29. Mai 2007

Ein Verfahren zur Lösung des Problems der kryptographischen Langzeitsicherheit medizinischer Daten, die in einer Infrastruktur gespeichert werden.

Georgios Raptis[1]

Abstract

Medizinische Daten, die - wie derzeit für die Telematik-Infrastruktur nach §291a SGB V spezifiziert - auch außerhalb der physischen Kontrolle der Eigentümer oder Ersteller (also z.B. außerhalb von Arztpraxen oder Klinken) auf Servern kryptographisch verschlüsselt gespeichert werden, müssen sehr lange vertraulich bleiben. Insbesondere darf der technische Betreiber des Servers, der die Daten speichert, keinen Zugriff erlangen. Es kann jedoch keine verlässliche Aussage dahingehend getroffen werden, ob die heute eingesetzten kryptographischen Algorithmen in 30 oder 40 Jahren die Vertraulichkeit der medizinischen Daten weiterhin gewährleisten. Es wird ein Verfahren vorgestellt, welches das Problem der langfristigen Sicherheit von verschlüsselt gespeicherten medizinischen Daten aus kryptographischer Sicht löst. Die Anwendung des Verfahrens wird am Beispiel einer nach den derzeit bekannten gematik-Spezifikationen definierten Infrastruktur veranschaulicht. Es wird von einer getrennten Speicherung von verschlüsselten medizinischen Daten und Schlüsselmaterial ausgegangen. Die Daten werden an der Datenquelle (Konnektor, z.B. eines Arztes) mit einem Einmalblock (One Time Pad, OTP) verschlüsselt. Sie sind damit beweisbar sicher verschlüsselt, weil das One-Time-Pad-Verschlüsselungsverfahren beweisbar „perfekt geheim“ ist. Der OTP-Schlüssel wird mit einem symmetrischen Schlüssel verschlüsselt, der wiederum mit den asymmetrischen Schlüsseln aller Zugriffsberechtigten verschlüsselt wird. Die kryptographische, technische und organisatorische Sicherheit des Verfahrens sowie seine Voraussetzungen und Kosten werden analysiert.

Problemstellung

In Infrastrukturen müssen medizinische Daten, die auf einem Server, der sich nicht in der physischen Kontrolle des Eigentümers oder Erstellers der Daten befindet gespeichert werden, für sehr lange Zeit vertraulich bleiben. Diese Zeit kann mehrere Jahrzehnte betragen. Beispielsweise sind psychiatrische Erkrankungen von Jugendlichen über diesen Zeitraum hinaus schützenswert.

Problematisch ist dabei, dass über die heute gängigen Verschlüsselungsalgorithmen und Schlüssellängen keine verlässliche Aussage bzw. Garantie über ihre Wirksamkeit nach 30 oder 40 Jahren getroffen werden kann bzw. von ihrer langfristigen Sicherheit nicht ausgegangen werden kann [Buchmann2006]. So können sowohl asymmetrische als auch symmetrische Verschlüsselungsalgorithmen im Laufe der Jahre geschwächt werden. Dies kann sowohl durch Steigerung der Rechenleistung kombiniert mit technischer Innovation (z.B. Bau von leistungsfähigen Quantencomputern) als auch durch Durchbrüche in der Lösung von grundlegenden mathematischen Problemen oder große Fortschritte in der Kryptoanalyse (inklusive der Entdeckung von Schwachstellen in den derzeitigen Kryptosystemen) erzielt werden. So prognostiziert Lenstra in seiner Analyse [Lenstra2004] zwar eine langfristige Sicherheit für den symmetrischen Kryptoalgorithmus AES-256. Dies allerdings unter der Voraussetzung, dass keine Schwachstellen gefunden bzw. Durchbrüche in der Kryptoanalyse erzielt werden.

[1] Dipl.-Inform Georgios Raptis, Referent Projekt elektronischer Arztausweis der Bundesärztekammer

Medizinische Daten haben einen sehr hohen Schutzbedarf. Folglich darf auch der Betreiber des Servers, in dem sie gespeichert werden, keinen Zugriff darauf erhalten. Der Serverbetreiber (also ein Innentäter als Angreifer) kann jedoch heute gespeicherte verschlüsselte Daten archivieren, damit er sie Jahre später entschlüsseln kann, wenn die eingesetzten Verschlüsselungsalgorithmen oder Schlüssellängen schwach geworden sind. Dieser Angriff muss verhindert werden, also muss die Verschlüsselung der Daten über mindestens 30-40 Jahre bzw. noch länger garantiert sicher sein.

Ausgangslage

In Deutschland wird derzeit eine IT-Infrastruktur („Telematik-Infrastruktur", TI) für das Gesundheitswesen spezifiziert und implementiert, in der teilweise medizinische Daten persistent in Servern, die nicht unter der physischen Kontrolle des Eigentümers der Daten befinden, gespeichert werden sollen. Ihre Vertraulichkeit wird im Wesentlichen durch Verschlüsselung gewahrt.

Die Verschlüsselung der Daten entspricht dem heute gebräuchlichen Schema einer Hybridverschlüsselung: Die Daten sollen im ersten Schritt symmetrisch mit AES verschlüsselt werden, dann wird der symmetrische Schlüssel asymmetrisch mit den öffentlichen Schlüsseln (RSA) der Zugriffsberechtigten verschlüsselt. Die Art der Verschlüsselung unterstützt zudem das Berechtigungskonzept für medizinische Daten, weil nur Berechtigte in der Lage sind, sie zu entschlüsseln. Die Verschlüsselungsparameter werden vom Bundesamt für Sicherheit in der Informationstechnik (BSI) in einer Technischen Richtlinie [BSI-TR03116] festgelegt. So wird heute vom BSI für verschlüsselte medizinische Daten in der Telematik-Infrastruktur (Anwendungen nach §291a SGB V) eine symmetrische Verschlüsselung mit AES-256 und eine asymmetrische Verschlüsselung mit RSA mit 2048 bit Schlüssellänge festgelegt [BSI-TR03116].

Die Verschlüsselung der medizinischen Daten erfolgt bereits bei der „Datenquelle" (z.B. dem Arzt), im so genannten Konnektor, der das Bindeglied zwischen Arztpraxis und Telematik-Infrastruktur darstellt, als Application-Proxy für die TI-Anwendungen funktioniert und kryptographische Funktionen anbietet. Medizinische Daten verlassen somit stets in verschlüsselter Form die Arztpraxis.

In der Telematik-Infrastruktur existieren verschlüsselte medizinische Daten und so genannte Objekt-Tickets. Verschlüsselte medizinische Daten werden über einen eindeutigen Objekt-Identifier adressiert, der im Objekt-Ticket enthalten ist. Die Objekt-Tickets beschreiben die medizinischen Daten und enthalten u.a. die Schlüsselinformationen für die Zugriffsberechtigten [gemGesamtarchitektur]. In einem Objekt-Ticket ist also u.a. für jeden Zugriffsberechtigten der mit seinem öffentlichen RSA-Schlüssel verschlüsselte symmetrische Schlüssel (AES-256) abgelegt, mit dem die medizinischen Daten entschlüsselt werden können [gemTicketKonzept].

