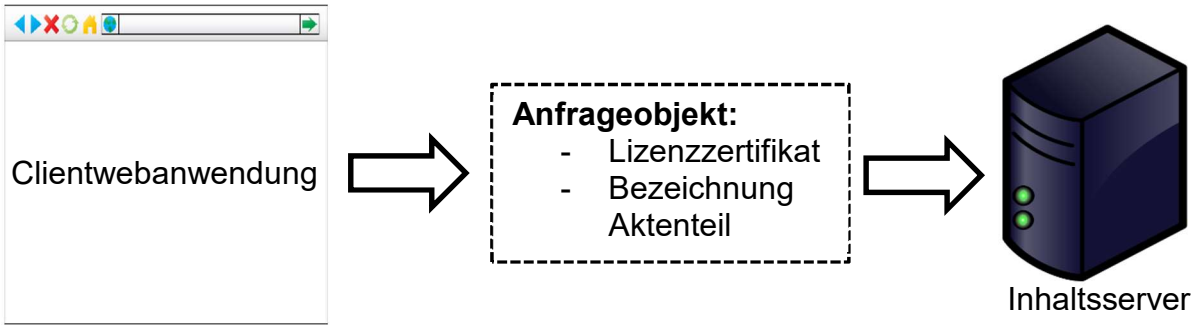

Abbildung 17 - Übersicht Erstellung von einer Lizenz

Um den neuen Lizenzinhaber auch dem Inhaltsserver mitzuteilen, muss ein neues Anfrageobjekt (siehe Abbildung 17) erstellt werden. Für jeden Aktenteil, der in dem Lizenzzertifikat gelistet ist, muss eine neue Anfrage erstellt werden.

Das Anfrageobjekt beinhaltet das neue Lizenzzertifikat und die Bezeichnung des Aktenteils für das der neue Lizenzinhaber angemeldet werden soll. Das Lizenzzertifikat wird entsprechend bei dem Inhaltsserver sowie bei der Erstellung einer Akte geprüft. Also werden Ablaufzeitpunkt, Rechte, Aktenteile und die Signaturen überprüft. Um eine Lizenz zu erstellen benötigt der Lizenzinhaber das Recht „Lizenz“.

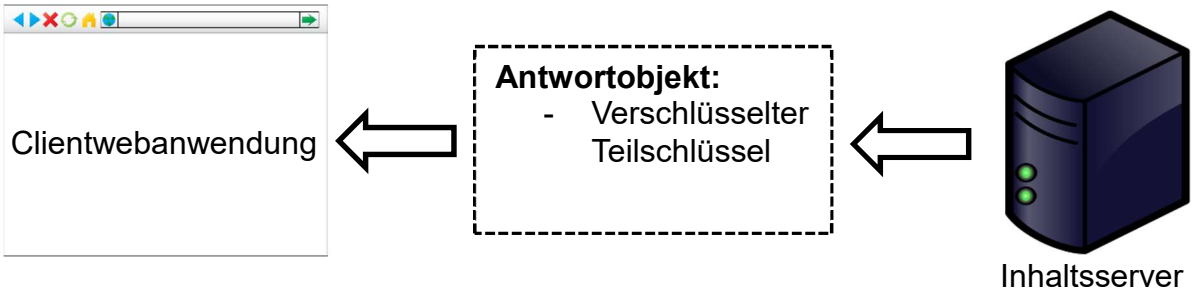

Abbildung 18 - Antwort des Inhaltsservers

Ist das Lizenzzertifikat gültig, selektiert der Inhaltsserver die entsprechende Schlüsselinfo des Lizenzerstellers (der Benutzer). Der verschlüsselte Teilschlüssel wird dann zurück an die Clientwebanwendung gesendet (Abbildung 18). Der Lizenzersteller besitzt den privaten Schlüssel, um den verschlüsselten Teilschlüssel zu entschlüsseln. Nach dem Entschlüsseln liegt der Teilschlüssel im Klartext in der Clientwebanwendung vor.

Damit der neue Lizenzinhaber diesen Schlüssel zu einem späteren Zeitpunkt von dem Inhaltsserver abfragen und entschlüsseln kann, wird dieser mit dem öffentlichen Schlüssel des neuen Lizenzinhabers verschlüsselt.

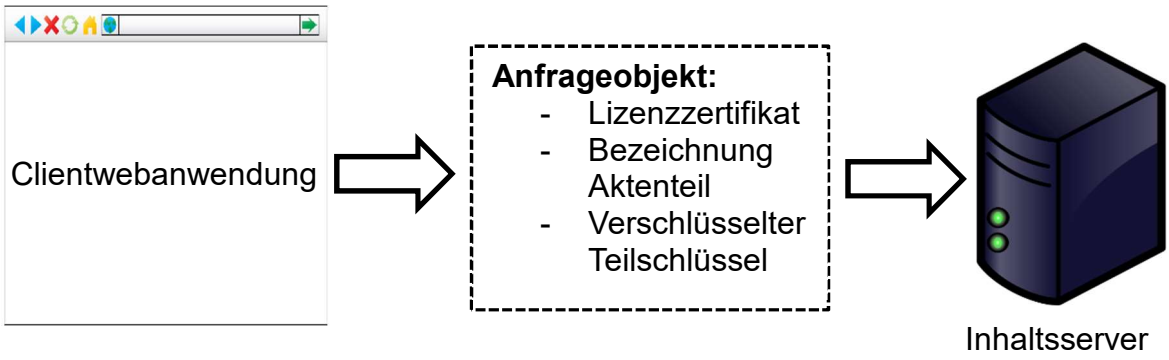

Abbildung 19 -Übersicht senden verschlüsselter Teilschlüssel

Der verschlüsselte Teilschlüssel von dem neuen Lizenzinhaber wird dann an den Inhaltsserver zusammen mit dem Lizenzzertifikat und der Bezeichnung des Aktenteils gesendet (siehe Abbildung 19). Der Inhaltsserver verifiziert das Lizenzzertifikat. Dieses muss dieselben Bedingungen erfüllen wie in der Anfrage zuvor (Abbildung 17).

