

Begleitende Information zur Security Schnittstelle Version 1.5 für den Datenaustausch im Gesundheitswesen

1 Grundsätze der Kryptosicherheit

Die Zuverlässigkeit von Kryptosystemen ist unmittelbar mit der fortschreitenden Entwicklung der Rechenleistung von IT-Systemen, der Entwicklung neuerer Algorithmen sowie der Forschung auf dem Gebiet der Kryptoanalyse verknüpft. Durch die Steigerung der Leistungsfähigkeit von IT-Systemen können bisher als sicher geltende Kryptoalgorithmen bzw. Schlüssellängen zukünftig möglicherweise kompromittiert werden.

1.1 Schlüsselbreiten

Bei asymmetrischen Verfahren sollte daher die Mechanismenstärke so gewählt werden, dass die Lösung der zu Grunde liegenden mathematischen Probleme einen unvertretbar großen bzw. praktisch unmöglichen Rechenaufwand erfordert (die zu wählende Mechanismenstärke hängt daher vom gegenwärtigen Stand der Algorithmik und der Rechentechnik ab). Das Bundesamt für Sicherheit in der Informationstechnik geht derzeit davon aus, dass Modullängen z. B. von 1024 Bit bei RSA ausreichende Sicherheit bieten. Um bei der geschilderten Dynamik eine gewisse Kontinuität zu erreichen, sind Modullängen erforderlich, die längerfristige Sicherheit bieten können. Die für das Gesundheitswesen festgelegten 2048-Bit bzw. 160-Bit basierenden Verschlüsselungsfunktionen bieten nach heutigem Kenntnisstand eine langfristige Sicherheit. Analysen haben in diesem Zusammenhang ergeben, dass damit von einer Sicherheit der Kryptoalgorithmen für mindestens die nächsten 6 Jahre ausgegangen werden kann.

1.2 Security-Schnittstelle für das Gesundheitswesen

Die erwähnte rasche technische Weiterentwicklung der PKI-Komponenten, die Integration der Internet Online-Dienste und die Anforderungen des Signaturgesetzes machen nun eine dementsprechende Aktualisierung der Security-Schnittstelle für das Gesundheitswesen erforderlich.

Die neue Fassung (Version 1.5) der Security-Schnittstelle für das Gesundheitswesen ist daher als die zwingende Fortschreibung der bisherigen Definitionen (Version 1.3, Stand: 23.07.2001) zu sehen.

Die Umstellung der bestehenden Sicherheitsverfahren erfolgt im Sinne einer Migration. Die Migrationsansätze sehen vor, dass die vorhandenen Anwendungen für einen bestimmten Zeitrahmen weiter genutzt werden können. Die Beteiligten sollen den Einsatzzeitpunkt für die modifizierten Applikationen, soweit keine unabdingbare Notwendigkeit gegeben ist, selbst bestimmen können. Dementsprechend soll sowohl die heute bestehende, als auch die sich aus den nachfolgenden Definitionen ergebende Security-Technologie bis zum Zeitablauf der im Umlauf befindlichen Teilnehmer-Schlüssel (PEM-Basis) parallel eingesetzt werden können (PKCS#7-/ neben PEM-Verschlüsselung).

Begleitende Information zur Security Schnittstelle Version 1.5 für den Datenaustausch im Gesundheitswesen

1.3 Elektronische Signatur

Neben den Minimalanforderungen, die von Kommunikations-Applikationen für das Gesundheitswesen erfüllt werden können, sind in der aktuellen Security-Schnitt-Stelle für das Gesundheitswesen auch optionale Definitionen im Hinblick auf das Signaturgesetz (elektronische Signatur) enthalten.

Das Signaturgesetz unterscheidet in Übereinstimmung mit der EG-Signaturrechtlinie folgende Signaturen:

- Elektronische Signatur (§ 2 Nr. 1 SigG),
- fortgeschrittene elektronische Signatur (§ 2 Nr. 2 SigG),
- qualifizierte elektronische Signatur (§ 2 Nr. 3 SigG),
- qualifizierte elektronische Signatur mit Anbieter-Akkreditierung (§ 15 Abs. 1 Satz 4 SigG).

Die qualifizierte elektronische Signatur dürfte wohl der EG-Mindeststandard sein. Sie hat folgende Merkmale:

- Der Anbieter erklärt, dass die Anforderungen des Signaturgesetzes erfüllt sind (behauptete Sicherheit ohne Nachweis).
- Die Signatur braucht nur mindestens sechs Jahre überprüfbar zu sein (anschließend darf der Anbieter die Zertifikate aus seinen Verzeichnissen löschen).

Die qualifizierte elektronische Signatur mit Anbieter-Akkreditierung – hier ist die Sicherheit nachgewiesen (durch gesetzlich anerkannte fachkundige Dritte) und dauerhaft überprüfbar (mindestens 30 Jahre).