<u>Sicherheit durch Trennung von Nutzdaten und Authentisierungs-/Autorisierungsdaten</u>

In der bisherigen Spezifikation des Ticketkonzeptes der gematik [gemTicketKonzept] ist eine logische Trennung zwischen Objekt-Tickets und verschlüsselten medizinischen Daten vorgesehen. Diese Trennung von Nutzdaten und Authentisierungs-/Autorisierungsdaten und -systemen ist für komplexe Architekturen üblich und empfohlen (s. [eGovClientServArch]), weil sie die informationstechnische Sicherheit des Gesamtsystems erhöht. Wird die logische Trennung konsequent organisatorisch und technisch durchgesetzt, trägt dies auch zur Erhöhung langfristigen kryptographischen Sicherheit der Daten bei. Werden also Objekt-Tickets von den medizinischen Daten getrennt gespeichert (4-Augen-Prinzip), hat der Serverbetreiber der die medizinischen Daten speichert (Serverbetreiber A, vgl. Abb. 1) keinen Zugriff auf das Schlüsselmaterial (RSA-verschlüsselte AES-256-Schlüssel in den

Objekt-Tickets bei einem Serverbetreiber B). Wird also RSA-2048 nach mehreren Jahren schwach, kann ein Angreifer (Serverbetreiber B), der in missbräuchlicher Absicht die Objekt-Tickets archiviert hat, die symmetrischen AES-Schlüssel zwar lesen. Ein Angriff damit auf die medizinischen Daten ist dennoch nicht durchführbar, weil der Angreifer die eigentlichen Daten nicht besitzt. Voraussetzung dafür ist, dass der Betreiber des Servers, auf denen die medizinischen Daten liegen, keine Objekt-Tickets mit Schlüsselmaterial bekommt und umgekehrt. Dies ist ein mit Mitteln der organisatorischen und technischen Sicherheit grundsätzlich lösbares Problem.

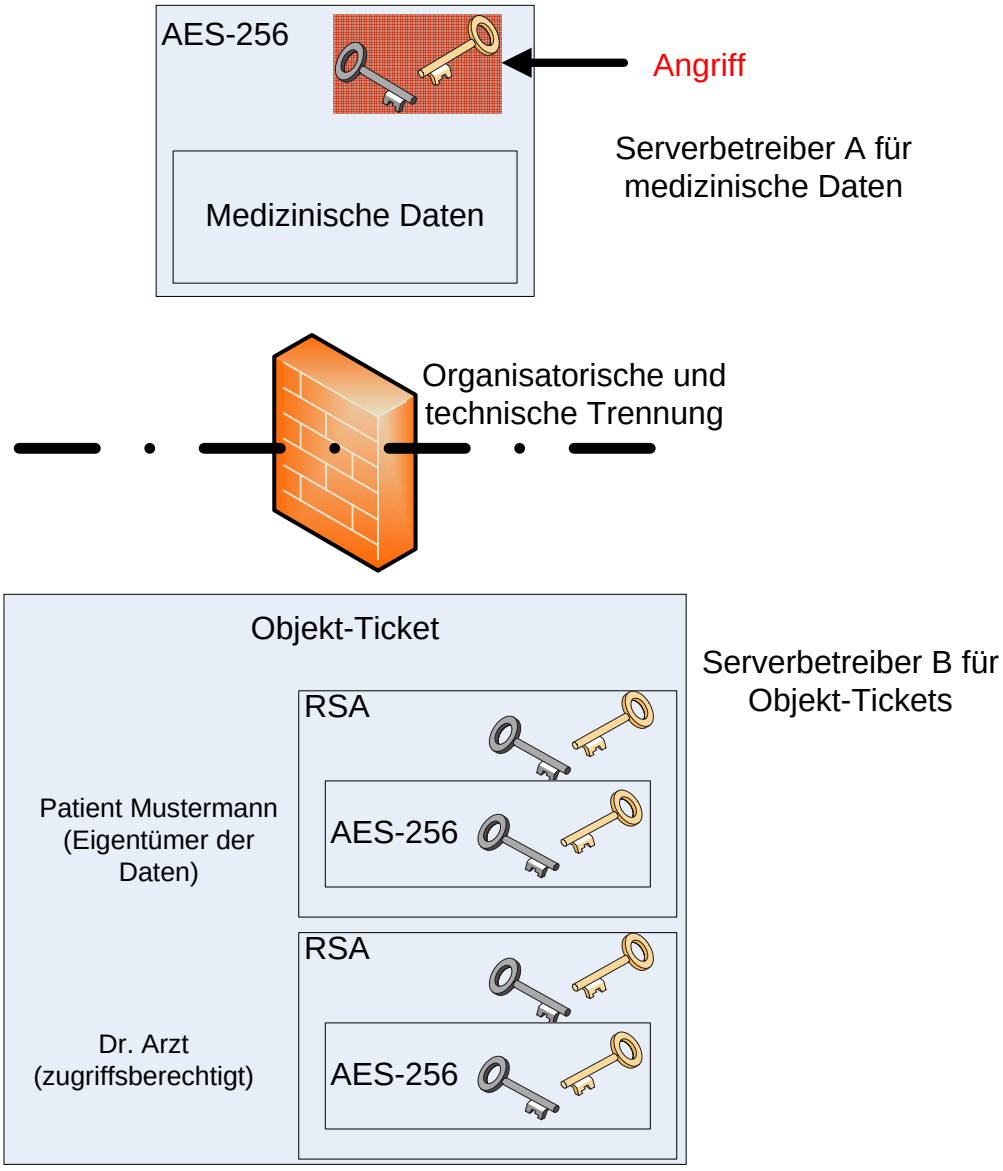


Abb. 1: Hybridverschlüsselung medizinischer Daten, Ausgangslage

Damit sind die gespeicherten medizinischen Daten langfristig sicher vor einer Schwächung der **asymmetrischen** Verschlüsselungsalgorithmen. Außerdem können, wie vom BSI in [BSI-TR03116] empfohlen, wirksame Maßnahmen für eine Umschlüsselung der Daten bzw. des Schlüsselmaterials mit einem höherwertigen Algorithmus oder Schlüssel durchgeführt werden, bevor Verschlüsselungsparameter unsicher werden. Die Umschlüsselung wäre sonst wirkungslos, würde eine solche Trennung nicht vorgenommen werden, weil der Angreifer (Serverbetreiber) die Daten missbräuchlich vor der Umschlüsselung archivieren kann.

