Elektronische Signaturen in der Telematikinfrastruktur

Andreas Hallof, Manuel Koch, Sven Marx, Arno Elmer

Datenschutz und Datensicherheit
gematik mbH
Friedrichstraße 136
10117 Berlin
Informationssicherheit@gematik.de

Abstract: Ziel der Telematikinfrastruktur (TI) ist es, durch eine Vernetzung der Beteiligten des Gesundheitswesens die Qualität, Transparenz und Wirtschaftlichkeit der Behandlung für Patientinnen und Patienten zu verbessern. Befunde und notwendige Behandlungsdaten sollen unter Einwilligung der Patientinnen und Patienten den behandelnden Leistungserbringern zügig und sicher zur Behandlung zur Verfügung stehen. Unnötige und zum Teil medizinisch schädliche Mehrfachuntersuchungen sind vermeidbar. Kommunikationsprozesse und Behandlungsdokumentationen sollen rechtssicher elektronisch gestaltet und somit effizienter werden, um den Leistungserbringern im Gesundheitswesen mehr Zeit für die Versorgung von Patientinnen und Patienten zu geben. Ein Mittel, das für die Erreichung dieses Ziels angewandt wird, sind elektronische Signaturen. Der Beitrag soll darstellen wie elektronische Signaturen in der aktuellen Ausbaustufe der TI ermöglicht werden und dann anwendbar sind.

1 Einleitung

Die moderne medizinische Versorgung ist gekennzeichnet durch eine zunehmende Spezialisierung der Fachrichtungen. Der heutige Regelfall bei der Behandlung der Patientinnen und Patienten ist das (oft institutionsübergreifende) Zusammenwirken von mehreren Leistungserbringern. Befunde und notwendige Behandlungsdaten müssen im Laufe der Behandlung grundsätzlich unter Einwilligung des Patienten zeitnah und sicher ausgetauscht werden.

Aufgrund der Anzahl an unterschiedlichen Leistungserbringern ist dazu eine umfassende Kommunikationsinfrastruktur notwendig. Eine solche wird um so wertvoller für den einzelnen Nutzer, je mehr andere Nutzer durch diese erreichbar sind [And01, Kapitel 19.6]. Dies hat zur Folge, dass die Zugangsbedingungen zur Nutzung der Kommunikationsinfrastruktur der einzelnen Nutzer möglichst einfach sein sollten, um eine Verbesserung der Versorgungsqualität bestmöglich zu unterstützen.

2 Sicherheitsziele der Telematikinfrastruktur

Gleichzeitig gibt es ein notwendig herzustellendes und aufrecht zu erhaltendes Sicherheitsniveau, insbesondere ableitbar aus dem Bundesdatenschutzgesetz (BDSG), dem Sozialgesetzbuch (SGB) V, dem Sozialgesetzbuch X und §203 Strafgesetzbuch (StGB).

Dies führt u. a. zu folgenden Sicherheitszielen:

- Identifizierung: Zugriff auf Daten in der TI darf nur durch berechtige Teilnehmer erfolgen. Basis dafür ist die sichere Identifizierung der Teilnehmer.
- Integrität: Die Daten dürfen in der TI nicht unberechtigt verändert werden.
- Rechtssicherheit: Die Verarbeitung der Daten der medizinischen Behandlungsdokumentation muss rechtssicher erfolgen, damit die Daten für die weitere Behandlung genutzt werden können.

2.1 Sicherheitsziel Identifizierung

Die sichere Identifizierung der Teilnehmer ist die Basis für eine Zugriffskontrolle auf personenbezogene medizinische Daten.

Leicht zu etablierende Authentisierungsmechanismen wie Nutzername/Passwort-Verfahren erreichen für sich genommen keine hohe Mechanismenstärke [Bon12]. Sie können nur eingesetzt werden, wenn die Umgebung zusätzliche Sicherungsleistungen erbringen kann.

