Bundesamt
für Sicherheit in der
Informationstechnik

Technische Richtlinie BSI TR-03116-1

Kryptographische Vorgaben für Projekte der Bundesregierung

Teil 1: Telematikinfrastruktur

Version:	3.19
Datum:	03.12.2015
Autoren:	Technische Arbeitsgruppe TR-03116-1
Status:	Veröffentlichung
Fassung:	Dezember 2015

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-111
E-Mail: zertifizierung@bsi.bund.de
Internet: http://www.bsi.bund.de

1 ZIELSTELLUNG 6

2 GRUNDSÄTZE 7

2.1 Sicherheitsziele für den Einsatz kryptographischer Verfahren im Gesundheitswesen 7

2.2 Grundsätze der Sicherheitsbewertung 8

3 KRYPTOGRAPHISCHE ALGORITHMEN UND PARAMETER 9

3.1 Instanzauthentisierung und Schlüsselvereinbarung 9
3.1.1 Protokolle mit symmetrischen Kryptoalgorithmen 10
3.1.2 Protokolle mit asymmetrischen Kryptoalgorithmen 10

3.2 Datenauthentisierung 11
3.2.1 Hashfunktionen 11
3.2.2 Message Authentication Code 12
3.2.3 Signaturalgorithmen 12

3.3 Verschlüsselung 13
3.3.1 Symmetrische Verschlüsselung 13
3.3.2 Asymmetrische Verschlüsselung 15

3.4 Erzeugung von Zufallszahlen 15

3.5 Schlüsselerzeugung 16
3.5.1 Symmetrische Schlüssel 17
3.5.2 Asymmetrische Schlüssel 17

3.6 Schlüsselvereinbarung 18

4 ANWENDUNG KRYPTOGRAPHISCHER VERFAHREN 18

4.1 Instanzauthentisierung 18
4.1.1 Einsatzbereich 18
4.1.2 Kryptographische Verfahren 19

4.2 Qualifizierte elektronische Signatur 20
4.2.1 Einsatzbereich 21
4.2.2 Kryptographische Verfahren 21

4.3 Digitale nicht-qualifizierte elektronische Signaturen 21
4.3.1 Kryptographische Verfahren 22

4.4 Verschlüsselung von Dokumenten 22
4.4.1 Einsatzbereich 22

4.4.2 Kryptographische Verfahren 22

4.5 Kommunikation 23
4.5.1 Einsatzbereich 23
4.5.2 Kryptographische Verfahren 23

4.6 Bestandsanwendungen eGK Generation 1 25
4.6.1 eGK Generation 1 25
4.6.2 Kryptographische Verfahren 25

4.7 Schlüsselmanagement 26
4.7.1 Einsatzbereich 26
4.7.2 Kryptographische Verfahren 26

5 LITERATUR 27

Vorwort

Die Technische Richtlinie BSI TR-03116 stellt eine Vorgabe für Projekte der Bundesregierung dar. Die Technische Richtlinie ist in vier Teile gegliedert:

- Der vorliegende Teil 1 der Technischen Richtlinie legt die im Gesundheitswesen verbindlichen Sicherheitsanforderungen und –vorgaben für den Einsatz kryptographischer Verfahren für die elektronische Gesundheitskarte (eGK), den Heilberufsausweis (HBA) und die technischen Komponenten der Telematikinfrastruktur fest.
- Teil 2 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren in hoheitlichen Ausweisdokumenten [TR-03116-2].
- Teil 3 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für den Einsatz kryptographischer Verfahren für die Infrastruktur von intelligenten Messsystemen im Energiesektor [TR-03116-3].
- Teil 4 der Technischen Richtlinie beschreibt die Sicherheitsanforderungen für die Verwendung von SSL/TLS, S/MIME und OpenPGP in eGovernment-Anwendungen [TR-03116-4].

1 Zielstellung

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gibt mit dieser Technischen Richtlinie eine Bewertung der Sicherheit und eine langfristige Orientierung für den Einsatz kryptographischer Verfahren der elektronischen Gesundheitskarte, des Heilberufsausweises, der technischen Komponenten und der Dienste der Telematikinfrastruktur des Gesundheitswesens.

Diese Technische Richtlinie richtet sich an die gematik, die Hersteller von technischen Komponenten, die Herausgeber von elektronischen Gesundheitskarten (eGK), Heilberufsausweisen (HBA) und Secure Module Cards (SMC) und die Anbieter von Diensten und Anwendungen in der Telematikinfrastruktur. Sie ist verbindlich bei der Auswahl der kryptographischen Algorithmen.

Die in dieser Technischen Richtlinie betrachteten kryptographischen Verfahren wurden unter Berücksichtigung ihrer Sicherheit und Vertrauenswürdigkeit und des gegenwärtigen Standes der Spezifikationen ausgewählt. Für die genaue Spezifikation der kryptographischen Verfahren wird auf die einschlägige Literatur verwiesen.

Dieses Dokument soll in Übereinstimmung mit der weiteren Entwicklung des Einsatzgebietes, der kryptologischen Forschung und der Erfahrungen mit praktischen Realisierungen jährlich durch das BSI aktualisiert und bei Bedarf ergänzt werden.

Kapitel 2 beschreibt die Sicherheitsziele und die Grundsätze zur Bewertung des Einsatzes kryptographischer Verfahren im Gesundheitswesen.

In Kapitel 3 wird die **grundsätzliche Eignung von Algorithmen bzw. Sicherheitsverfahren** – unabhängig von der konkreten Applikation sowie Einsatzumgebung bzw. Anwendung in Komponenten in der Telematik im Gesundheitswesen – gegeben. Hierzu werden die Angaben anhand des vorgesehenen Sicherheitsmechanismus gegliedert. Dadurch kann ein spezifischer Algorithmus (z.B. AES) auch mehrfach genannt werden, sofern der Algorithmus für die Anwendung in verschiedenen Sicherheitsmechanismen (z.B. Authentisierung von Komponenten, Datenverschlüsselung und Schlüsselverwaltung) als geeignet bewertet wird.

Zu den in Kapitel 3 grundsätzlich als geeignet bewerteten kryptographischen Verfahren werden in Kapitel 4 **Empfehlungen zum Einsatz kryptographischer Verfahren für eine spezifische Anwendungen bzw. Einsatzumgebung** gegeben.

Generell enthält diese Technische Richtlinie nur Aussagen über die Eignung kryptographischer Verfahren bis Ende 2021. Abgesehen von unvorhergesehenen kryptographischen Durchbrüchen, die nicht vollkommen ausgeschlossen werden können aber unwahrscheinlich sind, lassen sich über einen Zeitraum von ca. 7 Jahren relativ verlässliche Aussagen machen. Ist eine weitere Verwendung des Verfahrens über diesen Zeitraum hinaus aus heutiger Sicht nicht ausgeschlossen, so wird dies mit 2021+ gekennzeichnet.

In dieser Technischen Richtlinie geht es um Aussagen zur Sicherheit von kryptographischen Algorithmen. Die Aussage „es wird die Verwendung von Algorithmus X empfohlen“ ist so zu verstehen, dass der Algorithmus X das in der vorliegenden technischen Richtlinie ange-

strebte Sicherheitsniveau erreicht. Dabei kann es durchaus vorkommen, dass manche empfohlenen Algorithmen ein höheres Sicherheitsniveau aufweisen als andere: zum Beispiel ist SHA-512 gegen heute absehbare Angriffe sicherer als SHA-256. Es kann auch vorkommen, dass in dieser Technischen Richtlinie nicht empfohlene kryptographische Algorithmen tatsächlich kryptographisch stark sind. Insgesamt werden nur gut untersuchte und für den praktischen Einsatz relevante Verfahren empfohlen, die gegen alle für den Vorhersagezeitraum als relevant eingeschätzten kryptoanalytischen Angriffsvektoren sicher sind.

Die langfristige Vertraulichkeit verschlüsselter Daten wirft grundsätzliche Probleme auf. Bei Verwendung der bis Ende 2021 als generell, d.h. ohne Beschränkung auf spezielle Anwendungen geeignet eingestuften und empfohlenen Verfahren zur Schlüsselvereinbarung und zur symmetrischen bzw. asymmetrischen Verschlüsselung (z. B. für Schlüsselaustausch) dürfte die Vertraulichkeit der verschlüsselten Daten nach Einschätzung des BSI im Zeitraum von ca. 10 Jahren (bis Ende 2025) noch ausreichend gesichert sein. Diese Einschätzung ist allerdings schon mit einem höheren Maß an Spekulation verbunden als die Aussagen über 7 Jahre und daher weniger belastbar. Aussagen zur Sicherheit über mehr als ein Jahrzehnt sind dagegen kaum möglich.

Da ein Angreifer die über das Internet übertragenen Daten langfristig speichern kann, um sie später zu entschlüsseln, kann ein ***langfristiger Schutz solcher Daten grundsätzlich nicht garantiert*** *werden.*

Daraus ergeben sich folgende Konsequenzen:

- Die über das Internet übertragene vertrauliche Information ist auf das notwendige Maß zu beschränken.
- Die Infrastruktur muss für einen Übergang auf stärkere kryptographische Verfahren ausgelegt sein. Insbesondere sind (z.B. auf Servern) gespeicherte vertrauliche Daten bei einem solchen Übergang neu zu verschlüsseln und die alten Datensätze zu löschen.

Bemerkung zu der Hashfunktion SHA-1: Die Kollisionsangriffe der Arbeitsgruppe um die chinesische Kryptologin X. Wang haben eine dynamische Entwicklung bei der kryptographischen Analyse von Hashfunktionen ausgelöst. Daher muss die weitere Entwicklung bei der Hashfunktion SHA-1 im Auge behalten werden; alle Aussagen dieses Papiers hierzu sind als vorläufig zu betrachten und können sich im Rahmen der vorgesehenen jährlichen Anpassung (oder einer Anpassung bei Bedarf) der technischen Richtlinie ändern.