Angriff auf die symmetrische Verschlüsselung der medizinischen Daten

Die beim Serverbetreiber A gespeicherten medizinischen Daten sind durch eine symmetrische Verschlüsselung mit AES-256 geschützt. Der Betreiber des Servers, in dem sie gespeichert sind (Serverbetreiber A), kann sie also entschlüsseln, falls AES-256 gebrochen werden kann. Dazu braucht er die Objekt-Tickets nicht. Eine Umschlüsselung, wie in [BSI-TR03116] empfohlen, kann den Angriff nicht abwehren, weil der Angreifer die Daten missbräuchlich archivieren kann (z.B. indem er Kopien der Backup-Medien erstellt), bevor sie umverschlüsselt werden. Auch eine Löschung der Daten durch den Eigentümer (den Patienten) hilft nicht weiter, weil sie vom Angreifer bereits vor der Löschung archiviert sein können. Zudem wird das festgelegte 4-Augen-Prinzip (Trennung von Daten und Schlüsselmaterial) unterwandert, weil der Serverbetreiber A den Angriff allein durchführen kann.

Die kryptographische Langzeitsicherheit der Daten ist also in Bezug auf die eingesetzten symmetrischen Verschlüsselungsalgorithmen (derzeit AES-256) nicht gegeben. Es kann nicht ausgeschlossen werden, dass der Betreiber des Servers, in dem medizinische Daten gespeichert sind, nach mehreren Jahren die Verschlüsselung der Daten brechen kann.

Verfahren zur Lösung des Problems der kryptographischen Langzeitsicherheit medizinischer Daten in einer Infrastruktur

Vorgeschlagen wird ein Verfahren, das aus kryptographischer Sicht beweisbare Sicherheit für die gespeicherten Daten herstellt, so dass auch der Serverbetreiber, der die Daten speichert, nach beliebig langer Zeit sie mit kryptoanalytischen Mitteln nicht brechen kann. Dazu wird ein Einmalblock (One Time Pad, OTP, Vernam-One-Time-Pad) verwendet.
Das Verfahren wird am Beispiel einer Infrastruktur nach den derzeit bekannten gematik-Spezifikationen veranschaulicht. Es kann jedoch grundsätzlich auf jegliche Daten angewendet werden, die in einem Server außerhalb der physischen Kontrolle des Eigentümers der Daten gespeichert werden und für eine lange Zeit vertraulich bleiben müssen.

Verschlüsselung

Werden (medizinische) Daten verschlüsselt soll die Datenquelle (an Beispiel der gematik-Infrastruktur: der Konnektor) zunächst einen zufälligen Schlüssel in gleicher Länge zum Klartext erzeugen, der allen Sicherheitsanforderungen (s.u. Betrachtung der kryptographischen Sicherheit) für einen One Time Pad-Schlüssel entspricht.

Die medizinischen Daten werden mit dem One Time Pad Schlüssel verschlüsselt[2]:
Es ist $P = C = K = \{0,1\}^n$.

Für Schlüssel $k \in \{0,1\}^n$, (n sei eine natürliche Zahl, die die Bitstring-Länge von Klartext und Schlüssel repräsentiert) ist die Verschlüsselungsfunktion:
$E_k : \{0,1\}^n \to \{0,1\}^n, p \mapsto p \oplus k$

Die Entschlüsselungsfunktion zum Schlüssel k sieht identisch aus.

Der Schlüssel wird mit einem als derzeit sicher geltenden gängigen symmetrischen Algorithmus (z.B. AES-256) verschlüsselt. Der AES-256 symmetrische Schlüssel wird dann mit

[2] Kryptosystem mit Klartextraum *P*, Schlüsseltextraum *C*, Schlüsselraum *K*, Verschlüsselungsfunktion $E_k, k \in K$, Entschlüsselungsfunktion $D_k, k \in K$, Klartext wird mit *p*, Schlüsseltext mit *c* repräsentiert.

den öffentlichen RSA Schlüsseln der Berechtigten verschlüsselt und in ein Datenpaket, welches Schlüsselmaterial speichert (am Beispiel der gematik-Infrastruktur: im Objekt-Ticket) aufgenommen. Dadurch kann das Verfahren ein kryptographisch abgesichertes Berechtigungskonzept ermöglichen und unterstützen.

In das Objekt-Ticket (allgemein: Datenpaket mit Schlüsselmaterial für die Daten) wird auch der symmetrisch verschlüsselte OTP-Schlüssel aufgenommen.

Der Konnektor schickt die OTP-verschlüsselten medizinischen Daten („Ciphertext“) zum Server (Serverbetreiber A). Er schickt das Objekt-Ticket mit den Schlüsselinformationen zu einem anderen Server (Serverbetreiber B).

Die Anforderung der organisatorischen und technischen Trennung, wie oben unter „Ausgangslage“ bereits beschrieben bleibt bestehen und ist Voraussetzung für die Wirksamkeit des beschriebenen Verfahrens: Verschlüsselte (medizinische) Daten müssen getrennt vom Schlüsselmaterial gespeichert werden.

Entschlüsselung

Der Konnektor (allgemein: Datenquelle) erhält gemäß den jeweils spezifizierten Authentisierungs- und Berechtigungskonzepten (am Beispiel gematik: [gemGesamtarchitektur]) sowohl das Objekt-Ticket (allgemein: Schlüsselmaterial) als auch die verschlüsselten medizinischen Daten.

Er entschlüsselt zunächst mit dem privaten RSA-Schlüssel den symmetrischen AES Schlüssel. Damit kann er den OTP-Schlüssel entschlüsseln

Mit dem OTP-Schlüssel entschlüsselt der Konnektor die medizinischen Daten.

