C_11325: Änderung in gemSpec_Krypt

in Abschnitt 1.1:

~~Dieses Dokument folgt den Konventionen der TR. Diese hat einen Betrachtungszeitraum von sechs bzw. sieben Jahren. Analog zu Kapitel 1 [BSI-TR-03116-1] bedeutet eine Aussage „Algorithmus X ist geeignet bis Ende 2023+“ generell nicht, dass Algorithmus X nach Ende 2023 nicht mehr geeignet ist, sondern lediglich, dass über die Eignung nach Ende 2023 in der TR keine explizite Aussage gemacht wird und dass aus heutiger Sicht die weitere Eignung nicht ausgeschlossen ist. Aussagen über den Betrachtungszeitraum hinaus sind „mit einem höheren Maß an Spekulation verbunden“~~.

in Abschnitt 2.1.1.1:

... Die Anforderung GS-A_4357-01 wird zu GS-A_4357-02 aufgrund folgender Aktualisierungen (Tab_KRYPT_002 und _002a) ...

Tabelle 1: Tab_KRYPT_002 Algorithmen für X.509-Identitäten zur Erstellung nicht-qualifizierter Signaturen für die Schlüsselgeneration „RSA“

Anwendungsfall	Vorgaben
Art und Kodierung des öffentlichen Schlüssels	RSA (OID 1.2.840.113549.1.1.1) zu verwendende Schlüssellänge: 2048 Bit, zulässig bis [ZL1][ZL2][HA3] ~~Ende 2023 [BSI-TR-03116-1]~~, gemäß [SOGIS-2020], vgl. auch A_15590
Signatur eines Zertifikats Signatur einer OCSP-Response Signatur eines OCSP-Responder-Zertifikates Signatur einer CRL Signatur des Zertifikats das Basis der Signaturprüfung einer CRL ist	sha256withRSAEncryption (OID 1.2.840.113549.1.1.11) zu verwendende Schlüssellänge: 2048 Bit, zulässig bis ~~Ende 2023 [BSI-TR-03116-1]~~ gemäß [SOGIS-2020], vgl. auch A_15590

...

Tabelle 2: Tab_KRYPT_002a Algorithmen für X.509-Identitäten zur Erstellung nicht-qualifizierter Signaturen für die Schlüsselgeneration „ECDSA“

Anwendungsfall	Vorgabe
Art und Kodierung des öffentlichen Schlüssels	ecPublicKey {OID 1.2.840.10045.2.1} **Entweder** auf der Kurve brainpoolP256r1 [RFC-5639#3.4, brainpoolP256r1] zulässig bis gemäß [SOGIS-2020] ~~Ende 2023+~~ **oder** auf der Kurve P-256 [FIPS-186-4]

	zulässig bis gemäß [SOGIS-2020] ~~Ende 2023+~~ Verständnishinweis: vgl. auch A_23139 bezüglich der Entweder-Oder-Beziehung Die Kodierung des öffentlichen Punkt erfolgt nach [RFC5480, Abschnitt 2], vgl. Beispiel in Abschnitt 5.2) Der privater Schlüssel muss zufällig und gleichverteilt aus {1, …, q-1} gewählt werden. (q ist die Ordnung des Basispunkts und ceil($\log_2$ q)=256).
Signatur eines Zertifikats Signatur einer OCSP-Response Signatur eines OCSP-Responder-Zertifikates Signatur einer CRL Signatur des Zertifikats das Basis der Signaturprüfung einer CRL ist	ecdsa-with-SHA256 [RFC-3279] {OID 1.2.840.10045.4.3.2} **Entweder** auf der Kurve brainpoolP256r1 [RFC-5639#3.4, brainpoolP256r1] zulässig bis gemäß [SOGIS-2020] ~~Ende 2023+~~ **oder** auf der Kurve P-256 [FIPS-186-4] zulässig bis gemäß [SOGIS-2020] ~~Ende 2023+~~ vgl. Beispiel in Abschnitt 5.2 Der privater Schlüssel muss zufällig und gleichverteilt aus {1, …, q-1} gewählt werden. (q ist die Ordnung des Basispunkts und ceil($\log_2$ q)=256).