2 Grundsätze

2.1 Sicherheitsziele für den Einsatz kryptographischer Verfahren im Gesundheitswesen

Der Einsatz kryptographischer Verfahren im Gesundheitswesen erfolgt mit den folgenden übergreifenden Sicherheitszielen:

1. Die kryptographischen Verfahren sollen die Vertraulichkeit personenbezogener insbesondere medizinischer Daten bei deren Übertragung und während ihrer Speicherung in technischen Systemen der Telematikinfrastruktur des Gesundheitswesens auch langfristig sichern.

2. Die kryptographischen Verfahren sollen die Authentizität und Verbindlichkeit insbesondere personenbezogener Verordnungen, medizinischer Daten und anderer Dokumente durch qualifizierte elektronische Signatur und in gesondert ausgewiesenen Anwendungsbereichen durch fortgeschrittene Signatur bei vergleichbarer kryptographischer Sicherheit gewährleisten.

3. Die kryptographischen Verfahren sollen die sichere Authentisierung der Kommunikationspartner als Voraussetzung für die Zugriffskontrolle auf die Ressourcen der Telematikinfrastruktur sowie den Schutz der Vertraulichkeit und Integrität der Kommunikation technischer Komponenten unabhängig von den oben genannten Sicherheitsanforderungen gewährleisten.

Bemerkung: Das Sicherheitsziel der Verfügbarkeit der technischen Komponenten sowie die Sicherung der Systeme wie Primärsysteme, die zum Zugriff auf die Klardaten autorisiert sind, stehen außerhalb der Betrachtung dieser TR.

Die kryptographischen Verfahren sollen durch nachgewiesen vertrauenswürdige technische Komponenten implementiert werden. Die Vertrauenswürdigkeit der technischen Komponenten soll jeweils dem vorgesehenen Einsatzzweck angemessen durch Common Criteria Zertifikate, ergänzende Verfahren des BSI oder andere Sicherheitsgutachten nachgewiesen werden.

Mit den Sicherheitsvorgaben dieser Technischen Richtlinie wird ein Sicherheitsniveau von mindestens 100 Bit angestrebt. Anwendungsspezifische Ausnahmen müssen begründet werden.

2.2 Grundsätze der Sicherheitsbewertung

Die Sicherheitsbewertung der kryptographischen Verfahren erfolgt auf dem gegenwärtigen Stand kryptographischer Erkenntnisse in Übereinstimmung mit den Sicherheitserfordernissen und unter Berücksichtigung der Einsatzbedingungen der elektronischen Gesundheitskarte, des Heilberufsausweises und technischer Komponenten der Telematikinfrastruktur des Gesundheitswesens. Die in diesem Dokument getroffenen Sicherheitsbewertungen kryptographischer Verfahren sind an die beschriebenen Einsatzbereiche gebunden. Ebenfalls wird vorausgesetzt, dass die Implementierungen und Hintergrundsysteme (wie z.B. die eingesetzten PKIs) dem Stand der kryptographischen Forschung entsprechen und korrekt arbeiten.

Die Sicherheitsbegutachtung der Produkte soll die Implementierung kryptographischer Verfahren einschließen. Die notwendige Vertrauenswürdigkeit kann aber im Rahmen der Produktevaluierung nur für solche kryptographischen Verfahren erreicht werden, zu denen bereits ausreichend gesicherte kryptographische Erkenntnisse vorliegen. Dieses Dokument

unterstützt die Evaluierung und Zertifizierung der technischen Komponenten als Referenz auf sichere kryptographische Verfahren, da deren Bewertung nicht innerhalb der Produktevaluierung geleistet werden kann.

Für eine langfristige Planungssicherheit der Spezifikation, Entwicklung, Produktion und Anwendung der Produkte werden Empfehlungen zur weiteren Entwicklung der kryptographischen Verfahren gegeben. Die Orientierung an den Prognosen muss mit der kontinuierlichen Überwachung der Systemsicherheit und der Vorbereitung fallbezogener Maßnahmen zum Erhalt und ggf. zur Wiederherstellung der Systemsicherheit verbunden sein.

Es ist vorgesehen, die in diesem Dokument getroffenen Bewertungen und Orientierungen regelmäßig, mindestens jährlich zu überprüfen.

3 Kryptographische Algorithmen und Parameter

In diesem Kapitel werden die folgenden Sicherheitsmechanismen betrachtet:

- Instanzauthentisierung (Gegenseitige Authentisierung von Komponenten) mit bzw. ohne Schlüsselvereinbarung,
- Datenauthentisierung (Message Authentication Code, Hashfunktionen, Signaturverfahren),
- Verschlüsselung,
- Erzeugung von Zufallszahlen und
- Schlüsselerzeugung.

Zu den einzelnen Algorithmen bzw. Sicherheitsmechanismen werden relevante internationale Standards angegeben.

Empfehlungen bzw. Einschränkungen werden in diesem Kapitel nur getroffen, sofern diese nicht an eine bestimmte Anwendung gebunden sind.

3.1 Instanzauthentisierung und Schlüsselvereinbarung

Unter kryptographischer Instanzauthentisierung wird im Folgenden die Authentisierung einer technischen Komponente (Beweisender) als Nachweis einer angegebenen Identität (Identifizierung) gegenüber einer anderen technischen Komponente (Prüfender) durch ein kryptographisches Protokoll verstanden. Der Beweisende weist dabei die Kenntnis (oder allgemeiner die Fähigkeit zur Anwendung) eines Geheimnisses (Verifikationsdaten) nach. Bei symmetrischen kryptographischen Primitiven ist dies ein geheimer kryptographischer Schlüssel und bei asymmetrischen kryptographischen Primitiven ein privater kryptographischer Schlüssel (Verifikationsdaten). Der Prüfende nutzt bei symmetrischen kryptographischen Primitiven den gleichen geheimen kryptographischen Schlüssel und bei asymmetrischen kryptographischen Primitiven einen zum privaten kryptographischen Schlüssel passenden öffentlichen Schlüssel (Referenzdaten). Die Authentisierung kann auch gegenseitig erfolgen.

Zweckmäßigerweise wird die Instanzauthentisierung mit der Vereinbarung geheimer kryptographischer Schlüssel verbunden, um die Vertraulichkeit und Integrität einer anschließenden Kommunikation zwischen den Komponenten zu sichern.

Die Authentisierung mit Chipkarten nutzt die Authentisierung durch Wissen (z. B. PIN) gegenüber der Chipkarte, die danach eine kryptographische Instanzauthentisierung z. B. gegenüber einem Server durchführen kann.

Das PACE-Protokoll verbindet die Authentisierung von Personen mit PIN bzw. Passwort gegenüber einer Chipkarte mit der gegenseitigen Authentisierung und der Vereinbarung von symmetrischen Schlüsseln zwischen dem benutzten Kartenterminal und der Chipkarte zur Verschlüsselung und Datenintegritätssicherung der Kommunikation (siehe Secure Messaging im Kapitel 4.5.2). Es verbindet somit die Benutzerauthentisierung und die Instanzauthentisierung.

3.1.1 Protokolle mit symmetrischen Kryptoalgorithmen

Für den Einsatz in der Telematik im Gesundheitswesen werden grundsätzlich die folgenden symmetrischen Kryptoalgorithmen für Protokolle zur Instanzauthentisierung ggf. mit Aushandlung von kryptographischen Schlüsseln als geeignet bewertet:

- AES-128 (AES mit 128 Bit langem Schlüssel)
- AES-192 (AES mit 192 Bit langem Schlüssel)
- AES-256 (AES mit 256 Bit langem Schlüssel)

Die Anwendung des AES erfolgt gemäß [FIPS 197].

Das Protokoll zur Authentisierung von Chipkarten gemäß [EN-14890-1, Abschnitt 8.8] und die Ableitung der Sessionkeys auf Grundlage von [ANSI X9.62, Abschnitt 5.6.3] sind geeignet. Zur Ableitung von Sessionkeys ist eine hierzu geeignete Hashfunktion (siehe Abschnitt 3.2.1) einzusetzen.

3.1.2 Protokolle mit asymmetrischen Kryptoalgorithmen

Für den Einsatz in der Telematik im Gesundheitswesen werden grundsätzlich die folgenden asymmetrischen Verfahren zur Instanzauthentisierung ggf. mit Aushandlung von kryptographischen Schlüsseln als geeignet bewertet:

- RSA Geräteauthentisierung gemäß [eGK Teil1, Abschnitt 16.4.2] und Schlüsselvereinbarung gemäß [eGK Teil 1, Abschnitt 7.2.1],
- Diffie-Hellman-Schlüsselvereinbarung mit Authentisierung gemäß [EN-14890-1, Anhang A.3.1.2],
- PACE gemäß [TR-03110] mit ECDH und AES.

Als grundlegende Algorithmen werden RSA, DSA sowie DSA-Varianten auf elliptischen Kurven als geeignet bewertet. Wenn die gegenseitige Authentisierung von Komponenten mit Schlüsselvereinbarung mit TLS gemäß [RFC4346] (TLS Version 1.1), [RFC5246] (TLS Version 1.2) oder mit dem Internet Key Exchange IKEv2 gemäß [RFC 7296] bzw. [RFC 5996] erfolgen soll, sind nur geeignete Kryptoalgorithmen (asymmetrisch: RSA, DSA, DSA-Varianten auf elliptischen Kurven und Diffie-Hellman-Protokolle; symmetrisch: AES-128, AES-192 und AES-256) zu verwenden. Anwendungsspezifische Einschränkungen werden in Kapitel 4 definiert.