Sicherlich sind alle genannten Arten der elektronischen Signatur je nach Verwendungszweck einsetzbar. Für einige Verfahren (z. B. optische Archivierung) ist aufgrund verfahrensrechtlicher Vorschriften die qualifizierte elektronische Signatur mit Anbieter-Akkreditierung vorgeschrieben (denn nur diese Art ist der eigenhändigen Unterschrift gleichgestellt). Daher ist auch zur Vermeidung verschiedener Sicherheitsstufen, eine einheitliche Stufe vorgesehen. Es erscheint sinnvoller, umfassende Sicherheit zu haben auch für die Kommunikationsabläufe, die dies nicht unbedingt notwendig machen. Daher wird, soweit eine elektronische Signatur angesprochen wird, von der qualifizierten elektronischen Signatur mit Anbieter-Akkreditierung (§ 15 Abs. 1 Satz 4 SigG) ausgegangen.

Begleitende Information zur Security Schnittstelle Version 1.5 für den Datenaustausch im Gesundheitswesen

2 Migration

Angesichts der absehbaren Entwicklungen Signaturgesetzkonformer Verfahren hat sich die Technische Arbeitsgruppe der gesetzlichen Krankenversicherung dafür ausgesprochen, die Weiterentwicklung (im Sinne einer Migration) in verschiedenen Phasen zu realisieren.

In der ersten Phase soll die Umstellung auf PKCS#7-basierende Verschlüsselungsverfahren erfolgen. Neben den daraus resultierenden zwangsläufigen Anpassungen soll in dieser Phase die Aktualisierung der Schlüssellänge des RSA-Algorithmus realisiert werden. Weiterhin wird als Hash-Funktion der SHA-1 Algorithmus der Einsatz von X.509 v3-Zertifikaten (ISIS-MTT Spezifikationen V1.0.2) und die Verwendung des Triple-DES mit dieser ersten Phase vorgeschrieben.

2.1 Investitionsschutz

Die sich aus der aktualisierten Version 1.5 der Security-Schnittstelle im Gesundheitswesen zwangsläufig ergebende Änderung bei den Mailspezifikation hin zu MIME bzw. S/MIME soll Gegenstand einer späteren Umstellungsphase sein. Bis dahin gelten insoweit die Spezifikationen (PEM) der Version 1.3 der Security-Schnittstelle im Gesundheitswesen unverändert weiter. Dies betrifft im besonderen die Datenformate (2.1), zur Zertifizierungsanforderung (4.4.1), zum Certification Request (4.8) und zum Kommunikationssystem (5.3).

Mit dieser Vorgehensweise sollen die Verfahrensänderungen, die Zusammenhang mit einer Umstellung von der File-Verschlüsselung (PEM) zur E-Mail-Verschlüsselung (S/MIME) entstehen, zunächst vermieden werden.

2.2 Zeitlicher Rahmenplan

Die Migrationsschritte analog des gewählten Phasenmodells stellen sich im einzelnen wie folgt dar:

1. ab Herbst 2003 wird ein Test der Basiskomponenten mit ausgewählten Kommunikationspartnern durchgeführt. Die Beteiligung erfolgt auf freiwilliger Grundlage, soweit die Voraussetzungen im Einzelfall gegeben sind. Die ITSG-GmbH stellt den Testteilnehmern der GKV-Verbände (bzw. deren Datenannahmestellen) bei entsprechender Bedarfsmeldung (z. B. wenn die jeweilige interne Applikation den Anforderungen bis dahin nicht genügt), eine PKCS#7-basierende Komponente (ohne Support) zur Verfügung.
2. Ab 01.12.2003 beteiligt sich mindestens eine Datenannahmestelle jeder Kas-
senart am Testverfahren.

**Begleitende Information zur
Security Schnittstelle Version 1.5
für den Datenaustausch im Gesundheitswesen**

3. Ab 01.07.2004 nehmen Datenannahmestellen am beschriebenen Testverfahren teil. Angestrebtes Ziel ist es dabei, die Tests auf der Grundlage der jeweiligen, den beschriebenen Anforderungen angepassten internen Applikationen, durchzuführen.
4. Die Entwicklungen und Erprobungen sind bis 31.12.2004 abgeschlossen. Der Praxisbetrieb im Parallelverfahren (Ausgangs- und Zielsystem) beginnt frühestens am 01.01.2005.

Die dargestellte Zeitrahmen ist als erste Planung zu verstehen. Soweit sich im weiteren Verlauf Erkenntnisse oder Notwendigkeiten ergeben, die Änderungen im zeitlichen Ablauf erforderlich machen, werden entsprechenden Korrekturen in gemeinsamer Abstimmung zwischen den Beteiligten vorgenommen.