gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur

Version:	1.3.0
Stand:	26.03.2008
Status:	freigegeben

Dokumentinformationen

Änderungen zur Vorversion

Die Änderungen zur letzten freigegebenen Version betreffen:

- Spezifikation des Verfahrens zur gleichwertigen Geheimnisaufteilung
- Spezifikation der Algorithmen für hybride Verschlüsselung binärer Daten
- Algorithmen für OCSP-Signaturen und OCSP-Responder-Zertifikate

Die vorgenommenen Änderungen gegenüber der Vorversion wurden farblich hervorgehoben. Sofern ganze Kapitel eingefügt oder wesentlich geändert wurden, wurde zur besseren Lesbarkeit lediglich die Überschrift durch gelbe Markierung hervorgehoben.

Referenzierung des Dokumentes:

Die Referenzierung in weiteren Dokumenten der gematik erfolgt unter:

[gemSpec_Krypt]	gematik (26.03.2008): Einführung der Gesundheitskarte - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur Version 1.3.0

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.0.1	02.03.07		Erstellung des Dokumentes	gematik, AG1
0.0.5	26.03.07		Einarbeitung von Kommentaren und editorische Überarbeitung	gematik, AG1
0.0.6	27.03.07		Formatierungen, RS/GR	gematik, AG1
0.0.9	05.0407		Einarbeitung von Kommentaren der iQS und editorische Überarbeitung	gematik, AG1
0.9.0	04.05.07		freigegeben	gematik
0.9.0.1	15.05.07		Ergänzung kryptographischer Algorithmen für XML-Dokumente	gematik AG1
0.9.1	15.05.07		freigegeben	gematik
0.9.2	31.05.07		Unterscheidung zwischen Netz und Anwendungskonnektor bei den betroffenen Systemen	gematik, AG1
0.9.3	12.07.07		Vorgabe zum Initialisierungsvektor für Verschlüsselung nach AES CBC Vorgabe zur Speicherung des Initialisierungsvektors bei	ITS/AP, CHG

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
			der Speicherung von eVerordnungen auf der eGK für Verschlüsselung nach AES CBC	
0.9.4	12.07.07		Freigegeben	gematik
0.9.5	09.08.07	Alle 3 6 	Anpassung HASH Algorithmen für Zertifikate Einarbeitung externe Kommentierung Aufnahme der Eingangsanforderungen Schlüsselableitung für Auditeinträge Verschlüsselung für Auditeinträge SSL-Verbindungen zwischen dezentralen Komponenten der TI Einarbeiten der SRQs: SRQ0642, SRQ0643	ITS/AP, CHG
1.0.0	24.08.07		freigegeben	gematik
1.0.1	27.08.07		Überarbeitung der Formatvorlage	ITS/AP, CHG
1.0.2	23.11.07	5.1 5.1, 6.4 3 4 5 6 6.1.6 6.5.1	Neue Darstellung der Anforderungen an XML Signaturen Einarbeitung der Änderungen zu Kartengeneration 1 und Auflösung der dadurch bislang offenen Punkte Übernahme des aktuellsten Stands der Anforderungen aus dem Anforderungsmanagement Überarbeitung der Erläuterung der Dokumentenstruktur Erläuterung der verwendeten Struktur für X.509 Identitäten Aufnahme von SHA256 als verpflichtenden Algorithmus für XML Signaturen Aufnahme von RSA-OAEP für die Generierung von Hybridschlüsseln Aufnahme des Verfahrens zur Generierung eines versichertenindividuellen Schlüssels im Auditservice	ITS/AP, CHG
1.1.0	18.12.07		freigegeben	gematik
1.1.3	23.01.08	 6.7 6.8	Aufnahme des Abschnitts: Verfahren zur gleichwertigen Geheimnisaufteilung Hybride Verschlüsselung binärer Daten	ITS/AP, CHG
1.2.0	29.02.08		freigegeben	gematik
1.2.2	25.03.08	5.1	Algorithmen für OCSP-Signaturen und OCSP-Responder-Zertifikate	ITS/AP, CHG
1.3.0	26.03.08		freigegeben	gematik

Inhaltsverzeichnis

1 Zusammenfassung

Innerhalb der Telematikinfrastruktur (TI) werden kryptographische Algorithmen zum Schutz der Authentizität, Integrität und Vertraulichkeit sowie in den Fällen der qualifizierten Signatur zur rechtsverbindlichen Willenserklärung verwendet. Sie dienen als Stützpfeiler der Sicherheitsarchitektur der TI. Die Vorgaben des Kryptokonzeptes [gemSiKo#AnhF] sowie der Technischen Richtlinie für eCard-Projekte der Bundesregierung [BSI-TR03116] bilden hierfür einen normativen Rahmen möglicher, aber nicht verpflichtend zu implementierender Algorithmen, der alle für die Verwendung in der TI zulässigen Algorithmen definiert.

Dieser Rahmen lässt allerdings den Herstellern und Betreibern einzelner Dienste oder Komponenten der TI einen weiten Spielraum. Dieser Spielraum hat zur Folge, dass jede Komponente, die kryptographische Daten erzeugt, eine Auswahl an Algorithmen zur Verfügung hat und dass alle Komponenten, die diese kryptographischen Daten verwenden, in der Lage sein müssten, alle zur Auswahl stehenden Algorithmen ebenfalls anwenden zu können. Dies stellt für die direkte Kommunikation (z. B. mittels IPSec oder TLS) kein Problem dar sofern zumindest ein von beiden Teilnehmern gemeinsam unterstützter Algorithmus existiert, da die verwendeten Algorithmen zu Beginn der Kommunikation ausgehandelt werden. Bei verschlüsselt oder signiert hinterlegten Objekten findet das Aushandeln jedoch nicht statt und entschlüsselnde oder eine Signatur prüfende Komponenten müssten alle zulässigen Algorithmen implementieren, da sonst potentiell das Entschlüsseln oder Prüfen einer Signatur nicht möglich ist.

Die Implementierung aller zulässigen Algorithmen würde in einem unverhältnismäßigen Aufwand für die Implementierung des Konnektors sowie die notwendigen Integrationstests zwischen Komponenten verschiedener Hersteller resultieren. Aus diesem Grund müssen zu verwendende kryptographische Algorithmen für konkrete Anwendungsfälle, die über Betreiber- oder Herstellergrenzen hinaus wirken, normativ festgelegt werden. Nicht näher festgelegt werden muss die Verwendung kryptographischer Algorithmen innerhalb der Grenzen eines Betreibers. Algorithmen für Szenarien, die nicht betreiberübergreifend eingesetzt werden, unterliegen den normativen Vorgaben des Kryptokonzeptes [gemSiKo#AnhF], sind aber ansonsten nicht weiter eingeschränkt, da sie keine Auswirkung auf die Interoperabilität zwischen Betreibern haben.

Innerhalb dieses Dokumentes werden daher die für die Verwendung in der TI vorgesehenen Algorithmen für einzelne Einsatzszenarien weiter eingeschränkt, so dass die zu verwendenden kryptographischen Bibliotheken auf ein sinnvolles Maß reduziert werden und somit die Interoperabilität gewährleistet wird. In diesem Dokument nicht aufgeführte Schlüssellängen sind unzulässig und dürfen nicht verwendet werden. Dabei bewegen sich alle verwendeten Algorithmen innerhalb des durch [gemSiKo#AnhF] und [BSI-TR03116] vorgegebenen Rahmens.

Bei der Verwendung der Algorithmen ist darauf zu achten, dass durch [gemSiKo#AnhF] die Anforderung besteht, kryptographische Algorithmen austauschen zu können. Dies KANN z. B. durch den Austausch der entsprechenden Bibliotheken, eine Anpassung der Software oder (wie zum Beispiel bei Karten) durch den Austausch der Komponente bzw. Teilen der Komponente erfolgen. Bei den Migrationsstrategien für kryptographische Algorithmen ist darauf zu achten, dass hinterlegte Objekte entweder umzuschlüsseln sind

oder die Algorithmen, die zur Erstellung verwendet wurden, weiterhin unterstützt werden müssen.

2 Einführung

2.1 Zielsetzung und Einordnung des Dokuments

Ziel des Dokumentes ist es, das breite Spektrum der durch [gemSiKo#AnhF] vorgegebenen kryptographischen Algorithmen, sofern sie betreiberübergreifend verwendet werden, weiter einzuschränken, um einzelnen Einsatzszenarien konkrete Algorithmen vorzugeben.

Weiteres Ziel ist die Spezifikationen von Kryptoalgorithmen an zentraler Stelle. Dadurch die Verwendung Referenzierung aus anderen Dokumenten wird einerseits die Einheitlichkeit der verwendeten Algorithmen über verschiedene Dokumente sichergestellt und gleichzeitig die Möglichkeit geboten die Diskussion über Algorithmen von der Diskussion über die Spezifikation von Komponenten zu entkoppeln. Hierdurch wird auch die Planung von Migrationsszenarien vereinfacht.

Da das Dokument den Vorgaben des Kryptokonzeptes folgt, wird bei neuen Erkenntnissen über die verwendeten kryptographischen Algorithmen, die zu einer Änderung des Kryptokonzeptes führen, gegebenenfalls auch eine Anpassung dieses Dokumentes erfolgen. Für Verwendungszwecke, bei denen bereits eine Migration zu stärkeren Algorithmen in Planung ist oder die Verwendung von Algorithmen unterschiedlicher Stärke zulässig ist, wird ein Ausblick gegeben, bis wann welche Algorithmen ausgetauscht sein müssen.

2.2 Zielgruppe

Das Dokument richtet sich an Mitarbeiter der gematik, die an der Erstellung von Spezifikationen und Architekturen arbeiten. Spezifikationen und Dokumente der gematik SOLLEN die zu verwendenden kryptographischen Algorithmen nicht direkt aufzählen, sondern bei der Verwendung von kryptographischen Algorithmen den entsprechenden Abschnitt dieses Dokumentes referenzieren.

Gleichzeitig richtet sich das Dokument an Hersteller von TI-Komponenten, um die für sie relevanten kryptographischen Algorithmen vorzugeben.

2.3 Geltungsbereich

Das Dokument gibt die zu verwendenden kryptographischen Algorithmen normativ vor. Die Festlegungen in dieser Version der Spezifikation stehen im Zusammenhang mit der Einführung der Karten der Generation 1 und gelten für Umgebungen und Releases, in denen diese eingesetzt werden dürfen.

2.4 Arbeitsgrundlagen

Rechtliche Grundlage für die Arbeiten sind die §§ 291a und 291b des SGB V und die Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte [RVO2006]. Hinzu kommen weitere Vorschriften aus SGB V und dem Datenschutzgesetz sowie Verordnungen auf Basis dieser Gesetze. Diese Grundlagen sind an den jeweiligen Verwendungsstellen referenziert.

Als Rahmen für die zur Verfügung stehenden Algorithmen ist [gemSiKo#AnhF] normativ, das selbst wiederum wo relevant auf [BSI-TR03116], [SigÄndG], [SigV01] und den Vorgaben der Bundesnetzagentur basiert.

Die Auswahl der Algorithmen orientiert sich an den in Bibliotheken und Entwicklungsumgebungen verfügbaren Algorithmen.

2.5 Abgrenzung des Dokuments

Aufgabe des Dokumentes ist es nicht, eine Sicherheitsbewertung von kryptographischen Algorithmen vorzunehmen. Dieser Gesichtspunkt wird in [gemSiKo#AnhF] und [BSI-TR03116] behandelt. Es werden lediglich die in [gemSiKo#AnhF] vorgegebenen Algorithmen weiter eingeschränkt, um die Herstellung der Interoperabilität zu unterstützen.

Es ist nicht Ziel dieses Dokumentes, den Prozess zum Austauschen von Algorithmen zu definieren, sondern lediglich den zeitlichen Rahmen für die Gültigkeit von Algorithmen festzulegen und somit auf den Bedarf für die Migration hinzuweisen.

Das Dokument gibt keinen Ausblick auf Kartengenerationen nach Generation 1.

2.6 Methodik

2.6.1 Verwendung von Schüsselworten

Für die genauere Unterscheidung zwischen normativen und informativen Inhalten werden die dem RFC 2119 [RFC2119] entsprechenden in Großbuchstaben geschriebenen, deutschen Schlüsselworte verwendet:

MUSS bedeutet, dass es sich um eine absolutgültige und normative Festlegung bzw. Anforderung handelt.

DARF NICHT bezeichnet den absolutgültigen und normativen Ausschluss einer Eigenschaft.

SOLL beschreibt eine dringende Empfehlung. Abweichungen zu diesen Festlegungen sind in begründeten Fällen möglich. Wird die Anforderung nicht umgesetzt, müssen die Folgen analysiert und abgewogen werden.

SOLL NICHT kennzeichnet die dringende Empfehlung, eine Eigenschaft auszuschließen. Abweichungen sind in begründeten Fällen möglich. Wird die Anforderung nicht umgesetzt, müssen die Folgen analysiert und abgewogen werden.

KANN bedeutet, dass die Eigenschaften fakultativ oder optional sind. Diese Festlegungen haben keinen Normierungs- und keinen allgemeingültigen Empfehlungscharakter.

2.6.2 Normative und informative Kapitel

Alle in diesem Dokument enthaltenen Kapitel sind normativ, sofern dies nicht explizit ausgeschlossen ist.

2.6.3 Hinweis auf offene Punkte

Offene Punkte, die bis zur nächsten Dokumentversion bearbeitet werden, sind vorläufig mit den folgenden Konventionen gekennzeichnet

Das Kapitel wird in einer späteren Version des Dokumentes ergänzt.

3 Anforderungen und Annahmen

Die nachfolgend aufgeführten Eingangsanforderungen entstammen dem Anforderungsmanagement der gematik und sind dort über die jeweilige Anforderungsidentifikation (AFO-ID) auffindbar.