3.2 Datenauthentisierung

Unter kryptographischer Datenauthentisierung werden im Folgenden Verfahren verstanden, die eine Prüfung erlauben, ob Daten bei einer Übertragung oder Speicherung verändert wurden. Ein Datensender (Beweisender) erzeugt unter Verwendung eines Geheimnisses (kryptographischer Schlüssel) für die zu authentisierenden Daten eine Prüfsumme. Der Datenempfänger (Prüfender) prüft, ob die vorgelegte Prüfsumme mit dem Geheimnis des angegebenen Beweisenden für die vorgelegten Daten erzeugt wurden. Bei symmetrischer Datenauthentisierung benutzen Beweisender und Prüfender das gleiche Geheimnis. In diesem Fall kann also auch nicht zwischen dem Beweisenden und dem Prüfenden als möglichem Erzeuger der Prüfsumme gegenüber einem Dritten unterschieden werden. Bei asymmetrischen Verfahren benutzt der Beweisende seinen privaten Schlüssel zur Erzeugung der Prüfsumme und der Prüfende den dazugehörigen öffentlichen Schlüssel zur Prüfung der Daten und der Prüfsumme. Die Zuordnung des öffentlichen Schlüssels zum Besitzer des dazugehörigen privaten Schlüssels erfolgt durch ein Zertifikat.

3.2.1 Hashfunktionen

Eine Hashfunktion berechnet aus einer beliebigen endlichen Zeichenkette eine binäre Folge einer festen Länge (Hashwert). Die wichtigste Eigenschaften kryptographischer Hashfunktionen sind folgend aufgelistet:

- Kollisionsresistenz: Es soll praktisch unmöglich sein, zwei verschiedene Nachrichten zu finden, die den gleichen Hashwert haben.
- Preimage-Resistenz: Zu einem gegebenen zufälligen Hashwert soll es praktisch unmöglich sein, eine Nachricht mit diesem Hashwert zu konstruieren.
- Second-Preimage-Resistenz: Zu einer gegebenen Nachricht soll es praktisch unmöglich sein, eine andere zweite Nachricht zu finden, die den gleichen Hashwert hat.
- Für verschiedene Anwendungen von Hashfunktionen wird oft verlangt, dass die Hashfunktion - beziehungsweise genauer gesagt ein abgeleitetes schlüsselabhängiges kryptographisches Konstrukt wie ein HMAC, der die Hashfunktion als kryptographische Kernkomponente verwendet - nicht unterscheidbar sein soll von einer Zufallsfunktion.

Die Kollisionsresistenz ist unter diesen Eigenschaften den größten praktischen Bedrohungen ausgesetzt.

Für den Einsatz in der Telematik im Gesundheitswesen werden grundsätzlich die Hashfunktionen gemäß der aktuellen [BKryA], Kapitel 2 „Geeignete Hashfunktionen“ mit den dort angegebenen Zeiträumen als geeignet bewertet.

Derzeit wird der SHA-1 ([FIPS 180-4] und [ISO10118-3]) für den Einsatz in den Verfahren HMAC, Schlüsselableitung und Erzeugung von Zufallszahlen auch noch längerfristig als geeignet bewertet. Allerdings sollten auch für diese Anwendungen, wenn immer möglich, die Hashfunktionen SHA-256, SHA-384, SHA-512 genutzt werden.

3.2.2 Message Authentication Code

Ein Message Authentication Code (MAC) ist ein symmetrisches Datenauthentisierungsverfahren, das sich üblicherweise auf Blockchiffrieralgorithmen und Hashfunktionen als kryptographische Primitive stützt.

Für den Einsatz in der Telematik im Gesundheitswesen werden die folgenden Verfahren zur Erzeugung und Prüfung von Message Authentication Codes als grundsätzlich geeignet bewertet:

- AES-*k* mit $k \in \{128,192,256\}$ CMAC [FIPS 197], [SP800-38B]
- HMAC-SHA-1 [RFC 2104] bzw. [RFC 2404] mit einer Schlüssellänge von mind. 16 Bytes und mit der Hashfunktion SHA-1 [FIPS 180-4] und [ISO10118-3]
- HMAC-SHA-224, -SHA256, -SHA-384, -SHA-512 [RFC 2104] mit einer Schlüssellänge von mind. 16 Bytes und mit den Hashfunktionen SHA-224, SHA-256, SHA-384, SHA-512 [FIPS 180-4]

Die Anwendung des AES erfolgt gemäß [FIPS 197] und CMAC gemäß [SP800-38B]. Bei Verwendung eines CMACs mit einer MAC-Länge kleiner als 128 Bit, ist zu begründen, warum die MAC-Länge im konkreten Anwendungsfall vertretbar ist (vgl. [SP800-38B, Appendix A]).

Das Verfahren HMAC-SHA-1 gilt als geeignet für das in TLS und IKE verwendete Verfahren HMAC. Darüber hinaus kann auch eine der Hashfunktionen SHA-224, SHA-256, SHA-384 und SHA-512 verwendet werden. Gegenüber dem HMAC-SHA1 sind die auf den letztgenannten Hashfunktionen basierenden HMAC-Konstruktionen aus Sicherheitssicht vorzuziehen.

3.2.3 Signaturalgorithmen

Für den Einsatz in der Telematik im Gesundheitswesen werden grundsätzlich die Algorithmen für digitale Signaturen, d. h. elektronische Signaturen auf Basis von asymmetrischen Kryptographieverfahren (bspw. RSA, ECDSA etc.), als geeignet bewertet, die die Anforderungen gemäß der aktuellen [BKryA], Kapitel 3 „Geeignete Signaturverfahren“ erfüllen.

Für die Anwendung der qualifizierten elektronischen Signatur im Gesundheitswesen werden die Kryptoalgorithmen RSA, DSA in Körpern der Form F_p mit einer Primzahl p und die DSA-Varianten auf geeigneten elliptischen Kurven über Körpern der Charakteristik p, p > 2 empfohlen. Im Hinblick auf die Auswahl geeigneter elliptischer Kurven bietet sich die Verwendung von gut analysierten Kurvenparametern an; die vorliegende Technische Richtlinie empfiehlt den Einsatz von Brainpool-Kurven mit geeigneter Bitlänge. Bei den Verfahren ECDSA, ECGDSA und EC-KCDSA sollte die Bitlänge der verwendeten Hashwerte gemäß [TR-03111] gleich der Bitlänge der Ordnung q der Punktegruppe sein (vgl. Abschnitt 3.6), anderenfalls muss der Hashwert standardkonform abgeschnitten werden (vgl. [TR-03111, Abschnitt 4.2]).

Für die Formatierung des Inputs des Signaturverfahrens (Digital Signature Input – DSI bzw. Digest Info – DI) können grundsätzlich die Verfahren[1] verwendet werden, die auch gemäß der aktuellen [BKryA], Kapitel 3.1 „RSA-Verfahren“ als geeignet angesehen werden.

Die Schlüssellängen und andere Parameter der Signaturalgorithmen unterliegen Einschränkungen in Abhängigkeit vom Zeitraum der Gültigkeit und des vorgesehenen Anwendungsbereiches. Sie werden im Kapitel 4 beschrieben.

Anmerkung: Für die Anwendung von elliptischen Kurven wird auch auf die Dokumente [TR-03111] und [ECCBP] verwiesen.

3.3 Verschlüsselung

Die Verschlüsselung dient der Gewährleistung der Vertraulichkeit von Informationen unter der Bedingung, dass Unbefugte die verschlüsselten Daten zur Kenntnis erhalten und nur der Entschlüsselungsschlüssel geheim gehalten wird. Die Integrität der Daten wird allein durch Verschlüsselung nicht geschützt. Die verwendeten Verschlüsselungsverfahren werden für den hier betrachteten Einsatzbereich als bekannt vorausgesetzt. Verschlüsselungsverfahren werden bei der Datenübertragung und der Datenspeicherung eingesetzt.

3.3.1 Symmetrische Verschlüsselung

Bei der symmetrischen Verschlüsselung erfolgt die Verschlüsselung und die Entschlüsselung mit dem gleichen geheimen Schlüssel.

Für den Einsatz in der Telematik im Gesundheitswesen werden grundsätzlich die folgenden symmetrischen Verfahren zur Verschlüsselung als geeignet bewertet:

- AES-*k* im CBC Mode mit $k \in \{128,192,256\}$,
- AES-*k* im Counter Mode (CTR) mit $k \in \{128,192,256\}$ und

[1] Im nachfolgenden Text des Vorgabenkatalogs ist für das Signaturformat ISO-9796-2 [ISO9796-2] immer DS2 bzw. DS3 gemeint.

- AES-*k* im Galois/Counter Mode (GCM) mit $k \in \{128,192,256\}$.

Die Anwendung des AES erfolgt gemäß [FIPS 197]. Empfehlungen zu den Betriebsarten finden sich in [SP800-38A] und [SP800-38D].

Bei der Verwendung der empfohlenen Betriebsarten für Blockchiffren sind die Hinweise aus [TR-02102-1, Abschnitt 2.1.2] zu beachten. Insbesondere dürfen sich Zählerstände im Counter-Modus und im GCM-Modus nicht innerhalb einer Schlüsselperiode [SP800-57, Abschnitt 2.1] wiederholen. Im CBC-Modus ist die Verwendung unvorhersagbarer oder verschlüsselter Initialisierungsvektoren wie in [TR-02102-1, Abschnitt B.2] sicherzustellen. Im CBC-Modus und im Counter-Modus sind noch keine kryptographischen Mechanismen zum Schutz der Integrität übertragener Daten enthalten. Es ist im Allgemeinen notwendig, bei Verwendung dieser Betriebsarten einen Integritätsschutz durch separate kryptographische Mechanismen zu implementieren, zum Beispiel durch einen CMAC oder HMAC über die verschlüsselten Daten. Beim Galois/Counter Mode müssen die Anwendungsvorgaben aus [SP800-38D], insbesondere auf die Wahl des Initialisierungsvektors und die maximale Anzahl der Verschlüsselungen mit dem selben Schlüssel eingehalten werden. Weitere anwendungsbezogene Festlegungen erfolgen im Kapitel 4.