Der für die TI gewählte Ansatz ist die Mehr-Faktor-Authentisierung mit Hilfe von kryptographischen Algorithmen und Verfahren wie sie bspw. auch bei der qualifizierten elektronischen Signatur verwendet werden. Die sichere Entitäten- und Rollenidentifikation bildet die Basis für Zugriffskontrollmechanismen. Die kryptographischen Verfahren setzen voraus, dass die einzelnen Kommunikationsteilnehmer jeweils private Schlüssel besitzen, die

1. ausschließlich von ihnen verwendet werden können und
2. an korrekt erhobene und beglaubigte Identifizierungsdaten gebunden sind.

Die erste Forderung führte zur Designentscheidung, sicherheitszertifizierte[1] Smartcards als sicheren Schlüsselspeicher für kryptographische Schlüssel und als sichere Ausführungseinheit für kryptographische Verfahren mit diesen Schlüsseln für jeden Kommunikationsteilnehmer zu definieren und auszugeben.

Die zweite Forderung führt zu einer gemeinsamen Public Key Infrastructure (PKI) der TI. Diese verbindet schon bestehende PKI-Systeme der Kostenträger und der Leistungserbringer mittels des „Trust-service Status List"-Konzeptes ([NFS08], [ETS09]) in einem gemeinsamen Vertrauensraum. Die gemeinsame verpflichtende Certificate-Policy und die

[1] Beispiel: [BSI09]. Die veröffentlichen Spezifikationen der in der TI verwendeten Smartcards sind kostenfrei zugänglich unter http://www.gematik.de.

nachgewiesene Umsetzung (u. a. durch ein unabhängig geprüftes Sicherheitskonzept und Auditierungen vor Ort) der dort definierten Sicherheitsziele und Maßnahmen sorgen für eine korrekte Zuweisung der kryptographischen Schlüssel und eine korrekte Erzeugung von Zertifikaten. Die Informationssicherheitsmanagmentsysteme[2] (ISMS) der einzelnen Teil-PKI-en und das koordinierende ISMS der TI sorgen für die Aufrechterhaltung des notwendigen Datenschutz- und Informationssicherheitsniveaus.

2.2 Sicherheitsziel Integrität

Für die Sicherung der Integrität (im Sinne des IT-Grundschutzes,[3] vgl. auch [BA10]) der Daten in der TI werden digitale Signaturen, also elektronische Signaturen auf Basis von asymmetrischen Kryptographieverfahren, verwendet.

Institutionen des Gesundheitswesens erhalten Institutionskarten. Auf diesen gibt es Schlüssel und entsprechende Zertifikate, auf deren Grundlage digitale Signaturen zur Sicherung der Integrität und Authentizität von Dokumenten ermöglicht werden.

Kryptographische Schlüssel müssen stets zweckbestimmt verwendet werden ([ANS10, S. 20f], [NIS07, S. 44]). Bestimmte Verwendungszwecke, wie die Authentisierung mittels vom Angreifer bestimmbarer „zufälliger“ Challenges und die Dokumentensignatur schließen einander leicht ersichtlich aus. Andere „Mehrfachverwendungen“ von Schlüsseln erzeugen weit schwerer zu erkennende Sicherheitsprobleme. Daher ist es wichtig, dass für digitale Signaturen von Dokumenten nur speziell für diesen Zweck bestimmtes Schlüsselmaterial eingesetzt wird.

2.3 Sicherheitsziel Rechtssicherheit

Der Begriff Rechtssicherheit ist nicht klar definiert und setzt sich im Allgemeinen aus „Rechtmäßigkeit“ und „Beweissicherheit“ zusammen [S$^+$10]. Das Signaturgesetz bildet die Basis für die rechtliche Anerkennung eines qualifiziert elektronisch signierten Dokuments.