3.1 Funktionale Eingangsanforderungen

Tabelle 1: Funktionale Eingangsanforderungen

AFO-ID	Klasse	Titel	Beschreibung	Quelle
A_00166	F	Ziel der Testmaßnahmen: funktionales Zusammenwirken der Komponenten und Dienste	[Die Testmaßnahmen zur Überprüfung und Weiterentwicklung der Telematikinfrastruktur] .... richten sich insbesondere auf deren (Komponenten und Dienste) funktionales ….Zusammenwirken innerhalb der Telematikinfrastruktur....	RVO 2006 § 2 Absatz 1 Satz 1.2
A_00251	F	Die eGK muss technisch geeignet sein, Authentifizierung, Verschlüsselung und elektronische Signatur zu ermöglichen.	Die elektronische Gesundheitskarte ... MUSS technisch geeignet sein, Authentifizierung, Verschlüsselung und elektronische Signatur zu ermöglichen.	SGB V § 291 Absatz 2a Satz 3 vom 20. Dezember 1988 (BGBl. I S. 2477, 2482); zuletzt geändert durch Artikel 20 des Gesetzes vom 5. September 2006 (BGBl. I S. 2098) Rechtsstand 1. September 2006
A_00697	F	Komponenten über Netz nur verschlüsselt	Alle Daten, die über das Netz gehen, MÜSSEN für den Transport zwischen den einzelnen Komponenten der TI verschlüsselt werden.	Workshop GA mit GV-Beteiligung Absatz Top 4
A_00700	F	Ende-zu-Ende Vertraulichkeit für medizinische Daten	Medizinische Daten MÜSSEN für alle Fachdienste auf Anwendungsebene Ende-zu-Ende so verschlüsselt werden, dass sie für Vermittlungskomponenten der TI nicht lesbar sind.	Workshop GA mit GV-Beteiligung Absatz Top 5
A_00716	F	Verantwortung der gematik bedeutet: Interoperabilität	(1) Im Rahmen der Aufgaben nach § 291a Abs. 7 Satz 2 hat die Gesellschaft für Telematik ... Die Gesellschaft für Telematik hat Aufgaben nur insoweit wahrzunehmen, wie dies zur Schaffung einer interoperablen und kompatiblen Telematikinfrastruktur erforderlich ist. Mit Teilaufgaben der Gesellschaft für Telematik können einzelne Gesellschafter oder Dritte beauftragt werden; hierbei sind durch die Gesellschaft für Telematik Interoperabilität, Kompatibilität und das notwendige Sicherheitsniveau der Telematikinfrastruktur zu gewährleisten. ...	SGB V § 291 b Absatz 1 vom 20. Dezember 1988 (BGBl. I S. 2477, 2482); zuletzt geändert durch Artikel 20 des Gesetzes vom 5. September 2006 (BGBl. I S. 2098) Rechtsstand 1. September 2006

AFO-ID	Klasse	Titel	Beschreibung	Quelle
A_00912	F	Identitätsbezogene Gemeinschaftsschlüssel	Innerhalb der Telematikinfrastruktur MÜSSEN immer identitätsbezogene Schlüssel verwendet werden. (Auch für Gemeinschaften, rollenbezogene Schlüssel sind verboten.)	
A_01098	F	Verschlüsselung von Daten bei Speicherung	Verschlüsselung von Daten bei Speicherung auf serverbasierten Fachdiensten für §291a-Anwendungen: Servergespeicherte medizinische Daten, die innerhalb der §291a-Anwendungen der Telematikinfrastruktur gespeichert werden, MÜSSEN verschlüsselt gespeichert werden, es MÜSSEN dabei Hybridschlüssel verwendet werden.	
A_01473	F	Nutzbarkeit der Anwendungen mit allen gültigen eGK-Versionen	Es MUSS sichergestellt sein, dass die Anwendungen der eGK mit allen aktuellen und gültigen eGK-Versionen ausgeführt werden können.	Meldung

3.2 Nicht-Funktionale Eingangsanforderungen

Tabelle 2: Nicht-Funktionale Eingangsanforderungen

AFO-ID	Klasse	Titel	Beschreibung	Quelle
A_00162	N	Ziel der Testmaßnahmen: Interoperabilität	[Die Testmaßnahmen zur Überprüfung und Weiterentwicklung der Telematikinfrastruktur] .... richten sich insbesondere auf Interoperabilität, …der einzelnen Komponenten und Dienste …	RVO 2006 § 2 Absatz 1 Satz 1.2
A_00163	N	Ziel der Testmaßnahmen: Kompatibilität	[Die Testmaßnahmen zur Überprüfung und Weiterentwicklung der Telematikinfrastruktur] .... richten sich insbesondere auf… Kompatibilität, …der einzelnen Komponenten und Dienste …	RVO 2006 § 2 Absatz 1 Satz 1.2
A_00164	N	Ziel der Testmaßnahmen: Stabilität	[Die Testmaßnahmen zur Überprüfung und Weiterentwicklung der Telematikinfrastruktur] .... richten sich insbesondere auf...Stabilität …der einzelnen Komponenten und Dienste …	RVO 2006 § 2 Absatz 1 Satz 1.2
A_00167	N	Ziel der Testmaßnahmen: technisches Zusammenwirken der Komponenten und Dienste	[Die Testmaßnahmen zur Überprüfung und Weiterentwicklung der Telematikinfrastruktur] .... richten sich insbesondere auf deren (Komponenten und Dienste) ... technisches Zusammenwirken innerhalb der Telematikinfrastruktur....	RVO 2006 § 2 Absatz 1 Satz 1.2
A_01298	N	Betrieb: Sicherung der Interoperabilität	gematik MUSS die Interoperabilität aller Telematikkomponenten sicherzustellen. Dies gilt im Sinne der: * Spezifikationsverantwortung * Verantwortung für das Test- und Zulassungsverfahren * Betriebsverantwortung (Betriebsprozesse sowie das einzuhaltende Sicherheitsniveau) * Sicherstellung der Interoperabilität über alle PKI-Strukturen der Telematikinfrastruktur des	

AFO-ID	Klasse	Titel	Beschreibung	Quelle
			Gesundheitswesens Dieses MUSS durch ein Zugangs- und Überprüfungsrecht im Rahmen von Audits und der permanenten technischen und organisatorischen Betriebsüberwachung gewährleistet sein.	

3.3 Sicherheitsanforderungen

Tabelle 3: Sicherheitsanforderungen

AFO-ID	Klasse	Titel	Beschreibung	Quelle
A_00165	S	Ziel der Testmaßnahmen: Sicherheit	[Die Testmaßnahmen zur Überprüfung und Weiterentwicklung der Telematikinfrastruktur] .... richten sich insbesondere auf... Sicherheit der einzelnen Komponenten und Dienste …	RVO 2006 § 2 Absatz 1 Satz 1.2
A_00514	S	Verschlüsselung	Transport und Speicherung medizinischer Daten jeglicher Art auf Servern MÜSSEN verschlüsselt werden. (Öffentlicher Schlüssel des Versicherten)	Grundsatzpositionen und -entscheidungen zu Telematikanwendungen der Gesundheitskarte 0.5.5
A_00687	S	Audit-Dienst, Verschlüsselung	Die Audit-Daten MÜSSEN verschlüsselt werden. (medizinische Daten)	Workshop GA mit GV-Beteiligung Absatz Top 5
A_00738	S	Die dezentralen Komponenten Primärsystem, Konnektor und Kartenterminals sind LAN-gestützt verbunden.	Die dezentralen Komponenten Primärsystem, Konnektor und Kartenterminals sind LAN-gestützt verbunden.	Releasedefinition 1 V0.9.0
A_00803	S	Identifizierende Informationsobjekte dürfen nicht von eGK auf andere Medien übertragen werden	Technische Informationsobjekte (wie private Schlüssel), die in der virtuellen Welt als einziges Merkmal zur Herstellung von Authentizität und Unabstreitbarkeit herangezogen werden (können), MÜSSEN vor Übertrag auf andere elektronische Medien als die eGK geschützt werden. Die Nutzung technischer Informationsobjekte, die als einziges Merkmal zur Herstellung von Authentizität und Unabstreitbarkeit herangezogen werden, muss durch ein Authentifikationsverfahren, das einen eindeutigen Bezug zum der eGK zugeordneten Versicherten zulässt, geschützt werden.	Releasedefinition 2 V1.0.0
A_01439	S	LAN-Verbindung zwischen Kartenterminal und Konnektor MUSS zur Absicherung verschlüsselt sein.	LAN-Verbindung zwischen Kartenterminal und Konnektor MUSS zur Absicherung verschlüsselt sein.	Releasedefinition 1 V0.9.0
A_40345	S	Schutz Daten des Versicherten	Die Daten des Versicherten MÜSSEN durch starke Sicherheitsdienste vor missbräuchlicher Benutzung geschützt werden. (mind. Hoher Schutzbedarf)	
A_40584	S	Verfügungsgewalt für medizinische Daten in der TI hat der	Medizinische Daten in der Telematikinfrastruktur MÜSSEN grundsätzlich verschlüsselt und nicht im	

AFO-ID	Klasse	Titel	Beschreibung	Quelle
		Versicherte	Klartext verfügbar und bearbeitbar sein. Die Verschlüsselungsschlüssel MÜSSEN in der alleinigen Verfügungsgewalt des Versicherten sein, damit dieser und nur dieser entscheiden kann welche Daten welchen dritten Personen zugänglich gemacht werden.	

3.4 Eingangsanforderungen ohne Referenz des Anforderungsmanagements

Neben den durch das Anforderungsmanagement bestätigten Anforderungen wurden durch das Sicherheitskonzept [gemSiKo] weitere Anforderungen angemeldet. Diese Anforderungen sind bislang noch nicht als Anforderungen im Anforderungskatalog aufgenommen, werden jedoch berücksichtigt und werden in die vorangehenden Abschnitte übernommen sobald sie eine AFO-ID erhalten haben.

Tabelle 4: Anforderungen ohne AFO-ID

ID in gemSiKo	Beschreibung
AS_EP_03	Schutz der Informationen durch starke Kryptoalgorithmen Die unautorisierte Modifikation oder Zerstörung von Daten, die unautorisierte Bekanntgabe von Informationen MÜSSEN beim Transfer von Daten, bei deren Verarbeitung und Speicherung in der Telematikinfrastruktur mit Kryptoalgorithmen mindestens der Mechanismenstärke „hoch“ erkannt bzw. verhindert werden. Konsequenzen: Sicherheitsdienste und Sicherheitsinfrastrukturen der Mechanismenstärke „hoch“ und „sehr hoch“ MÜSSEN von der Telematikinfrastruktur bereitgestellt werden und MÜSSEN entsprechend der Schutzbedarfsfestlegung für die fachlichen und technischen Objekte verwendet werden. Der aktuell gültige Algorithmenkatalog der gematik MUSS verwendet werden (siehe [gemSiko] Anhang F).
AS_EP_04	Versichertenindividuelle Verschlüsselung Medizinische Daten sind in der Telematikinfrastruktur immer verschlüsselt (siehe [Grundsatzentscheidung]) und im Klartext nicht verfügbar und bearbeitbar. Die Verschlüsselungsschlüssel sind in der alleinigen Verfügungsgewalt des Versicherten, damit dieser und nur dieser entscheiden kann, welche Daten welchen dritten Personen zugänglich gemacht werden. Konsequenzen: Die Anforderungen an die Verwaltung der Verschlüsselungsschlüssel werden in [gemSiko] Anhang F – Kryptographiekonzept festgelegt.
AS-Krypt-01	Für kryptographische Operationen in der Telematikinfrastruktur MÜSSEN stets nach dem Stand der Wissenschaft und Technik geeignete Algorithmen und Parameter entsprechend der Technische Richtlinie des BSI [BSI TR-03116] eingesetzt werden.
AS-Krypt-02	Die Liste der in der Telematikinfrastruktur verwendbaren Algorithmen MUSS von der gematik mindestens einmal jährlich und bei Bedarf (z.B. bei neuen wissenschaftlichen Erkenntnissen bzw. bei Änderungen in [BSI TR-03116]) überprüft und ggf. angepasst werden.
AS-Krypt-03	Die Hard- und Softwarearchitektur MUSS den Austausch kryptographischer Algorithmen und Parameter erlauben und eine Migrationsfähigkeit zur Anpassungen, u. a. bei Änderungen von [BSI TR-03116], vorsehen.
AS-Krypt-	Die Kommunikations-Protokolle bzw. Sicherheitskomponenten MÜSSEN so gestaltet sein, dass ein Erzwingen des Einsatzes von Algorithmen oder Parametern, deren Sicherheitseignung nicht mehr gegeben ist, nicht

ID in gemSiKo	Beschreibung
04	möglich ist.
AS-Krypt-05	Während einer im Anlassfall zu definierenden Übergangsphase MÜSSEN sowohl neue als auch alte Algorithmen und Parameter verarbeitet werden können. Hinweis: Eine Anpassung der Schlüssellänge/Tausch des Verfahrens jedes eingesetzten Verfahrens SOLL innerhalb von 6 Monaten[1] für alle im Einsatz befindlichen Schlüssel/Verfahren möglich sein. Während dieser Übergangsphase müssen sowohl neue als auch alte Schlüssel/Verfahren verarbeitet werden können.
AS-Krypt-07	Alle Sicherheitskomponenten SOLLEN für jedes kryptographische Primitiv die notwendige Migrationsfähigkeit von Algorithmen unterstützen. Nähere Vorgaben SOLLEN in den jeweiligen Einsatzumgebungen der einzelnen Anwendungsbereiche festgelegt werden,
AS-Krypt-08	Für jeden Schlüssel MÜSSEN die relevanten Abläufe während des kompletten Lebenszyklus festgelegt werden. Der Lebenszyklus eines Schlüssels umfasst nach ISO 11770 Erzeugung (Generation), Aktivierung (Activation) mit Installation jeweils optional Zertifikatserzeugung, Schlüsselableitung, Schlüsselverteilung, Registrierung des Schlüssels/Zertifikats, Speicherung des Schlüssels, sowie Deaktivierung (Deactivation), Reaktivierung (Reactivation) und Zerstörung des Schlüssels (Destruction).
Keine	Online gespeicherte medizinische Daten MÜSSEN hybrid verschlüsselt werden, d. h. der für einen Datensatz spezifische (symmetrische) Schlüssel wird wiederum mit dem öffentlichen ENC-Schlüssel der eGK verschlüsselt. Eine unverschlüsselte Speicherung des spezifischen Schlüssels DARF NICHT erfolgen. Damit sind zunächst alle Daten gegen Zugriffe geschützt.
Keine	Die vertrauliche Kommunikation zwischen Leistungserbringer zu den Kostenträgern sowie zu allen relevanten Diensten MUSS gewährleistet sein (Einsatz von kryptographischen Verfahren, welche dem aktuellen Stand der Wissenschaft und Technik entsprechen).
Keine	Eine sichere Identifikation und Authentisierung des Kartenterminals durch den Konnektor mit Hilfe kryptographischer Verfahren MUSS sichergestellt sein.