Bei Verwendung des AES im CBC-Modus müssen die zu verschlüsselnden Anwendungsdaten mit einem Padding-Verfahren vor der Verschlüsselung behandelt werden, da im Allgemeinen nicht davon auszugehen ist, dass die Länge der Anwendungsdaten immer ein Vielfaches der Blocklänge der AES-Chiffre ist. Wir gehen aber im Folgenden davon aus, dass die Länge der zu übermittelnden Daten wenigstens immer einer ganzen Anzahl von Bytes entspricht. Außerdem nehmen wir an, dass die Blocklänge der verwendeten Blockchiffre kleiner als 256 Byte ist; da der AES als einzige empfohlene Blockchiffre eine Blocklänge von 16 Byte aufweist, ist dies in der Praxis keine Einschränkung. Folgende Padding-Verfahren sind dann zulässig:

- ISO-Padding (vgl. [ISO7816-4]): Es werden mindestens ein ’80’-Byte und so viele ‘00’-Bytes an die zu verschlüsselnden Anwendungsdaten angehängt, bis die Länge dieser ergänzten Anwendungsdaten in Byte ein Vielfaches der Blocklänge des Blockchiffrieralgorithmus (16 Byte für AES) ist.
- Padding gemäß [RFC 5652]: Bei einer Blocklänge von *b* Bytes und einer Nachricht von *n* Bytes wird mit $b - (n \bmod b)$ Bytes des Wertes $b - (n \bmod b)$ (vorzeichenlose 1-Bytezahlen) aufgefüllt.
- ESP-Padding gemäß [RFC 4303][2]: Das erste Padding-Byte ist ’01’, die folgenden Padding-Bytes bilden eine fortlaufende Folge ’02’, ’03’ … (vorzeichenlose 1-Bytezahlen) bis ein Vielfaches der Blocklänge für den Blockchiffrieralgorithmus (16 Byte für AES) erreicht ist.

[2] RFC 4303 lässt bis zu 255 Padding-Bytes zu.

- Padding gemäß [XMLEnc]: Bei einer Blocklänge von *b* Bytes und einer Nachricht von *n* Bytes werden zunächst *b* - (*n* mod *b*) - 1 zufällige Bytes angehängt und abschließend das Byte mit dem Wert *b*-(*n* mod *b*) angehängt. An die Erzeugung der zufälligen Bytes werden hierbei keine der in Abschnitt 3.4 beschriebenen Anforderungen gestellt.

Bei der Verwendung des CBC-Modus ist darauf zu achten, dass nicht aufgrund von Fehlermeldungen Seitenkanalangriffe ermöglicht werden (siehe bspw. [Vaudenay-2002] und [BreakingXMLEnc]).

3.3.2 Asymmetrische Verschlüsselung

Bei der asymmetrischen Verschlüsselung erfolgt die Verschlüsselung mit dem öffentlichen Schlüssel und die Entschlüsselung mit dem privaten Schlüssel, wobei der private Schlüssel praktisch nicht allein aus dem öffentlichen Schlüssel berechnet werden kann.

Für den Einsatz in der Telematik im Gesundheitswesen werden grundsätzlich die folgenden asymmetrischen Verfahren zur Verschlüsselung von Schlüsseln als geeignet bewertet:

- RSA [RSA]
- EC-KAEG [TR-03111] (eine Variante des ECIES aus ANSI X9.63)

Bei der Verschlüsselung mittels RSA müssen die zu verschlüsselnden Daten zunächst durch ein geeignetes Verfahren formatiert werden. Die folgenden Verfahren (Encoding Schemes) sind dafür zulässig:

- RSAES-PKCS1-v1_5 [PKCS #1 v2.1]
- RSAES-OAEP [PKCS #1 v2.1]

Es wird empfohlen, nicht das PKCS1-v1_5 Verfahren zu verwenden, da bei diesem Verfahren spezielle Maßnahmen gegen gewisse Seitenkanalangriffe nötig sind (vgl. Abschnitt 7.2, insbesondere die Bemerkung auf S. 25 von [PKCS #1 v2.1]). Falls das Verfahren verwendet wird, müssen die dort beschriebenen Maßnahmen umgesetzt werden.

Asymmetrische Verschlüsselungen werden im allgemeinen nur zur Verschlüsselung von Schlüsseln und nicht zur Verschlüsselung von Anwendungsdaten verwendet.

Im Kapitel 4 sind geeignete Schlüssellängen für ausgewählte Anwendungen aufgelistet.

3.4 Erzeugung von Zufallszahlen

Die Erzeugung von Zufallszahlen ist erforderlich für die Erzeugung von

- Challenges in Authentisierungsprotokollen,
- zufälligen Paddingbits bzw. Saltwerten sowie
- kryptographischen Schlüsseln bzw. Systemparametern.

Grundsätzlich können für die Erzeugung von Zufallszahlen physikalische Zufallszahlengeneratoren oder Pseudozufallszahlengeneratoren eingesetzt werden. Entsprechend dem gewählten Generator sind die Anforderungen gemäß [AIS 20] für Pseudozufallszahlengeneratoren und [AIS 31] für physikalische Zufallszahlengeneratoren einzuhalten.

Die Erzeugung von **kryptographischen Schlüsseln und Systemparametern** wird in Kapitel 3.5 behandelt.

Für die Erzeugung einer **Challenge in Authentisierungsprotokollen** und von **zufälligen Padding- und Saltbits** sind die folgenden Anforderungen einzuhalten:

- Ein Pseudozufallszahlengenerator muss mindestens ein K3-DRNG mit Stärke der Mechanismen „Hoch“ oder ein DRG.2 jeweils im Sinne der AIS 20 [AIS 20] sein. Der Seed muss mindestens 100 Bit Entropie besitzen.
- Ein physikalischer Zufallszahlengenerator muss mindestens ein P2-TRNG mit Stärke der Mechanismen „Hoch“ oder ein PTG.2 jeweils im Sinne der AIS 31 [AIS 31] sein. Bei Nutzung von PACE darf als physikalischer Zufallszahlengenerator nur ein PTG.3 im Sinne der AIS 31 [AIS 31] verwendet werden.

3.5 Schlüsselerzeugung

Bei der Schlüsselerzeugung für Sicherheitsverfahren werden Zufallszahlen benötigt, an die entsprechende kryptographische Anforderungen zu stellen sind, um die Sicherheit des Gesamtsystems zu gewährleisten. Für die Schlüsselerzeugung können physikalische Zufallszahlengeneratoren oder Pseudozufallszahlengeneratoren eingesetzt werden. Für Zufallszahlen zur Schlüsselerzeugung gelten die Anforderungen gemäß [BKryA], Kapitel 4 „Erzeugung von Zufallszahlen“. D.h. insbesondere: Jeder erzeugte Schlüssel muss mindestens 100 Bit Entropie besitzen. Über die Anforderungen gemäß [BKryA] hinaus gilt folgendes:

Es wird generell empfohlen, zur Schlüsselerzeugung einen physikalischen Zufallszahlengenerator zu verwenden, der ein PTG.3 im Sinne der AIS 31 [AIS 31] sein sollte.

Pseudozufallszahlengeneratoren für die Erzeugung von Schlüsseln müssen K4-DRNGs mit Stärke der Mechanismen und Funktionen „Hoch“ oder ein DRG.3 jeweils im Sinne der AIS 20 [AIS 20] sein. Physikalische Zufallszahlengeneratoren für die Erzeugung von Schlüsseln müssen P2-TRNGs mit Stärke der Mechanismen und Funktionen „Hoch“ oder ein PTG.2 jeweils im Sinne der AIS 31 [AIS 31] sein. Für symmetrische Schlüssel muss die Seedlänge mindestens gleich der Schlüssellänge sein und die Entropie des Seeds im Wesentlichen so groß wie seine Länge, derart, dass die Entropie des Schlüssels im Wesentlichen seiner Länge entspricht. Bei der Erzeugung von asymmetrischen Schlüsseln sollte beachtet werden, dass jeder im Laufe der Schlüsselerzeugung erzeugte Zufallswert, mit dessen Kenntnis eine praktische Ermittlung des privaten Schlüssels aus dem öffentlichen Schlüssel möglich wäre, für sich genommen mindestens 100 Bit Entropie besitzen muss (empfohlen mindestens 120 Bit, bei hybriden Systemen mindestens so viel Entropie wie der symmetrische Verschlüsselungsschlüssel). Ist die Entropie eines solchen Zufallswertes

wesentlich niedriger als seine Bitlänge, dann muss darüber hinaus sichergestellt sein, dass es einem Angreifer praktisch unmöglich ist, wesentliche Teile des Zufallswertes richtig zu ermitteln, ohne diesen ganz zu erraten. Für einen Anwender ausnutzbare Zusammenhänge zwischen verschiedenen solchen Zufallswerten dürfen nicht bestehen, selbst wenn diese durch einen deterministischen Zufallsgenerator aus gemeinsamer Seed-Entropie erzeugt wurden.

Jeder asymmetrische Schlüssel muss mindestens 100 Bit Entropie besitzen; empfohlen wird aber auch hier eine wesentlich höhere Entropie von mindestens 120 Bit. Bei hybrider Verschlüsselung wird empfohlen, die Entropie für den asymmetrischen Schlüssel mindestens in der Größenordnung der Entropie des symmetrischen Schlüssels zu wählen. Diese Anforderungen begründen sich in der langfristigen Speicherung verschlüsselter Dokumente. Hierbei handelt es sich um verschlüsselte Dokumentationen, die auf zentralen Servern gespeichert werden.