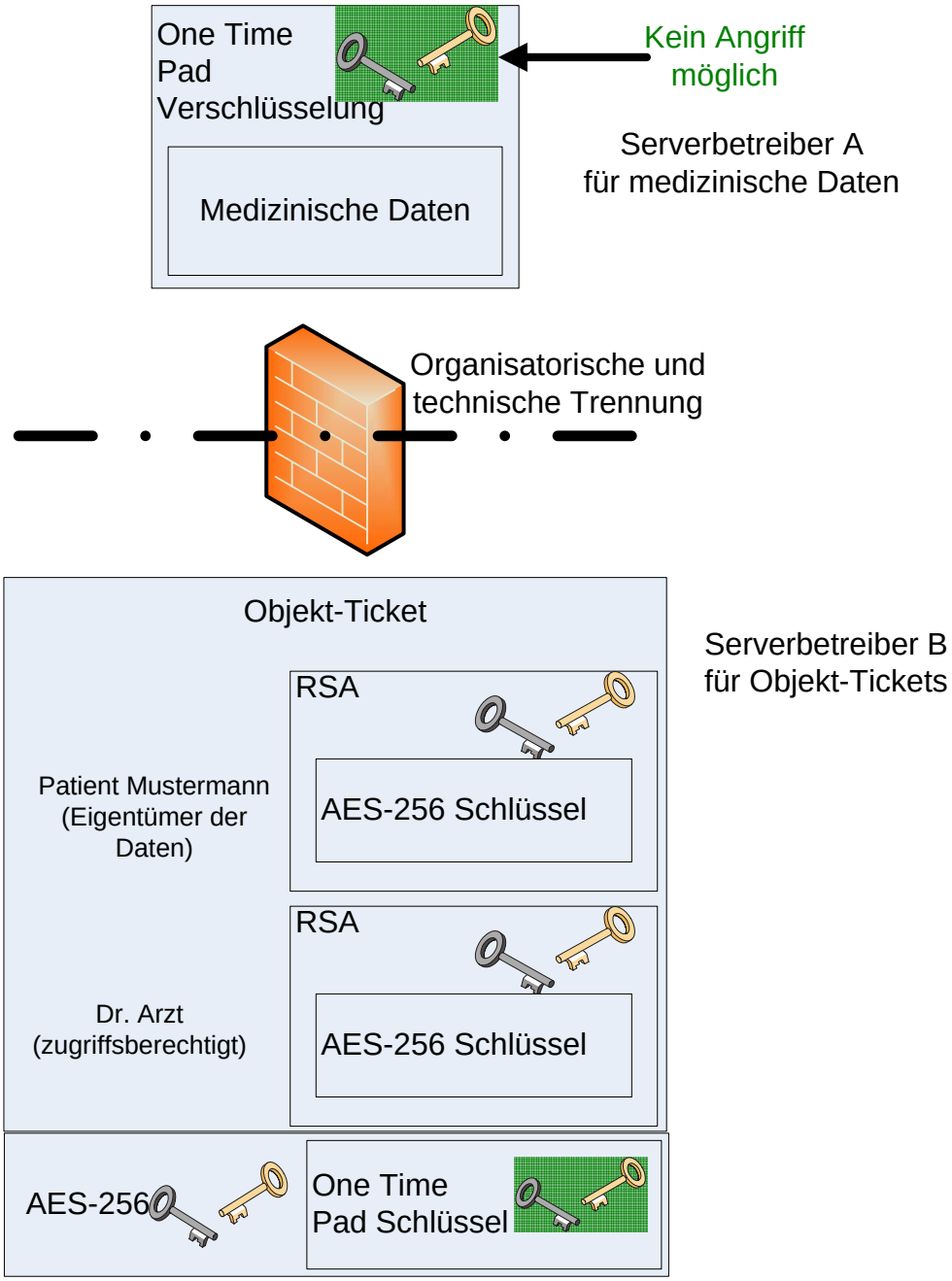


Abb. 2: Verschlüsselung der Daten mit OTP, kryptographische Langzeitsicherheit gewährleistet

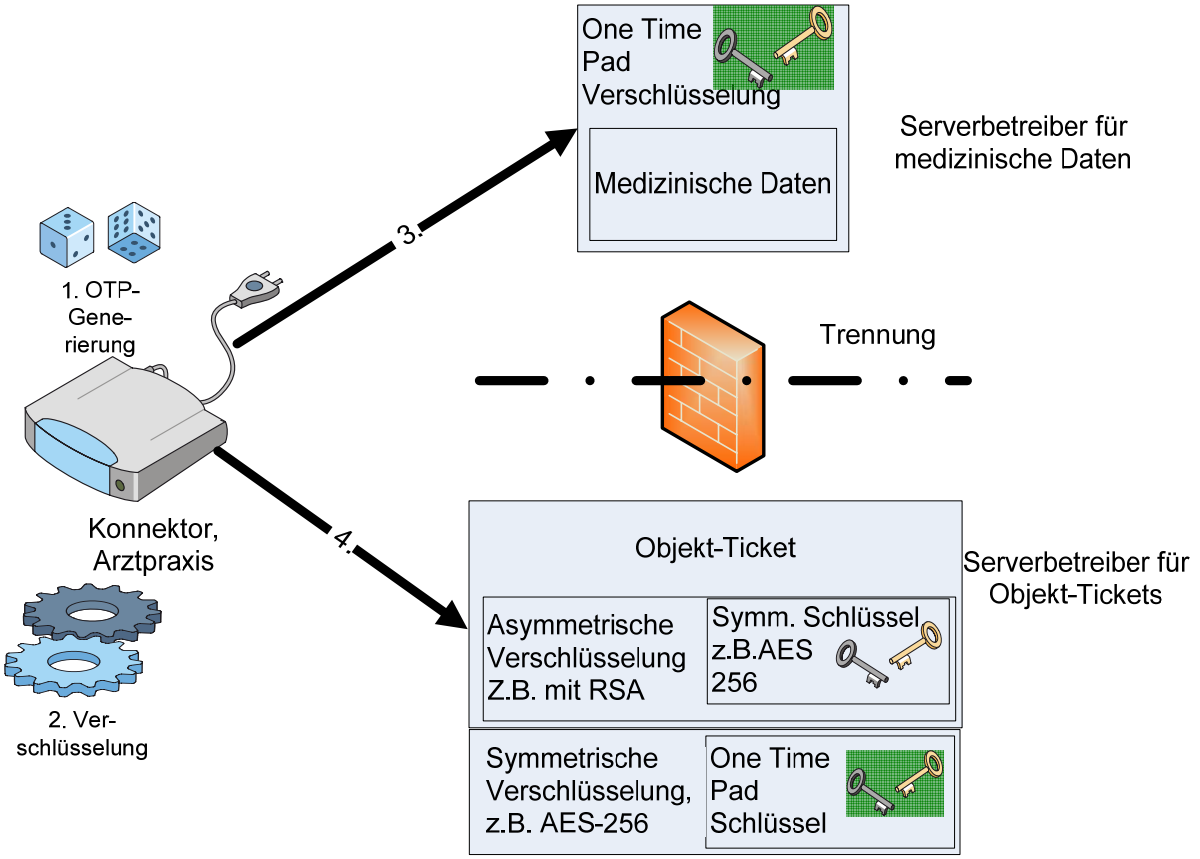


Abb. 3: Verfahren, Ablauf

Übersicht über das kryptographische Verfahren (am Beispiel der gematik-Infrastruktur)

Verschlüsselung:

