Sicherheitsinfrastruktur im Gesundheitswesen

Gedankenskizze

(Entwurf Stand 05.06.00)

Dipl. Inform. Jürgen Sembritzki
Zentralinstitut für die kassenärztliche Versorgung
Höninger Weg 115, 50969 Köln
Tel.: 0221-4005-118, Fax: 0221-4005-147, E-mail: JSembritzki@kbv.de

Hinsichtlich der Einrichtung einer Sicherheitsinfrastruktur gibt es heute bereits eine Reihe von Definitionen, Standards und etablierter Verfahren und Mechanismen, deren Nutzung im Hinblick auf nationale und internationale Interoperabilität unumgänglich ist. Daneben existieren einige Wahlmöglichkeiten, deren Festlegungen entschieden werden müssen. Mehrere Standardisierungsgremien, internationale Gruppierungen und Projekte haben entsprechende Festlegungen getroffen und diese in zumeist frei verfügbaren Papieren publiziert. Zu nennen wären hier insbesondere (in alphabetischer Reihenfolge ohne Anspruch auf Vollständigkeit):

- DIN NI 17.4 Spezifikation der Schnittstelle zu Chipkarten mit Digitaler Signatur Anwendung
- HCP-Protokoll Spezifikation (Projekt unter Leitung der KV Bayerns)
- HPC-Spezifikation Version 1.1 (Elektronischer Arztausweis)
- Industrial Signature Interoperability Specification (ISIS)
- Kryptoreport der AG 3 “Medizinische Anwendungen einer vertrauenswürdigen Informationstechnik” im TeleTrusT Deutschland e.V.
- MailTrusT-Spezifikation Version 2 des TeleTrusT Deutschland e.V.
- Maßnahmenkatalog für digitale Signaturen Version 1.0 (RegTP)
- MKT-Spezifikation 1.0
- Netlink Workpackage 02 ”Requirements for Interoperability”
- Signaturgesetz SigG von 1997 (Gesetzgeber)
- Signatur-Interoperabilitätsspezifikation (BSI)
- Signaturverordnung SigV
- ThrustHealth-Dokumente
- VDAP Communication Standard

Weitere detailliertere Definitionen sind den genannten Papieren in deren Kapiteln “”Berücksichtigte Standards” bzw. den “Literaturangaben” zu entnehmen. Hier wird insbesondere auch deutlich, welcher Stellenwert einer noch ausstehenden Standardisierung eingeräumt wird.

Darüber hinaus bemühen sich neben den vorstehend bereits mit ihren Papieren Genannten eine ganze Reihe weiterer Organisationen um die Fortführung, Modifikation und Harmonisierung der bisherigen Definitionen. Dies sind u.a. (ohne Anspruch auf Vollständigkeit):

- Arbeitskreis „Sicherheitsinfrastruktur“ der AG „Karten und vernetzte Strukturen im Gesundheitswesen“
- Arbeitsgemeinschaft Trust-Center für digitale Signaturen

- CEN TC 251 “Health Informatics” WG III “Safety, Security and Quality”
- European Electronic Signature Standardization Initiative (EESSI)
- European Health Telematics Association (ETHEL)
- DIN AG INDI (Interoperabilität Digitaler Identität)
- DIN NI 17.4
- ISO TC 215 ”Health Informatics” WG 4 ”Security”

Die nachfolgende exemplarische Auflistung einzelner Komponenten einer Sicherheitsinfrastruktur mit zum Teil bereits konsensfähigen Festlegungen soll verdeutlichen, dass es als übergeordneter Aufgabe weniger um die eigentlichen Definitionen geht als vielmehr um die verbindlichen Entscheidungen für deren Einsatz und die Weichenstellungen dort, wo es einen Entscheidungsspielraum gibt. Es wäre sogar im Hinblick auf eine zügige Implementierung kontraproduktiv, bereits vielfach Hinterfragtes erneut einer Prüfung unterziehen zu wollen.

Kommunikation
Hinsichtlich des Aufbaus einer sicheren Kommunikation haben sich vor allem der Einsatz von SSL sowie zum Versand und Empfang SMTP/POP3 und S/MIME als Transportprotokoll als die von den meisten Applikationen unterstützten Standards herauskristallisiert.