... analog zu A_15590 für die TSP der TI wird für den Konnektor festgelegt

A_23458 - Konnektor, Zulässigkeitszeiträume kryptographische Algorithmen
Der Konnektor SOLL NICHT [DS4][HA5]die Zulässigkeitszeiträume kryptographischer Algorithmen technisch durchsetzen.**[<=]**

Erläuterung: Analog zu A_15590 für die TSP der TI gilt, dass die Unterbindung der Verwendung von RSA mit Schlüssellängen unter 3000 Bit durch die gematik erfolgt durch die Herausnahme der entsprechenden RSA-basierten Sub-CA-Zertifikate aus der TSL zum Zeitpunkt des Ablaufens der Zulässigkeit (gemäß TIP1-A_2062). Andere Zulässigkeitszeiträume sind für einen Konnektor nicht relevant, weil nach [SOGIS-2020] die RSA-Schlüssellänge die kleinste obere Schranke im Vergleich zu den anderen Vorgaben darstellt.

in Abschnitt 2.1.1.2:

... Die Anforderung GS-A_4358 wird zu GS-A_4358-01 aufgrund folgender Aktualisierungen (Tab_KRYPT_003 und _003a) ...

Tabelle 3: Tab_KRYPT_003 Algorithmen für X.509-Identitäten zur Erstellung qualifizierter elektronischer Signaturen für die Schlüsselgeneration „RSA"

Anwendungsfälle	Vorgaben

Signatur des VDA-Zertifikats	Nachdem die eIDAS-Verordnung das Signaturgesetz vollständig abgelöst hat, steht es einem VDA frei zu entscheiden welche Signatur (bspw. signiert von einer beliebigen VDA-internen CA) sein VDA-Zertifikat haben soll. Insbesondere kann die Signatur mit einem Nicht-RSA-Verfahren erstellt werden. Eine auswertende Komponente muss mit beliebigen (also auch nicht-RSA basierten) Signaturen eines VDA-Zertifikats umgehen können (bspw. Signatur des VDA-Zertifikats nicht auswerten, Authentizität und Integrität des Zertifikats wird über die Vertrauensliste sichergestellt).
Art und Kodierung des öffentlichen EE-Schlüssels	RSA-Signaturvariante: **Entweder** OID 1.2.840.113549.1.1.1 (rsaEncryption) (zulässig bis ~~Ende 2022~~ gemäß [SOG-IS-2020]) **oder** OID 1.2.840.113549.1.1.10 (id-RSASSA-PSS) [RFC-5756]. (~~ohne zeitliche Beschränkung der Zulässigkeit [SOG-IS-2020]~~ zulässig bis gemäß [SOG-IS-2020]) Die Auswahl obliegt dem EE-Zertifikatsausgebenden VDA. RSA-Schlüssellänge: zu verwendende Schlüssellänge: 2048 Bit, zulässig bis vgl. Angabe in [SOG-IS-2020]
Signatur eines Zertifikats, Signatur einer OCSP-Response oder Signatur eines OCSP-Responder-Zertifikates	**Entweder** sha256withRSAEncryption (OID 1.2.840.113549.1.1.11) (zulässig bis ~~Ende 2022~~ gemäß [SOG-IS-2020]) [ZL6][HA7] **oder** id-RSASSA-PSS (1.2.840.113549.1.1.10) [RFC-5756] (~~ohne zeitliche Beschränkung der Zulässigkeit [SOG-IS-2020]~~ zulässig bis gemäß [SOG-IS-2020]) zu verwendende Schlüssellänge: 2048 Bit, zulässig bis vgl. Angabe in [SOG-IS-2020] Die Hashfunktion für die Hashwertberechnung der TBSCertificate-Datenstruktur MUSS eine nach [SOG-IS-2020] zulässige Hashfunktion („Agreed Hash Function“) sein. Als Hashfunktion SOLL SHA-256 [FIPS-180-4] verwendet werden. Als MGF MUSS MGF1 [PKCS#1] verwendet werden. Die innerhalb der MGF1 verwendete Hashfunktion MUSS die gleiche Hashfunktion sein, wie die Hashfunktion der Hashwertberechnung der TBSCertificate-Datenstruktur. (Dies entspricht der Empfehlung aus [RFC-5756] bzw. [RFC-4055, 3.1] und dient der Komplexitätsreduktion.) Die Saltlänge MUSS mindestens 256 Bit betragen.(Die Maximallänge des Salts ergibt sich nach [PKCS#1] in Abhängigkeit von der Länge des Moduls.)