3.5.1 Symmetrische Schlüssel

Die Erzeugung von symmetrischen Schlüsseln erfolgt durch die Erzeugung „kryptographisch sicherer“ Zufallszahlen (im Sinne obiger Ausführungen zu [BKryA], Kapitel 4) inklusive einer Nachbehandlung der Zufallszahlen zur Schlüsselformatierung (z.B. Anpassung an die Schlüssellänge).

Im Weiteren gelten die folgenden algorithmenspezifischen Anforderungen:

AES

Für den AES sind weder schwache noch semi-schwache Schlüssel bekannt, es gibt keine Einschränkung bei der Schlüsselauswahl (vgl. [FIPS 197, Kapitel 6.2]).

3.5.2 Asymmetrische Schlüssel

Für die Erzeugung von asymmetrischen Schlüsseln werden „kryptographisch sichere“ Zufallszahlen (im Sinne obiger Ausführungen zu [BKryA], Kapitel 4) benötigt. Im Weiteren gelten die algorithmenspezifischen Anforderungen gemäß [BKryA], Kapitel 3.1 „RSA-Verfahren“[3] und Kapitel 3.2 „DSA“.

Bei allen DSA-Varianten sollten PTG.3-konforme RNGs verwendet werden. Auf jeden Fall muss gewährleistet sein, dass bei der Erzeugung des für jede Signatur individuell generierten „ephemeral key“ *k* keine nachweisbaren statistischen Schwächen auftreten.

[3] Auch wenn die zu erzeugenden RSA-Schlüssel als Verschlüsselungsschlüssel (mittels RSA/PKCS#1) verwendet werden, gelten die Vorgaben für die RSA-Schlüsselgenerierung in [BKryA, Abschnitt 3.1] auch für diese Schlüssel.

Generell wird empfohlen, für ECC-Verfahren Standardkurven aus [TR-03111] zu verwenden; konkrete freigegebene Kurven können auch beim BSI erfragt werden. Bei den Verfahren ECDSA, ECGDSA und EC-KCDSA sollte die Bitlänge der verwendeten Hashwerte gemäß [TR-03111] nicht größer als die Bitlänge der Ordnung *q* der Punktegruppe sein.

3.6 Schlüsselvereinbarung

Die Protokolle zur Schlüsselvereinbarung wurden im Zusammenhang mit der gegenseitigen Authentisierung von Komponenten einschließlich Schlüsselvereinbarung behandelt (siehe Kapitel 3.1).

4 Anwendung kryptographischer Verfahren

4.1 Instanzauthentisierung

4.1.1 Einsatzbereich

In der Telematikinfrastruktur wird die Instanzauthentisierung für die einseitige und gegenseitige Authentisierung von Chipkarten (eGK, HBA, SMC), Kartenterminals, Konnektoren, VPN-Konzentratoren, Intermediäre und Webservices angewandt.

Die Chipkarten implementieren kryptographische Verfahren zur gegenseitigen Authentisierung von Karten (Card-to-Card Authentication) ohne oder mit Aufbau eines sicheren Kanals (s. Abschnitt 4.6.2) zwischen eGK, HBA und SMC. Zur Durchführung der Card-to-Card Authentisierung verfügen die Karten über asymmetrische Schlüssel und CV-Zertifikate (CVC), mit denen die Authentizität der öffentlichen Schlüssel verifiziert werden kann. Die öffentlichen Schlüssel der Wurzelinstanz der CVC-PKI haben eine lange Gültigkeit, die Zertifikate der darunter liegenden Zertifizierungsinstanzen haben eine etwas kürzere Gültigkeit, während die Gültigkeit der CV-Zertifikate von Chipkarten auf den Nutzungszeitraum der jeweiligen Chipkarte begrenzt ist.

Wegen der anwendungsübergreifenden Standardisierung und der begrenzten Update-Möglichkeiten der Chipkarten wird ein langfristiger Übergang und eine Migrationsstrategie auf größere Schlüssellängen und auf ein stärkeres Paddingverfahren für die öffentlichen Schlüssel der Wurzel- und Zertifizierungsinstanzen der CVC-PKI empfohlen.

Im Falle der Kommunikation einer eGK mit dem Versichertenstammdatendienst (VSDD) oder einem Card Application Management System (CAMS) erfolgt eine gegenseitige Authentisierung der Komponenten mit Schlüsselvereinbarung auf der Grundlage symmetrischer Verfahren. Analog kann auch die Kommunikation zwischen einer HBA und einem CAMS auf Grundlage einer Authentisierung mit symmetrischen Verfahren erfolgen. Die symmetrischen Schlüssel sollen für jede Chipkarte verschieden und auf die Lebensdauer der jeweiligen Chipkarte begrenzt sein. Ersteres kann durch eine Schlüsselgenerierung mit ausreichender Entropie (vgl. Abschnitt 3.5) gewährleistet werden.

Die Chipkarten eGK ([eGK Teil 2], [eGK-G2-ObjSys]), HBA ([HBA-ObjSys]) und SMC Typ B ([SMC-B-ObjSys]) speichern und verwenden private Authentisierungsschlüssel und verfügen

über X.509-Zertifikate für die zugehörigen öffentlichen Schlüssel für eine kartengestützte client-seitige Authentisierung anderer technischer Komponenten gegenüber Intermediäre und Webservices. Die Kartenterminals und Konnektoren ihrerseits speichern und verwenden ebenfalls private Authentisierungsschlüssel in Sicherheitsmodulen (SM-K, SM-KT) und verfügen über X.509-Zertifikate für die zugehörigen öffentlichen Schlüssel zur Authentisierung gegenüber Chipkarten, dezentralen und zentralen Komponenten. VPN-Konzentratoren, Intermediäre und Server zentraler Dienste sollen ihre privaten Authentisierungsschlüssel ebenfalls in Sicherheitsmodulen sicher speichern und verwenden. Die X.509-Zertifikate für die zugehörigen öffentlichen Schlüssel zur Authentisierung gegenüber Chipkarten, dezentralen und zentralen Komponenten werden in einer X.509-PKI verwaltet.

Die öffentlichen Schlüssel der Wurzelinstanz der X.509-PKI und darunter liegender Zertifizierungsinstanzen haben eine sehr lange Gültigkeit, für die ein langfristiger Übergang und eine Migrationsstrategie auf größere Schlüssellängen (3000 Bit RSA, 3000 Bit DSA, 3000 Bit Diffie-Hellman in endlichen Körpern, 250 Bit ECDH, ECDSA) empfohlen wird. Die X.509-Zertifikate müssen kurzfristig sperrbar und deren Gültigkeit online abfragbar sein.

4.1.2 Kryptographische Verfahren

Verfahren: Asymmetrische Authentisierung ohne Schlüsselvereinbarung (technische Komponenten, Anwendung Card-to-Card-Authentisierung):

- Es gelten bez. der Verfahren RSA, DSA und ECDSA die kryptographischen Anforderungen aus [BKryA].
- Bez. der zu verwendenden Hashfunktion gelten die Anforderungen aus [BKryA].
- Bez. des Paddings zur Erzeugung von Signaturen gelten die Anforderungen aus [BKryA].
- Nicht nur bei der Erstellung, sondern auch bei der Prüfung digitaler Signaturen sollte sichergestellt werden, dass die zu prüfende Signatur mit einem der nach [BkryA] als geeignet eingestuften Verfahren signiert wurde. Dies schließt jeweils neben der Signatur einer Nachricht selbst die gesamte Zertifikatskette bis zu dem passenden Wurzelzertifikat ein.

Im Rahmen der Authentisierung werden CV-Zertifikate verwendet. Für die Erzeugung (Signatur) der Zertifikate und die in den Zertifikaten bestätigten Schlüssel gelten ebenfalls die Vorgaben aus den drei vorhergehenden Spiegelstrichen. Für das Padding der CV-Zertifikate gelten die Vorgaben gemäß [BKryA] (vgl. auch Abschnitt 4.6.2).

Verfahren: Asymmetrische Authentisierung mit Schlüsselvereinbarung (Anwendung Card-to-Card-Authentisierung inkl. anschließendem Secure Messaging):

- Es gelten die Anforderungen der vier vorhergehenden Spiegelstriche.

- Im Rahmen der Schlüsselvereinbarung zulässige Hashfunktionen für die Ableitung der symmetrischen Schlüssel (Schlüsselableitungsfunktion gemäß [ANSI X9.63]): SHA-1, SHA-224, SHA-256,SHA-384, SHA-512 bis Ende 2021+

Bei Verwendung einer spezifischen Hashfunktion ist auf die zu erzielende Schlüssellänge zu achten. Beispielsweise erzeugt das Verfahren gemäß [EN-14890-1], Kapitel 8.9 einen Output von 160 Bit. Entsprechende Anpassungen sind deshalb erforderlich.

Verfahren: symmetrische Authentisierung gemäß [EN-14890-1] mit Schlüsselvereinbarung (Card-to-Server-Authentisierung; z.B. CAMS oder VSDD):

- AES-128, AES-192, AES-256: bis Ende 2021+

Verfahren: Client-Server-Authentisierung (Authentisierung einer Chipkarte gegenüber einem Server bzw. Kartenterminal):

- RSA gemäß [BKryA]
- DSA: gemäß [BKryA]
- ECDSA über *GF(p)*: gemäß [BKryA]
- PACE [TR-03110]

4.2 Qualifizierte elektronische Signatur

Fortgeschrittene elektronische Signaturen sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen, wobei diese

a) ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sind,
b) die Identifizierung des Signaturschlüssel-Inhabers ermöglichen,
c) mit Mitteln erzeugt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann, und
d) mit den Daten, auf die sie sich beziehen, so verknüpft sind, dass eine nachträgliche Veränderung der Daten erkannt werden kann (Definition nach [SigG] §2, Absätze 1 und 2).