1. Zu verschlüsselnde (medizinische) Daten stehen fest und haben die Länge n
2. Generierung des zufälligen One Time Pad Schlüssels der Länge n in der Datenquelle (im Konnektor)
3. Verschlüsselung (XOR-Operation) der Daten mit dem OTP-Schlüssel: $c = E_{kOTP}(p)$
4. Verschlüsselte medizinische Daten können an Serverbetreiber A verschickt werden
5. Generierung eines derzeit sicheren symmetrischen Schlüssels (AES-256)
6. Verschlüsselung des OTP-Schlüssels mit AES-256 (oder einem anderen derzeit sicheren symmetrischen Verschlüsselungsalgorithmus): $c_{OTP} = E_{kAES}(k_{OTP})$
7. Liste der Berechtigten und deren öffentlichen asymmetrischen Schlüsseln (derzeit RSA-2048) steht fest
8. Verschlüsselung des symmetrischen AES-Schlüssels mit dem asymmetrischen Schlüssel (z.B. RSA) jedes Berechtigten: $c_{AESn} = E_{kRSAn}(k_{AES})$
9. Datenpaket mit Schlüsselmaterial (Objekt-Ticket) wird gebildet, o.g. Schlüsselmaterial wird aufgenommen (AES-verschlüsselter OTP-Schlüssel (c_{OTP}), ggf. mehrere RSA-verschlüsselte AES-Schlüssel ($c_{AES1}, c_{AES2}, ...c_{AESn}$))
10. Objekt-Ticket kann an Serverbetreiber B verschickt werden

Entschlüsselung:

1. Datenanforderung an die Infrastruktur gemäß den spezifizierten Konzepten, Authentisierung/Autorisierung, Lieferung von Objekt-Ticket und verschlüsselten Daten („medizinisches Datenobjekt“), verschlüsselte Daten sowie Objekt-Ticket liegen dem Konnektor vor

2. Entschlüsselung eines asymmetrisch (RSA-)verschlüsselten symmetrischen (AES-) Schlüssels aus dem Objekt-Ticket mit dem privaten asymmetrischen (RSA-) Schlüssel eines Berechtigten (des Arztes oder Patienten)
3. Mit dem entschlüsselten AES-Schlüssel Entschlüsselung des AES-verschlüsselten OTP-Schlüssels aus dem Objekt-Ticket
4. Mit dem entschlüsselten OTP-Schlüssel Entschlüsselung der medizinischen Daten

Abruf der Daten

Der Abruf der Daten unter den Bedingungen des beschriebenen Verfahrens muss in Hinblick auf die geforderte Trennung zwischen Daten und Schlüsselmaterial entsprechend modelliert werden. Denkbar ist ein Ansatz in Anlehnung an das Kerberos-Protokoll, jedoch unter Einsatz asymmetrischer Kryptographie und Nutzung der Berechtigungskonzepte, die durch die Hybridverschlüsselung ermöglicht werden. Z.B. kann der Abruf mit einer von einem Berechtigten signierte Anforderung nach einem Datenobjekt starten, die an Server B (speichert Objekttickets, bietet den Dienst Authentisierung/Autorisierung an) gestellt wird. Der Server B prüft die Anforderung und (bei erfolgreicher Prüfung) schickt das zugehörige Objektticket mit dem Schlüsselmaterial dem Berechtigten zu. Ferner stellt Server B eine kurzlebige elektronische Bescheinigung aus („<Berechtigter> mit öffentlichem Schlüssel <Zertifikat> ist berechtigt, vom Server A das Datenobjekt mit <OID> bis <Zeitpunkt> zu bekommen“) und signiert sie. Der Berechtigte schickt eine signierte Anforderung zusammen mit der vom Server B ausgestellte Bescheinigung an Server A und bekommt daraufhin die verschlüsselten Daten.

Betrachtung der kryptographischen Sicherheit

Die (medizinischen) Daten sind mit dem beweisbar sicheren One-Time-Pad Verfahren verschlüsselt. Für OTP ist bewiesen [Shannon1949], dass damit verschlüsselte Daten nicht entschlüsselt werden können, solange die relevanten Sicherheitsanforderungen erfüllt (Schlüssel ist zufällig, gleich lang wie der Klartext und darf nur einmal verwendet werden) werden. Eine Entschlüsselung ist auf Grund der beweisbaren Sicherheit auch nach Jahrzehnten nicht möglich, da OTP nicht etwa durch gesteigerte Rechenleistung oder technischen oder kryptoanalytischen Fortschritt gebrochen werden kann.

Somit ist die Langzeitsicherheit gespeicherter medizinischer Daten aus kryptographischer Sicht gegeben. Auch der Betreiber des Servers für medizinische Daten kann diese nicht entschlüsseln.

Voraussetzung dafür ist die Einhaltung der getrennten Speicherung von verschlüsselten Daten und Schlüsselmaterial (4-Augen-Prinzip). Der Betreiber des Servers für medizinische Daten darf nicht im Besitz der verschlüsselten OTP-Schlüssel (also der Objekt-Tickets) kommen. Dies ist eine Anforderung an die organisatorische und technische Sicherheit, die auch in anderen sicherheitsrelevanten Kontexten üblich ist und mit Mitteln der IT-Sicherheit umgesetzt werden kann.

<u>Sicherheitsanforderungen an die OTP-Verschlüsselung und Bewertung</u>

Ist der Schlüssel nicht über einen echten (Hardware-) RNG (Random Number Generator) sondern über einen PRNG (Pseudo Random Number Generator) erzeugt worden, ist das Verfahren nur „computationally secure“ und nicht perfekt geheim, d.h. es ist möglich, dass in der Zukunft ein Angriff auf den PRNG durchgeführt werden könnte. Trotzdem ist die Sicherheit höher als die einer konventionellen Hybridverschlüsselung mit AES/RSA, weil auch der AES-Schlüssel von dieser möglichen Schwachstelle betroffen wäre. Der Einsatz eines echten RNG wird gleichwohl dringend empfohlen.

Ein One Time Pad Schlüssel darf nur einmal verwendet werden. Diese Anforderung kann im geschilderten Szenario erfüllt werden, indem der Konnektor für jedes zu verschlüsselnde Datenobjekt einen neuen OTP-Schlüssel generiert. Aus Performance-Gründen kann der Konnektor permanent oder in Inaktivitätsphasen einen zufälligen Bitstrom für OTP-Schlüssel über seinen RNG erzeugen und in seinem Speicher zur zukünftigen Nutzung ablegen, wenn technisch sichergestellt werden kann, dass dieser Speicher nicht unbefugt gelesen werden kann.

Die One Time Pad Verschlüsselung ist theoretisch anfällig für Known Plaintext Angriffe (der Angreifer kennt den verschlüsselten Text und den Klartext und will den Schlüssel wissen). Diese Angriffe sind hier nicht relevant, weil ein OTP-Schlüssel nur einmal verwendet wird.

Die One Time Pad Verschlüsselung ist theoretisch anfällig für aktive Angriffe, in denen ein Angreifer den verschlüsselten Text an bestimmten vorhersehbaren Stellen (blind) manipuliert und somit auch den Klartext nach der Entschlüsselung manipuliert. Beispielsweise kann ein Angreifer in einer mit OTP verschlüsselten Banküberweisung den verschlüsselten Text an der Stelle, wo der Betrag vermutet wird, manipulieren, so dass nach Entschlüsselung ein evtl. größerer Betrag ausgewiesen wird. Diese Angriffe sind hier nicht relevant, weil die Integrität medizinischer Daten durch elektronische Signaturen geschützt ist.