Tabelle 4: Tab_KRYPT_003a Algorithmen für X.509-Identitäten zur Erstellung qualifizierter Signaturen für die Schlüsselgeneration „ECDSA"

Anwendungsfall	Vorgabe
Signatur des VDA-Zertifikats	Nachdem die eIDAS-Verordnung das Signaturgesetz vollständig abgelöst hat, steht es einem VDA frei zu entscheiden welche Signatur (bspw. signiert von einer beliebigen VDA-internen CA) sein VDA-Zertifikat haben soll. Insbesondere kann die Signatur mit einem Nicht-ECDSA-Verfahren erstellt werden. Eine auswertende Komponente muss mit beliebigen (also auch nicht-ECDSA basierten) Signaturen eines VDA-Zertifikats umgehen können (bspw. Signatur des VDA-Zertifikats nicht auswerten, Authentizität und Integrität des Zertifikats wird über die Vertrauensliste sichergestellt).
Art und Kodierung des öffentlichen EE-Schlüssels	ecPublicKey {OID 1.2.840.10045.2.1} auf der Kurve brainpoolP256r1 [RFC-5639#3.4, brainpoolP256r1] ~~zulässig bis Ende 2023+~~ zulässig bis gemäß [SOG-IS-2020] Die Kodierung des öffentlichen Punkt erfolgt nach [RFC5480, Abschnitt 2], vgl. Beispiel in Abschnitt 5.2). Der private Schlüssel muss zufällig und gleichverteilt aus {1, …, q-1} gewählt werden. (q ist die Ordnung des Basispunkts und ceil($\log_2$ q)=256).
Signatur eines Zertifikats, Signatur einer OCSP-Response oder Signatur eines OCSP-Responder-Zertifikates	ecdsa-with-SHA256 [RFC-3279] {OID 1.2.840.10045.4.3.2} auf Kurve der brainpoolP256r1 [RFC-5639#3.4, brainpoolP256r1] ~~zulässig bis Ende 2023+~~ zulässig bis gemäß [SOG-IS-2020] vgl. Beispiel in Abschnitt 5.2

in Abschnitt 2.1.1.3:

... Die Anforderung GS-A_4359 wird zu GS-A_4359-01 aufgrund folgender Aktualisierungen (Tab_KRYPT_002 und _002a) ...

in Abschnitt 2.1.1.4:

... Die Anforderung GS-A_4360 wird zu GS-A_4360-01 aufgrund folgender Aktualisierungen (Tab_KRYPT_002 und _002a) ...

in Abschnitt 2.1.1.5:

... Die Anforderung GS-A_4361 wird zu GS-A_4361-01 aufgrund folgender Aktualisierungen (Tab_KRYPT_002 und _002a) ...

in Abschnitt 2.1.1.6:

... Die Anforderung GS-A_4362 wird zu GS-A_4362-01 aufgrund folgender Aktualisierungen (Tab_KRYPT_002 und _002a) ...

in Abschnitt 2.1.2.1:

... Die Anforderung GS-A_4365 wird zu GS-A_4365-01 aufgrund folgender Aktualisierungen (Tab_KRYPT_006) ...