Qualifizierte elektronische Signaturen sind fortgeschrittene elektronische Signaturen, die

a) auf einem zum Zeitpunkt ihrer Erzeugung gültigen qualifizierten Zertifikat beruhen und
b) mit einer sicheren Signaturerstellungseinheit erzeugt werden (Definition nach [SigG] §2, Absatz 3).

Qualifizierte Zertifikate sind elektronische Bescheinigungen, mit denen Signaturprüfschlüssel einer natürlichen Person zugeordnet werden und die Identität dieser Person bestätigt wird, und die die Anforderungen des Signaturgesetzes erfüllen (Definition nach [SigG] §2, Absätze 6 und 7).

4.2.1 Einsatzbereich

Der elektronische Heilberufsausweis verfügt über die Anwendung DF.QES, mit der die Erzeugung von qualifizierten Signaturen ermöglicht wird. In der elektronischen Gesundheitskarte ist die Anwendung DF.QES optional. Der elektronische Heilsberufsausweis bzw. optional die elektronische Gesundheitskarte verfügen über den privaten Schlüssel PrK.HP.QES (HBA) bzw. PrK.CH.QES (eGK).

4.2.2 Kryptographische Verfahren

Für Algorithmen im Kontext qualifizierter Signaturen gilt der Algorithmenkatalog „Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001“ in der jeweils aktuellen Fassung.

Gemäß der Signaturverordnung, Anlage 1, 2 Algorithmen – Veröffentlichung und Neubestimmung der Eignung wird die jeweils aktuelle Fassung durch die zuständige Behörde (Bundesnetzagentur) im Bundesanzeiger veröffentlicht [BKryA]. Sie kann auch über die Web-Seiten der Bundesnetzagentur (s. www.bundesnetzagentur.de) abgerufen werden.

Die Signaturverordnung legt in Anlage 1, Punkt 2 zur Veröffentlichung und Neubestimmung der Eignung Folgendes fest:

> *„Die zuständige Behörde veröffentlicht im Bundesanzeiger eine Übersicht über die Algorithmen und zugehörigen Parameter, die zur Erzeugung von Signaturschlüsseln, zum Hashen zu signierender Daten oder zur Erzeugung und Prüfung qualifizierter Signaturen als geeignet anzusehen sind, sowie den Zeitpunkt, bis zu dem die Eignung jeweils gilt. Der Zeitpunkt soll mindestens sechs Jahre nach dem Zeitpunkt der Bewertung und Veröffentlichung liegen. Die Eignung ist jährlich sowie bei Bedarf neu zu bestimmen. Die Eignung ist gegeben, wenn innerhalb des bestimmten Zeitraums nach dem Stand von Wissenschaft und Technik eine nicht feststellbare Fälschung von qualifizierten elektronischen Signaturen oder Verfälschung von signierten Daten mit an Sicherheit grenzender Wahrscheinlichkeit ausgeschlossen werden kann. Die Eignung wird nach Angaben des Bundesamtes für Sicherheit in der Informationstechnik unter Berücksichtigung internationaler Standards festgestellt. Experten aus Wirtschaft und Wissenschaft sind zu beteiligen.“*

Im Rahmen der Vorgaben dieser Technischen Richtlinie für das Gesundheitswesen werden keine zusätzlichen Einschränkungen an die Eignung von Algorithmen und Parametern zusätzlich zu den in [BKryA] aufgeführten Vorgaben gemacht.

4.3 Digitale nicht-qualifizierte elektronische Signaturen

Die technischen Anforderungen des Signaturgesetzes an qualifizierte elektronische Signaturen und Zertifikate (vgl. Kapitel 4.2) sind soweit möglich auch für digitale Signaturen (vgl.

3.2.3), die nicht-qualifizierte elektronische Signaturen sind, bzw. für die zur Authentifizierung dienenden Zertifikate einzuhalten.

4.3.1 Kryptographische Verfahren

Es wird die Verwendung der kryptographischen Verfahren für qualifizierte elektronische Signaturen empfohlen.

4.4 Verschlüsselung von Dokumenten

4.4.1 Einsatzbereich

In der Telematikinfrastruktur muss die Vertraulichkeit von Dokumenten (oder Dokumentteilen) bei deren Übertragung zwischen dem Konnektor und den Telematikdiensten sowie bei deren Speicherung durch die Telematikdienste gewährleistet werden. Die Verschlüsselung erfolgt durch Hybridverfahren, bei denen die Daten der Dokumente symmetrisch mit Dokumentenschlüsseln verschlüsselt werden und die (asymmetrische) Entschlüsselung der Dokumentenschlüssel durch Chipkarten (eGK, HBA oder SMC) oder Hardwaresicherheitsmodule erfolgt.

Wegen der langfristigen Vertraulichkeit der zu schützenden Dokumente und der Schwierigkeit langfristiger Vorhersagen zur Sicherheit der vorgesehenen Kryptoalgorithmen werden die Sicherheitsaussagen unter der Voraussetzung getroffen, dass

- die vertraulichen Dokumente vor der Übertragung über das Internet verschlüsselt werden,
- die Kommunikationskanäle zur Übermittlung der Dokumente selbst verschlüsselt sind,
- für die Speicherung der vertraulichen Dokumente Verfahren vorzusehen sind, die bei Notwendigkeit eine Umschlüsselung oder Überschlüsselung der Dokumente mit stärkeren kryptographischen Verfahren ermöglichen. Im Rahmen einer Umschlüsselung oder Überschlüsselung müssen die alten Chiffrate sicher gelöscht werden. Überschlüsselung bedeutet hierbei die erneute Verschlüsselung eines bereits verschlüsselten Dokuments. Verglichen mit einer Umschlüsselung hat ein solches Vorgehen den Vorteil, dass auf eine große Anzahl von Dokumenten angewendet werden kann, ohne diese zwischenzeitlich entschlüsseln zu müssen; es hat den Nachteil, dass das unter dem zu ersetzenden Chiffriersystem genutzte Schlüsselmaterial nach Abschluss des Vorgangs weiterhin vorgehalten werden muss.

4.4.2 Kryptographische Verfahren

Verfahren: Hybridverschlüsselung unter Verwendung von [XMLEnc] oder S/MIME [RFC 5751] bzw. Cryptographic Message Syntax (CMS) [RFC 5652]:

- asymmetrische Verschlüsselung des symmetrischen Dokumentenschlüssels (key transport):

- RSA: bis Ende 2021+: 2048 Bit
- RSAES-PKCS1-v1_5 [PKCS #1 v2.1] bis Ende 2017
- RSAES-OAEP, MGF1 mit SHA-256, [PKCS #1 v2.1] bis Ende 2021+
- EC-KAEG, q: 256 Bit: bis Ende 2021+

- Symmetrische Verschlüsselung der Dokumentendaten:
  - AES-256 CBC mit zufälligem Initialisierungsvektor bis Ende 2021+
  - AES-256 GCM mit zufälligem Initialisierungsvektor und Tag-Länge von 128 Bit bis Ende 2021+[4]

    Die Bitlänge des Initialisierungsvektors bei der Verwendung von AES-GCM soll 96-Bit sein. Es wird die Verwendung von AES-256 GCM mit der Tag-Länge von 128 Bit empfohlen und als langfristig geeignet bewertet.

Aufgrund der in der Praxis oft beobachteten Anfälligkeit von Implementierungen gegen Seitenkanalangriffe bei Verwendung des CBC-Modus (vgl. [Vaudenay-2002] und [BreakingXMLEnc]) wird die Verwendung von AES/GCM [SP800-38D] empfohlen.

4.5 Kommunikation

4.5.1 Einsatzbereich

Die Telematikinfrastruktur benutzt kryptographische Verfahren zum Schutz der Vertraulichkeit und der Integrität der zweiseitigen Online-Kommunikation zwischen den Chipkarten, den technischen Komponenten der Telematikinfrastruktur im lokalen Netz der Leistungserbringer (Kartenterminal, Konnektor), zwischen dem Konnektor und dem VPN-Konzentrator, dem Intermediär und gegebenenfalls weiteren Komponenten.

4.5.2 Kryptographische Verfahren

Verfahren: Secure Messaging zwischen Chipkarten (Card-to-Card-Kommunikation bzw. Absicherung der Kommunikation zwischen Karte und Server bzw. Kartenterminal):

- symmetrische Schlüsselvereinbarung nach [EN-14890-1], PACE [TR-03110] und [ANSI X9.63]: siehe Angaben in Kapitel 4.1.2
- asymmetrische Schlüsselvereinbarung nach [EN14890-1]: siehe Angaben in Kapitel 4.1.2

[4] Die Anwendungsvorgaben aus [SP800-38D] insbesondere auf die Wahl des Initialisierungsvektors und die maximale Anzahl der Verschlüsselungen mit dem selben Schlüssel müssen eingehalten werden.

- Verschlüsselung mittels AES-n CBC mit zufälligem Initialisierungsvektor oder mittels AES-n CTR mit zufälligem Initialwert des Zählers (jeweils mit n=128, 192 oder 256) geeignet bis Ende 2021+.
  Wenn der CBC-Initialisierungsvektor (IV) nicht zufällig gewählt wird oder gewählt werden kann, so muss der Verschlüsselungsalgorithmus durch einen anderen Mechanismus dynamisiert werden (z.B. IV ist ein verschlüsselter[5] Counter bzw. als IV wird (wie bei IPsec) der vorherige Output des verwendeten Blockchiffrieralgorithmus genommen). Der CBC-Initialisierungsvektor darf nicht vorhersagbar werden.
- Integritätsschutz: AES-128 CMAC [FIPS 197], [SP800-38B] geeignet bis Ende 2021+

Bei einer Anwendung des Secure Messaging über offene Netze (z.B. bei einer Card-to Server-Kommunikation) muss die Kommunikation durch zusätzliche Sicherheitsmechanismen zur Wahrung der Vertraulichkeit und Datenauthentizität geschützt werden (z.B. mittels IPsec).