[1] Welche Vorlaufzeit tatsächlich benötigt wird kann im Einzelfall bewertet und entschieden werden. Die technische Lösung muss aber eine Anpassung innerhalb dieses Zeitraums ermöglichen. Die Laufzeiten von ggf. zu tauschenden Karten sind in diesen 6 Monaten nicht enthalten.

4 Struktur und Verwendung des Dokumentes

Wie in Kapitel 2 dargestellt, ist das Ziel des Dokumentes, die Verwendung eindeutiger kryptographischer Algorithmen zur Unterstützung der Interoperabilität normativ festzulegen. Um die Anpassung von weiteren Dokumenten auf Grund der Änderung von Algorithmen zu verhindern, MÜSSEN alle relevanten Informationen zu verwendeten kryptographischen Algorithmen in diesem Dokument aufgeführt und aus anderen Dokumenten wie in Abschnitt 4.1 dargestellt, referenziert werden.

Die Anforderung, Algorithmen aus anderen Dokumenten der gematik zu referenzieren, wirkt sich auf die Struktur dieses Dokumentes aus. Es wurden die folgenden Kriterien bei der Struktur dieses Dokumentes berücksichtigt.

- **Eine Anpassung der Algorithmen soll nicht zu Anpassungen in den referenzierenden Dokumenten führen.** Hieraus leitet sich implizit ab, dass zwei Arten von kryptographischen Identitäten oder Einsatzszenarien für Algorithmen in diesem Dokument nur dann unter der gleichen Referenz aufgeführt werden dürfen, wenn sichergestellt ist, dass sie auch in Zukunft immer die gleichen Anforderungen besitzen. Sofern dies nicht sichergestellt ist, müssen zwei separat referenzierbare Abschnitte mit gleichen Algorithmen aufgeführt werden.
- **GemSpec_Krypt soll nicht für jeden Einsatzzweck kryptographischer Identitäten direkt Algorithmen festlegen.** Die Festlegung der Algorithmen für jeden einzelnen Anwendungsfall würde zwar die Anforderung an die Flexibilität erfüllen, würde jedoch dazu führen, dass eine Anpassung dieses Dokumentes für jede neue Identität notwendig wäre.
- **Vollständigkeit der referenzierbaren Abschnitte.** Es ist das Ziel des Dokumentes, alle Festlegungen zu einer konkreten Identität oder alle Festlegungen für einen konkreten Sachverhalt in dem jeweiligen Abschnitt zusammen zu fassen. Dies hat zu Redundanzen geführt, die aufgrund der Referenzierbarkeit bewusst in Kauf genommen werden.

Das Dokument definiert zunächst in Kapitel 5 grundlegende einsatzszenarienübergreifende Algorithmen, wie zum Beispiel zulässige kryptographische Identitäten. Diese werden in Kapitel 6 für spezifische Einsatzszenarien verwendet und näher spezifiziert.

4.1 Referenzierung der Algorithmen aus Dokumenten der gematik

Das Ziel des Dokumentes ist u. a. für weitere Dokumente der gematik eine Basis zur Referenzierung der kryptographischen Algorithmen zu bilden. Zur einheitlichen Darstellung der Referenzierung MUSS das folgende Prinzip verwendet werden.

Alle Verweise aus anderen Dokumenten MÜSSEN auf konkrete Abschnitte dieses Dokumentes verweisen. Die Referenz enthält hierbei zunächst das Kürzel des Dokumentes (gemSpec_Krypt), gefolgt von einem Hash-Symbol (#) als Trennzeichen, gefolgt von dem zu referenzierenden Abschnitt.

Beispielsweise wäre die Referenzierung der Beschreibung von X.509-Zertifikaten für die Erstellung qualifizierter Signaturen aus anderen Dokumenten [gemSpec_Krypt#5.1.1.3]. Der korrespondierende Eintrag der Referenzierungstabelle wäre:

[gemSpec_Krypt]	gematik (26.03.2008): Einführung der Gesundheitskarte - Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 1.3.0
[gemSpec_Krypt#5.1.1.3]	Kap. 5.1.1.3 - X.509-Identitäten für die Erstellung qualifizierter Signaturen

Bei der Erstellung des Dokumentes wurde versucht, die Anforderungen abhängig von der Schachtelungstiefe detaillierter werden zu lassen. Das bedeutet z.B., dass Abschnitt 5.1.1 die übergreifenden Anforderungen an X.509-Zertifikate definiert. In den entsprechenden Unterabschnitten werden diese Anforderungen weiter detailliert. Aus diesem Grund SOLLEN Dokumente, die auf [gemSpec_Krypt] verweisen, auf ein möglichst detailliertes Kapitel verweisen.

5 Einsatzszenario übergreifende Algorithmen

Nachfolgend werden grundlegende Festlegungen zur Verwendung von Algorithmen innerhalb der Telematikinfrastruktur getroffen. Diese Anforderungen sind unabhängig von den im nachfolgenden Kapitel definierten Einsatzszenarien und werden durch diese verwendet.

5.1 Identitäten

Der Begriff kryptographische Identität (nachfolgend nur noch als Identität bezeichnet) bezeichnet einen Verbund aus Identitätsdaten und einem kryptographischen Objekt, der zur Authentisierung und Authentifizierung verwendet werden kann. Im Allgemeinen handelt es sich um Schlüsselpaare, bestehend aus öffentlichem und privatem Schlüssel, sowie einem Zertifikat, das die Kombination aus Authentifizierungsmerkmal und öffentlichem Schlüssel durch eine übergeordnete Instanz (CA – Certification Authority) bestätigt.

Bei den Algorithmenvorgaben für Identitäten muss spezifiziert werden, für welche Algorithmen die Schlüssel verwendet werden und welche Algorithmen für die Signatur des Zertifikates verwendet werden müssen. Zudem muss angegeben werden, mit welchen Algorithmen die OCSP Responses signiert werden und wie die Zertifikate des OCSP Responders signiert sind.

Offener Punkt - Die Abstimmung der OCSP Algorithmen mit dem BSI ist noch nicht abgeschlossen

Die ausgewählten Algorithmen wurden bislang nicht durch das BSI bestätigt und können sich potentiell noch ändern. Aus PKI-Sicht ist die Verwendung von OCSP Respondern mit unterschiedlichen Algorithmen innerhalb eines Trust Centers mit immensem Aufwand verbunden. Aus diesem Grund ist geplant, für alle OCSP Responder einheitlich SHA1 und RSA1024 zu verwenden.

Die Verwendung dieser schwächeren Algorithmen stellt aus folgenden Gründen keine Bedrohung dar:

- *Alle OCSP Responder Zertifikate sind neben der Signatur, die sie selbst schützt, auch in eine TSL eingebettet, die mit SHA256 und RSA2048 signiert ist. Auf der reinen Verteilungsebene werden somit stärkere Algorithmen für den Integritätsschutz verwendet.*
- *Die Lebensdauer der signierten OCSP Responses ist sehr kurz. Dadurch verringert sich das Zeitfenster für die Durchführung eines Angriffs.*
- *Angriffe, die auf Schwächen in SHA1 basieren, sind nur dann möglich, wenn ein zweiter Text gefunden werden kann, der zu dem gleichen Hashwert führt. Diese Angriffe werden dadurch erschwert, dass die Struktur der OCSP Response sehr statisch ist und somit die Bestandteile, die zur Erzeugung einer OCSP Response mit gleichem Hashwert führen, sehr stark eingeschränkt werden.*

5.1.1 X.509-Identitäten

Eine X.509-Identität ist eine Identität gemäß Abschnitt 5.1, bei der als Zertifikat ein X.509-Zertifikat verwendet wird.

Bei der Aufteilung von X.509-Identitäten wurden die Identitäten zunächst nach Gruppen für verschiedene Einsatzzwecke des Schlüssels unterteilt und diese bei Bedarf um einen notwendigen Einsatzkontext erweitert. Aus dieser Aufteilung ergibt sich die nachfolgend tabellarisch dargestellte Übersicht der Arten von X.509-Identitäten. Der exemplarische Einsatzort der Identitäten ist hierbei rein informativ und die Hoheit über die Zuordnung der der Algorithmen liegt bei dem Spezifikateur der Identität und muss durch diesen anhand der relevanten Anforderungen entschieden werden:

Tabelle 5: Übersicht über Arten von X.509 Identitäten

Referenz	Gruppe	Kontext	Exemplarische Identitäten zur Verwendung (nicht vollständig)
5.1.1.2	Identitäten für die Erstellung von Signaturen	Identitäten für die Erstellung fortgeschrittener Signaturen	AUT Identität der eGK AUTN Identität der eGK AUT Identität des HBA OSIG Identität der SMC-B
5.1.1.3		Identitäten für die Erstellung qualifizierter Signaturen	QES Identität des HBA
5.1.1.6		Signatur Identitäten die in den Diensten der TI und den Fachdiensten zum Einsatz kommen.	Fachdienst Signatur Zentrale Komponente TI für Signatur Code-Signatur gematik
5.1.1.4	Identitäten für die Client Server Authentifizierung	Identitäten für den Aufbau von SSL Verbindungen	AUT Identität der SMC-B AUT Identität des Konnektors AUT Identität des Kartenterminals Fachdienst SSL – Server zentrale TI SSL – Server zentrale TI SSL – Client
5.1.1.5		Identitäten für den Aufbau von IPSec Verbindungen	SM-K-IPSEC-CERT IPSEC-CERT VPN-Konzentrator
5.1.1.7	Verschlüsselungszertifikate	Identitäten für die medizinische Daten verschlüsselt werden	ENC Identität der eGK ENCV Identität der eGK ENC Identität des HBA ENC Identität der SMC-B

Es wird erwartet, dass zukünftig unterschiedliche Zertifikatstypen abweichende Anforderungen an Algorithmen stellen werden. Dies wird insbesondere für Zertifikate qualifizierter Signaturen der Fall sein, da hier die Anforderungen vermutlich schneller steigen werden, als dies für fortgeschrittene Zertifikate der Fall ist. Aus Gründen der einfacheren Referenzierbarkeit werden bereits jetzt die entsprechenden Abschnitte vorgesehen, auch wenn bislang keine abweichenden Anforderungen bestehen und Inhalte redundant aufgeführt werden. Dies bietet die Möglichkeit, die Anforderungen an Algorithmen entkoppelt zu betrachten, auch wenn man aus technischen Gründen die Algorithmen zunächst identisch behalten wird.

Für den Aufbau der X.509-Zertifikate gelten die Vorgaben aus den jeweiligen Spezifikationen der X.509-Zertifikate. In der tabellarischen Darstellung der Gültigkeiten für Algorithmen wird für das jeweils in der Kopfzeile angegebene Jahr die Gültigkeit der Algorithmen angegeben. Die Kürzel sind wie folgt zu verstehen:

A,V – Der Algorithmus ist bis zum Ende des angegebenen Jahres zulässig. Die **A**usgabe und die **V**erwendung von Identitäten, bei deren Erstellung der Algorithmus verwendet wurde und die für die Verwendung mit diesem Algorithmus geeignet sind, sind zulässig. Es obliegt der Hoheit des Herausgebers einen der zulässigen Algorithmen zu wählen, hierbei SOLL der Herausgeber den Gültigkeitszeitraum des Algorithmus beachten.

V – Dieser Algorithmus DARF für neu herausgegebene Identitäten zu dem entsprechenden Zeitpunkt NICHT mehr **v**erwendet werden, es ist jedoch für einen Übergangszeitraum zulässig, Identitäten die bereits herausgegeben wurden mit diesen Algorithmen zu verwenden. (Dieser Status wird derzeit nicht verwendet)

E – Die Gültigkeit dieses Algorithmus ist abgelaufen (**E**xpired) und die Verwendung des Algorithmus stellt ein potentielles Sicherheitsrisiko dar. Alle mit diesem Algorithmus im Umlauf befindlichen Identitäten MÜSSEN bis zum Beginn des angegebenen Jahres ausgetauscht und durch Identitäten, die einen zulässigen Algorithmus unterstützen, ersetzt werden.

O – Dieser Algorithmus ist **o**ptional. Sofern angegebene Algorithmen optional sind, muss in dem entsprechenden Abschnitt eine Erläuterung für die Verwendung erfolgen.

Nicht aufgeführte Algorithmen und Schlüssellängen DÜRFEN NICHT eingesetzt werden. Dies gilt auch für Algorithmen und Schlüssellängen, die als kryptographisch stärker und somit sicherer gelten, da diese nicht gefordert sind und somit nicht sichergestellt ist, dass diese auf allen Komponenten unterstützt werden.

5.1.1.1 (Abschnitt entfällt) Zusammenfassende Anforderungen an X.509-Identitäten

Der Abschnitt hat in früheren Versionen eine Übersicht über alle zulässigen Algorithmen dargestellt. Dies hat bei dem Kommentatoren und Herstellern zu Verwirrung geführt, der Abschnitt wurde daher entfernt.

Da sich durch das Entfernen des Abschnitts die Referenzierung für alle folgenden Abschnitte ändern würde, wurde der Abschnitt als Platzhalter beibehalten.

5.1.1.2 X.509-Identitäten für die Erstellung fortgeschrittener Signaturen

Bei Identitäten dieses Typs soll keine Einschränkung auf fortgeschrittene Zertifikate nach [SigÄndG] erfolgen, sondern diese Gruppe umfasst alle Zertifikate, die in der Algorithmenstärke an fortgeschrittene Zertifikate nach [SigÄndG] angelehnt sind. Dies sind insbesondere fortgeschrittene Zertifikate nach [SigÄndG], Organisationszertifikate und technische Signaturzertifikate.

Identitäten für fortgeschrittene Signaturen MÜSSEN den in Tabelle 6 gestellten Anforderungen an Algorithmen genügen.

Tabelle 6: Algorithmen für X.509-Identitäten zur Erstellung fortgeschrittener Signaturen

Algorithmen Typ	Algorithmen	Schlüssel länge	2008	2009	2010	2011	2012	2013
Verwendung der Schlüssel	RSA	1024	E	E	E	E	E	E
		2048	A,V	A,V	A,V	A,V	A,V	A,V

Signatur des Endnutzer- und CA-Zertifikates	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	E	E	E	E	E	E
		2048	E	E	E	E	E	E
	sha256withRSAEncryption (OID 1.2.840.113549.1.1.11)	1024	E	E	E	E	E	E
		2048	A,V	A,V	A,V	A,V	A,V	A,V
Signatur der OCSP Response	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	A,V	A,V	A,V	A,V	A,V	A,V
Signatur des OCSP Responder Zertifikates	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	A,V	A,V	A,V	A,V	A,V	A,V

Die Lebensdauer der Schlüssel und somit die in einem Zertifikat angegebene Gültigkeitsdauer SOLL gemäß [gemSiKo#AnhF] maximal 5 Jahre betragen.