Tabelle 5: Tab_KRYPT_006 Algorithmen für CV-Zertifikate

Algorithmen Typ	Algorithmus	Schlüssellänge
über das Zertifikat bestätigtes Schlüsselpaar	**Authentisierung ohne Sessionkey-Aushandlung** [RFC-5639#3.4, brainpoolP256r1] ecdsa-with-SHA256 {OID 1.2.840.10045.4.3.2} **Authentisierung mit Sessionkey-Aushandlung** [RFC-5639#3.4, brainpoolP256r1] authS_gemSpec-COS-G2_ecc-with-sha256 {OID 1.3.36.3.5.3.1}	256 Bit zulässig bis ~~Ende 2023+~~ gemäß [SOGIS-2020]
Signatur des Endnutzerzertifikats	[RFC-5639#3.4, brainpoolP256r1] ecdsa-with-SHA256 {OID 1.2.840.10045.4.3.2}	256 Bit zulässig bis ~~Ende 2023+~~ gemäß [SOGIS-2020]

in Abschnitt 2.1.2.2:

... Die Anforderung GS-A_4366 wird zu GS-A_4366-01 aufgrund folgender Aktualisierungen (Tab_KRYPT_007) ...

Tabelle 6: Tab_KRYPT_007 Algorithmen für CV-CA-Zertifikate

Algorithmen Typ	Algorithmus	Schlüssellänge
über das Zertifikat bestätigtes Schlüsselpaar	[RFC-5639#3.4, brainpoolP256r1] ecdsa-with-SHA256 {OID 1.2.840.10045.4.3.2}	256 Bit zulässig bis ~~Ende 2023+~~ gemäß [SOGIS-2020]
Signatur des CA-Zertifikates	[RFC-5639#3.4, brainpoolP256r1] ecdsa-with-SHA256 {OID 1.2.840.10045.4.3.2}	256 Bit zulässig bis ~~Ende 2023+~~ gemäß [SOGIS-2020]

in Abschnitt 3.1.1

... Die Anforderung GS-A_4371 wird zu GS-A_4371-01 aufgrund folgender Aktualisierungen (Tab_KRYPT_009) ...

Tabelle 7: Tab_KRYPT_009 Algorithmen für die Erzeugung von nicht-qualifizierten elektronischen XML-Signaturen

Signaturbestandteil	Beschreibung	Algorithmus	Anmerkung
Signaturstandard	Signaturstandard	ETSI TS 101 903 V1.4.2 (2010-12) Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES) [ETSI-XAdES]	Die Verwendung des Standards ist für die Signatur von XML-Dokumenten verpflichtend, die nicht über CMS [RFC-5652] signiert werden.
kryptographisches Signaturverfahren	Algorithmus für die Berechnung des Nachrichten Digest und die Verschlüsselung mit dem privaten Schlüssel	RSASSA-PSS mit SHA256 ~~bis nach Ende 2024+ verwendbar (Ende des Betrachtungshorizonts)~~ verwendbar bis gemäß [SOGIS-2020] (Hinweis: siehe Abschnitt 4.1)	Die Verwendung des Algorithmus ist verpflichtend. Alle hier aufgeführten Signaturverfahren müssen von einer Signaturprüfenden Komponente überprüfbar sein.
DigestMethod	Methode zur Berechnung eines Digest der zu signierenden Bereiche	SHA-256 Die [XMLDSig] 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 2.1.1.1	Die Auswahl des kryptographischen Tokens ist von dem jeweiligen Einsatzzweck abhängig.

in Abschnitt 3.1.2

... Die Anforderung GS-A_4372 wird zu GS-A_4372-01 aufgrund folgender Aktualisierungen (Tab_KRYPT_010) ...