Verfahren: IPsec

Die IPsec-Kommunikation zwischen dem Konnektor und dem VPN-Konzentrator und die TLS-Kommunikation zwischen Konnektor und Fachdiensten dürfen generell nur langfristig geeignete Kryptoalgorithmen gemäß Kapitel 3 verwenden. Für die Parameter und Schlüssellängen gelten generell die Festlegungen wie zur Client-Server-Authentisierung des Kapitels 4.1. Allerdings gilt bis Ende 2020 für die Schlüsselerzeugung: Für die Erzeugung symmetrischer Schlüssel ist die Verwendung eines Pseudozufallszahlengenerators der Klasse K4 mit Stärke der Mechanismen „Hoch“ oder der Klasse DRG.3 gemäß [AIS 20] ausreichend; alternativ genügt eine nachvollziehbare Begründung des Antragstellers, dass das Fehlen der K4-spezifischen Eigenschaft im vorgesehenen Einsatzszenario keine zusätzlichen Sicherheitsrisiken induziert; die Entropie des Seeds muss mindestens gleich der Schlüssellänge sein; es wird empfohlen, dass für die Seedgenerierung bzw. für die Schlüsselgenerierung ein PTG.3 im Sinne der AIS 31 [AIS 31] verwendet wird.

Empfehlungen für die Verwendung von IKE/IPsec findet man in [TR-02102-3].

Bei der Verwendung von IKE/IPsec muss Forward Secrecy (authentisierte DHE oder ECDHE) gewährleistet werden. Für die Authentisierung (Signatur) der ephemeren (EC)-DH-Parameter muss eine nach [BKryA] zulässige Hashfunktion verwendet werden. Es wird empfohlen die IKEv2-Erweiterung nach [RFC 7427] zu verwenden.

Ephemere Schlüssel und Sitzungsschlüssel müssen nach ihrer Verwendung unwiderruflich gelöscht werden. Ephemere bzw. Sitzungsschlüssel dürfen nur für eine Sitzung benutzt werden und dürfen grundsätzlich nicht persistent abgespeichert werden. Dies gilt auch für

[5] Der IV darf nicht gleich dem Counter gewählt werden.

Ephemeralschlüssel, die für die Authentisierung eines Diffie-Hellman-Schlüsseltausches genutzt werden.

Verfahren: TLS

Empfehlungen für die Verwendung von TLS findet man in [TR-02102-2]. Es dürfen nur Ciphersuiten Verwendung finden, die Forward Secrecy ermöglichen. Vorgaben für Ephemere und Sitzungsschlüssel gelten analog zu IPsec. Es wird die komplette Migration von TLS Version 1.1 auf die Version 1.2 angestrebt. Andere Versionen von TLS oder von SSL sind in der TI nicht zulässig. Es wird die Verwendung einer CipherSuite empfohlen, die AES im GCM verwendet.

4.6 Bestandsanwendungen eGK Generation 1

4.6.1 eGK Generation 1

Wissenschaftliche Entwicklungen im Bereich der Kryptographie und technische Entwicklungen in der IT erfordern eine ständige Weiterentwicklung der Komponenten und der Prozesse der Telematikinfrastruktur. Die aktuell im Feld befindliche elektronische Gesundheitskarte der Generation 1 (eGK G1) wird schrittweise durch Karten der Generation 2 ersetzt. Auch diese Karten werden zukünftig wieder durch Karten einer Folgegeneration ersetzt werden.

Im Folgenden sind verbindliche Vorgaben für kryptographische Verfahren, die im Rahmen der Anwendungsprozesse um die eGK G1 Verwendung finden, aufgeführt. Die Vorgaben basieren auf aktuellen Erkenntnissen und Veröffentlichungen bez. der Sicherheit der aufgeführten Verfahren und werden ggf. zukünftig an aktuelle Entwicklungen angepasst.

4.6.2 Kryptographische Verfahren

Verfahren: Verschlüsselung

- 3TDES (Triple-DES (TDEA[6]) mit 168 Bit langem Schlüssel) geeignet bis Ende 2018

Das Verfahren 3TDES ist in [SP-800-67r1] definiert als TDEA Keying Option 1. Der 3TDES (Triple-DES 168 Bit Schlüssel) im CBC-Modus ist in der TI nur für Anwendungen im Rahmen der eGK G1 zulässig (VSDD und CAMS-Anwendungen). Es dürfen nur wesentlich weniger als 2^{32} Nachrichtenblöcke mit dem gleichen Schlüssel bearbeitet werden. Die Verwendung von schwachen sowie von semi-schwachen Schlüsseln als Teilschlüssel eines TDES Schlüssels (siehe z.B. [SP800-67r1, Kapitel 3.4.2]) ist praktisch auszuschließen. Darüber

[6] Triple Data Encryption Algorithm

hinaus sind die drei Teilschlüssel unabhängig und zufällig zu wählen, so dass diese praktisch paarweise verschieden sind.

Der 2TDES (Triple-DES mit 112 Bit langem Schlüssel / TDEA Keying Option 2 [SP-800-67r1]) wird als nicht geeignet bewertet.

Verfahren: Integritätsschutz

- Das nichtstandardisierte 3TDES basierte MAC-Verfahren „3TDES - Retail CBC MAC“ mit 168 Bit Schlüssel, das in [eGK Teil 1, Abschnitt 7.6] (bzw. [gemSpec_COS, Abschnitt 6.6.1.1]) beschrieben wird, ist nur analog bis Ende 2018 für Anwendungen der eGK G1 zulässig.

Voraussetzung dabei ist, dass der gemäß [eGK Teil 1] Abschnitt 7.2.1 gemeinsam mit dem MAC-Schlüssel K_{mac} abgeleitete, dort als SSC_{mac} bezeichnete und gemäß Abschnitt 14.2 verwendete IV (Initialisierungsvektor) wie ein weiterer 64-Bit Teilschlüssel behandelt (d.h. mit der erforderlichen Entropie erzeugt und genau wie K_{mac} geheim gehalten) wird und dass maximal 2^{16} Nachrichtenblöcke mit dem gleichen Schlüssel bearbeitet werden.

Verfahren: DS1-Signaturen [ISO9796-2] unter Verwendung von SHA-256

In [EN-14890-1] wird ein Padding für CV-Zertifikate beschrieben, das dem DS1 aus ISO 9796-2 entspricht. Dieses Padding-Verfahren ist nicht SigG-konform. Deshalb wird dringend empfohlen, auch für CV-Zertifikate eines der in [BKryA] aufgeführten Verfahren zu verwenden. Für CV-Zertifikate mit der DS1-Variante gemäß den Abschnitten 7.6 und 8 [eGK Teil 1] muss bei der Erstellung der CV-Zertifikate (neben der Verwendung von RSA-Schlüsseln der Länge 2048 Bit und der Hashfunktion SHA-256) folgendes gewährleistet sein:

Die CV-Zertifikate werden beim Kartenherstellungsprozess unmittelbar nach Generierung des Schlüsselpaars, die von einem Angreifer nicht beeinflusst werden kann, erstellt. Auch die übrigen Felder des Nachrichtenstrings M gemäß (N 005500) und (N 006300) in Abschnitt 8 von [eGK Teil 1] können nicht von einem Angreifer beeinflusst werden.

Das Verfahren ist im Rahmen der Anwendungen der eGK G1 bis Ende 2018 zulässig.

4.7 Schlüsselmanagement

4.7.1 Einsatzbereich

Die kryptographischen Verfahren der Telematikinfrastruktur erfordern den Betrieb spezifischer PKI für fortgeschrittene elektronische Signatur, die X.509-Zertifikate für Verschlüsselung und Authentisierung sowie die CV-Zertifikate.

4.7.2 Kryptographische Verfahren

Zurzeit werden keine spezifischen kryptographischen Verfahren für das Schlüsselmanagement verlangt.

5 Literatur

[AIS 20] AIS 20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren, Version 3, 15.05.2013, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.pdf?__blob=publicationFile

[AIS 31] AIS 31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren, Version 3, 15.05.2013, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_pdf.pdf?__blob=publicationFile

[ANSI X9.62] American National Standard X9.62 – 2005, Public Key Cryptography for the Financial Service Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA), 2005 (ersetzt ANSI X9.62-1998)

[ANSI X9.63] American National Standard X9.63 – 2001, Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography, 2001

[BKryA] Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom: 15.12.2014, Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen (auch online verfügbar: https://www.bundesnetzagentur.de/cln_1912/DE/Service-Funktionen/QualifizierteelektronischeSignatur/WelcheAufgabenhatdieBundesnetzagentur/GeeigneteAlgorithmenfestlegen/geeignetealgorithmenfestlegen-node.html
bzw. unter https://www.bundesanzeiger.de mit dem Suchbegriff „BAnz AT 30.01.2015 B3“)

[BreakingXMLEnc] How to Break XML Encryption, Tibor Jager, Juraj Somorovsky, 2011, http://www.nds.rub.de/media/nds/veroeffentlichungen/2011/10/22/HowToBreakXMLenc.pdf

[ECCBP] ECC Brainpool: Standard Curves and Curve Generation, Vers. 1.0, 2005; online http://www.teletrust.de/fileadmin/files/oid/oid_ECC-Brainpool-Standard-curves-V1.pdf, siehe auch RFC 5639

[eGK-G2-ObjSys] Spezifikation der elektronischen Gesundheitskarte, Version 3.8.0, 26.08.2014;
http://www.gematik.de/cms/de/spezifikation/release_1_4_ors1/r1_4_konzepte_und_spezifikationen/r1_4_konzepte_und_spezifikationen.jsp

[eGK Teil 1] Spezifikation der elektronischen Gesundheitskarte, Teil I: Spezifikation der elektrischen Schnittstelle, Version 2.2.0, 20.03.2008,

http://gematik.de/cms/de/spezifikation/wirkbetrieb/release_0_5_3/release_0_5_3_egk/release_0_5_3_spezifikationenderegkteil1.jsp