Daraufhin speichert er bei Gültigkeit des Lizenzzertifikates den neuen verschlüsselten Teilschlüssel und den Namen des Schlüsselbesitzers als Schlüsselinfo zu den anderen Schlüsselinfos der Akte.

Wurde dieser Prozess für alle Aktenteile in dem Lizenzzertifikat abgeschlossen, kann der neue Benutzer sein Lizenzzertifikat von dem Lizenzserver Abfragen und bei dem Inhaltsserver verwenden.

6.1.4 Lesen und bearbeiten einer Akte

Das Bearbeiten einer Patientenakte beinhaltet alle nötigen Schritte des Lesezugriffs. Damit der Benutzer Daten verändern kann, muss er diese auch kennen, um diese anschließend bearbeiten zu können, somit muss zuerst die Akte gelesen und dann bearbeitet werden.

Im Allgemeinen fordert der Patient bei dem Lizenzserver ein Lizenzzertifikat an. Dieses leitet er weiter an den Inhaltsserver und fragt das gewünschte Aktensegment und seine dazugehörige Schlüsselinfo an. Die Gesamtverschlüsselung (siehe Abbildung 3) der Daten des Aktensegmentes wird von dem Inhaltsserver mit dem Gesamtschlüssel entschlüsselt. Mit der Schlüsselinfo kann der Benutzer die Teilverschlüsselung der Daten

des Aktensegmentes entschlüsseln und diese lesen. Hier kann er bei entsprechenden Rechten diese Daten bearbeiten, mit dem Teilschlüssel verschlüsseln und zusammen mit dem Lizenzzertifikat zurücksenden. Der Inhaltsserver verschlüsselt die Daten erneut mit dem Gesamtschlüssel und speichert diese ab.

Zu Beginn des Prozesses, um eine Patientenakte zu lesen, hat der eingeloggte Benutzer die Möglichkeit, in der Clientwebanwendung eine Liste mit allen Lizenzen, bei denen er selbst der Lizenzinhaber ist, einzusehen. Die Liste wird von dem Lizenzserver bereitgestellt und beinhaltet somit nur gültige Einträge.

Der Benutzer ist nun in der Lage, eine beliebige Lizenz auszuwählen, um diese zu nutzen. Hat der Benutzer sich entschieden, wird eine Anfrage an den Lizenzserver gesendet, um das Lizenzzertifikat anzufordern. Der Lizenzserver überprüft den Ablauftermin, die Signatur des Lizenzerstellers und signiert als Bestätigung die Lizenz zusammen mit dem verschlüsselten Gesamtschlüssel. Das hieraus erstellte gültige Lizenzzertifikat wird anschließend an die Clientwebanwendung gesendet.

Das Lizenzzertifikat wird in der Clientwebanwendung gespeichert. Hier kann nun der Benutzer entscheiden, welches Aktensegment er einsehen möchte. Er kann immer nur ein Aktensegment zur selben Zeit lesen und bearbeiten. Die zur Verfügung stehenden Aktenteilnamen kann die Clientwebanwendung aus dem Lizenzzertifikat entnehmen und somit dem Benutzer eine Auswahlmöglichkeit bieten.

So wie in Abbildung 17 visualisiert, wird eine Anfrage mit dem Lizenzzertifikat und dem gewählten Aktenteilnamen an den Inhaltsserver gesendet. Dieser überprüft das Lizenzzertifikat. Ist dieses gültig, selektiert der Inhaltsserver das passende Aktensegment. Um die Gesamtverschlüsselung (siehe Abbildung 3) zu entschlüsseln, muss der Inhaltsserver den mitgelieferten verschlüsselten Gesamtschlüssel entschlüsseln. Diesen kann er mit seinem privaten Schlüssel entschlüsseln. Kennt der Inhaltsserver den Gesamtschlüssel wird die Gesamtverschlüsselung der Daten entschlüsselt. Übrig bleiben die Daten des Datensegmentes, welche noch teilverschlüsselt sind. Hier wird zunächst überprüft, ob der mitgesendete Gesamtschlüssel richtig ist. Hierfür wird der Name des Aktenteils mit den ersten Zeichen der entschlüsselten Daten verglichen. Der

Aktenteilname müsste komplett in den Daten als Klartext vorhanden sein, da bei der Verschlüsslung dieser zur Überprüfung angehängt wurde.

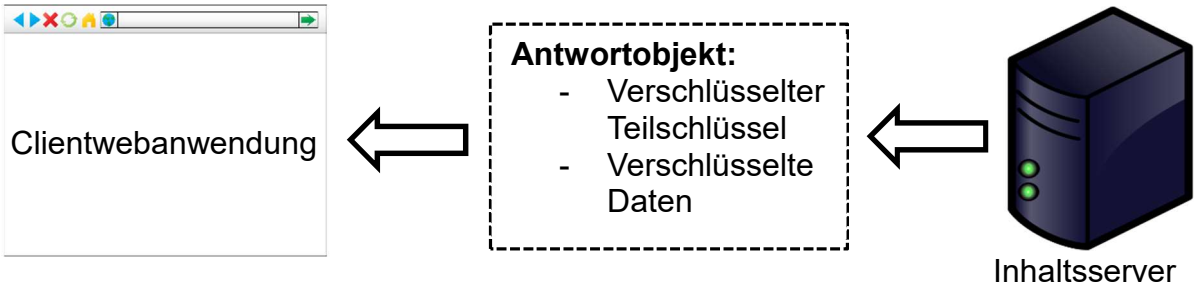

Abbildung 20 - Übersicht von der Ausgabe eines Datenpaktes zusammen mit der Schlüsselinfo

Ist das Lizenzzertifikat und der Gesamtschlüssel gültig, werden die Daten des Aktensegmentes, welche nur noch teilverschlüsselt sind, zusammen mit dem verschlüsselten Teilschlüssel der Schlüsselinfo des spezifischen Lizenzinhabers an die Clientwebanwendung zurückgesendet (siehe Abbildung 20).