Offener Punkt - Die Abstimmung der OCSP Algorithmen mit dem BSI ist noch nicht abgeschlossen.

Die ausgewählten Algorithmen wurden bislang nicht durch das BSI bestätigt und können sich potentiell noch ändern. Eine ausführlichere Bewertung befindet sich in Abschnitt 5.1

5.1.1.3 X.509-Identitäten für die Erstellung qualifizierter Signaturen

Identitäten für qualifizierte Signaturen MÜSSEN den in Tabelle 7 gestellten Anforderungen an Algorithmen genügen.

Tabelle 7: Algorithmen für X.509-Identitäten zur Erstellung qualifizierter Signaturen

Algorithmen Typ	Algorithmus	Schlüssel länge	2008	2009	2010	2011	2012	2013
Verwendung der Schlüssel	RSA	1024	E	E	E	E	E	E
		2048	A,V	A,V	A,V	A,V	A,V	A,V
Signatur des Endnutzer- und CA-Zertifikates	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	E	E	E	E	E	E
		2048	E	E	E	E	E	E
	sha256withRSAEncryption (OID 1.2.840.113549.1.1.11)	1024	E	E	E	E	E	E
		2048	A,V	A,V	A,V	A,V	A,V	A,V
Signatur der OCSP Response	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	A,V	A,V	A,V	A,V	A,V	A,V
Signatur des OCSP Responder Zertifikates	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	A,V	A,V	A,V	A,V	A,V	A,V

Die Lebensdauer der Schlüssel und somit die in einem Zertifikat angegebene Gültigkeitsdauer SOLL gemäß [gemSiKo#AnhF] maximal 5 Jahre betragen.

Offener Punkt - Die Abstimmung der OCSP Algorithmen mit dem BSI ist noch nicht abgeschlossen

Die ausgewählten Algorithmen wurden bislang nicht durch das BSI bestätigt und können sich potentiell noch ändern. Eine ausführlichere Bewertung befindet sich in Abschnitt 5.1

5.1.1.4 X.509-Identitäten für die TLS/SSL-Authentifizierung

Identitäten für die TLS/SSL-Authentifizierung MÜSSEN den in Tabelle 8 gestellten Anforderungen an Algorithmen genügen.

Tabelle 8: Algorithmen für X.509-Identitäten zur TLS/SSL-Authentifizierung

Algorithmen Typ	Algorithmus	Schlüssel länge	2008	2009	2010	2011	2012	2013
Verwendung der Schlüssel	RSA	1024	A,V	A,V	A,V	A,V	A,V	A,V
		2048	O	O	O	O	O	O
Signatur des Endnutzer- und CA-Zertifikates	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	A,V	A,V	A,V	A,V	A,V	A,V
		2048	O	O	O	O	O	O
	sha256withRSAEncryption (OID 1.2.840.113549.1.1.11)	1024	O	O	O	O	O	O
		2048	O	O	O	O	O	O
Signatur der OCSP Response	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	A,V	A,V	A,V	A,V	A,V	A,V
Signatur des OCSP Responder Zertifikates	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	A,V	A,V	A,V	A,V	A,V	A,V

Alle Komponenten, die TLS/SSL verwenden, MÜSSEN Identitäten, die mit „A,V“ angegeben sind, unterstützen und eine Identität dieses Typs besitzen. Dies ist notwendig um sicherzustellen, dass im Rahmen von Handshakes immer ein durch beide Komponenten unterstütztes Verfahren als „kleinster gemeinsamer Nenner“ zur Verfügung steht. Zusätzlich KANN eine zweite Identität für die optionalen Algorithmen vorhanden sein. Sofern sich im Rahmen des Verbindungsaufbaus eine der optionalen Identitäten als interoperabel rausstellt, so kann diese Identität für den Verbindungsaufbau genutzt werden. Sollte dies nicht der Fall sein, so steht immer der Verbindungsaufbau über die mittels „A,V“ angegebene Identitäten zur Verfügung.

Die Lebensdauer der Schlüssel und somit die in einem Zertifikat angegebene Gültigkeitsdauer SOLL gemäß [gemSiKo#AnhF] maximal 5 Jahre betragen.

Offener Punkt - Die Abstimmung der OCSP Algorithmen mit dem BSI ist noch nicht abgeschlossen

Die ausgewählten Algorithmen wurden bislang nicht durch das BSI bestätigt und können sich potentiell noch ändern. Eine ausführlichere Bewertung befindet sich in Abschnitt 5.1

5.1.1.5 X.509-Identiäten für die IPSec Authentifizierung

Identitäten für die IPSec Authentifizierung MÜSSEN den in Tabelle 9 gestellten Anforderungen an Algorithmen genügen.

Tabelle 9: Algorithmen für X.509-Identitäten zur IPSec Authentifizierung

Algorithmen Typ	Algorithmus	Schlüssel länge	2008	2009	2010	2011	2012	2013
Verwendung der Schlüssel	RSA	1024	A,V	A,V	A,V	A,V	A,V	A,V
		2048	O	O	O	O	O	O
Signatur des Endnutzer- und CA-Zertifikates	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	A,V	A,V	A,V	A,V	A,V	A,V
		2048	O	O	O	O	O	O
	sha256withRSAEncryption (OID 1.2.840.113549.1.1.11)	1024	O	O	O	O	O	O
		2048	O	O	O	O	O	O
Signatur der OCSP Response	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	A,V	A,V	A,V	A,V	A,V	A,V
Signatur des OCSP Responder Zertifikates	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	A,V	A,V	A,V	A,V	A,V	A,V

Alle Komponenten, die IPSec verwenden, MÜSSEN Identitäten, die mit „A,V „angegebenen sind, unterstützen und eine Identität dieses Typs besitzen. Dies ist notwendig um sicherzustellen, dass im Rahmen von Handshakes immer ein durch beide Komponenten unterstütztes Verfahren als „kleinster gemeinsamer Nenner“ zur Verfügung steht. Zusätzlich KANN eine zweite Identität für die optionalen Algorithmen vorhanden sein. Sofern sich im Rahmen des Verbindungsaufbaus eine der optionalen Identitäten als interoperabel rausstellt, so kann diese Identität für den Verbindungsaufbau genutzt werden. Sollte dies nicht der Fall sein, so steht immer der Verbindungsaufbau über die mittels „A,V“ angegebene Identitäten zur Verfügung.

Die Lebensdauer der Schlüssel und somit die in einem Zertifikat angegebene Gültigkeitsdauer SOLL gemäß [gemSiKo#AnhF] maximal 5 Jahre betragen.

Offener Punkt - Die Abstimmung der OCSP Algorithmen mit dem BSI ist noch nicht abgeschlossen

Die ausgewählten Algorithmen wurden bislang nicht durch das BSI bestätigt und können sich potentiell noch ändern. Eine ausführlichere Bewertung befindet sich in Abschnitt 5.1

5.1.1.6 X.509-Identitäten für fortgeschrittene Signaturen durch TI Komponenten

Identitäten für fortgeschrittene Signaturidentitäten in TI-Komponenten MÜSSEN den in Tabelle 10 gestellten Anforderungen an Algorithmen genügen.

Tabelle 10: Algorithmen für fortgeschrittene X.509-Signatur-Identitäten für TI Komponenten

Algorithmen Typ	Algorithmus	Schlüssel länge	2008	2009	2010	2011	2012	2013
Verwendung der Schlüssel	RSA	1024	E	E	E	E	E	E
		2048	A,V	A,V	A,V	A,V	A,V	A,V
Signatur des Endnutzer- und CA-Zertifikates	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	E	E	E	E	E	E
		2048	E	E	E	E	E	E
	sha256withRSAEncryption	1024	E	E	E	E	E	E

	(OID 1.2.840.113549.1.1.11)	2048	A,V	A,V	A,V	A,V	A,V	A,V
Signatur der OCSP Response	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	A,V	A,V	A,V	A,V	A,V	A,V
Signatur des OCSP Responder Zertifikates	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	A,V	A,V	A,V	A,V	A,V	A,V

Die Lebensdauer der Schlüssel und somit die in einem Zertifikat angegebene Gültigkeitsdauer SOLL gemäß [gemSiKo#AnhF] maximal 5 Jahre betragen.

Offener Punkt - Die Abstimmung der OCSP Algorithmen mit dem BSI ist noch nicht abgeschlossen

Die ausgewählten Algorithmen wurden bislang nicht durch das BSI bestätigt und können sich potentiell noch ändern. Eine ausführlichere Bewertung befindet sich in Abschnitt 5.1

5.1.1.7 X.509-Verschlüsselungszertifikate

Verschlüsselungszertifikate MÜSSEN den in Tabelle 11 gestellten Anforderungen an Algorithmen genügen.

Tabelle 11: Algorithmen für Verschlüsselungszertifikate

Algorithmen Typ	Algorithmus	Schlüssel länge	2008	2009	2010	2011	2012	2013
Verwendung der Schlüssel	RSA	1024	E	E	E	E	E	E
		2048	A,V	A,V	A,V	A,V	A,V	A,V
Signatur des Endnutzer- und CA-Zertifikates	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	E	E	E	E	E	E
		2048	E	E	E	E	E	E
	sha256withRSAEncryption (OID 1.2.840.113549.1.1.11)	1024	E	E	E	E	E	E
		2048	A,V	A,V	A,V	A,V	A,V	A,V
Signatur der OCSP Response	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	A,V	A,V	A,V	A,V	A,V	A,V
Signatur des OCSP Responder Zertifikates	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	A,V	A,V	A,V	A,V	A,V	A,V

Die Lebensdauer der Schlüssel und somit die in einem Zertifikat angegebene Gültigkeitsdauer SOLL gemäß [gemSiKo#AnhF] maximal 5 Jahre betragen.

Offener Punkt - Die Abstimmung der OCSP Algorithmen mit dem BSI ist noch nicht abgeschlossen

Die ausgewählten Algorithmen wurden bislang nicht durch das BSI bestätigt und können sich potentiell noch ändern. Eine ausführlichere Bewertung befindet sich in Abschnitt 5.1

5.1.1.8 X.509-Identitäten zur Authentifizierung für SSL/TLS Verbindungen mit erhöhtem Schutzbedarf

Identitäten für die TLS/SSL Authentifizierung für Verbindungen mit erhöhtem Schutzbedarf MÜSSEN den in Tabelle 12: Algorithmen für X.509-Identitäten gestellten Anforderungen an Algorithmen genügen.

Tabelle 12: Algorithmen für X.509-Identitäten zur Authentifizierung von SSL/TLS Verbindungen mit erhöhtem Schutzbedarf

Algorithmen Typ	Algorithmus	Schlüssel länge	2008	2009	2010	2011	2012	2013
Verwendung der Schlüssel	RSA	1024	E	E	E	E	E	E
		2048	A,V	A,V	A,V	A,V	A,V	A,V
Signatur des Endnutzer- und CA-Zertifikates	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	E	E	E	E	E	E
		2048	E	E	E	E	E	E
	sha256withRSAEncryption (OID 1.2.840.113549.1.1.11)	1024	E	E	E	E	E	E
		2048	A,V	A,V	A,V	A,V	A,V	A,V
Signatur der OCSP Response	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	A,V	A,V	A,V	A,V	A,V	A,V
Signatur des OCSP Responder Zertifikates	sha1withRSAEncryption (OID 1.2.840.113549.1.1.5)	1024	A,V	A,V	A,V	A,V	A,V	A,V

Die Lebensdauer der Schlüssel und somit die in einem Zertifikat angegebene Gültigkeitsdauer SOLL gemäß [gemSiKo#AnhF] maximal 5 Jahre betragen.

Offener Punkt - Die Abstimmung der OCSP Algorithmen mit dem BSI ist noch nicht abgeschlossen

Die ausgewählten Algorithmen wurden bislang nicht durch das BSI bestätigt und können sich potentiell noch ändern. Eine ausführlichere Bewertung befindet sich in Abschnitt 5.1

5.1.2 CV-Identitäten

CV-Identitäten werden für die Authentifizierung zwischen Karten verwendet. Für Migrationsszenarien muss beachtet werden, dass die Karten eine lange Lebensdauer haben und durch verschiedene Organisationen herausgegeben werden. Sollte eine Migration der Algorithmen erfolgen, so ist insbesondere die Abwärtskompatibilität zu berücksichtigen und zu gewährleisten, dass alle eGKs, die zu diesem Zeitpunkt gültige Algorithmen verwenden, auch weiterhin verwendet werden können. Insbesondere bedeutet dies, dass für HBAs und SMCs eine Möglichkeit gefunden werden muss, um mit allen im Umlauf befindlichen eGKs eine Card-to-Card Authentisierung durchführen zu können.

Aus diesem Grund wird zunächst nur ein einziger Algorithmus für C2C-Authentifzierung betrachtet.

5.1.2.1 CV-Zertifikate

CV-Zertifikate MÜSSEN den in Tabelle 13 gestellten Anforderungen an Algorithmen genügen.

Tabelle 13: Algorithmen für CV-Zertifikate

Algorithmen Typ	Algorithmus	Schlüssel-länge	2008	2009	2010	2011	2012	2013
Über das Zertifikat betätigtes Schlüsselpaar	authS_ISO9796-2 Withrsa_sha256_mutual (OID 1.3.36.3.5.2.4)	1024	E	E	E	E	E	E
		2048	A,V	A,V	A,V	A,V	A,V	A,V
Signatur des Endnutzer- und CA-Zertifikates	sigS_ISO9796-2Withrsa_sha1 (OID 1.3.36.3.4.2.2.1)	1024	E	E	E	E	E	E
		2048	E	E	E	E	E	E
	sigS_ISO9796-2Withrsa_sha256 (OID 1.3.36.3.4.2.2.4)	1024	E	E	E	E	E	E
		2048	A,V	A,V	A,V	A,V	A,V	A,V

In einem CV-Zertifikat wird keine Gültigkeitsdauer angegeben. Die Lebensdauer der Schlüssel und des Zertifikats entsprechen der Nutzbarkeitsdauer der Chipkarte, in der diese gespeichert sind. Die Lebensdauer der Schlüssel SOLL gemäß [gemSiKo#AnhF] maximal 5 Jahre betragen.

