Entwurf

Nachtrag vom 22.02.2016

mit Wirkung zum 01.03.2016

zur

Fortschreibung vom 20. September 2013

der

Rahmenvereinbarung zur Datenübertragung von Abrechnungsdaten bei Krankenhausleistungen in Verbindung mit § 17c KHG

Erläuterungen zu einzelnen Nachträgen

Nachtrag 1:

Gemäß der Vorgaben zu kryptographischen Verfahren des Bundesamtes für Sicherheit in der Informationstechnik (BSI TR 2102-1) wird die Verwendung des Triple-DES Verfahrens zum 29.2.2016 eingestellt, ab 1.3.2016 kommt als Verschlüsselungsalgorithmus AES-256 zur Anwendung. Dies ist bereits bei den Datenannahmestellen der Krankenkassen umgesetzt und ist nun ebenfalls in der technischen Anlage 4 der §301-Vereinbarung klarzustellen.

Nachträge zur Anlage 4

Nachtrag 1:

Anhang zu Anlage 4 (Verschlüsselung, Übertragungsdateien)

Vorbemerkung

Die nachfolgenden Regelungen dienen der Übernahme der für die Datenübermittlung nach § 301 SGB V bestehenden Verfahrenslösungen zwischen Krankenhäusern und Krankenkassen. Die Partner dieser Rahmenvereinbarung streben eine einheitliche Sicherheitsinfrastruktur für eine vertrauenswürdige und rechtssichere Kommunikation an.

1. Verschlüsselung

Als Basis für die Verschlüsselung wird ein asymmetrisches Verfahren für die Kommunikation eingesetzt, das folgenden Anforderungen genügt:

- Das Verschlüsselungsverfahren beruht auf RSA/~~DES~~AES.
- Die Schlüsselerzeugung erfolgt dezentral.
- Das Schlüsselmanagement erfolgt zentral über Trust-Center.

1.1 Datenformate

Die Datenformate sind entsprechend PKCS#7 (Public Key Cryptography Standard #7) zu strukturieren.

1.2 Session-Key

Als Session-Key ist ~~tripleDES~~ AES (RFC 3565) mit einer Schlüssellänge von 256 Bit und CBC-Betriebsmodus (id-aes256-cbc) vorzusehen.

~~Gemäß Migrationsplan zum AES ist ab 02.01.2015 bei allen Annahmestellen eine parallele Datenannahme von Triple-DES- und AES-verschlüsselten Nachrichten und Rücklieferung an die Teilnehmer (Krankenhäuser) mit Triple-DES-Algorithmus vorzusehen. Ab 01.03.2016 erfolgt ein kompletter Umstieg auf AES-Algorithmus bei Hin- und Rückweg; Triple-DES-verschlüsselte Nachrichten werden abgewiesen.~~

1.3 Interchange Key

Als Interchange Key ist RSA mit den unter 1.10 beschriebenen Parametern einzusetzen.

1.4 Hashfunktion/Signaturalgorithmus

Als Hash Funktion ist SHA-256 (Secure Hash Algorithm) vorzusehen. ~~Bis zur Ablauf der Migrationsphase kann auch SHA-1 verwendet werden.~~

1.5 RSA Schlüssellänge

Die RSA Schlüssellänge muss 2048 Bit (Standard) betragen.

1.6 Öffentlicher Exponent des RSA Algorithmus

Als RSA Exponent soll die 4. Fermat~~-4~~ Zahl (2^{16}+1) gewählt werden (siehe X.509~~, Annex C~~).

1.7 Public Key Format

Hier ist die ASN.1 Syntax [1)] sowie X.509 [2)] einzuhalten.

1.8 Zertifikate

Zertifikate sind in ASN.1 entsprechend X.509 zu implementieren. Bei der Codierung der Zertifikate sind die Distinguished Encoding Rules (DER) entsprechend X.509, Kapitel 8.7, einzuhalten.

Für die Schlüsselverwaltung wird eine Lösung entsprechend X.500 [3)] vorgesehen.

1.9 Struktur der X.500-Adresse

Die X.500-Adresse hat den Empfehlungen / Standards nach X.500 ff. zu entsprechen.

C	Country	DE
O	Organization	(Name des Trust Centers)
OU	Organization Unit	(Name der Institution)
OU	Organization Unit	(IK der Institution)
CN	Common Name (Allgemeiner Name)	(Name des Ansprechpartners)

1.10 Zusammenfassende Darstellung der Schnittstelle

Datenformate:	PKCS#7
Hash:	SHA-256
RSA Schlüssellänge:	2048 Bit
RSA Exponent:	4. Fermat~~-4~~ Zahl: (2^{16} + 1)
Public Key Format:	ASN.1 / X.509
Private Key Format:	nicht definiert
Zertifikate:	ASN.1 / X.509

Literaturhinweise

1) ASN.1 X.208 CCITT Recommendation X.208: Specification of Abstract Syntax Notation One (ASN.1), 1988
X.209 CCITT Recommendation X.209: Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1), 1988

2) X.509 CCITT Recommendation X.509: The Directory - Authentication Framework. 1988.

3) X.500 CCITT Recommendation X.500: The Directory - Overview of Concepts, Models and Services. 1988.