Folgernd kennt die Clientwebanwendung den Teilschlüssel, da sie den verschlüsselten Teilschlüssel mit dem privaten Schlüssel des Benutzers entschlüsseln kann. Mit dem Teilschlüssel kann die Webanwendung das verschlüsselte Datenpaket entschlüsseln. Die entschlüsselten Daten werden dann entweder in Form eines veränderbaren oder eines nichtveränderbaren Textfeldes angezeigt. Dies ist abhängig von den verfügbaren Rechten des Lizenzinhabers und wird von der Clientwebanwendung aus dem Lizenzzertifikat gelesen und entsprechend dargestellt.

Mit der Darstellung eines nichtveränderbaren Textfeldes endet die Funktion für das Lesen einer Akte. Möchte der Benutzer einen anderen Teil lesen, werden alle Schritte in Bezug auf den Inhaltsserver wiederholt. Es ist nicht nötig, für jedes Aktensegment erneut das Lizenzzertifikat anzufordern, da es für alle verfügbaren Aktenteile des Aktenbesitzers gilt.

Hat der Benutzer das Recht die Daten des Aktensegmentes zu bearbeiten, kann er in dem veränderbaren Textfeld seine Änderungen vornehmen. Hat der Benutzer die Bearbeitung der Daten abgeschlossen, verschlüsselt die Clientwebanwendung die unverschlüsselten Daten mit dem bekannten Teilschlüssel.

Die verschlüsselten Daten werden nun zusammen mit dem aktuellen Datum und der Uhrzeit mittels dem privaten Schlüssel des Lizenzinhabers (der Benutzer) signiert.

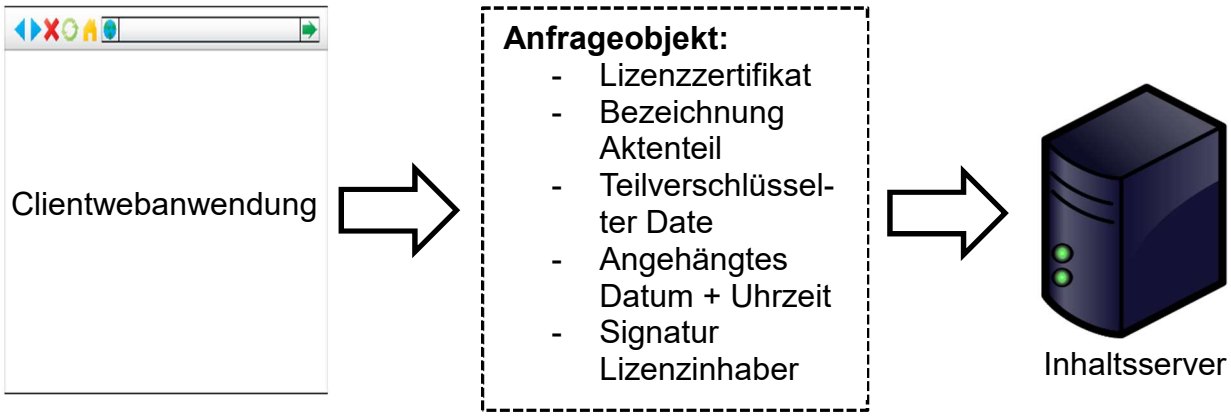

Abbildung 21 - Übersicht einer Anfrage zum Bearbeiten eines Objektes

Das Lizenzzertifikat, der Name für das Aktenteil und das verschlüsselte Datenpaket, welches nun den bearbeiteten Inhalt besitzt, werden nun an den Inhaltsserver gesendet (siehe Abbildung 21). Zusätzlich wird das angehängte Datum zusammen mit der Uhrzeit und der Signatur des Lizenzinhabers mitgesendet.

Der Inhaltsserver validiert das Lizenzzertifikat und selektiert das entsprechende Aktensegment des Patienten. Beinhaltete das Lizenzzertifikat das Recht „Schreiben“, dürfen die Daten des Aktensegmentes überschrieben werden. Vor dem Überschreiben wird überprüft, ob der Lizenzinhaber die Änderungen vorgenommen hat, indem die Signatur des neuen teilverschlüsselten Datenteils zusammen mit dem Datum und der Uhrzeit verifiziert wird. Das Datum und die Uhrzeit dürfen nicht älter als fünf Minuten sein, da sonst die Änderungen für ungültig erklärt werden.

Stimmen alle Daten, entschlüsselt der Inhaltsserver den verschlüsselten Gesamtschlüssel, welcher in dem Lizenzzertifikat aufgeführt ist und verschlüsselt mit diesem die neuen teilverschlüsselten Daten zusammen mit dem Namen des Aktensegmentes.

Letztlich wird der alte Eintrag des Aktensegmentes mit dem neuen Eintrag überschrieben.

Hiermit ist das Bearbeiten der Daten des Aktensegmentes abgeschlossen. Die Funktionsweise des Inhaltsservers wiederholt sich für jedes einzelne Aktensegment, welches der Benutzer bearbeiten möchte. Wie bei dem Lesen von den Daten eines Aktensegmentes muss auch bei dem Bearbeiten nur anfangs einmal das Lizenzzertifikat von dem Lizenzserver angefordert werden.