5.1.2.2 CV-Certification Authority (CV-CA) Zertifikat

CV-CA Zertifikate MÜSSEN den in Tabelle 14 gestellten Anforderungen an Algorithmen genügen.

Tabelle 14: Algorithmen für CV-CA-Zertifikate

Algorithmen Typ	Algorithmus	Schlüssel-länge	2008	2009	2010	2011	2012	2013
Über das Zertifikat betätigtes Schlüsselpaar	authS_ISO9796-2 Withrsa_sha256_mutual (OID 1.3.36.3.5.2.4)	1024	E	E	E	E	E	E
		2048	A,V	A,V	A,V	A,V	A,V	A,V
Signatur des Endnutzer- und CA-Zertifikates	sigS_ISO9796-2 Withrsa_sha1 (OID 1.3.36.3.4.2.2.1)	1024	E	E	E	E	E	E
		2048	E	E	E	E	E	E
	sigS_ISO9796-2 Withrsa_sha256 (OID 1.3.36.3.4.2.2.4)	1024	E	E	E	E	E	E
		2048	A,V	A,V	A,V	A,V	A,V	A,V

In einem CV-Zertifikat wird keine Gültigkeitsdauer angegeben. Die Gültigkeitsdauer der CV-Zertifikate für eine CVC-CA entspricht der Lebensdauer der CA-Schlüssel. Diese SOLL gemäß [gemSiKo#AnhF] maximal 5 Jahre betragen.

5.2 Zufallszahlengeneratoren

Alle kryptographischen Verfahren basieren darauf, dass ein Angreifer nicht in die Kenntnis eines Geheimnisses gelangen kann. Aus diesem Grund besteht für alle Algorithmen eine Abhängigkeit zu den Zufallszahlengeneratoren mit denen dieses Geheimnis erzeugt wird.

Die Algorithmen für die Erzeugung von Zufallszahlen müssen nicht TI übergreifend normiert werden, da lediglich das Ergebnis der Generierung Verwendung findet. Um ein einheitliches Sicherheitsniveau zu garantieren müssen allerdings die Anforderungen an Zufallszahlengeneratoren spezifiziert werden. Zulässig sind Deterministische Zufallszahlengeneratoren (PRNGs – Pseudo Random Number Generators) sowie Nicht-Deterministische Zufallszahlengeneratoren (RNGs – Random Number Generators).

Es wird empfohlen generell Nicht-Deterministische Zufallszahlengeneratoren zu verwenden. Der Einsatz von Deterministischen Zufallszahlengeneratoren ist der gematik anzuzeigen und zu genehmigen. Die Detailspezifikationen von Komponenten KANN detailliertere Aussagen zur Verwendung von deterministischen und nicht-deterministischen Zufallszahlengeneratoren treffen. Nachfolgend werden die Anforderungen an nicht-deterministische und deterministische Zufallszahlengeneratoren spezifiziert. Die Anforderungen entstammen aus dem vom Bundesamt für Sicherheit in der Informationstechnik erarbeiteten und von der Bundesnetzagentur veröffentlichten Algorithmenkatalog [ALGCAT].

5.2.1 Deterministische Zufallszahlengeneratoren (PRNGs – Pseudo Random Number Generators)

[ALGCAT]: „Der innere Zustand des Pseudozufallszahlengenerators wird durch den so genannten Seed initialisiert. In jedem Schritt wird der innere Zustand erneuert und hieraus eine Zufallszahl abgeleitet. Der innere Zustand des Pseudozufallszahlengenerators muss gegen Auslesen und Manipulation (physikalisch, durch Seitenkanalangriffe, über Schnittstelle etc.) ebenso sicher geschützt sein wie die geheimen Signaturschlüssel. Denn mit Kenntnis des inneren Zustands könnte ein potentieller Angreifer zumindest alle zukünftig erzeugten Zufallszahlen mühelos bestimmen.

Jeder Pseudozufallszahlengenerator, der im Zusammenhang mit digitalen Signaturen genutzt wird, muss mindestens ein K3-DRNG mit Stärke der Mechanismen bzw. Funktionen „Hoch“ im Sinne der AIS 20 [AIS20] sein. Qualitativ bedeutet dies: Es ist einem Angreifer nicht praktisch möglich, zu einer ihm bekannten Zufallszahlenteilfolge Vorgänger oder Nachfolger dieser Teilfolge oder gar einen inneren Zustand zu errechnen, oder diese mit einer Wahrscheinlichkeit zu erraten, die nichtvernachlässigbar über der Ratewahrscheinlichkeit ohne Kenntnis der Teilfolge liegt. Die Entropie des Seed beträgt mindestens 80 Bit; empfohlen wird eine Entropie von mindestens 100 Bit.

Anderenfalls muss das entsprechende Verfahren zur digitalen Signatur als potenziell unsicher angesehen werden. Darüber hinaus sollte der Pseudozufallszahlengenerator ein K4-DRNG mit Stärke der Mechanismen bzw. Funktionen „Hoch“ im Sinne der AIS 20 [AIS20] sein. Qualitativ bedeutet dies, dass zusätzlich folgende Bedingung erfüllt ist: Es ist einem Angreifer praktisch unmöglich, aus Kenntnis eines inneren Zustands Vorgängerzufallszahlen oder innere Vorgängerzustände zu errechnen oder diese mit einer Wahrscheinlichkeit zu erraten, die nichtvernachlässigbar über der Ratewahrscheinlichkeit ohne Kenntnis des inneren Zustands liegt.

Die obigen Bedingungen werden bis Ende 2009 als ausreichend betrachtet. Ab Anfang 2010 wird darüber hinaus verlangt: Die Entropie des Seed beträgt mindestens 100 Bit; empfohlen werden mindestens 120 Bit.

Der Pseudozufallszahlengenerator muss grundsätzlich der Klasse K4 im Sinne der AIS 20 [AIS20] mit Stärke der Mechanismen bzw. Funktionen "Hoch" angehören. Alternativ genügt eine nachvollziehbare Begründung des Antragstellers, dass das Fehlen der K4-spezifischen Eigenschaft im vorgesehenen Einsatzszenario keine zusätzlichen Sicherheitsrisiken induziert.

5.2.2 Nicht-Deterministische Zufallszahlengeneratoren (RNGs – Random Number Generators)

[ALGCAT]: „Für diese Zwecke bieten sich als Zufallszahlengeneratoren solche Systeme an, die eine physikalische Rauschquelle, die beispielsweise auf elektromagnetischen, elektromechanischen oder quantenmechanischen Effekten beruht, und ggf. eine algorithmische Nachbehandlung der digitalisierten Rauschsignale besitzen. Die Eigenschaften der digitalisierten Rauschsignalfolge sollten sich hinreichend gut durch ein stochastisches Modell beschreiben lassen.

Der physikalische Zufallszahlengenerator sollte ein P2-Generator (Stärke der Mechanismen bzw. Funktionen: hoch) im Sinne der AIS 31 [AIS31] sein; ab Anfang 2011 ist diese Bedingung verbindlich, d. h. der Zufallzahlengenerator muss dann ein P2-Generator sein. Qualitativ bedeutet dies: Der durchschnittliche Entropiezuwachs pro Zufallsbit liegt oberhalb einer Mindestschranke. Die digitalisierten Rauschsignale müssen im laufenden Betrieb des Zufallszahlengenerators permanent oder zumindest in regelmäßigen Abständen statistischen Tests unterzogen werden („Onlinetests“). Im Idealfall sollte der Onlinetest dem mathematischen Modell der Rauschquelle angepasst sein. In jedem Fall müssen der Onlinetest selbst und das Aufrufschema geeignet sein, nicht akzeptable statistische Defekte oder Verschlechterungen der statistischen Eigenschaften der digitalisierten Rauschsignalfolge in angemessener Zeit zu erkennen. Auf einen Rauschalarm muss angemessen reagiert werden (z. B. weitere Tests, Stilllegen der Rauschquelle). Insbesondere muss ein etwaiger Totalausfall der Rauschquelle umgehend erkannt werden. Es wird dringend empfohlen, zur Schlüsselerzeugung einen physikalischen Zufallszahlengenerator zu verwenden.“

6 Konkretisierung der Algorithmen für spezifische Einsatzszenarien

In den nachfolgenden Abschnitten werden die kryptographischen Algorithmen für verschiedene Einsatzszenarien spezifiziert. Hierbei sind ausschließlich die kryptographischen Elemente der Einsatzszenarien relevant. Eine Beschreibung der weiteren Parameter verschiedener Protokolle erfolgt nicht. Sofern notwendig, wird aus dem jeweiligen Szenario auf eine detaillierte Beschreibung in einer Spezifikation der gematik verwiesen

Die eingesetzten Algorithmen werden als langfristig sicher angesehen. Aus diesem Grund erfolgt keine Angabe von Gültigkeitszeiträumen.

6.1 Kryptographische Algorithmen für XML-Dokumente

XML-Signaturen sind bezüglich der verwendeten Algorithmen selbst beschreibend, das bedeutet, die für die Erstellung einer Signatur verwendeten Algorithmen sind in der Signatur aufgeführt.

Zur vollständigen Spezifikation der Algorithmen für XML-Signaturen müssen für alle Signaturbestandteile Algorithmen spezifiziert werden. Abschnitt 6.1.1 stellt die zulässigen Algorithmen in einer Übersicht dar, die nachfolgenden Abschnitte wählen dann aus der Menge der zulässigen Algorithmen die jeweiligen Algorithmen für die einzelnen Einsatzszenarien aus.

Die Referenzierung von Algorithmen in XML-Signaturen und XML-Verschlüsselungen erfolgt nicht wie in Zertifikaten oder Signaturen binärer Daten über OIDs sondern über URIs. Es ist nicht der unter dem Link befindliche Inhalt sondern der gemäß Spezifikation über die URI bezeichnete Algorithmus relevant.

6.1.1 (Abschnitt entfällt) Übergreifende Anforderungen an XML-Signaturen

Der Abschnitt hat in früheren Versionen eine Übersicht über alle zulässigen Algorithmen dargestellt. Dies hat bei dem Kommentatoren und Herstellern zu Verwirrung geführt, der Abschnitt wurde daher entfernt.

Da sich durch das Entfernen des Abschnitts die Referenzierung für alle folgenden Abschnitte ändern würde, wurde der Abschnitt als Platzhalter beibehalten.

6.1.2 XML-Signaturen für fortgeschrittene Signaturen

Tabelle 15: Algorithmen für die Erzeugung von fortgeschrittenen XML Signaturen

Signaturbestandteil	Beschreibung	Algorithmus	Anmerkung
CanonicalizationMethod	Kanonisierung des SignedInfo Elementes	**Exklusive XML-Kanonisierung** Die [XMLSig] konforme Bezeichnung lautet: http://www.w3.org/2001/10/xml-exc-c14n#	Die Verwendung des Algorithmus ist verpflichtend
SignatureMethod	Algorithmus für die	**RSASSA-PKCS1-v1_5 mit SHA256**	Die Verwendung

Signaturbestandteil	Beschreibung	Algorithmus	Anmerkung
	Berechnung des Nachrichten Digest und die Verschlüsselung mit dem privaten Schlüssel	Die [XMLSig] konforme Bezeichnung lautet: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256	des Algorithmus ist verpflichtend
Transform	Algorithmus für die Transformation der zu signierenden Bereiche. Für eine Signatur können mehrere Transformationen nacheinander angewendet werden. In diesem Fall ist die Reihenfolge normativ.	**Enveloped Signature Transfomation:** Verwendung für Signaturen bei denen sich die ds:Signature Datenstruktur innerhalb der signierten fachlichen Daten befindet. Die [XMLSig] konforme Bezeichnung lautet: http://www.w3.org/2000/09/xmldsig#enveloped-signature	Der Algorithmus darf nur bei enveloped Signatures verwendet werden. Für Detached Signatures DARF er NICHT verwendet werden und muss entfallen.
		X-PATH-Transformation: X-Path Transformationen sind zulässig, müssen aber für den entsprechenden Fall im Detail definiert werden, da der konkrete Einsatz des Verfahrens vom Kontext abhängig ist.	Der Einsatz ist von dem konkreten Szenario abhängig. Bislang ist kein Einsatzszenario bekannt, der Algorithmus ist aber zulässig und soll nicht ausgeschlossen werden. Daher wurde der Algorithmus mit aufgenommen.
		Exklusive XML-Kanonisierung: Transformation zur Kanonisierung der XML Struktur Die [XMLSig] konforme Bezeichnung lautet: http://www.w3.org/2001/10/xml-exc-c14n#	Bei allen XML Signaturen MUSS zusätzlich als letzte Transformation exklusive XML Kanonisierung durchgeführt werden.
DigestMethod	Methode zur Berechnung eines Digest der zu Signierenden Bereiche	**SHA-256** Die [XMLSig] konforme Bezeichnung lautet: http://www.w3.org/2001/04/xmlenc#sha256	Die Verwendung des Algorithmus ist verpflichtend
Kryptographisches Token	Kryptographisches Token für die Signatur bestehend aus einem Privaten Schlüssel und einem zugehörigen X.509 zertifikat	Identitäten gemäß einem der folgenden Abschnitte 5.1.1.2 5.1.1.6	Die Auswahl des kryptographischen Tokens ist von dem jeweiligen Einsatzzweck abhängig.

Tabelle 16: Betroffene Systeme – XML-Signaturen für fortgeschrittene Signaturen

System	Einsatz
Fachdienste	Alle Fachdienste müssen die Validierung einer fortgeschrittenen XML-Signatur zur Authentifizierung der Datenautorität sowie zur Validierung des Integritätsschutzes von Tickets unterstützen.
Anwendungskonnektor	Der Konnektor muss sowohl die Erstellung einer fortgeschrittenen Signatur im Zuge der

System	Einsatz
	Authentisierung der Datenautorität oder zur Erstellung von Tickets als auch die Validierung dieser Signaturen unterstützen.
Broker	Der Broker prüft die mathematische Korrektheit der Nachrichtensignaturen als Basis für die Erstellung eines Auditeintrags. Der Broker prüft die Signatur der Brokersequenzen.
Trusted Service, Security Validation Service und Security Confirmation Service	Die Dienste TrustedS, SVS und SCS setzen die Anonymisierung von Heilberuflersignaturen um. In diesem Zusammenhang prüfen sie Nachrichtensignaturen und erstellen Nachrichtensignaturen.
Alle TI-Komponenten	Nahezu alle Komponenten der TI nutzen die TSL als Vertrauensanker und müssen daher in der Lage sein, die XML-Signatur der TSL zu validieren.
TSL Provider	Der TSL-Provider muss in der Lage sein, die Signatur der TSL gemäß den zuvor angegebenen Algorithmen zu erstellen.

