Nachtrag
vom 22.02.2016

zur Fortschreibung der § 301-Vereinbarung
vom 20.03.2014

mit Wirkung zum 01.03.2016

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:

11 Anhang zur Anlage 4 (Verschlüsselung, Übertragungsdateien) *wird wie folgt geändert:*

11.1 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 Zertifizierungs- bzw. Schlüsselverwaltungsstellen.

11.1.1 Datenformate

Die Datenformate sind entsprechend PKCS#7 zu strukturieren. ~~Solange die Formate nach PEM (Privacy Enhanced Mail) [1] noch gültig sind, können diese weiter verwendet werden (spätestens zum 30.06.2010 auslaufend).~~

11.1.2 Session-Key

Als Session-Key ist ~~tripleDES~~ AES (RFC 3565) mit einer Schlüssellänge von 256 Bit und CBC-Betriebsmodus (id-aes256-cbc) vorzusehen. ~~Für die Weiterverwendung der Formate nach PEM ist der Data Encryption Standard Algorithmus im Cipher Block Chaining Mode (DES-CBC, beschrieben in PEM, Request for Comments – RFC 1423 –) vorzusehen.~~

11.1.3 Interchange Key

Als Interchange Key ist RSA mit den unter 11.1.10 beschriebenen Parametern einzusetzen.

11.1.4 Hashfunktion/Signaturalgorithmus

Als Hash Funktion ist SHA-256 vorzusehen. ~~Für die Weiterverwendung der Formate nach PEM ist MD5 [2] vorzusehen.~~

11.1.5 RSA Schlüssellänge

Die RSA Schlüssellänge beträgt 2048 Bit (Standard). ~~Für die Weiterverwendung der Formate nach PEM muss die RSA Schlüssellänge 768 Bit betragen (siehe auch RFC 1423 Kap. 4.1.1).~~

11.1.6 Öffentlicher Exponent des RSA Algorithmus

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

11.1.7 Public Key Format

Hier ist die ASN.1 Syntax [3] sowie X.509 [4] einzuhalten.

11.1.8 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 [5)] vorgesehen.

Die Vereinbarungspartner sehen jeweils für ihre Zuständigkeitsbereiche ein oder mehrere Trust-Center/Schlüsselvergabestellen vor. Sie sorgen dafür, daß das/die Trust-Center bzw. die Schlüsselvergabestelle(n) der Spitzenverbände der Krankenkassen für die Krankenkassen und das/die Trust-Center bzw. die Schlüsselvergabestelle(n) der DKG für die Krankenhäuser ihre Schlüssel-Management-Politik abstimmen. Die Spitzenverbände der Krankenkassen und die DKG geben die jeweils von ihnen eingerichteten/bestellten Trust-Center/Schlüsselvergabestellen allen am Verfahren Beteiligten spätestens im 4. Quartal 1996 bekannt.

11.1.9 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)

11.1.10 Zusammenfassende Darstellung der Schnittstelle

Datenformate:	PKCS#7~~, bisher PEM~~
Hash:	SHA-256~~, bisher MD5 (Message Digest 5)~~
RSA Schlüssellänge:	2048 bit~~, bisher 768 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

11.1.11 Literaturhinweise

1) RFC 1421 J. Linn. RFC 1421: Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures. February 1993

RFC 1422 S. Kent. RFC 1422: Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management, February 1993.

RFC 1423 D. Balenson. RFC 1423: Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes and Identifiers February 1993.

RFC 1424 B. Kaliski. RFC 1424: Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services. February 1993.

2)	RFC1321	R. Rivest. RFC 1321; The MD5 Message Digest Algorithm
3)	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
4)	X.509	CCITT. Recommendation X.509: The Directory – Authentication Framework. 1988.
5)	X.500	CCITT. Recommendation X.500: The Directory Overview of Concepts, Models and Services. 1988.