6.1.5 Lizenz abgelaufen

Eine Lizenz ist so lange gültig, bis der entsprechende Ablaufzeitpunkt überschritten ist. Ist die Lizenz nicht mehr gültig, muss sichergestellt werden, dass der Lizenzinhaber weder in der Lage ist, das Lizenzzertifikat von dem Inhaltsserver abzufragen, noch mit einem lokal kopierten und gespeicherten Lizenzzertifikat die Daten von dem Inhaltsserver abzufragen und zu verwenden.

Die Server haben keinen Zugriff auf den Klartext der Teilschlüssel, somit können sie diesen nicht ändern. Da es nötig wäre, die Daten erst mit dem alten Teilschlüssel zu entschlüsseln und mit dem Neuen wieder zu verschlüsseln, können die Server den Teilschlüssel nicht wechseln. Um den Zugriff auf die Patientendaten mit ungültige Lizenzzertifikaten zu vermeiden, muss der Lizenzserver sicherstellen, dass der Gesamtschlüssel, welcher von einem Benutzer potentiell gespeichert wurde, nicht mehr gültig ist. Um einen Gesamtschlüssel abzuschaffen muss eine Kommunikation zwischen Lizenzserver und Inhaltsserver herrschen, da der Gesamtschlüssel bei dem Lizenzserver bei Bedarf erzeugt wird und bei dem Inhaltsserver in Verwendung kommt.

Die Kommunikation zwischen den Servern fungiert über die REST API des Inhaltsservers. Der Lizenzserver benötigt bei dem Inhaltsserver ein administratives Benutzerkonto, damit sich dieser als Lizenzserver Authentifizieren kann. Bei jeder Anfrage an den Inhaltsserver muss sich der Lizenzserver authentifizieren.

Damit die Ablauftermine der Lizenzen überprüft werden, ist es notwendig, dass eine Funktion in einem festgelegten Intervall diese inspiziert und gegebenenfalls die Lizenz bei Überschreitung des Termins erkennt und verwirft.

Hat die prüfende Funktion eine abgelaufene Lizenz gefunden, muss ein neuer Gesamtschlüssel generiert und mit dem Inhaltsserver abgeglichen werden. Sobald der neue Gesamtschlüssel generiert ist, wird dieser mit dem öffentlichen Schlüssel des Inhaltsservers verschlüsselt. Der neue verschlüsselte Gesamtschlüssel ersetzt den alten verschlüsselten Gesamtschlüssel, dieser wird vor dem endgültigen Löschen zwischengespeichert. Zudem werden alle Aktenteile gesucht, für die die Lizenz abgelaufen ist und es keinen Nutzen mehr gibt, Schlüsselinfos für den Lizenzinhaber zu spei-

chern. Sobald der Nutzer mehr als eine Lizenz für dieselbe Patientenakte besitzt, dürfen nicht alle Schlüsselinfos verworfen werden, da andere gültige Lizenzen noch verwendet werden soll.

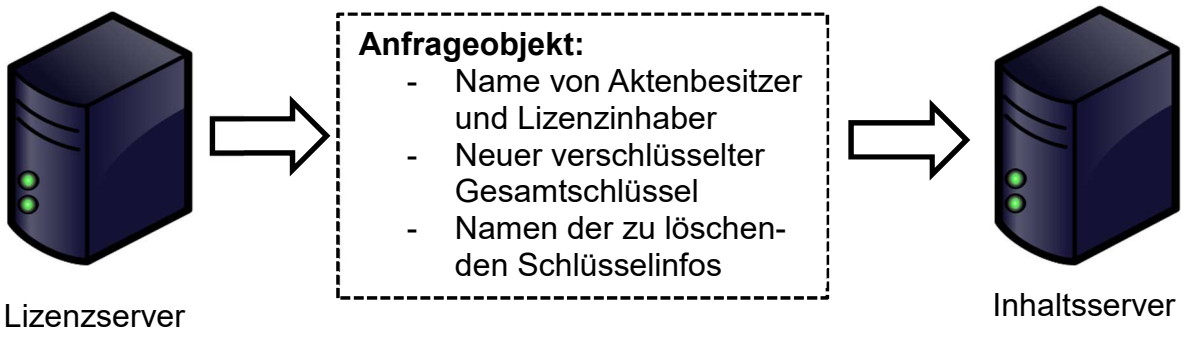

Abbildung 22 - Übersicht einer Anfrage um neuen Gesamtschlüssel festzulegen

Der neue und der alte verschlüsselte Gesamtschlüssel werden dann zusammen mit dem Namen des Aktenbesitzers und dem Lizenzinhaber zu dem Inhaltsserver gesendet (siehe Abbildung 22). Außerdem wird dem Inhaltsserver mitgeteilt, welche Namen die Aktenteile besitzen, dessen Schlüsselinfos gelöscht werden sollen.

Der Inhaltsserver entschlüsselt zunächst beide Gesamtschlüssel. Mit dem alten Gesamtschlüssel kann der Inhaltsserver die Gesamtverschlüsselung der Akte entschlüsseln. Daraufhin kann er die Daten wieder mit dem neuen Gesamtschlüssel verschlüsseln und mit den neu verschlüsselten Daten die alten Einträge überschreiben. Nun ist der neue Gesamtschlüssel für die Akte gültig. Zusätzlich werden die zu löschenden Schlüsselinfos des Lizenzinhabers der abgelaufenen Lizenz gelöscht. Der alte Gesamtschlüssel kann nun sowohl auf dem Lizenzserver als auch auf dem Inhaltsserver gelöscht werden.

Alle neu angeforderten Lizenzenzzertifikate erhalten nun den neuen verschlüsselten Gesamtschlüssel.