6.1.3 XML-Signaturen für qualifizierte Signaturen

Die Vorgaben an Algorithmen für qualifizierte Signaturen gehen zum derzeitigen Zeitpunkt nicht über die Vorgaben an Algorithmen für nicht qualifizierte Signaturen hinaus, es muss jedoch eine Identität gemäß Abschnitt 5.1.1.3 zur Validierung verwendet werden. Es sei an dieser Stelle darauf hingewiesen, dass die angegebenen Algorithmen den Vorgaben des Algorithmenkataloges [ALGCAT] dadurch entsprechen, dass sie als Eingangsanforderungen bei der Erstellung des Dokumentes [gemSiKo#AnhF] eingegangen sind.

Tabelle 17: Algorithmen für qualifizierte XML Signaturen

Signaturbestandteil	Beschreibung	Algorithmus	Anmerkung
CanonicalizationMethod	Kanonisierung des SignedInfo Elementes	**Exklusive XML-Kanonisierung** Die [XMLSig] konforme Bezeichnung lautet: http://www.w3.org/2001/10/xml-exc-c14n#	Die Verwendung des Algorithmus ist verpflichtend
SignatureMethod	Algorithmus für die Berechnung des Nachrichten Digest und die Verschlüsselung mit dem privaten Schlüssel	**RSASSA-PKCS1-v1_5 mit SHA256** Die [XMLSig] konforme Bezeichnung lautet: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256	Der Algorithmus MUSS für alle qualifizierten Signaturen verwendet werden.
Transform	Algorithmus für die Transformation der zu signierenden Bereiche. Für eine Signatur können mehrere Transformationen nacheinander angewendet werden. In diesem Fall ist die Reihenfolge normativ.	**Enveloped Signature Transfomation:** Verwendung für Signaturen bei denen sich die ds:Signature Datenstruktur innerhalb der signierten fachlichen Daten befindet. Die [XMLSig] konforme Bezeichnung lautet: http://www.w3.org/2000/09/xmldsig#enveloped-signature	Der Algorithmus darf nur bei enveloped Signatures verwendet werden. Für Detached Signatures DARF er NICHT verwendet werden und muss entfallen.
		X-PATH-Transformation: X-Path Transformationen sind zulässig, müssen aber für den entsprechenden Fall im Detail definiert werden, da der konkrete Einsatz des Verfahrens vom Kontext abhängig ist.	Die Verwendung von X-PATH Transformationen SOLL vermieden werden. Sofern eine X-PATH Transformation

Signaturbestandteil	Beschreibung	Algorithmus	Anmerkung
			notwendig ist, muss sie vor der exklusiven XML Transformation durchgeführt werden.
		Exklusive XML-Kanonisierung: Transformation zur Kanonisierung der XML Struktur Die [XMLSig] konforme Bezeichnung lautet: http://www.w3.org/2001/10/xml-exc-c14n#	Bei allen XML Signaturen MUSS zusätzlich als letzte Transformation exklusive XML Kanonisierung durchgeführt werden.
DigestMethod	Methode zur Berechnung eines Digest der zu Signierenden Bereiche	**SHA-256** Die [XMLSig] konforme Bezeichnung lautet: http://www.w3.org/2001/04/xmlenc#sha256	Der Algorithmus MUSS für alle qualifizierten Signaturen verwendet werden.
Kryptographisches Token	Kryptographisches Token für die Signatur bestehend aus einem Privaten Schlüssel und einem zugehörigen X.509 zertifikat	Identitäten gemäß einem der folgenden Abschnitte 5.1.1.3	Es darf nur eine Identität die den Ansprüchen qualifizierter Signaturen entspricht verwendet werden.

Tabelle 18: Betroffene Systeme – XML-Signaturen für qualifizierte Signaturen

System	Einsatz
Anwendungskonnektor	Der Anwendungskonnektor muss sowohl die Algorithmen für die Hashwert-Berechnung einer qualifizierten Signatur z. B. für die Erstellung von Verordnungen als auch die Algorithmen für die Validierung dieser Signatur ermöglichen.
HBA	Der HBA muss die asymmetrischen Verfahren zur Erstellung der qualifizierten Signatur unterstützen.

6.1.4 Webservice Security Standard (WSS)

Tabelle 19: Algorithmen für WSS Signaturen

Signaturbestandteil	Beschreibung	Algorithmus	Anmerkung
CanonicalizationMethod	Kanonisierung des SignedInfo Elementes	**Exklusive XML-Kanonisierung** Die [XMLSig] konforme Bezeichnung lautet: http://www.w3.org/2001/10/xml-exc-c14n#	Die Verwendung des Algorithmus ist verpflichtend
SignatureMethod	Algorithmus für die Berechnung des Nachrichten Digest und die Verschlüsselung mit dem privaten Schlüssel	**RSASSA-PKCS1-v1_5 mit SHA256** Die [XMLSig] konforme Bezeichnung lautet: http://www.w3.org/2001/04/xmldsig-more#rsa-sha256	Die Verwendung des Algorithmus ist verpflichtend
Transform	Algorithmus für die Transformation der zu signierenden	**Exklusive XML-Kanonisierung:** Transformation zur Kanonisierung der XML	Bei allen WSS Signaturen MUSS exklusive XML

Signaturbestandteil	Beschreibung	Algorithmus	Anmerkung
	Bereiche. Für eine Signatur können mehrere Transformationen nacheinander angewendet werden. In diesem Fall ist die Reihenfolge normativ.	Struktur Die [XMLSig] konforme Bezeichnung lautet: http://www.w3.org/2001/10/xml-exc-c14n#	Kanonisierung durchgeführt werden.
DigestMethod	Methode zur Berechnung eines Digest der zu Signierenden Bereiche	**SHA-256** Die [XMLSig] konforme Bezeichnung lautet: http://www.w3.org/2001/04/xmlenc#sha256	Die Verwendung des Algorithmus ist verpflichtend
Kryptographisches Token	Kryptographisches Token für die Signatur bestehend aus einem Privaten Schlüssel und einem zugehörigen X.509 zertifikat	Identitäten gemäß einem der folgenden Abschnitte 5.1.1.2 5.1.1.6	Die Auswahl des kryptographischen Tokens ist von dem jeweiligen Einsatzzweck abhängig.

Tabelle 20: Betroffene Systeme - Webservice Security Standard (WSS)

System	Einsatz
Fachdienste	Alle Fachdienste, Konnektoren und Broker MÜSSEN in der Lage sein WSS Nachrichtensignaturen zu erstellen und diese Nachrichtensignaturen zu validieren.
Anwendungskonnektor	
Broker	

6.1.5 XML-Verschlüsselung – Symmetrisch

Zur Verschlüsselung von XML-Dokumenten MUSS [XMLEnc] verwendet werden. Es sind des Weiteren die folgenden Algorithmen normativ:

- Als Block Encryption Algorithmus MUSS AES mit einer Schlüssellänge von 256 Bit im Cipher Block Chaining Mode (CBC) verwendet werden. Die [XMLEnc] konforme Bezeichnung lautet: http://www.w3.org/2001/04/xmlenc#aes256-cbc. Der verwendete Algorithmus wird durch eine Vielzahl von Herstellern unterstützt, ist ausreichend performant und nach derzeitigen Einschätzungen bis 2013 als sicher eingestuft. Es wird daher kein Migrationspfad angegeben.
- Als Padding-Algorithmus MUSS ISO-10126 Padding verwendet werden.
- Der Initialisierungsvektor (IV) SOLL zufällig gewählt werden. Wenn dies nicht möglich ist, so MUSS der Initialisierungsvektor durch einen anderen Mechanismus dynamisiert werden.

Tabelle 21: Betroffene Systeme – XML-Verschlüsselung – Symmetrisch

System	Einsatz
Anwendungskonnektor	Der Konnektor MUSS die Verschlüsselung und Entschlüsselung von XML-Dokumenten unterstützen.

6.1.6 XML-Verschlüsselung – Hybrid

Bei der hybriden Verschlüsselung von XML-Dokumenten wird das XML-Dokument selbst gemäß Abschnitt 6.1.5 symmetrisch verschlüsselt und der hierzu verwendete Schlüssel dann asymmetrisch für eine spezifische Person verschlüsselt. Als Algorithmus für den Schlüsseltransport MUSS RSA OAEP gemäß RFC 2437 [PKCS#1] verwendet werden.

Die [XMLEnc] konforme Bezeichnung lautet:

http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p

Der verwendete Algorithmus wird durch eine Vielzahl von Herstellern unterstützt, ist ausreichend performant und nach derzeitigen Einschätzungen bis 2013 als sicher eingestuft. Es wird daher kein Migrationspfad angegeben.

Bestätigung der Interoperabilität mit Karten *–Das angegebene Verfahren (RSA-OAEP) ist in der eGK-Spezifikation für Kartengeneration 1 gefordert. Die Interoperabilität zu den bestehenden XML-Implementierungen ist zwar sehr wahrscheinlich, konnte allerdings bislang nicht an einem Prototypen bestätigt werden, da bislang keine Karten mit RSA-OAEP Implementierung zur Verfügung stehen. Die Bestätigung der Interoperabilität erfolgt daher im Rahmen der Zulassungsverfahren für Karten.*

Sollten Interoperabilitätsprobleme auftreten, so kann immer noch der bereits getestete RSA 1.5 Algorithmus (XML ENC Bezeichnung: http://www.w3.org/2001/04/xmlenc#rsa-1_5) verwendet werden. Die Interoperabilität diese Algorithmus zwischen Karten und XML Frameworks wurde bereits getestet, allerdings ist der Algorithmus durch das BSI nicht als langfristig sicher bewertet.

Tabelle 22: Betroffene Systeme – XML-Verschlüsselung – Hybrid

System	Einsatz
Anwendungskonnektor	Der Konnektor muss die Erzeugung von Hybridschlüsseln zur Hinterlegung in Objekttickets sowie die Entschlüsselung von Hybridschlüssel als Grundlage für die Entschlüsselung von Objekten unterstützen.
Karten (egk, HBA, SMC-B)	Karten mit Verschlüsselungszertifikaten MÜSSEN Hybridschlüssel, die unter Verwendung von RSA-OAEP erzeugt wurden, entschlüsseln können.

6.2 Verschlüsselung von Verordnungen für die Speicherung auf der eGK

Die Speicherung von Verordnungen auf der eGK erfolgt in verschlüsselter und komprimierter Form. Für die Speicherung ist immer zuerst die Komprimierung und im Anschluss die Verschlüsselung durchzuführen. Die Verschlüsselung erfolgt in symmetrischer Form und MUSS die folgenden Algorithmen verwenden:

- Als Verschlüsselungsalgorithmus MUSS AES mit einer Schlüssellänge von 128 BIT im CBC-Mode verwendet werden. Der verwendete Algorithmus wird durch eine Vielzahl von Herstellern unterstützt, ist ausreichend performant und nach derzeitigen Einschätzungen bis 2013 als sicher eingestuft. Es wird daher kein Migrationspfad angegeben.
- Als Padding-Algorithmus MUSS ISO-10126 Padding verwendet werden.

- Der Initialisierungsvektor (IV) SOLL zufällig gewählt werden. Wenn dies nicht möglich ist, so MUSS der Initialisierungsvektor durch einen anderen Mechanismus dynamisiert werden.
- Der Initialisierungsvektor (IV), der bei Verwendung von AES CBC verwendet wird, ist dem verschlüsselten Datenstrom voranzustellen. Zur Entschlüsselung muss also zunächst der IV gelesen werden und die nachfolgenden Daten können dann damit entschlüsselt werden.

Tabelle 23: Betroffene Systeme - Verschlüsselung von Verordnungen für die Speicherung auf der eGK

System	Einsatz
Anwendungskonnektor	Der Konnektor MUSS Objekten zur Speicherung auf der eGK verschlüsseln und entschlüsseln können.
eGK	Die eGK MUSS die Speicherung eines Schlüssels der entsprechenden Länge unterstützen.

6.3 Karten verifizierbare Authentifizierung und Verschlüsselung

Kartenspezifische Algorithmen *– Kartenspezifische Algorithmen, das bedeutet Algorithmen die zur Verwendung in einer Karte implementiert werden, sind in den eGK Spezifikationen definiert. Diese müssen in einer Folgeversion dieses Dokumentes übernommen werden.*

6.3.1 Card-to-Card Authentisierung

Für die Card-to-Card Authentisierung gelten die folgenden normativen Vorgaben:

- Als authentifizierendes Merkmal MUSS eine CV-Identität gemäß Abschnitt 5.1.2.1 verwendet werden.
- Das Verfahren zur Durchführung der Card-to-Card Authentisierung wird in [gemSpec_eGK_P2] spezifiziert.

Tabelle 24: Betroffene Systeme - Card-to-Card Authentisierung

System	Einsatz
eGK	Die angegebenen müssen die Card-to-Card Authentisierung mit den zuvor angegebenen Algorithmen unterstützen. Hierbei wird die Authentifizierung jeweils von HBA, SMC-A oder SMC-B angestoßen, und die eGK reagiert auf diese Anforderung.
HBA	
SMC-A	
SMC-B	
SM-K	

6.3.2 Card-to-Server (C2S) Authentisierung und Trusted Channel

Für die Card-to-Server Authentifizierung gelten die folgenden normativen Vorgaben:

- Die Authentisierung MUSS gemäß [prEN14890-1] Kapitel 8.8 erfolgen
- Die Schlüsselvereinbarung MUSS gemäß [prEN14890-1] Kapitel 8.8.2 erfolgen.
- Das Verfahren zur Durchführung der Card-to-Server Authentisierung wird in [gemFA_CMSeGK] spezifiziert.

C2S-Authentisierung bzw. der Trusted-Channel wird zwischen der eGK, dem zugeordneten CMS und dem zugeordneten VSD verwendet. Aus diesem Grund sind die in der nachfolgenden Tabelle dargestellten Verwendungen für Algorithmen wie folgt zu verstehen.

A,V – Der Algorithmus ist für die **A**usgabe neuer Karten bis zum Ende des Angegebenen Jahres und die **V**erwendung mit bereits ausgegebenen Karten zulässig. Es obliegt der Hoheit des Kartenherausgebers einen der zulässigen Algorithmen zu wählen, er hat aber gleichzeitig sicherzustellen, dass noch mit allen von ihm herausgegebene Karten durch das CMS und den VSDD kommuniziert werden kann. Sofern sich keine aktive Karte eines mit **A** oder **V** gekennzeichneten Algorithmus eines Herstellers im Umlauf befindet, muss dieser Hersteller den entsprechenden Algorithmus nicht unterstützen.