Betrachtung der technischen und organisatorischen Sicherheit

Kooperieren zwei Angreifer, so dass verschlüsselte medizinische Daten und Objekt-Tickets in der Gegenwart zusammen kommen, sind die Daten durch die eingesetzten Verschlüsselungsverfahren (OTP, AES und RSA) erstmal für einige Jahre sicher, d.h. die kurz- und mittelfristige Vertraulichkeit wird durch die konventionelle Hybridverschlüsselung gewährleistet. Die Verschlüsselung des Schlüsselmaterials (RSA und AES) kann – wie in der [BSI-TR03116] vorgesehen – durch rechtzeitige Umschlüsselung mit einem höherwertigen Verschlüsselungsalgorithmus oder Schlüssel „erneuert“ werden. Ein Angriff ist also nur dann durchführbar, wenn beide Angreifer heute bereits missbräuchlich sowohl verschlüsselte Daten als auch Objekt-Tickets archivieren, damit sie den eigentlichen Angriff 30 oder 40 Jahre später durchführen, wenn RSA oder AES potentiell gebrochen sind. Dies ist sehr unwahrscheinlich und kann (und muss) mit organisatorischen und technischen Maßnahmen verhindert werden.
Es ist ersichtlich, dass das hier beschriebene Verfahren das festgelegte 4-Augen-Prinzip wirksam durchsetzt, d.h. ein Angreifer allein (der Serverbetreiber) ist nicht in der Lage den Angriff durchzuführen.

Kosten des Verfahrens

Ein Nachteil des Verfahrens ist die Verdoppelung der erforderlichen Speicherkapazität. Die OTP-Schlüssel müssen die gleiche Länge aufweisen, wie die zu verschlüsselnden medizinischen Daten und dürfen nur einmal verwendet werden. Eine Verdoppelung des Speicherbedarfs ist jedoch heutzutage nicht kostenkritisch. Sie ist beispielsweise in üblichen Ausfallsicherheitskonzepten (Datenspiegelung) gängige Praxis und wird in diesem Kontext aufgrund des damit verbundenen Nutzens (Schutz der Daten vor Verlust) in Kauf genommen. Der hier beschriebene Nutzen der zusätzlichen langfristigen kryptographischen Sicherheit dürfte die Kosten für den Speicherbedarf rechtfertigen.

OTP-Schlüssel müssen zufällig sein. Der Konnektor muss also in der Lage sein, zufällige Schlüssel zu erzeugen. Dies ist allerdings eine Anforderung, die auch für die Generierung sicherer AES-256 Schlüssel erfüllt sein muss und verursacht somit keine weitere Kosten. Weitere Machbarkeitsaspekte werden in [Raptis_BIOSIG07] erläutert.

Literatur

[Shannon1949] Claude Shannon: Communication Theory of Secrecy Systems. Bell Sys. Tech. Jour., 28:656-715, 1949

[Lenstra2004] Arjen K. Lenstra, Key Lengths, Contribution to The Handbook of Information Security, 30.06.2004

[BSI-TR03116] Technische Richtlinie für die eCard-Projekte der Bundesregierung, Version 1.0 vom 23.03.2007, BSI

[gemTicketKonzept] Spezifikation Ticketservice, Version 0.9.0 vom 02.03.2007, gematik

[gemGesamtarchitektur] Gesamtarchitektur, Version 0.3.0 vom 02.03.2007, gematik

[eGovClientServArch] Sichere Client-Server-Architekturen für E-Government, E-Government-Handbuch, BSI, 2005

[Buchmann,2006] J. Buchmann et al, Krypto 2020 - Aussichten für langfristige kryptographische Sicherheit, <kes>, 5;2006)

[Raptis_BIOSIG07] G. Raptis, Elektronische Arztausweise – Architektur, Stand und Erwartungen, BIOSIG-Konferenz 2007, Darmstadt, 13.07.2007

Elektronische Arztausweise
Architektur, Stand und Erwartungen

BIOSIG 2007

Verkürzte Fassung, Beschreibung des Verfahrens zur langfristigen Vertraulichkeit archivierter medizinischer Daten

13. Juli 2007

Georgios Raptis
Projektbüro eArztausweis in der Bundesärztekammer

Langfristige Sicherheit medizinischer Daten

- Was bedeutet „**Langfristige Sicherheit**“ in diesem Kontext? Primär **Langfristige Vertraulichkeit**
- Beispiel: Psychiatrische Erkrankung eines Jugendlichen. Auch 40-50 Jahre später muss der Eintrag in die elektronische Patientenakte vertraulich bleiben
- Problem bei Datenspeicherung in einer Infrastruktur: keine Kontrolle mehr über die verschlüsselten Daten.
- Zentrale Datenbanken sind verlockendes Angriffsziel, auch für den Serverbetreiber
- Kann jemand garantieren, dass RSA2048 und AES-256 in 40-50 Jahren die Vertraulichkeit der heute verschlüsselten Daten weiterhin gewährleisten?

2

Langzeitsicherheit: Kryptographisches Problem 1/2

- Problematisch: Fortschritte in der Kryptoanalyse können die heute üblicherweise eingesetzten Kryptosysteme schwächen
  - Es existiert ein Beweis, dass RSA mit einem Quanten-computer in polynomieller Zeit gebrochen werden kann. (Gibt es in 40 Jahren einen entsprechend leistungsfähigen Quantencomputer? Prognosen?)
  - Neue Kryptoanalyseverfahren könnten entdeckt werden. (z.B. die differentielle Kryptoanalyse (1990 entdeckt) war vom DES (1977 von der NSA spezifiziert) bereits berücksichtigt…)
  - Schwachstellen in den symmetrischen Kryptoalgorithmen könnten entdeckt werden (ob Rijndael (derzeit sicher!) trotzdem zum AES gekürt wäre, hätte man algebraische Angriffe früher entdeckt?)

3

Langzeitsicherheit: Kryptographisches Problem 2/2

- Übliche Hybridverschlüsselung (RSA / AES) bietet keine beweisbare kryptographische Sicherheit
- Prognosen gibt es nur unter der Annahme, dass keine Durchbrüche in der Kryptoanalyse erzielt werden (z.B. [Lenstra, Key Lenghts, 2004])
- „Ungelöst bleibt aus Sicht der heutigen Kryptographie das Problem der langfristigen Vertraulichkeit: Ein praktikables Verfahren, das die Vertraulichkeit einer verschlüsselten Nachricht über einen sehr langen Zeitraum sicherstellt, ist derzeit nicht bekannt. “ (J. Buchmann et al, Krypto 2020, <kes>, 5;2006)
- Technische Richtlinie 03116 des BSI: Regelmäßige Umschlüsselung der Daten mit stärkeren Kryptoverfahren muss vorgesehen werden
- Es kann aber nicht ausgeschlossen werden, dass ein Angreifer (z.B. der Betreiber des zentralen Servers) die Daten heute (vor der Umschlüsselung) archivieren kann, um sie später zu entschlüsseln, wenn die eingesetzten Algorithmen und Schlüssellängen schwach geworden sind.