6.1.6 Benutzer löscht Lizenz

Der Benutzer kann in der Clientwebanwendung eine Übersicht aufrufen, die alle Lizenzen anzeigt, die für seine Patientenakte gültig sind. Hier kann er einzelne Lizenzen nach Belieben löschen. Wählt er eine Lizenz zum Löschen aus, bearbeitet der Lizenzserver diesen Aufruf. Hier findet derselbe Ablauf statt, der auch bei dem Ablauf eines Ablauftermins ausgeführt wird, nur das hier das Datum gültig ist und die Lizenz entfernt wird.

6.2 Sicherheitsanalyse

Bei der Abwicklung und Durchführung der einzelnen Use-Cases steht vor allem die Sicherheit der Daten der einzelnen Benutzer von der elektronischen Patientenakte im Vordergrund. Es soll nun auf die verschiedenen sicherheitsrelevanten Themen wie Integrität, Vertraulichkeit und Verfügbarkeit der einzelnen Anwenderfunktionen eingegangen werden. Hier wird die Ist-Situation von dem Prototyp analysiert.

Außerdem wird das Thema Authentifikation in Bezug auf die einzelnen Server aufgegriffen und dessen Funktionsweise geschildert.

6.2.1 Authentifikation

Damit sich der Benutzer in die Clientwebanwendung einloggen kann, wird der Benutzername und das Passwort verlangt. Bei der Kommunikation mit dem Lizenzserver wird dieser Login und das damit bereitgestellte Cookie benötigt, um sich fortlaufend zu authentifizieren. Dies wird benötigt, um die Daten des Benutzers zu schützen. Ein unbefugter Zugriff auf ein Benutzerkonto kann die Patientenakte weder lesen noch bearbeiten. Hier wird der private Schlüssel des Eigentümers des Benutzerkontos benötigt, um den von dem Inhaltsserver erhaltenen verschlüsselten Teilschlüssel zu entschlüsseln. Ohne den Teilschlüssel kann die Anwendung die Patientendaten nicht lesen. Bei der Bearbeitung von Patientendaten werden die teilverschlüsselten geänderten Daten zusammen mit dem aktuellen Datum und Uhrzeit mittels dem eigenen privaten Schlüssel signiert. Dies sorgt dafür, dass der Inhaltsserver authentifizieren kann, dass die Änderungen von dem Lizenzträger (dem Benutzer) gemacht wurden. Das Datum und die Uhrzeit verhindern, dass ein gültiges teilverschlüsseltes Datensegment zusammen mit dessen Signatur abgehört und später wieder für ein anderes Aktensegment verwendet werden kann, um Daten ohne privaten Schlüssel zu überschreiben, da die Signatur bereits vorhanden und gültig ist. Mit der Implementierung von Datum und Uhrzeit kann selbst bei mitgehörter Kommunikation das Paket nicht mehr verwendet werden. Die Signatur ist zwar gültig, aber die Uhrzeit beziehungsweise die Gültigkeit läuft nach kurzer Dauer ab.

Sind dem Angreifer Benutzername und Passwort bekannt, kann er alle Lizenzen einsehen, die der Benutzer erstellt hat und für die er als Lizenzinhaber eingetragen ist. Um dies zu vermeiden, ist es sinnvoll einen zusätzlichen Authentifizierungsfaktor mit

einzubauen. Dies könnte zum Beispiel, neben dem Wissensfaktor Login Daten, ein Fingerabdruck als Biometrischer Faktor oder eine Smartcard als Besitz Faktor sein.

Zudem kann er auch ohne privaten Schlüssel die Lizenzzertifikate nach Belieben löschen, da der Lizenzserver keine zusätzliche Authentifikation bei dem Löschprozess durchführt, sondern lediglich den Login-Cookie überprüft. Mit der Implementation einer Funktion, die bei dem Löschen einer Lizenz die Anfrage zusätzlich signiert, könnte der Lizenzserver verhindern, dass ein unbefugte Nutzer Lizenzen löschen kann, solange er den privaten Schlüssel nicht kennt.

6.2.2 Integrität

Die Daten dürfen während der Übertragung zwischen den Servern und auf den Datenbanken nicht verändert werden. Veränderungen von Daten sollten sofort auffallen und für ungültig erklärt werden.

Bei der Kommunikation zwischen dem Lizenzserver und der Clientwebanwendung werden überwiegend Zertifikate und Zertifikatslizenzen übertragen.

Bei dem ersten Schritt der Erstellung einer Akte (siehe Abbildung 13) und bei der Erstellung weiterer Lizenzen kann möglicherweise ein Angreifer das Paket abfangen und modifizieren. Das Paket beinhaltet die Lizenz und die Signatur des Lizenzerstellers. Verändert der Angreifer die Lizenz, ist die Signatur nicht mehr gültig, da sich somit der Signaturstring ändert. Der Angreifer hat keine Möglichkeit die Signatur selbst zu erzeugen, da er den privaten Schlüssel des Lizenzerstellers nicht kennt. Der Lizenzserver verwirft alle Anfragen, die Lizenzen beinhalten, die eine ungültige Signatur aufweisen. Somit ist bei der Anfrage zu dem Lizenzserver die Integrität sichergestellt.

Die Integrität der Lizenzen, welche in dem Lizenzserver gespeichert sind, ist ebenfalls über die Signatur des Lizenzerstellers gewährleistet. Sollten sich die Daten in der Lizenz oder die Signatur ändern, würde der Inhaltsserver bei der Lizenz des Lizenzzertifikates (siehe Abbildung 3) eine ungültige Signatur von dem Lizenzersteller erkennen und das Paket verwerfen.