Tabelle 8: Tab_KRYPT_010 Algorithmen für qualifizierte XML-Signaturen

Signaturbestandteil	Beschreibung	Algorithmus	Anmerkung
Signaturstandard	Signaturstandard	ETSI TS 101 903 V1.4.2 (2010-12) Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES) [ETSI-XAdES]	Die Verwendung des Standards ist für die Signatur von XML-Dokumenten verpflichtend, die nicht über CMS [RFC-5652] signiert werden.
kryptographisches Signaturverfahren	Algorithmus für die Berechnung des Nachrichten-Digest und die Verschlüsselung mit dem privaten Schlüssel	RSASSA-PSS mit SHA256 ~~bis nach Ende 2023+ verwendbar (Ende des Betrachtungshorizonts)~~ verwendbar bis gemäß [SOGIS-2020] (Hinweis: siehe Abschnitt 4.1)	Der Algorithmus muss für alle qualifizierten Signaturen verwendet werden. Alle hier aufgeführten Signaturverfahren müssen von einer Signaturprüfenden Komponente überprüfbar sein.
DigestMethod	Methode zur Berechnung eines Digest der zu signierenden Bereiche	SHA-256 Die [XMLDSig] 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 dem folgenden Abschnitt 2.1.1.2	Es darf nur eine Identität, die den Ansprüchen qualifizierter Signaturen entspricht, verwendet werden.

in Abschnitt 3.2.2

... Die Anforderung GS-A_4381 wird zu GS-A_4381-01 aufgrund folgender Aktualisierungen (Tab_KRYPT_012) ...

Tabelle 9: Tab_KRYPT_012 Algorithmen für Card-to-Server-Authentifizierung

Algorithmen Typ	Algorithmus	Schlüssellänge
Authentifizierung und Verschlüsselung der Authentisierungsdaten	AES im CBC-Modus (OID 2.16.840.1.101.3.4.1)	128 Bit zulässig bis ~~Ende 2023+~~ gemäß [SOGIS-2020]

in Abschnitt 3.3.1

GS-A_4382-02 - IPsec-Kontext - Schlüsselvereinbarung
Alle Produkttypen, die die Authentifizierung, den Schlüsselaustausch und die verschlüsselte Kommunikation im IPsec-Kontext durchführen, MÜSSEN die Schlüsselvereinbarung mittels IKEv2 [RFC-7296] gemäß den folgenden Vorgaben durchführen:

- Zur Authentisierung MUSS eine Identität mit einem X.509-Zertifikat gemäß [gemSpec_Krypt#GS-A_4360] verwendet werden.
- Für „Hash und URL" MUSS SHA-1 verwendet werden.
- Die Diffie-Hellman-Gruppe Gruppe 14 (definiert in [RFC-3526], verwendbar bis ~~Ende 2023~~ gemäß [SOGIS-2020]) MUSS für den Schlüsselaustausch unterstützt werden. Zusätzlich KÖNNEN Gruppen aus [BSI-TR-02102-3, Abschnitt 3.2.4, Tabelle 5], bei denen der Verwendungszeitraum ein „+" enthält, verwendet werden.
- Der private DH-Exponent für den Schlüsselaustausch MUSS eine Länge von mindestens 256 Bit haben.
- Die Authentisierung der ephemeren (EC)DH-Parameter erfolgt durch eine Signatur der Parameter durch den jeweiligen Protokollteilnehmer. Bei dieser Signatur MUSS SHA-256 als Hashfunktion verwendet werden. Es SOLL die Authentisierungsmethode „Digital Signature" nach [RFC-7427] dabei verwendet werden.