4

Ausgangslage 1/3, Trennung Daten und Schlüssel

- Medizinische Daten verlassen die Arztpraxis stets verschlüsselt. Verschlüsselung im Konnektor des Arztes
- Hybridverschlüsselung: Daten symmetrisch mit AES verschlüsselt, AES-Schlüssel mit den RSA-Schlüsseln aller Berechtigten verschlüsselt
- Telematik-Infrastruktur: Serviceorientierte Architektur
- Best Practice: **Trennung** von Backend-Systemen (Datenspeicherung) und Authentisierung/Autorisierung
- D.h. **Trennung von verschlüsselten Daten und Schlüsselmaterial** („Objekt-Ticket“) mit RSA-verschlüsselten AES-Schlüsseln

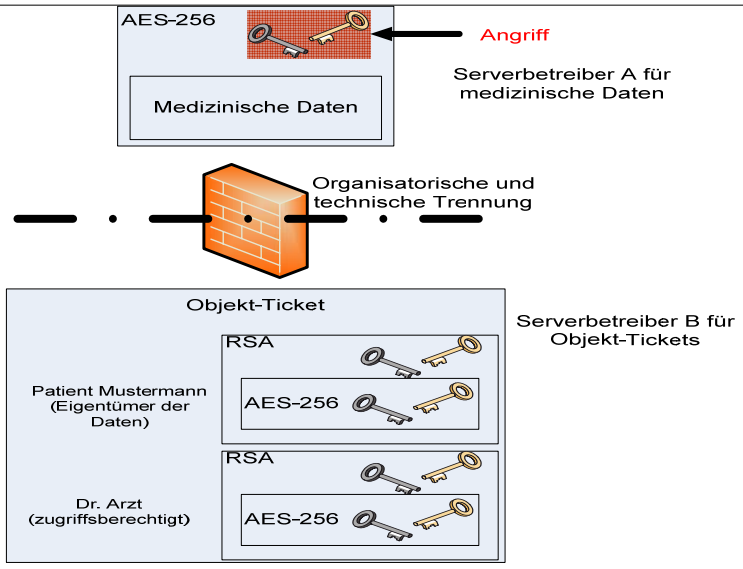
5

Ausgangslage 2/3, Auswirkungen auf Verschlüsselung

- Wird die Trennung von verschlüsselten Daten und Schlüsselmaterial („Objekt-Ticket“) **konsequent** durchgeführt (z.B. verschiedene Server(-betreiber)):
  - Server(-betreiber) A = Speichert nur verschlüsselte Daten
  - Server(-betreiber) B = Speichert nur Schlüsselmaterial (Objekt-Tickets)
- Nützlicher Nebeneffekt: Werden asymmetrische Algorithmen schwach, kann der Angreifer auf die Daten nicht zugreifen, weil er sie gar nicht hat.
- Bei Schwächung der symmetrischen Algorithmen kann jedoch der Serverbetreiber A, der die verschlüsselten Daten speichert, auf die Daten zugreifen

6

Ausgangslage 3/3, Angriff



7

Vorschlag zur Lösung des Problems, Erstveröffentlichung (soweit uns bekannt)

Es wird ein Verfahren vorgestellt, welches das Problem der langfristigen Vertraulichkeit der Daten aus kryptographischer Sicht löst

Ziel: **beweisbare kryptographische Sicherheit, Langfristige Vertraulichkeit**

Voraussetzung: Trennung von verschlüsselten Daten und Schlüsselmaterial

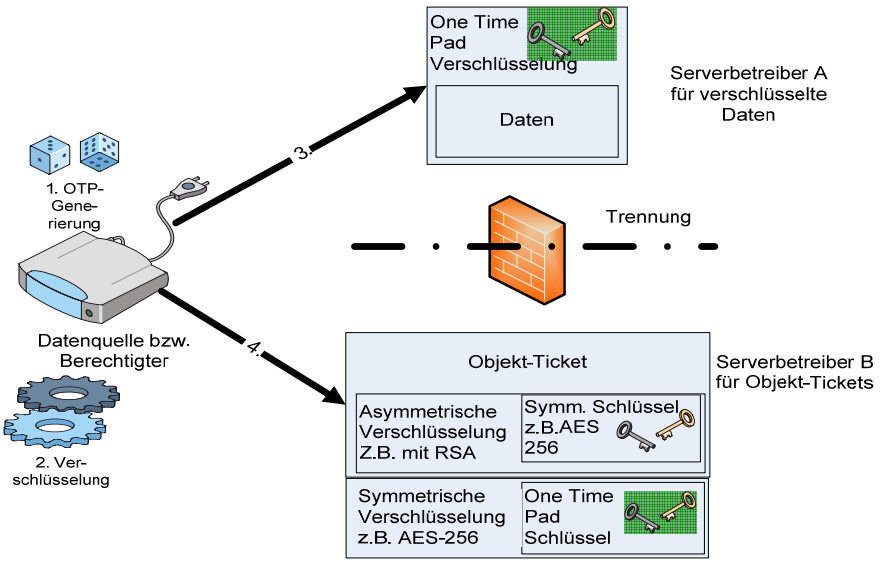
8

Beschreibung des Verfahrens, Verschlüsselung

1. Die Datenquelle (hier: Konnektor) generiert einen **One Time Pad** („OTP“, Einmalblock nach Vernam). Der Schlüssel muss zufällig sein, gleich lang wie die zu verschlüsselnden Daten und nur einmal verwendet werden.
2. Die Daten werden mit dem OTP-Schlüssel verschlüsselt (XOR-Operation) und an den Serverbetreiber A verschickt.
3. Der OTP-Schlüssel wird mit einem derzeit üblichen sicheren symmetrischen Verschlüsselungsalgorithmus (z.B. AES-256) verschlüsselt
4. Liste der Berechtigten und deren öffentlichen asymmetrischen Schlüsseln (derzeit RSA-2048) steht fest
5. Verschlüsselung des symmetrischen AES-Schlüssels mit dem asymmetrischen Schlüssel (z.B. RSA) jedes Berechtigten (wie üblich)
6. Datenpaket mit Schlüsselmaterial („Objekt-Ticket“) wird gebildet, o.g. Schlüsselmaterial wird aufgenommen (AES-verschlüsselter OTP-Schlüssel, ggf. mehrere RSA-verschlüsselte AES-Schlüssel)
7. Objekt-Ticket wird an Serverbetreiber B verschickt