[eGK Teil 2] Spezifikation der elektronischen Gesundheitskarte, Teil II: Grundlegende Applikationen, Version 2.2.0, 25.03.2008, http://gematik.de/cms/de/spezifikation/wirkbetrieb/release_0_5_3/release_0_5_3_egk/release_0_5_3_spezifikationenderegkteil2.jsp

[eGK Teil 3] Spezifikation der elektronischen Gesundheitskarte, Teil III: Äußere Gestaltung, Version 2.1.0, 20.12.2007, http://gematik.de/cms/de/spezifikation/wirkbetrieb/release_0_5_3/release_0_5_3_egk/release_0_5_3_spezifikationenderegkteil3.jsp

[EN-14890-1] DIN EN 14890-1:2008, Application Interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services

[FIPS 180-4] FIPS Publication 180-4: Secure Hash Standard (SHS), Federal Information Processing Standards Publication 180-4, U.S. Department of Commerce / NIST, National Technical Information Service, March 2012

[FIPS 186-2] FIPS Publication 186-2: Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, U.S. Department of Commerce / NIST, National Technical Information Service, January 2000 und Change Notice 1, October 2001

[FIPS 186-3] FIPS Publication 186-3: Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-3, U.S. Department of Commerce / NIST, National Technical Information Service, November 2008

[FIPS 197] FIPS Publication 197: Advanced Encryption Standard (AES), Federal Information Processing Standards Publication 197, U.S. Department of Commerce / NIST, National Technical Information Service, November 2001

[gemSiKo] Übergreifendes Sicherheitskonzept der Telematikinfrastruktur, Version 2.3.0 vom 17.07.2008, www.gematik.de

[gemSpec_COS] Spezifikation des Card Operating System (COS), Version 3.8.0, Stand 17.07.2015, http://www.gematik.de/cms/de/spezifikation/release_1_4_ors1/r1_4_konzepte_und_spezifikationen/r1_4_konzepte_und_spezifikationen.jsp

[gemSpec_Kon] Konnektorspezifikation, Version 4.7.0 vom 17.07.2015, https://www.gematik.de/cms/de/spezifikation/release_1_5_ors1/konzepte_und_spezifikationen_2/r1_5_konzepte_und_spezifikationen.jsp

[gemSpec_Krypt] Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 2.4.0 vom 17.07.2015, https://www.gematik.de/cms/de/spezifikation/release_1_5_ors1/konzepte_und_spezifikationen_2/r1_5_konzepte_und_spezifikationen.jsp

[HBA-ObjSys] Spezifikation des elektronischen Heilberufsausweises HBA-Objektsystem, 3.8.1, 17.07.2015, https://www.gematik.de/cms/de/spezifikation/release_1_5_ors1/konzepte_und_spezifikationen_2/r1_5_konzepte_und_spezifikationen.jsp

[ISO7816-4] ISO 7816-4: Identification Cards – Integrated Circuit(s) Cards, Part 4: Organization, security and commands for interchange, 2005

[ISO9796-2] ISO 9796-2: Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer Factorization based mechanisms, 2002

[ISO10118-3] ISO 10118-3, Information technology – Security techniques – Hash functions, Part 3: Dedicated hash functions, 2nd ed., 2004

[ISO11770-2] ISO 10770-2, Information technology – Security techniques – Key management, Part 2: Mechanisms using symmetric techniques, 2008

[ISO11770-3] ISO 10770-3, Information technology – Security techniques – Key management, Part 3: Mechanisms using asymmetric techniques, 2008

[IEEE P1363] IEEE P1363; Standard specification for public key cryptography, 2000.

[Lenstra 2000] Lenstra, A.K.; Verheul, E.R.: Selecting Cryptographic Key Sizes, PKC 2000, p 446-465, Januar 2000

[Lenstra 2004] Lenstra, A.K.: Key Lengths, Contribution to The Handbook of Information Security, 30. Juni 2004

[PKCS #1 v1.5] PKCS #1 v1.5: RSA Cryptography Standard, RSA Laboratories, November 1993

[PKCS #1 v2.1] PKCS #1 v2.1: RSA Cryptography Standard, RSA Laboratories, 14. Juni 2002

[RFC 2104] Krawczyk, H., Bellare, M., Canetti, R.: HMAC: Keyed-Hashing for Message Authentication, February 1997

[RFC 2404] Madson, C.; Glenn, R.: The Use of HMAC-SHA-1-96 within ESP and AH, RFC 2404, November 1998

[RFC 3526] Kivinen, T.; Kojo, M.: More Modular Exponential (MODP) Diffie-Hellman Groups for Internet Key Exchange (IKE), RFC 3526, May 2003

[RFC 4303] S. Kent: IP Encapsulating Security Payload (ESP), RFC 4303, December 2005

[RFC 4308] P. Hoffman: Cryptographic Suites for IPsec, December 2005

[RFC 4346] Dierks, S.; E. Rescorla: The Transport Layer Security (TLS) Protocol, Version 1.1, April 2006

[RFC 5246] Dierks, S.; E. Rescorla.: The TLS Protocol, RFC 2246, Version 1.2, August 2008

[RFC 5639] M. Lochter, J. Merkle: Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation, March 2010

[RFC 5652] R. Housley: Cryptographic Message Syntax (CMS), RFC 5652, September 2009

[RFC 5751] B. Ramsdell, S. Turner: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2, January 2010, https://tools.ietf.org/html/rfc5751

[RFC 5996] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen: Internet Key Exchange Protocol Version 2 (IKEv2), September 2010, https://tools.ietf.org/html/rfc5996

[RFC 7296] C. Kaufmanm, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen: Internet Key Exchange Protocol Version 2 (IKEv2), October 2014, https://tools.ietf.org/html/rfc7296

[RFC 7427] T. Kivinen, J. Snyder: Signature Authentication in the Internet Key Exchange Version 2 (IKEv2), January 2015, https://tools.ietf.org/html/rfc7427

[RSA] R. Rivest, A. Shamir, L. Adleman: A method for obtaining digital signatures and public key cryptosystems, Communications of the ACM, Vol. 21 No. 2, 1978

[SigG] Gesetz über Rahmenbedingungen für elektronische (Signaturgesetz - SigG vom 16. Mai 2001, BGBl. I S. 876, i. d. Fassung des Ersten Gesetzes zur Änderung des Signaturgesetzes (1. SigGÄndG) vom 4. Januar 2005, BGBl. I S.2

[SigV] Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), die zuletzt durch die Verordnung vom 15. November 2010 (BGBl. I S. 1542) geändert worden

[SMC-B-ObjSys] Spezifikation der Security Module Card SMC-B Objektsystem, Version 3.7.0, 26.08.2014, http://www.gematik.de/cms/de/spezifikation/release_1_4_ors1/r1_4_konzepte_und_spezifikationen/r1_4_konzepte_und_spezifikationen.jsp

[SP800-38A] NIST Special Publication 800-38A: Recommendation for Block Cipher Modes of Operation, Methods and Techniques, Special Publication 800-38A, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 2001 Edition

[SP800-38B] NIST Special Publication 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, Special Publication 800-38B, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, 2001 Edition

[SP800-38D] NIST Special Publication 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, National Institute of Standards and Technology, U.S. Department of Commerce, November 2007

[SP800-56A] NIST Special Publication 800-56A: Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Special Publication 800-56A, National Institute of Standards and Technology, March 2006

[SP-800-57] NIST Special Publication 800-57: Recommendation for Key Management – Part 1: General (Revision 3), Special Publication 800-57, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, July 2012

[SP800-67r1] NIST Special Publication 800-67 Revision 1: Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher, Revised January 2012, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, January 2012

[SP800-78] NIST Special Publication 800-78: Cryptographic Algorithms and Key Sizes for Personal Identity Verification, Special Publication 800-78, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, April 2005

[TR-02102-1] Technische Richtlinie BSI TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version: 2015-01, Stand 10. Februar 2015

[TR-02102-2] Technische Richtlinie TR-02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), Version: 2015-01

[TR-02102-3] Technische Richtlinie TR-02102-3, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2), Version: 2015-01

[TR-03110] Technical Guideline TR-03110 Advanced Security Mechanisms for Machine Readable Travel Documents – Part 2 – Extended Access Control Version 2 (EACv2),Password Authenticated Connection Establishment (PACE),and Restricted Identification (RI), Version 2.10, 20.3.2012.

[TR-03111] BSI. Technical Guideline: Elliptic Curve Cryptography, TR-03111, Version 2.00, 28.06.2012.

[TR-03116-2] Technische Richtlinie TR-03116-2, eCard-Projekte der Bundesregierung, Teil 2 – Hoheitliche Ausweisdokumente, Stand: 2015, Datum: 02.02.2015

[TR-03116-3] Technische Richtlinie TR-03116-3 eCard-Projekte der Bundesregierung, Teil 3 – Intelligente Messsysteme, Stand: 2015, Datum: 26.03.2015

[TR-03116-4] Technische Richtlinie TR-03116-4, eCard Projekte der Bundesregierung, Teil 4 – Kommunikationsverfahren im eGovernment, Stand: 2015, Datum: 02.02.2015

[Vaudenay-2002] Security Flaws Induced by CBC Padding: Applications to SSL, IPsec, WTLS … , Serge Vaudenay, Eurocrypt 2002, LNCS 2332/2002, 535-545

[XMLEnc] XML Encryption Syntax and Processing Version 1.1, W3C Recommendation, 11 April 2013, http://www.w3.org/TR/xmlenc-core1/

[XMLDSig] XML Signature Syntax and Processing (Second Edition), W3C Recommendation, 11 April 2013, http://www.w3.org/TR/xmldsig-core1/