V – Dieser Algorithmus darf für neu herausgegebene Karten zu dem entsprechenden Zeitpunkt nicht mehr implementiert werden. Das CMS und der VSDD des Herausgebers müssen den Algorithmus solange unterstützten (**V**erwenden), wie er aktiven Karten dieses Algorithmus im Umlauf hat. Ein Austausch der mit diesem Algorithmus implementierten Karten ist nicht notwendig

E – Die Gültigkeit dieses Algorithmus ist abgelaufen (**E**xpired) und die Verwendung des Algorithmus stellt ein potentielles Sicherheitsrisiko dar. Alle mit diesem Algorithmus im Umlauf befindlichen Karten sind bis zum Beginn des angegebenen Jahres auszutauschen und durch Karten die einen zulässigen Algorithmus unterstützen zu ersetzen.

O – Dieser Algorithmus ist **o**ptional. Sofern angegebene Algorithmen optional sind, muss in dem entsprechenden Abschnitt eine Erläuterung für die Verwendung erfolgen.

Tabelle 25: Algorithmen für Card-to-Server Authentifizierung

Algorithmen Typ	Algorithmus	Schlüssellänge	2008	2009	2010	2011	2012	2013
Authentifizierung und Verschlüsselung der Trusted Channel Kommunikation	3DES im CBC Mode (OID 1.3.6.1.4.1.4929.1.8)	168	A,V	A,V	A,V	A,V	A,V	A,V

Tabelle 26: Betroffene Systeme - Card-to-Server (C2S) Authentisierung und Trusted-Channel

System	Einsatz
eGK	Die eGK MUSS einen der in Tabelle 25 aufgeführten Algorithmen implementieren.
CMS	Die CMS- und VSDD-Systeme MÜSSEN die Algorithmen der jeweils ihnen zugeordneten eGK unterstützen.
VSDD	

6.4 Netzwerkprotokolle

Im Gegensatz zu kryptographischen Verfahren für den Integritätsschutz oder die Vertraulichkeit von Daten, bei denen keine direkte Kommunikation zwischen Sender bzw. dem Erzeuger und dem Empfänger stattfindet, kann bei Netzwerkprotokollen eine Aushandlung des kryptographischen Algorithmus erfolgen. Das Ziel der nachfolgenden Festlegungen ist es daher, jeweils genau einen verpflichtend zu unterstützenden Algorithmus festzulegen, so dass eine Einigung zumindest auf diesen Algorithmus immer möglich ist. Zusätzlich können aber auch optionale Algorithmen festgelegt werden, auf die sich Sender und Empfänger ebenfalls im Zuge der Aushandlung einigen können. Es darf jedoch durch keine der Komponenten vorausgesetzt werden, dass der Gegenpart diese optionalen Algorithmen unterstützt.

In der tabellarischen Darstellung der Gültigkeiten für Algorithmen sind die verwendeten Kürzel wie folgt zu verstehen.

M – Dieser Algorithmus **M**USS unterstützt werden, so dass in allen Fällen eine Einigung auf einen gemeinsamen Algorithmus möglich ist.

O – Dieser Algorithmus ist **o**ptional und KANN anstelle des verpflichtenden Verfahrens verwendet werden, sofern er von beiden Parteien unterstützt wird. Die Verfügbarkeit dieses Verfahrens DARF NICHT vorausgesetzt werden.

E – Die Gültigkeit dieses Algorithmus ist abgelaufen (**E**xpired) und die Verwendung des Algorithmus stellt ein potentielles Sicherheitsrisiko dar. Dieser Algorithmus DARF NICHT mehr eingesetzt werden

P – Diese Algorithmen sind derzeit in **P**lanung und es ist noch keine Entscheidung über die Möglichkeit des Einsatzes getroffen.

Anmerkung zum Migrationspfad: Die ohne Migrationspfad angegebenen Algorithmen sind durch eine Vielzahl von Herstellern unterstützt, ausreichend performant und für den vorgegebenen Einsatzbereich nach derzeitigen Einschätzungen bis 2013 als sicher eingestuft. Es wird daher kein Migrationspfad für diese Algorithmen angegeben.

6.4.1 IPSec-Kontext

Für die Authentifizierung, den Schlüsseltausch und die verschlüsselte Kommunikation im IPSec-Kontext gelten die folgenden normativen Vorgaben:

- Die Schlüsselvereinbarung MUSS mittels IKEv1 gemäß der folgenden Vorgaben erfolgen:
  - Als symmetrische Verschlüsselungsalgorithmen sind die Algorithmenverwendungen gemäß Tabelle 27 normativ.
  - Hashing und HMAC mittels SHA-1 MÜSSEN unterstützt werden. SHA-2 mit 256 Bit und größer KANN optional unterstützt werden.
  - Als Nachweis der Identität wird ein X.509-Zertifikat gemäß Abschnitt 5.1.1.5 verwendet.
  - Die Verwendung von Diffie-Hellman-Gruppen für den Schlüsseltausch gemäß Tabelle 28 ist verpflichtend.

- Die verschlüsselte Kommunikation MUSS die folgenden Eigenschaften erfüllen:
  - Als symmetrische Verschlüsselungsalgorithmen sind die Algorithmenverwendungen gemäß Tabelle 27 normativ.
  - Hashing und HMAC mittels SHA-1 MÜSSEN unterstützt werden. SHA-2 mit 256 Bit und größer KANN optional unterstützt werden.
  - Die Verwendung von Diffie-Hellman-Gruppen für den Schlüsseltausch gemäß Tabelle 28 ist verpflichtend.
  - Für die Schlüsselberechnung MUSS Perfect Forward Secrecy (PFS) unterstützt werden

Tabelle 27: Algorithmen zur symmetrischen Verschlüsselung für IPSec

Algorithmen Typ	Algorithmus	Schlüssellänge	2008	2009	2010	2011	2012	2013
Symmetrische Verschlüsselung des IPSec Transports	AES im CBC Mode (OID 2.16.840.1.101.3.4.1)	256	M	M	M	M	M	M

Tabelle 28: Diffie-Hellman-Gruppen für den Schlüsseltausch

Algorithmen Typ	Algorithmus	Modulus	2008	2009	2010	2011	2012	2013
Diffie-Hellman-Gruppe	5	1536	M	M	M	M	M	P

Tabelle 29: Betroffene Systeme – IPSec-Kontext

System	Einsatz
Netzkonnektor	Der Netzkonnektor dient in diesem Zusammenhang als IPSec-Client und MUSS die entsprechende Algorithmen implementieren
VPN-Konzentrator	Der VPN-Konzentrator dient als IPSec-Server.

6.4.2 TLS/SSL-Kontext

TLS/SSL-Verbindungen werden in Verbindungen mit normalem und niedrigem sowie in Verbindungen mit erhöhtem Schutzbedarf unterschieden. Die Vorgaben der Algorithmen dieses Abschnitts gelten für alle TLS/SSL-Verbindungen, auf die nicht die Kriterien für erhöhten Schutzbedarf zutreffen und die dementsprechend nicht in Tabelle 35 aufgeführt sind. Für alle in Tabelle 35 aufgeführten Verbindungen gelten die in Abschnitt 6.4.4 definierten Algorithmen.

Für die Übertragung mittels TLS sind die folgenden Vorgaben an Algorithmen normativ:

- Authentifizierendes Merkmal ist immer eine X.509-Identität gemäß Abschnitt Abschnitt 5.1.1.4.

Als Cipher Suite MUSS eine Cipher Suite gemäß der nachfolgenden Tabelle verwendet werden.

Tabelle 30: Algorithmen für SSL/TLS

Algorithmen Typ	Algorithmus	Symmetrische Schlüssellänge	2008	2009	2010	2011	2012	2013
SSL Cipher Suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA (Als authentifzierende X.509-Identitäten sind alle Identitäten gemäß Abschnitt 5.1.1.4 zulässig)	128	M	M	M	M	M	M
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA (Als authentifzierende X.509-Identitäten sind alle Identitäten gemäß Abschnitt 5.1.1.4 zulässig)	256	O	O	O	O	O	O
	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA (Als authentifzierende X.509-Identitäten sind alle Identitäten gemäß Abschnitt 5.1.1.4 zulässig)	168	O	O	O	E	E	E

Tabelle 31: Betroffene Systeme - SSL/TLS-Kontext

System	Einsatz
Anwendungskonnektor sowie alle Anwendungs- und Infrastrukturdienste der TI	Sämtliche betreiberübergreifende Kommunikation auf HTTPS-Basis innerhalb der TI MUSS mittels der oben angegebenen Algorithmen implementiert werden.

6.4.3 DNSSEC-Kontext

Zur Absicherung der DNS-Daten wird gemäß [gemNamD] die Verwendung von DNSSEC verwendet. Für die Verwendung von DNSSEC sind die nachfolgenden Algorithmen normativ. Hierbei werden die folgenden Kürzel verwendet.

M – Dieser Algorithmus **M**USS unterstützt werden, so dass in allen Fällen eine Einigung auf eine gemeinsame Cipher Suite möglich ist.

P – Die Festlegung der zulässigen Algorithmen ist noch nicht finalisiert und befindet sich in **P**lanung.

Tabelle 32: Algorithmen für DNSSEC

Algorithmen Typ	Algorithmus	Symmetrische Schlüssellänge	2008	2009	2010	2011	2012	2013
rndc – symmetrischer Schlüssel zur Absicherung der Steuerung einer Name Server Instanz via rndc	HMAC-MD5	256	M	M	M	M	P	P

Algorithmen Typ	Algorithmus	Symmetrische Schlüssellänge	2008	2009	2010	2011	2012	2013
TSIG – symmetrischer Schlüssel zur Absicherung der Transaktionskanäle zwischen zwei Name Server Instanzen bei Zonentransfers, Änderungsbenachrichtigungen, dynamischen Updates und rekursiven Queries.	HMAC-SHA	160	M	M	M	M	P	P
DNSSEC ZSK Asymmetrische Schlüssel zur Wahrung der Authentizität und Integrität von Zonendatenobjekten.	RSA-SHA1	1024	M	M	M	M	P	P
DNSSEC KSK Asymmetrische Schlüssel zur Wahrung der Authentizität und Integrität von Zonendatenobjekten.	RSA-SHA1	2048	M	M	M	M	P	P

Tabelle 33: Betroffene Systeme - DNSSEC-Kontext

System	Einsatz
Alle T0 Name Server Systeme (Telematik) Internal Root Zone	Für diese Systeme ist der Einsatz von DNSSEC verpflichtend und die zuvor angegebenen Algorithmen sind normativ.
Alle T1 Name Server Systeme (Telematik) Parent Zone	
Alle T2 Name Server Systeme (Telematik) Sub Zones	
Alle T0 Name Server Systeme (Telematik) Forward Zones	Die Verwendung von DNSSEC ist optional, sofern DNSSEC eingesetzt wird, sofern dies der Fall ist, ist die Unterstützung der zuvor angegebenen Algorithmen normativ.

6.4.4 TLS/SSL-Verbindungen mit erhöhtem Schutzbedarf

Diese Form der SSL-Verbindung MUSS verwendet werden, sofern Daten mit einem besonderen Schutzbedarf transportiert werden. Verbindungen, die dieser Vorgabe entsprechen und Daten mit erhöhtem Schutzbedarf transportieren werden in Tabelle 35 abschließend definiert. Die Entscheidung, ob eine Verbindung gemäß Abschnitt 6.4.2 oder Abschnitt 6.4.4 abgesichert werden muss, orientiert sich an der Schutzbedarfsanalyse des Sicherheitskonzeptes.

Für die Übertragung mittels TLS sind die folgenden Vorgaben an Algorithmen normativ:

- Zur Authentifizierung MUSS eine X.509-Identität gemäß den Vorgaben aus Abschnitt 5.1.1.8 verwendet werden.
- Als Cipher Suite MUSS eine Cipher Suite gemäß der nachfolgenden Tabelle verwendet werden.

Tabelle 34: Algorithmen für TLS/SSL

Algorithmen Typ	Algorithmus	Symmetrische Schlüssellänge	2008	2009	2010	2011	2012	2013

SSL Cipher Suite	TLS_DHE_RSA_WITH_AES_128_CBC_SHA	128	M	M	M	M	M	M
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA	256	O	O	O	O	O	O
	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA	168	O	O	O	E	E	E

Tabelle 35: Betroffene Systeme - SSL/TLS Verbindungen mit erhöhtem Schutzbedarf

System	Einsatz
Kartenterminals und Konnektoren	Die Kommunikation auf HTTPS-Basis zwischen Kartenterminals und Konnektoren MUSS mittels der oben angegebenen Algorithmen implementiert werden.

6.5 Masterkey Verfahren

6.5.1 Masterkey Verfahren zur Ableitung des versichertenindividuellen Schlüssels im Audit Service

Ziel des Masterkey Verfahrens zur Ableitung eines versichertenindividuellen Schlüssels im Auditservice ist es, aus einem geheimen Masterkey und einem öffentlichen[2] versichertenindividuellen Merkmal einen geheimen symmetrischen Schlüssel abzuleiten, der für die Verschlüsselung der Auditdaten verwendet wird. Die Vertraulichkeit der Daten MUSS durch die Geheimhaltung des Masterkeys gewährleistet sein. Das bedeutet, die Geheimhaltung anderer Daten als des Masterkeys DARF für die Vertraulichkeit der Daten NICHT notwendig sein. Die Durchführung dieses Verfahrens MUSS bei gleichen Eingangsparametern immer das gleiche Ergebnis generieren.

Es gibt keinen spezifizierten Algorithmus, der die Ableitung des Schlüssels direkt definiert, sondern es wird nachfolgend ein Verfahren unter Einbeziehung verschiedener kryptographischer Algorithmen spezifiziert. Für die Durchführung des Algorithmus wird neben dem Masterkey auch noch ein versichertenindividuelles Merkmal verwendet. Die Auswahl des Merkmals ist fachlich motiviert und wird daher in diesem Dokument nicht spezifiziert. Das Verfahren besteht aus einer Kombination von AES Verschlüsselung und Hashwertbildung. Die Schlüssel- bzw. Hashwertlänge ergibt sich gemäß Tabelle 37.