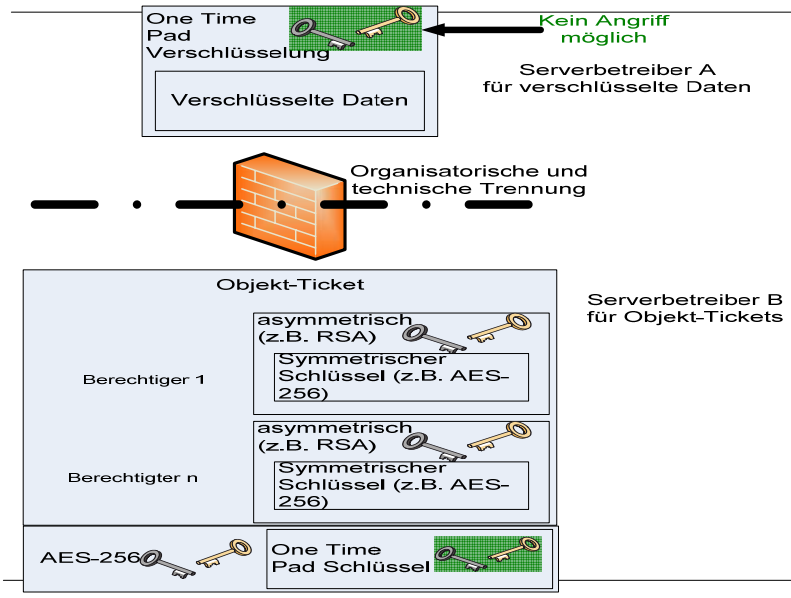
9

Beschreibung des Verfahrens, Darstellung



10

Beschreibung des Verfahrens, Darstellung



11

Beschreibung des Verfahrens, Entschlüsselung

1. Datenanforderung an die Infrastruktur gemäß den jeweils spezifizierten Berechtigungskonzepten, Authentisierung / Autorisierung, Lieferung von Objekt-Ticket und verschlüsselten Daten, verschlüsselte Daten sowie Objekt-Ticket liegen dem Berechtigten vor
2. Entschlüsselung eines asymmetrisch (z.B. RSA) verschlüsselten symmetrischen (z.B. AES-256) Schlüssels aus dem Objekt-Ticket mit dem privaten asymmetrischen (z.B. RSA) Schlüssel eines Berechtigten
3. Mit dem entschlüsselten AES-Schlüssel Entschlüsselung des verschlüsselten OTP-Schlüssels aus dem Objekt-Ticket
4. Mit dem entschlüsselten OTP-Schlüssel Entschlüsselung der Daten
5. Klartext-Daten liegen dem Berechtigten vor

12

Bewertung der kryptographischen Sicherheit

- Daten sind über eine One Time Pad Verschlüsselung kryptographisch geschützt
- One Time Pad Verschlüsselung ist **beweisbar sicher** (informationstheoretischer Beweis von Shannon, 1949). Sie kann auch nicht etwa durch gesteigerte Rechenleistung oder kryptoanalytischen Fortschritt gebrochen werden
- Somit ist die Langzeitsicherheit gespeicherter medizinischer Daten aus kryptographischer Sicht gegeben. Der Betreiber des Servers für medizinische Daten kann diese nicht entschlüsseln
- Voraussetzung ist die Einhaltung der getrennten Speicherung von verschlüsselten Daten und Schlüsselmaterial.
- **Dies ist eine Anforderung an die organisatorische und technische Sicherheit**, die auch in anderen Kontexten üblich ist und mit Mitteln der IT-Sicherheit umgesetzt werden kann.

13

Allgemeine Bewertung der Sicherheit

- Mögliche Angriffe auf OTP: s. Paper (auch unter www.baek.de)
- Garantiert das vorgestellte Verfahren absolute Sicherheit?
  ➔ Nein, nur beweisbare kryptographische, langfristige Sicherheit.
  - Technische, organisatorische und IT-Sicherheit weiterhin eine Herausforderung. Trennung zwischen Daten und Schlüssel-material muss sichergestellt werden. Angriffe auf dem Transportweg müssen abgewehrt werden (s. BSI TR-03116)
  - Das systemimmanente Problem der Langzeitsicherheit kryptographischer Algorithmen wird aber gelöst.
  - Eine spätere Umschlüsselung mit stärkeren Kryptoverfahren (nach BSI TR-03116), wird erst durch dieses Verfahren wirksam. Die Daten sich langfristig beweisbar sicher geschützt, auch wenn der Serverbetreiber sie vor der Umschlüsselung archiviert hat.

14

Allgemeine Bewertung der Sicherheit

- Wird das kryptographische Problem der langfristigen Sicherheit nicht einfach in die organisatorische und technische Sicherheit verlagert?
  - Ja, teilweise. Die heute übliche Kryptographie kann aber nun mal keine langfristige Sicherheit sicherstellen. Deshalb werden ihre Vorteile mit dem beweisbar sicheren One-Time-Pad Verfahren und mit Maßnahmen der organisatorischen und technischen Sicherheit kombiniert, um langfristige Sicherheit zu erreichen.
  - Ein durch Hybridverschlüsselung abgesichertes Berechtigungs-konzept funktioniert weiterhin. Minimaler Realisierungsaufwand
  - Die kurz- und mittelfristige Vertraulichkeit wird durch die Hybridverschlüsselung sichergestellt.
  - Ein Angriff auf die langfristige Vertraulichkeit müsste durch **beide** Serverbetreiber heute geplant und vorbereitet werden, damit er in 40-50 Jahren evtl. durchgeführt werden kann.

15

Machbarkeit und Kosten

- Machbarkeit im Kontext der Telematik-Infrastruktur:
  - OTP-Schlüssel über TPM generieren (Kosten für TPM unter 10.- EUR). Anforderungen an einen sicheren (P)RNG gelten auch heute für die Produktion sicherer AES-256 Schlüssel
  - Objekt-Ticket der gematik muss um den verschlüsselten OTP-Schlüssel erweitert werden (ein Eintrag mehr…)
  - Trennung: getrennte Server für Daten und Objekt-Tickets werden heute schon empfohlen. Am Besten: Konnektor setzt die Trennung durch. Andere Szenarien sind mit Einsatz zertifizierter Komponenten (Broker) denkbar.
- Kosten
  - Verdoppelung des Datenvolumens. Wird als übliche Praxis heute bei Datenspiegelungskonzepten in Kauf genommen

16

Fragen ?

Vielen Dank!

Georgios Raptis
Referent Projekt eArztausweis
Bundesärztekammer
georgios.raptis@baek.de
030 400456304

17