3 Elektronische Signaturen zum Erreichen der Sicherheitsziele

Der Konnektor ist eine sicherheitsevaluierte dezentrale Komponente[4] und bildet die Schnittstelle für ein System eines Leistungserbringers zum Zugang zu den Signaturfunktionen der in der TI zur Verfügung gestellten Smartcards. An ihm sind sicherheitszertifizierte

[2] vgl. ISO 27001

[3] https://www.bsi.bund.de/cln_174/DE/Themen/ITGrundschutz/itgrundschutz_node.html

[4] Diese Komponente unterliegt auch einer Common-Criteria-Evaluation/Zertifizierung, vgl. Protection Profile BSI-CC-PP-0046 (AK-EB), BSI-CC-PP-0047 (NK) und BSI-CC-PP-050 (AK-H).

eHealth-Kartenterminals angeschlossen, welche die Kontaktpunkte zu den Smartcards bilden.

3.1 Smartcards in der Telematikinfrastruktur

In der TI werden Smartcards als sicherer Schlüsselspeicher und Ausführungseinheit verwendet. Smartcards der TI speichern das kryptographische Schlüsselmaterial für Personen und Institutionen des Gesundheitswesens.[5] Die elektronische Gesundheitskarte (eGK) ist eine personenbezogene Smartcard für Versicherte, der elektronische Heilberufsausweis (HBA) eine personenbezogene Smartcard für Leistungserbringer (Ärzte, Zahnärzte, Apotheker, Psychotherapeuten etc.) und eine SMC-B eine Smartcard für Institutionen des Gesundheitswesen (u. a. Arztpraxen, Apotheken, Krankenhäuser, Krankenkassen). Für die Zuordnung der Smartcard zu einer Person bzw. zu einer Institution ist der jeweilige Kartenherausgeber verantwortlich:

- Die Kostenträger (Krankenkassen) sind für die eGK-Herausgabe inkl. der sich darauf befindlichen Zertifikate verantwortlich.
- Die Herausgabe von HBA und (nonQES) HBA-Zertifikaten liegt im Verantwortungsbereich der Leistungserbringerorganisationen bspw. der Ärztekammern auf Landesebene. Das QES-Zertifikat beantragt der Leistungserbringer selbstständig, wobei die Kammern als bestätigende Stelle für personenbezogene Attribute mitwirken. Der HBA ist eine sichere Signaturerstellungseinheit im Sinne des Signaturgesetzes.[6]
- Die Herausgabe und Erstellung von SMC-B erfolgen in der Verantwortungsdomäne der jeweiligen Sektorspitzenorganisationen (Deutsche Krankenhaus TrustCenter und Informationsverarbeitung GmbH, KV-Telematik ARGE für die Kassenärztliche Bundesvereinigung (KBV), Kassenzahnärztliche Bundesvereinigung (KZBV), Bundesärztekammer (BÄK), Bundespsychotherapeutenkammer (BPtK)) und die Gesetzliche Krankenversicherung (GKV).

Die folgende Tabelle zählt die Dateinamen (Elementary Files) der Zertifikate auf, die mit dem kryptographischen Schlüsselmaterial der eGK, des HBA und der SMC-B verbunden sind. Hierbei wird entsprechend der Sicherheitsziele zwischen Schlüsselmaterial für die Authentisierung, die elektronische Signatur zum Zwecke der Integrität und Authentizität sowie die qualifizierte elektronische Signatur zum Zwecke der Rechtssicherheit unterschieden.

[5] Smartcards werden auch für das kryptographische Schlüsselmaterial von technischen Komponenten genutzt. Die Smartcards technischer Geräte sind nicht Gegenstand dieses Beitrags.

[6] Das Schlüsselmaterial für die qualifizierte elektronische Signatur wird auf dem HBA mit geprüften Zufallsgenerator und Erstellungsverfahren erzeugt. Der private Signaturschlüssel verlässt niemals die sichere Signaturerstellungseinheit (HBA).