Tabelle 36: Ablauf zur Berechnung eines versichertenindividuellen Schlüssels im Audit Service

Reihenfolge	Beschreibung	Formale Darstellung
1	Bildung eines Hashwertes über dem versichertenindividuellen Merkmal.	HASH#1 = SHA256(versichertenindividuelles Merkmal)
2	AES Verschlüsselung des Resultats mit dem Masterkey unter Verwendung eines statischen Paddingverfahrens, das für jede Verschlüsselung mit gleichen Eingangsparametern ein identisches Resultat liefert.	ENC#1 = AES(HASH#1)
3	Bildung eines Hashwertes über dem Ergebnis des vorherigen Verarbeitungsschritts.	Versichertenindividueller Schlüssel = SHA(ENC#1)

[2] Öffentlich bedeutet an dieser Stelle nicht, dass die Merkmale selbst nicht schützenswert sind, es soll jedoch ausdrücken, dass die Vertraulichkeit des versichertenindividuellen Schlüssels nicht von der Geheimhaltung dieser Merkmale abhängt.

In der nachfolgenden Tabelle wurden die folgenden Kürzel verwendet.

M – Dieser Algorithmus **M**USS unterstützt werden.

E – Die Gültigkeit dieses Algorithmus ist abgelaufen (**E**xpired) und die Verwendung des Algorithmus stellt ein potentielles Sicherheitsrisiko dar. Der Algorithmus darf ab Beginn des angegebenen Jahres nicht mehr eingesetzt werden.

Tabelle 37: Algorithmen für die Ableitung eines versichertenindividuellen Schlüssels

Algorithmen Typ	Algorithmus	Schlüssellänge	2008	2009	2010	2011	2012	2013
Masterkey Verfahren für die Generierung des versichertenindividuellen Schlüssel des Auditservice	AES basiertes Verfahren gemäß vorheriger Definition	AES 256 SHA 256	M	M	M	M	M	M

Tabelle 38: Betroffene Systeme - Masterkey Verfahren zur Ableitung des versichertenindividuellen Schlüssels im Auditservice

System	Einsatz
Auditservice	Der Auditservice verwendet das Masterkey Verfahren, um aus versichertenindividuellen Parametern sowie einem Masterkey einen versichertenindividuellen Schlüssel abzuleiten. Interoperabilität nach außen ist nicht notwendig, da eine Umschlüsselung stattfindet, bevor die Daten die Hoheit des Auditservice verlassen.

6.6 Verschlüsselung der Auditeinträge

Die Speicherung von Auditeinträgen darf nur in verschlüsselter Form erfolgen. Die verschlüsselte Speicherung MUSS die folgenden Anforderungen erfüllen.

- Als Verschlüsselungsalgorithmus MUSS AES mit einer Schlüssellänge von 256 BIT im CBC-Mode verwendet werden.
- Als Padding-Algorithmus MUSS ISO-10126 Padding verwendet werden.
- Der Initialisierungsvektor (IV) MUSS zufällig gewählt werden.
- Der Initialisierungsvektor (IV), der bei Verwendung von AES CBC verwendet wird, ist dem verschlüsselten Datenstrom voranzustellen. Zur Entschlüsselung muss also zunächst der IV gelesen werden und die nachfolgenden Daten können dann damit entschlüsselt werden.

Tabelle 39: Betroffene Systeme – Verschlüsselung der Auditeinträge

System	Einsatz
Auditservice	Der Auditservice verwendet den Verschlüsselungsmechanismus zur internen Verschlüsselung der Daten. Interoperabilität nach außen ist nicht notwendig, da eine Umschlüsselung stattfindet, bevor die Daten die Hoheit des Auditservice verlassen.

6.7 Verfahren zur gleichwertigen Geheimnisaufteilung

Für die Umsetzung der Anforderung A_01709 aus [gemFK_DatErh] wird ein Verfahren benötigt, dass es ermöglicht einen geheimen Schlüssel in zwei Teilschlüssel aufzuteilen. Allgemeiner betrachtet bedeutet dies, es muss möglich sein, ein Geheimnis (G1) in zwei Teilgeheimnisse (TG1 und TG2) zu unterteilen, die unterschiedlichen Parteien zur Verfügung gestellt werden. Dabei gilt die Randbedingung, dass es einer Partei, die eines der Teilgeheimnisse (z.B. TG1) kennt, nicht leichter fallen darf, auf das ursprüngliche Geheimnis (G1) zu schließen, als dies ohne die Kenntnis des Geheimnisses möglich wäre.

Die Umsetzung der Geheimnisteilung in der TI MUSS gemäß dem folgenden Verfahren erfolgen:

1. Zunächst wird ein Zufallswert mit gleicher Länge wie das Geheimnis G1 generiert. Die Länge bezeichnet in diesem Fall die Anzahl der Bits in binärer Darstellung. Für die Generierung des Zufallswertes TG1 SOLL ein nicht-deterministischer Zufallszahlengenerator verwendet werden. Sofern ein deterministischer Zufallszahlengenerator verwendet wird, ist die Gleichwertigkeit zum nicht-deterministischen Zufallszahlengenerator nachzuweisen.
2. Dieser Zufallswert wird als Teilgeheimnis (TG1) verwendet.
3. Das zweite Teilgeheimnis (TG2) ergibt sich über eine „exklusive oder“ Verknüpfung des Teilgeheimnisses (TG1) mit dem Geheimnis (G1) **è** TG2 = TG1 XOR G1

Durch die Kenntnis eines der Teilgeheimnisse ist somit nicht auf das ursprüngliche Geheimnis G1 zu schließen. Die Zusammenführung der beiden Teilgeheimnisse (TG1 und TG2) erfolgt ebenfalls durch „exklusive oder“ **è** G1 = TG1 XOR TG2.

Bei der Anwendung dieses Verfahrens ist zu berücksichtigen, dass die Sicherheit der geheimen Information von Randbedingungen abhängig ist, die nicht durch das Verfahren selbst adressiert werden können. Diese Randbedingungen sind:

- Robustheit: Bei dem Verlust eines der Teilschlüssel kann das Geheimnis nicht wieder hergestellt werden.
- Vertraulichkeit der Teilgeheimnisse: Die Vertraulichkeit jedes Teilgeheimnisses muss über organisatorische oder technische Maßnahmen die außerhalb dieses Verfahrens liegen sichergestellt werden.

Tabelle 40: Betroffene Systeme – Verfahren zur Geheimnisaufteilung mit gleicher Entropie

System	Einsatz
Kartenherausgeber Systeme zur Umsetzung des Datenerhalts	Das Verfahren für den Datenerhalt gemäß [gemFK_DatErh]]] sieht eine Aufteilung des privaten Schlüssels der eGK in zwei Teilschlüssel vor. Systeme die in diesem Rahmen an der Umsetzung des Datenerhalts beteiligt sind müssen das entsprechende Verfahren umsetzen.
	Offener Punkt - Detaillierte Auflistung der umsetzenden Systeme *Bis zur Verfügbarkeit der Facharchitektur Datenerhalt [gemFA_DatErh] ist eine Auflistung der betroffenen Systeme nicht möglich. Die detaillierte Auflistung erfolgt daher zu einem späteren Zeitpunkt.*

6.8 Hybride Verschlüsselung binärer Daten

Die Hybride Verschlüsselung binärer Daten erfolgt durch die Kombination eines symmetrischen Verschlüsselungsverfahrens mit anschließender asymmetrischer Verschlüsselung des symmetrischen Schlüssels. Der angegebene Algorithmus geht von Binärdaten in Bytestrukturen aus. Bytestruktur bedeutet, dass die Anzahl der Bits einem vielfachen von 8 entspricht. Sofern es sich bei den zu verschlüsselnden Daten nicht um eine Bytestruktur handelt muss das Padding und Depadding auf vollständige Bytes durch die Anwendung erfolgen.

Für die hybride Verschlüsselung werden die Daten zunächst symmetrisch und im Anschluss asymmetrisch verschlüsselt.

Tabelle 41: Betroffene Systeme – Hybride Verschlüsselung Binärer Daten

System	Einsatz
Kartenherausgeber	Das Verfahren für den Datenerhalt gemäß [gemFK_DatErh] sieht die hybride Verschlüsselung des privaten Schlüssels der eGK vor. Systeme die in diesem Rahmen an der Umsetzung des Datenerhalts beteiligt sind müssen das entsprechende Verfahren umsetzen.
Systeme zur Umsetzung des Datenerhalts	
	Offener Punkt - Detaillierte Auflistung der umsetzenden Systeme *Bis zur Verfügbarkeit der Facharchitektur Datenerhalt [gemFA_DatErh] ist eine Auflistung der betroffenen Systeme nicht möglich. Die detaillierte Auflistung erfolgt daher zu einem späteren Zeitpunkt.*

6.8.1 Symmetrischer Anteil der hybriden Verschlüsselung binärer Daten im Kontext Datenerhalt

An den Algorithmus gelten die folgenden normativen Anforderungen:

- Als symmetrischen Block Encryption Algorithmus MUSS AES mit einer Schlüssellänge von 256 Bit im Cipher Block Chaining Mode gemäß [CBC] verwendet werden.
- Das Padding MUSS gemäß [RFC 3852], Abschnitt 6.3 durchgeführt werden.
- Der Initialisierungsvektor (IV) SOLL zufällig gewählt werden. Wenn dies nicht möglich ist, so MUSS der Initialisierungsvektor durch einen anderen Mechanismus dynamisiert werden.

Der verwendete Algorithmus wird durch eine Vielzahl von Herstellern unterstützt, ist ausreichend performant und nach derzeitigen Einschätzungen bis 2013 als sicher eingestuft. Es wird daher kein Migrationspfad angegeben.

6.8.2 Asymmetrischer Anteil der hybriden Verschlüsselung binärer Daten im Kontext Datenerhalt

- Als asymmetrisches Verschlüsselungsverfahren SOLL RSAES-OAEP gemäß [PKCS#1], Kapitel 7.1 verwendet werden.
- Sofern eine Implementierung der Systeme mit RSAES-OAEP nicht möglich ist, MUSS RSAES-PKCS1-v1-5 gemäß [PKCS#1]. Kapitel 7.2 verwendet werden. Die Gültigkeit dieses Verfahrens ist bis 2013 beschränkt.
- Als Mask Generation Funktion für die Verwendung in RSAES-OAEP MUSS MGF 1 mit SHA-256 als Hash-Funktion gemäß [PKCS#1], Anhang B.2.1 verwendet werden.

Die verwendeten Algorithmen werden durch eine Vielzahl von Herstellern unterstützt, sind ausreichend performant und nach derzeitigen Einschätzungen bis 2013 als sicher eingestuft. Es wird daher kein Migrationspfad angegeben.

Anhang A

A1 - Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

A2 - Abbildungsverzeichnis

Es werden im derzeitigen Stand des Dokuments keine Abbildungen verwendet.

A3 - Tabellenverzeichnis

A4 - Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ALGCAT]	Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 17. Dezember 2007 Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV Veröffentlicht am 05.Februar 2008 im Bundesanzeiger Nr. 19, Seite 376 http://www.bundesnetzagentur.de/media/archive/12198.pdf
[BSI-TR03116]	BSI TR-03116 (23.03.2007): Technische Richtlinie für die eCard-Projekte der Bundesregierung Version: 1.0 http://www.bsi.de/literat/tr/tr03116/BSI-TR-03116.pdf
[CBC]	Section 6.2 of NIST Special Publication 800-38A, Recommendation for Block, Cipher Modes of Operation, Methods and Techniques, Morris Dworkin, December 2001 Edition, http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf (zuletzt geprüft am 01.02.2008)
[gemFA_CMSeGK]	gematik (19.03.2008): Einführung der Gesundheitskarte - Facharchitektur Kartenmanagement eGK Version 1.5.0, www.gematik.de
[gemFA_DatErh]	gematik (Draft 2008): Einführung der Gesundheitskarte - Facharchitektur Weiternutzung der Daten des Versicherten bei Kartenwechsel (in Vorbereitung)
[gemFK_DatErh]	gematik (Draft 2008): Einführung der Gesundheitskarte - Fachkonzept Weiternutzung der Daten des Versicherten bei Kartenwechsel (in Vorbereitung)
[gemNamD]	gematik (25.03.2008): Einführung der Gesundheitskarte - Spezifikation Infrastrukturkomponenten: Namensdienst, Version 1.3.0 , www.gematik.de
[gemSiKo] [gemSiKo#AnhF]	gematik (10.03.2008): Einführung der Gesundheitskarte – Übergreifendes Sicherheitskonzept der Telematikinfrastruktur Version 2.2.0. Anhang F: Kryptographiekonzept

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemSpec_eGK_P2]	gematik (25.03.2008): Einführung der Gesundheitskarte – Die Spezifikation elektronische Gesundheitskarte ; Teil 2 – Grundlegende Applikationen Version 2.2.0, www.gematik.de
[ISO 10126]	ISO10126-1:1991 Banking -- Procedures for message encipherment (wholesale) Part 1: General principles
[PKCS#1]	RSA Laboratories (June 14, 2002): RSA Cryptography Standard v2.1 (earlier versions: V1.5: Nov. 1993, V2.0: July, 1998) ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-1/pkcs-1v2-1.pdf (zuletzt geprüft am 01.02.2008)
[prEN14890-1]	prEN 14890-1 (Draft: February 2007) Application Interface for smart cards used as secure signature Creation Devices - Part 1: Basic services
[RFC 3852]	RFC 3852 (July 2004) Cryptographic Message Syntax (CMS) R. Housley, http://www.ietf.org/rfc/rfc3852.txt
[RFC 4346]	RFC 4346 (April 2006): The Transport Layer Security (TLS) Protocol Version 1.1, T. Dierks, http://www.ietf.org/rfc/rfc4346.txt
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://www.ietf.org/rfc/rfc2119.txt
[RVO2006]	Bundesgesetzblatt I (2006) vom 10.10.2006, Seite 2199 ff.: Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte in der Fassung der Bekanntmachung vom 5. Oktober 2006
[SigÄndG]	Bundesgesetzblatt I (2005), S.2: 1.Gesetz zur Änderung des Signaturgesetzes
[SigV01]	Bundesgesetzblatt I (2001), S. 3074: Verordnung zur elektronischen Signatur – SigV
[XMLEnc]	Donald Eastlake, Joseph Reagle et. al. (2002): XML Encryption Syntax and Processing http://www.w3.org/TR/xmlenc-core
[XMLSig]	W3C Recommendation (02.2002): XML-Signature Syntax and Processing http://www.w3.org/TR/xmldsig-core/