- Bei den symmetrische Verschlüsselungsalgorithmen MUSS AES mit 256 Bit Schlüssellänge im CBC-Modus unterstützt werden (sowohl für IKE-Nachrichten als auch später für die Verschlüsselung von ESP-Paketen). Es KÖNNEN weitere Verfahren nach [BSI-TR-02102-3, Abschnitt 3.2.1, Tabelle 2] bzw. [BSI-TR-02102-3, Abschnitt 3.3.1, Tabelle 7] verwendet werden.
- Für den Integritätsschutz (sowohl innerhalb von IKEv2 als auch anschließend für ESP-Pakete) MUSS HMAC mittels SHA-256 unterstützt werden. Es KÖNNEN weitere Verfahren nach [BSI-TR-02102-3, Abschnitt 3.2.3, Tabelle 4] bzw. [BSI-TR-02102-3, Abschnitt 3.3.1, Tabelle 8] verwendet werden, andere Verfahren dürfen nicht verwendet werden.
- Als PRF MUSS PRF_HMAC_SHA2_256 unterstützt werden. Es KÖNNEN weitere Verfahren nach [BSI-TR-02102-3, Abschnitt 3.2.2, Tabelle 3] verwendet werden, andere Verfahren dürfen nicht verwendet werden.
- Schlüsselaktualisierung: die IKE-Lifetime darf maximal 24*7 Stunden betragen (Reauthentication). Die IPsec-SA-Lifetime darf maximal 24 Stunden betragen (Rekeying). Der Initiator soll nach Möglichkeit vor Ablauf der Lifetime das Rekeying anstoßen. Ansonsten muss der Responder bei Ablauf der Lifetime das Rekeying von sich aus sicherstellen, bzw. falls dies nicht möglich ist, die Verbindung beenden.
- Für die Schlüsselberechnung muss Forward Secrecy [BSI-TR-02102-1, S.ix] (in [RFC-7296] „Perfect Forward Secrecy" genannt) gewährleistet werden. Meint die Wiederverwendung von zuvor schon verwendeten (EC-)Diffie-Hellman-Schlüsseln ([RFC-7296, Abschnitt 2.12]) ist nicht erlaubt.

<=

in Abschnitt 3.3.2

A_23226-01 - TLS-Verbindung, Konnektor: Legacy-KT-Unterstützung
Der Konnektor MUSS für die Unterstützung von alten eHealth-KT folgende TLS-Vorgaben ebenfalls unterstützen:

- Als Cipher Suite MUSS TLS_DHE_RSA_WITH_AES_128_CBC_SHA oder TLS_DHE_RSA_WITH_AES_256_CBC_SHA unterstützt werden.
- Dabei MUSS für die Schlüsselaushandlung Gruppe 14 (definiert in [RFC-3526], verwendbar bis ~~Ende 2023~~ gemäß [SOGIS-2020]) verwendet werden.
- Der private DH-Exponent für den Schlüsselaustausch MUSS eine Länge von mindestens 256 Bit haben.

<=

in Abschnitt 3.4

Tabelle 10: Tab_KRYPT_019 eingesetzte Algorithmen für die Ableitung eines versichertenindividuellen Schlüssels

Algorithmen Typ	Algorithmus	Unterverfahren

Masterkey-Verfahren für die Generierung des versichertenindividuellen Schlüssel innerhalb eines CMS	AES basiertes Verfahren gemäß vorheriger Definition	AES-256 SHA-256 anwendbar bis~~Ende 2023+~~ gemäß [SOGIS-2020]

in Abschnitt 3.7

... Die Anforderung GS-A_5080 wird zu GS-A_5080-01 aufgrund folgender Aktualisierungen (Tab_KRYPT_020) ...

Tabelle 11: Tab_KRYPT_020 Algorithmen für die Erzeugung und Prüfung von binären Daten im Kontext von Dokumentensignaturen

Signaturbestandteil	Beschreibung	Algorithmus	Anmerkung
Signaturstandard	Signaturstandard	ETSI TS 101 733 V1.7.4 (2008-07) Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES) [ETSI-CAdES]	Die Verwendung des Standards ist für die Signatur von Dokumenten verpflichtend die mittels CMS [RFC-5652] erzeugt werden.
kryptographisches Signaturverfahren	Algorithmus für die Berechnung des Nachrichten Digest und die Verschlüsselung mit dem privaten Schlüssel	**RSASSA-PSS mit SHA256** verwendbar bis ~~nach Ende 2023+ verwendbar (Ende des Betrachtungshorizonts)~~ gemäß [SOGIS-2020]	Die Verwendung einer dieser Algorithmen ist verpflichtend. Alle hier aufgeführten Signaturverfahren müssen von einer Signaturprüfenden Komponente überprüfbar sein.
DigestMethod	Methode zur Berechnung eines Digest der zu signierenden Bereiche	SHA-256	Die Verwendung des Algorithmus ist verpflichtend.
Kryptographisches Token	Kryptographisches Token für die Signatur, bestehend aus einem privaten Schlüssel und einem	Identitäten gemäß einem der folgenden Abschnitte 2.1.1.1 2.1.1.2	Die Auswahl des kryptographischen Tokens ist von dem jeweiligen Einsatzzweck abhängig.

	zugehörigen X.509-Zertifikat		

in Abschnitt 3.8

... Die Anforderung GS-A_5081 wird zu GS-A_5081-01 aufgrund folgender Aktualisierungen (Tab_KRYPT_009) ...