Sicherheitsziel	eGK	HBA	SMC-B
Authentisierung	ID.CH.AUT, ID.CH.AUTN, ID.eGK.AUT_CVC	ID.HP.AUT, ID.HPC.AUTR_CVC	ID.HCI.AUT, ID.SMC.AUTR_CVC
Integrität und Authentizität	-	-	ID.HCI.OSIG
Rechtssicherheit	optional (ID.CH.QES)	ID.HP.QES	-

Auf der eGK befindet sich neben einer personenbezogenen kryptographischen Identität zur Authentisierung (ID.CH.AUT) ebenfalls eine kryptographische Identität zur pseudonymen Authentisierung des Versicherten (ID.CH.AUTN). Das Pseudonym wird vom Kartenherausgeber erzeugt und bei der Erstellung einer neuen eGK gewechselt.[7]

Die Smartcards besitzen neben kryptographischen Identitäten[8] basierend auf X.509-Zertifikaten[9] auch CV-Zertifikate[10] mit entsprechenden privaten Schlüsseln. Dieses Schlüsselmaterial wird zur gegenseitigen Authentisierung der eGK mit dem HBA bzw. der eGK mit der SMC-B verwendet. Dadurch wird u. a. sichergestellt, dass ein Zugriff auf die eGK nur durch Berechtigte erfolgen kann.

Weder die eGK noch der HBA besitzen neben dem (optionalen) QES-Schlüsseln kryptographisches Schlüsselmaterial dediziert für das Sicherheitsziel der Integrität (inkl. der Authentizität).

Die eGK kann optional Schlüsselmaterial für die Erzeugung einer qualifizierten elektronischen Signatur enthalten. Das entsprechende Schlüsselmaterial und Zertifikat muss der Versicherte selbstständig bei einem Zertifizierungsdiensteanbieter beantragen.

Die SMC-B enthält kein Schlüsselmaterial für die Erzeugung einer qualifizierten elektronischen Signatur, da es sich nicht um eine personenbezogene Smartcard handelt.

Die direkten Vorgaben für das kryptographische Schlüsselmaterial auf den Smartcards der TI erfolgen auf der Grundlage der Technischen Richtlinie TR-03116 [BSI12]. Eine Ausnahme hiervon bildet nur das Schlüsselmaterial für die qualifizierte elektronische Signatur, für die die Vorgaben der Bundesnetzagentur [BNe12] maßgeblich sind.

3.2 Anwendung von Signaturen

Der Konnektor erlaubt einem Anwendungssystem eines Leistungserbringers verschiedene Signaturvarianten von Dokumenten zu erzeugen. Für die qualifizierte elektronische Signatur ermöglicht er neben der Einzelsignatur von bspw. PDF/A-Dokumenten auch die Stapelsignatur [BSI07] von mehreren Dokumenten direkt hintereinander.

[7] Nur wenn ein Pseudonym regelmäßig gewechselt wird, dann ist die Pseudonymisierung ein wirksames Mittel gegen Profilbildung.

[8] ID.eGK.AUT_CVC, ID.HPC.AUTR_CVC, ID.SMC.AUTR_CVC

[9] RFC 5280

[10] vgl. DIN EN 14890-1:2009-03 Kapitel 14.3 (älter: ISO-7816 Teil 8) oder die kostenfrei zugängliche CWA 14890-1:2004 Kapitel 14.

Vor Beginn des Stapelsignatur-Prozesses wird eine Anzahl n von Signiervorgängen durch PIN-Eingabe autorisiert. Dann werden hintereinander (ohne zeitliche Unterbrechung) m Dokumente signiert mit $m \leq n$. Falls $n - m > 0$, entfallen die theoretisch noch autorisierten Signiervorgänge, und für weitere Signiervorgänge muss der Prozess inklusive Autorisierung neu gestartet werden.