Wenn der Benutzer ein Lizenzzertifikat anfordert, wird dieses von dem Lizenzserver an die Clientwebanwendung gesendet (siehe Abbildung 15). Dieses kann ebenfalls

nicht unbemerkt verändert werden, da die gesamte Lizenz zusammen mit dem verschlüsselten Gesamtschlüssel von dem Lizenzserver signiert wird (siehe Abbildung 14). Ebenfalls würde in diesem Fall der Inhaltsserver bei weiterer Verwendung des Lizenzzertifikates das ungültige Paket bei der Überprüfung der Signatur des Lizenzservers erkennen und verwerfen.

Somit lässt sich verallgemeinern, dass die Integrität der Lizenzen und der Lizenzzertifikate durch die Signatur des Lizenzerstellers und der des Lizenzservers gewährleistet ist. Diese werden bei jeder Serverinstanz geprüft. Somit können keine unbemerkten Änderungen an den Lizenzen oder den Lizenzzertifikaten vorgenommen werden.

Bekommt ein Angreifer Zugang zu dem Inhaltsserver, so kann er in der Datenbank die verschlüsselten Daten der Aktensegmente verändern. Bei einer zukünftigen Anfrage von einem Benutzer würde bei verändertem Aktensegmentdaten nicht mehr der Aktenteilname in der Zeichenkette von den gesamtentschlüsselten Daten vorkommen. Hier könnte es zwei Fehlerursachen geben. Entweder wurden die Daten des Aktensegmentes verändert oder der Gesamtschlüssel ist falsch. In diesem Fall würde der Inhaltsserver denken, der Gesamtschlüssel sei falsch und dem Patienten keinen Zugriff gewähren. In einem solchen Fall muss der Patient das Vorkommnis melden, damit der Serverbetreiber abgleichen kann, ob der richtige Gesamtschlüssel verwendet wurde. War der Gesamtschlüssel valide, muss die Fehlerursache in den verschlüsselten Daten des Aktensegmentes liegen und es müssen Schritte eingeleitet werden, um zu überprüfen, wie und von wem die Daten ungültig verändert wurden. Ein potentielles Backup System mit Versionskontrolle könnte in einem solchen Fall die älteren Daten wiederherstellen und würde bei Untersuchungen eines solchen Vorkommnisses Hilfestellungen bieten, da der Verlauf der Änderungen der Daten betrachtet werden könnte.

Würde der Angreifer nun zusätzlich Zugang zu dem Lizenzserver oder zu dem entsprechenden Gesamtschlüssel verfügen, so kann er die Gesamtverschlüsselung der Daten des Aktensegmentes entschlüsseln, den teilverschlüsselten Datenteil austauschen und wieder mit dem Gesamtschlüssel verschlüsseln. Da der Angreifer den Teilschlüssel nicht kennt, kann er die verschlüsselten Daten nicht lesen und kann bei einem Austausch lediglich eine zufällige Zeichenkette einsetzen. Bei einer Anfrage wäre so aber trotzdem der Aktenteilname in der gesamtentschlüsselten Zeichenkette der Daten enthalten. Der Inhaltsserver würde dann eine Anfrage für die verfälschten Daten

als gültig deuten und die Informationen weiter an die Clientwebanwendung senden. Wenn der Benutzer die ausgetauschten teilverschlüsselten Daten entschlüsselt, würde er feststellen, dass diese abgeändert wurden, da hier nun eine zufällige Zeichenfolge dargestellt wird. Auch hier müsste der Benutzer das Vorkommnis dem Serverbetreiber melden, damit dieser den Ursprung der Probleme herausfinden und die Sicherheitslücke beseitigen kann.

6.2.3 Vertraulichkeit

Die Vertraulichkeit wird sowohl durch die doppelte Verschlüsselung der Patientenakte aber auch durch die Lizenzen und Lizenzzertifikaten gewährleistet. Durch die nicht änderbaren Lizenzzertifikate (siehe 6.2.2 Integrität) sind die Rechte eindeutig über den Lizenzinhaber an die Benutzer gebunden. Die Teilverschlüsselung ermöglicht es, dass nur der berechtigte Benutzer selbst die Daten seiner Aktensegmente lesen kann. Um den Teilschlüssel zu entschlüsseln wird der private Schlüssel des Lizenzinhabers benötigt. So ist sichergestellt, dass nur der Lizenzinhaber die Lizenz verwenden kann, da nur er seinen privaten Schlüssel besitzt, den Teilschlüssel entschlüsseln und die Daten des Aktensegmentes verwenden kann. Wird der Bezug von den Servern auf die Patientendaten analysiert, so kann festgelegt werden, dass diese die Patientendaten zu keinem Zeitpunkt im Klartext sehen können, da der Teilschlüssel benötigt wird, um die letzte Instanz der Daten zu entschlüsseln (siehe Abbildung 3). Da die Teilschlüssel nur in verschlüsselter Form auf dem Inhaltsserver gespeichert sind, kann der Server selbst diese nicht verwenden.

Im Allgemeinen ist die Sicherstellung des Datenschutzes der Patienteninformationen gewährleistet. Es ist aber zu beachten, dass Daten trotzdem von dem Endanwender, also den Lizenzträgern kopiert und weitergegeben werden können. Aus technischer Sicht ist es nicht möglich, zu verhindern, dass der Endbenutzer zum Beispiel eine Fotografie macht oder die Daten notiert, um diese anschließend weiterzugeben. Um diesem Punkt entgegenzuwirken, sollten die Patienten auch nur vertrauenswürdigen Ärzten Rechte auf ihre Patientenakte gewährleisten.