Tabelle 12: Tab_KRYPT_021 Algorithmen für die Erzeugung und Prüfung von PDF/A-Dokumentensignaturen

Signaturbestandteil	Beschreibung	Algorithmus	Anmerkung
Signaturstandard	Signaturstandard	ETSI TS 102 778-3 V1.2.1, PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced – PAdES-BES and PAdES-EPES Profiles Technical Specification, 2010 [PAdES-3]	Die Verwendung des Standards ist für die Signatur von PDF/A [PDF/A-2] Dokumenten verpflichtend, die mittels eingebetteter Signaturen signiert werden.
kryptographisches Signaturverfahren	Algorithmus für die Berechnung des Nachrichten Digest und die Verschlüsselung mit dem privaten Schlüssel	**RSASSA-PSS mit SHA256** verwendbar bis ~~nach Ende 2023+ verwendbar (Ende des Betrachtungshorizonts)~~ gemäß [SOGIS-2020]	Die Verwendung einer dieser Algorithmen ist verpflichtend. Alle hier aufgeführten Signaturverfahren müssen von einer Signaturprüfenden Komponente überprüfbar sein.
DigestMethod	Methode zur Berechnung eines Digest der zu signierenden Bereiche	**SHA-256**	Die Verwendung des Algorithmus ist verpflichtend.
Kryptographisches Token	Kryptographisches Token für die Signatur, bestehend aus einem privaten Schlüssel und einem	Identitäten gemäß einem der folgenden Abschnitte 2.1.1.1 2.1.1.2	Die Auswahl des kryptographischen Tokens ist von dem jeweiligen Einsatzzweck abhängig.

	zugehörigen X.509-Zertifikat		

In Abschnitt 5

...

Für den qualifizierten Vertrauensraum ist nach ~~ab~~ Ende 2025 [SOG-IS-2020] und für die TI nach ~~ab~~ Ende ~~2023~~ 2025 ein Sicherheitsniveau von mindestens 120 Bit für alle kryptographischen Verfahren vorgeschrieben ~~[BSI-TR-03116-1]~~.

....

Es gibt bis maximal Ende ~~2023~~ 2025 (vgl. Abschnitt 2.1.1.1) einen Parallelbetrieb in der TI.

In Abschnitt 5.7.2

Für die Verschlüsselung muss nach Ende ~~2023~~ 2025 ECIES und nicht mehr RSA-OAEP verwendet werden.

In Abschnitt 6.14

~~SIKE: SIDH-p434, SIDH-p434-compressed, SIDH-p503, SIDH-p503-compressed, SIDH-p610, SIDH-p610-compressed, SIDH-p751, SIDH-p751-compressed, SIKE-p434, SIKE-p434-compressed, SIKE-p503, SIKE-p503-compressed, SIKE-p610, SIKE-p610-compressed, SIKE-p751, SIKE-p751-compressed~~

In Abschnitt 8

Die gematik beobachtet intensiv die laufenden Forschungs- und Evaluierungsaktivitäten [NIST-PQC] die voraussichtlich ~~2022/23~~ 2023/24 einen geeigneten Stand erreichen werden.

Änderungen in gemProdT_..._PTVx.y.z-n

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_...]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Afo-ID	Afo-Bezeichnung	Zuordnung Prüfkriterium
A_23458	Konnektor, Zulässigkeitszeiträume kryptographische Algorithmen	sicherheitstechnische Eignung: Herstellererklärung