Neben dieser Form einer Mehrfachsignatur (im Sinne von [BSI07]) gibt es auch die Möglichkeit von Mehrfachsignaturen im Sinne von CMS (PKCS#7) [Hou09], nämlich Parallelsignaturen und Gegensignaturen [HK06, S.71].

Bei einer Gegensignatur wird eine vorher (im Regelfall von einer anderen Person) erzeugte Signatur signiert („gegengezeichnet“).

Parallelsignaturen sind mehrere voneinander unabhängige Signaturen desselben Dokuments von unterschiedlichen Personen.

4 Ausblick

Die TI unterstützt elektronische Kommunikationsprozesse und rechtssichere Behandlungsdokumentationen und nutzt dazu elektronischen Signaturen. Durch technische und organisatorische Maßnahmen wird ein hohes Datenschutz- und Sicherheitsniveau erreicht. Das auf den Smartcards verteilte kryptographische Schlüsselmaterial und die notwendigen Prozesse der PKI tragen dazu bei, die Sicherheitsziele Identifizierung, Integrität und Rechtssicherheit zu erreichen.

In Bezug auf Sicherungsleistungen für Integrität und Authentizität von Dokumenten lässt sich die Leistungsfähigkeit der TI erhöhen. Das Einbringen von Schlüsselmaterial und entsprechende Zertifikate für eine digitale nicht-qualifizierte Signatur in den HBA und die eGK sind dafür Möglichkeiten.

Literatur

[And01] Ross Anderson. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley Publishing, Inc., 2001.

[ANS10] ANSSI. *Référentiel Général de Sécurité, Annexe B1, Règles et recommandations concernant la gestion des clés utilises dans des mécanismes cryptographiques*. Agence nationale de la sécurité des systèmes d'information, 26. Januar 2010.

[BA10] Mark Bedner und Tobias Ackermann. *Schutzziele der IT-Sicherheit*. DuD - Datenschutz und Datensicherheit, Mai 2010.

[BNe12] BNetzA. *Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), veröffentlicht am 18. Januar 2012 im Bundesanzeiger, Nr. 10, S. 243*. Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, April 2012.

[Bon12] Joseph Bonneau. *The science of guessing: analyzing an anonymized corpus of 70 million passwords*. 2012 IEEE Symposium on Security and Privacy, 2012.

[BSI07] BSI. *BSI TR-03114, Technische Richtlinie für die Stapelsignatur mit dem Heilberufsausweis*. Bundesamt für Sicherheit in der Informationstechnik, Oktober 2007.

[BSI09] BSI. *Protection Profile for electronic Health Card (eHC) - elektronische Gesundheitskarte (eGK), Version 2.6*. Bundesamt für Sicherheit in der Informationstechnik, 29. Juni 2009.

[BSI12] BSI. *BSI TR-03116, Technische Richtlinie für eCard-Projekte der Bundesregierung*. Bundesamt für Sicherheit in der Informationstechnik, April 2012.

[ETS09] ETSI. *ETSI TS 102 231: Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information*. ETSI, Dezember 2009.

[HK06] D. Hühnlein und U. Korte. *Grundlagen der elektronischen Signatur*. Schriftreihe des Bundesamt für Sicherheit in der Informationstechnik, Secumedia, 2006.

[Hou09] R. Housley. *Cryptographic Message Syntax (CMS)*. IETF, September 2009.

[NFS08] Frédéric Naujokat, Arno Fiedler und Wolfgang Schwab. *Akzeptanz von Vertrauensräumen in IT-Infrastrukturen*. DuD - Datenschutz und Datensicherheit, September 2008.

[NIS07] NIST. *NIST-SP-800-57 Recommendation for Key Management*. NIST, März 2007.

[S$^+$10] C. Seidel et al. *Empfehlungen für den Einsatz elektronischer Signaturen und Zeitstempel in Versorgungseinrichtungen des Gesundheitswesens*. Shaker Verlag, 2010.