Die Kommunikation selbst ist in den Prototypen über HTTP realisiert. Hier kann ein Dritter den Datenaustausch mithören. Jedoch werden nie relevante Daten im Klartext übergeben. Ein Angreifer kann lediglich auf diese Weise herausfinden, welchen Inhalt die einzelnen Lizenzen und Lizenzzertifikate besitzen. Er kann diese aber nicht nutzen,

um Daten von dem Inhaltsserver abzufragen und zu lesen, da ihm hierfür der private Schlüssel des Lizenzinhabers fehlt. Mit der Implementierung einer verschlüsselten Kommunikation können auch die Lizenzen und Lizenzzertifikate geheim gehalten werden.

Der Lizenzserver muss die Lizenzen im Klartext verwalten, da er diese regelmäßig überprüft und dessen Gültigkeit in Form von Lizenzzertifikaten validiert. Die Lizenzen und Lizenzzertifikate sind ein Werkzeug, um die eigentlichen Daten zu beschützen. Ein Schutz beziehungsweise eine Pseudonymisierung für die Benutzereinträge in den Lizenzen würde verhindern, dass bei im Klartext übertragenen Lizenzen oder Lizenzzertifikaten Relationen zwischen Ärzten und Patienten aufgedeckt werden könnten. Die Benutzerdaten im Inhaltsserver sind mehrfach verschlüsselt und können unabhängig von der Übertragung und Lagerung von Lizenzen und Lizenzzertifikaten sicher verwaltet werden.

Im Falle, dass die Teilschlüssel einer Patientenakte eines Benutzers im Klartext veröffentlicht werden, können die Patientendaten unter Umständen von unbefugten Instanzen ausgelesen werden. Hierfür bräuchte ein Angreifer besagte Teilschlüssel und müsste sich zu der entsprechenden Patientenakte ein gültiges Lizenzzertifikat beschaffen. Sollte er dies erreichen, kann er die Patientenakte lesen. Mit dem Lizenzzertifikat kann er den Inhaltsserver auffordern, mit dem im Lizenzzertifikat enthaltenen verschlüsselten Gesamtschlüssel die Gesamtverschlüsselung der Patientenakte zu entfernen. Die teilverschlüsselten Aktensegmente kann er dann mit dem veröffentlichten Teilschlüssel entschlüsseln. Hier ist jedoch abzuwägen, wie hoch das Risiko ist, dass Teilschlüssel im Klartext veröffentlicht werden und ein Angreifer ein passendes gültiges Lizenzzertifikat stehlen kann. Das Risiko hierfür lässt sich abhängig von dem Vertrauen an die Lizenzträger der vergebenen Lizenzen einschätzen. Nur ein lizensierter Benutzer und somit eine vertrauenswürdige Instanz wäre in der Lage, diese Schlüssel im Klartext zu veröffentlichen. Die Übertragung der Lizenzzertifikate ist im aktuellen Zustand des Prototyps nicht verschlüsselt und das Abhören dieser würde nur ein geringes Hindernis darstellen. Bei einer verschlüsselten Kommunikation kann der Angreifer keine Lizenzzertifikate abhören. Hier wäre das Risiko, dass ein externer Angreifer Patientendaten lesen kann, gering. Zu beachten ist aber, dass die Serverbetreiber ab dem Zeitpunkt der Veröffentlichung der Teilschlüssel in der Lage sind, die entsprechenden Patientendaten zu lesen. Da diese dann den Gesamtschlüssel und

den Teilschlüssel kennen würden und alle Verschlüsselungsebenen der Patientenakte entschlüsseln können. Um beiden Fällen entgegenzuwirken, sollte es dem Patienten möglich sein, jederzeit einen neuen Teilschlüssel generieren zu lassen, die Teilverschlüsselungen der kompletten Akte zu erneuern und in den Inhaltsserver als neue Schlüsselinfo einzuspeichern. Für jeden Lizenzinhaber in Bezug auf die Patientenakte müsste dann eine neue Schlüsselinfo mit dem neuen Teilschlüssel erstellt werden. So kann der Patient reagieren, falls sein Teilschlüssel veröffentlicht wurde. Der veröffentlichte Teilschlüssel wäre dann nicht mehr gültig.

6.2.4 Verfügbarkeit

Die Verfügbarkeit bei dieser Implementierung hängt von dem Inhaltsserver, dem Lizenzserver und der damit verbundenen Infrastruktur ab. Es muss immer Zugriff auf beide Server möglich sein. Da der Prototyp zu Entwicklungszwecken isoliert in einem eigenen Netzwerk auf verschiedenen virtuellen Maschinen arbeitet, ist dies gewährleistet. Im Allgemeinen ist die Ausfallwahrscheinlichkeit erhört, da zwei Server verwendet werden. Fällt ein Server aus, kann die elektronische Patientenakte in dem Ausfallzeitraum nicht ordnungsgemäß verwendet werden. Der Lizenzserver und der Inhaltsserver können mit derselben Funktionsweise auch kombiniert auf einem einzigen Server arbeiten, um so die Ausfallwahrscheinlichkeit zu senken.

7 Mögliche Verbesserungen „(Erweiterungen für Praxiseinsatz)“

Damit der Prototyp in der Praxis Verwendung finden kann, müssen noch Verbesserungen und Erweiterungen implementiert werden, damit dieser auch in einem Praxiseinsatz sicher funktioniert.

Die aktuelle Kommunikation zwischen den Servern und der Webanwendung selbst wird über das Protokoll „http“ realisiert. Dies bedeutet, die Kommunikation ist unverschlüsselt und kann mitgehört werden. Um dies zu vermeiden, muss das Protokoll „https“ implementiert werden. Hier wird der Datenverkehr verschlüsselt. Dies macht es Angreifern unmöglich, Informationen aus der Kommunikation zu erhalten.