Symmetrische Verschlüsselung
Hier werden der DES sowie der Triple DES am häufigsten genannt und von den meisten Applikationen auch unterstützt. Letzterer wird auch bzgl. der Digitalen Signatur als geeignet und zugelassen durch die RegTP genannt und dürfte von daher der Algorithmus der Wahl sein.
Allerdings werden im deutschen Gesundheitswesen auch andere Verfahren angewandt. So setzt die KBV zur Teilverschlüsselung der Abrechnungsdaten den IDEA ein, der als durchaus sicher anzusehen ist, jedoch keine allzu große Verbreitung hat.
Eine in diesem Zusammenhang noch ausstehende Aufgabe –nicht nur für die symmetrische Verschlüsselung- ist die Festlegung von Schlüssellängen, die für das Gesundheitswesen als zulässig und ausreichend beurteilt werden.

Asymmetrische Verschlüsselung
Der RSA mit einer Schlüssellänge von 1024 Bit ist hier der von allen akzeptierte Algorithmus. Er ist ebenfalls zur Digitalen Signatur zugelassen und sollte daher auch in dieser Form implementiert werden. Zwar gibt es auch Applikationen, die mit einer geringeren Schlüssellänge arbeiten, jedoch geht der Trend im Hinblick auf längerfristige Sicherheit zunehmend in Richtung längerer Schlüssel.
Frankreich setzt darüber hinaus derzeit noch den Diffie-Hellman Algorithmus zur sicheren Übermittlung des Session Keys ein.

Hashing
Hinsichtlich der Bildung des zu signierenden Hashwertes hat sich der SHA-1 mit 160 Bit eindeutig durchgesetzt. Allerdings werden auch häufig MD2 und MD5 unterstützt. Die Spezifikation des elektronischen Arztausweises nennt darüber hinaus auch den RIPEMD160 als mögliche Option.

Digitale Signatur
Die zum gesetzeskonformen Signieren zugelassenen Algorithmen werden von der RegTP im Bundesanzeiger veröffentlicht und sind somit verbindlich. Derzeit sind dies der Triple DES als symmetrischer Algorithmus sowie RSA 1024 Bit und Elliptische Kurven als asymmetrische Algorithmen.

Trust Center
Hinsichtlich einer gesetzeskonformen, "rechtsverbindlichen" Digitalen Signatur läßt das Signaturgesetz hier keinen Spielraum, gibt es doch eine zweistufige Hierarchie von Zertifizierungsstellen vor mit der RegTP als Wurzelinstanz. Auch die zu unterstützenden Dienste sind festgelegt.
Allerdings gibt es vor allem im Hinblick auf den Zeitstempeldienst noch erheblichen Definitionsbedarf.
Auch die Positionierung und Harmonisierung der Standpunkte und „Services" der Körperschaften und vergleichbaren Einrichtungen im Gesundheitswesen im Sinne einer geeigneten und abgestimmten „Policy" ist eine der vordringlich zu lösenden Aufgaben.

Zertifikatsstruktur
Hier besteht internationale Einigkeit, dass sich das Format der Zertifikate an dem Standard X.509v3 ausrichtet. Dennoch besteht auch hier noch ergänzender Definitionsbedarf hinsichtlich der Attributzertifikate.

Kartenterminals
Für die einzusetzenden Lesegeräte hat sich zumindest in Deutschland der Einsatz Multifunktionaler Kartenleser nach der MKT-Spezifikation 1.0 bzw. nach UCTS (Universal Chipcard Terminal Systemconcept) als konsensfähig herausgebildet. Andere Länder, vornehmlich Frankreich, verfolgen hier andere Konzepte, die zum Teil Sicherheitskomponenten in das Lesegerät integrieren. Auch die PC/SC Definitionen sind in diesem Zusammenhang zu beachten.

Diese Auflistungen sind exemplarisch und müssen weiter ausformuliert werden. Sie verdeutlichen allerdings bereits in diesem Stadium, dass die Definition einer Sicherheitsinfrastruktur schon jetzt von vielen Institutionen und Gremien intensiv vorangetrieben wird. Die Aufgabe einer nationalen Instanz, wie dem ATG, kann daher im wesentlichen "nur" darin bestehen, diese Festlegungen für die einzelnen Bereiche zu bewerten und über Empfehlungen so Stück für Stück die benötigte Kommunikationsplattform zu definieren.
Diese richtungsweisenden Entscheidungen würden dann gleichzeitig die Industrie in die Lage versetzen, die entsprechenden Soft- und Hardwarekomponenten sowie die notwendigen Dienstleistungen in großen Stückzahlen kostengünstig für eine entsprechende Implementation einer Sicherheitsinfrastruktur im Gesundheitswesen zur Verfügung zu stellen.