Außerdem wird bei der Erstellung eines Benutzers der generierte öffentliche und private Schlüssel in eine Textdatei geschrieben. Somit würde der Server den privaten Schlüssel kennen. Diese Verantwortung sollte auf eine vertrauenswürdige Instanz ausgelagert werden. Für diesen Fall muss eine Publik Key Infrastruktur System implementiert werden.

Für die Authentifizierung in dem Patientenakten-Verwaltungssystem wird der Benutzername und das Passwort verlangt. Zusätzlich sollte das Authentifizierungsverfahren auf eine weitere Ebene angehoben werden, damit zukünftig ein weiter Authentifizierungsfaktor geprüft wird.

Wie bereits in Kapitel 6.2.4 erläutert, müsste noch die Funktion für den Benutzer implementiert werden, dass dieser bei Bedarf seine Teilschlüssel neu generieren lassen kann. Dies würde einer Veröffentlichung von Teilschlüsseln entgegenwirken.

Zusätzlich wäre es Sinnvoll, dem Patienten die Möglichkeit zu bieten, Lizenzen für einzelne Dokumente auszustellen. So könnte er sowohl fachspezifische Teile seiner Patientenakte an die entsprechenden Ärzte lizensieren, als auch einzelne Dokumente und Befunde nutzen und einzeln verwalten.

8 Fazit

Mittels verschiedenen kryptografischen Verfahren ist es gelungen, einen Prototypen zu erstellen, der die Funktionsweise eines Digital Rights Management für eine elektronische Patientenakte vorführt und die erarbeitete Architektur testet, um dessen richtige Funktionsweise zu bestätigen. Mit diesem Konzept ist es möglich, dass der Urheber beziehungsweise der Patient, selbst Herr über seine eigenen Daten ist. Das bedeutet, nur, er bestimmt, welche Daten aufgenommen werden und wer diese einsehen und bearbeiten darf. Jeder einzelner Use-Case der Patientenakte wird durch die Server betreut und über die Lizenzen und Lizenzzertifikaten gesteuert. Mit asymmetrischer Verschlüsselung als Werkzeug können nur gewünschte Benutzer diese auch nutzen und die Daten des individuellen Patienten einsehen, insofern diese die geeigneten Rechte beziehungsweise Lizenzen besitzen. Die Akte ist zwei Mal verschlüsselt. Die Teilverschlüsselung ermöglicht das Zerteilen der Akte in verschiedene Unterkategorien und nutzt dem Patienten als Managementwerkzeug, um anderen Benutzern Rechte zu vergeben. Befugte Nutzer können dann ebenfalls diese entschlüsseln, um auf die Aktensegmente zuzugreifen. Die Zweite Verschlüsselung ist die Gesamtverschlüsselung, diese kann nur von dem Inhaltsserver entschlüsselt werden und wird geändert, sobald eine Lizenz abgelaufen und somit ungültig ist. Somit durchlaufen alle Patientendaten, bevor diese genutzt werden können eine zweiseitige Entschlüsselung beziehungsweise Verschlüsslung und können nicht mit Kenntnis von nur einem Schlüssel komplett entschlüsselt werden.

Auch wenn alle Patientendaten auf den Datenbanken der Server verwahrt werden, ist es somit selbst den Serverbetreibern nicht möglich, auf die Informationen zuzugreifen. Das bedeutet auch, dass ein Angreifer nicht in der Lage ist, Daten aus der Datenbank zu stehlen, selbst wenn dieser den vollen Zugriff auf den Lizenzserver und den Inhaltsserver hat.

Auf diese Weise könnten Ärzte zukünftig indirekt untereinander Patienteninformationen und Diagnosen sicher austauschen, um so den medizinischen Datenaustausch unter Berücksichtigung des Datenschutzes zu digitalisieren und zu verbessern.

9 Literaturverzeichnis

[ARZTPRAX]	https://www.bundesgesundheitsministerium.de/elektronische-patientenakte.html
[BERT]	Peter Haas, Elektronische Patientenakten Einrichtungsübergreifende Elektronische Patientenakten als Basis für integrierte patientenzentrierte Behandlungsmanagement-Plattformen
[BNDEPA]	https://www.bundesgesundheitsministerium.de/elektronische-patientenakte.html
[BSICRYP]	https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile
[BSIPKI]	https://www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/ElektronischeIdentitaeten/sicherPKI/sicherheitsmechanismen-PKI.html
[CRYPTO]	Nigel P. Smart, Cryptography Made Simple
[DATNS]	https://www.datenschutz-wiki.de/Datenschutzrecht
[DEFU]	https://www.deutschlandfunk.de/digitalisierte-gesundheit-elektronische-patientenakte.697.de.html?dram:article_id=474221
[DRMEXP]	Alapan Arnab and Andrew Hutchison, DIGITAL RIGHTS MANAGEMENT - AN OVERVIEW OF CURRENT CHALLENGES AND SOLUTIONS
[EHEA]	https://ehealth.gvg.org/cms/medium/676/MP_ePa_050124.pdf
[ENT]	Yang Yu Tzi–cker Chiueh, Enterprise Digital Rights Management: Solutions against Information Theft from Insiders
[ERFA]	Jürgen Klauber, Max Geraedts, Jörg Friedrich, Jürgen Wasem, Krankenhaus-Report 2019
[ITSEC]	Eric Maiwald, Network Security A Beginners Guide Third Edition
[RESTAPI]	Naren Yellavula, Building RESTful Web Services with Go : Learn How to Build Powerful RESTful APIs with Golang That Scale Gracefully
[REWO]	https://www.dut-report.de/2020/01/14/elektronische-patientenakte/
[ROSEN]	Bill Rosenblatt, Bill Trippe, Stephen Mooney: Digital Rights Management. Business and Technology. M & T Books, New York NY u. a. 2002
[URH]	https://www.urheberrecht.de/peer-to-peer/