gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Certificate Policy
Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL

Version:	1.8.0
Revision:	\main\rel_online\rel_ors1\rel_opb1\59
Stand:	21.04.2017
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemRL_TSL_SP_CP]

Dokumentinformationen

Object Identifier (OID) dieser Version des Dokumentes:

1.2.276.0.76.4.163

Soll die OID in anderen Dokumenten versionsunabhängig referenziert werden, so ist die Kennung oid_policy_gem_or_cp zu verwenden. Die Ermittlung der relevanten OID ist dann über das Dokument [gemSpec_OID] möglich.

Änderungen zur Vorversion

Anpassungen an Kartengeneration 2.1 und Änderungsliste P14.9

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.5.0	04.07.2012		Zur Abstimmung freigegeben	gematik
	04.09.2012	Alle	Einarbeitung Kommentierung Gesellschafter	gematik
1.0.0	15.10.12		freigegeben	gematik
1.1.0	12.11.12		Einarbeitung Kommentare aus der übergreifenden Konsistenzprüfung	gematik
1.2.0	06.06.13		Überarbeitung anhand interner Änderungsliste (Fehlerkorrekturen, Inkonsistenzen)	gematik
1.3.0	15.08.13		Einarbeitung gemäß Änderungsliste	gematik
1.4.0	03.05.16		Anpassungen zum Online-Produktivbetrieb (Stufe 1)	gematik
1.5.0	24.08.16		Einarbeitung weitere Kommentare	gematik
1.6.0	16.10.16		Aufnahme SMC-B für Organisationen der Gesellschafter, Anpassungen gemäß Änderungsliste	
1.7.0	02.12.16		freigegeben (eIDAS)	gematik
			Einarbeitung Anpassungen Kartengeneration G2.1, Änderungsliste P14.9	
1.8.0.	21.04.17		freigegeben	gematik

Inhaltsverzeichnis

1 Einordnung des Dokumentes

Nach Inkrafttreten der eIDAS-Verordnung wurde die Anforderungslage der gematik entsprechend angepasst. Signaturgesetz (SigG) und -verordnung (SigV) sind weiterhin gültig und finden dort Anwendung, wo sie der eIDAS-Verordnung nicht widersprechen. SigG und SigV sollen zukünftig durch das deutsche Vertrauensdienstegesetz (VDG) abgelöst werden. Mit Verabschiedung des Vertrauensdienstegesetzes kann es in diesem Dokument daher zu Anpassungen und Konkretisierungen entsprechend der geänderten Rechtslage kommen.

1.1 Zielsetzung

Dieses Dokument definiert die Anforderungen an die Aussteller von nicht-qualifizierten X.509-Zertifikaten (gematik Root-CA und TSP-X.509 nonQES). Hierbei werden die Sicherheitsanforderungen hinsichtlich der Erzeugung, Verwaltung und Sperrung von Zertifikaten definiert.

Die Dokumentenstruktur lehnt sich dabei an [RFC3647] an.

1.2 Zielgruppe

Das Dokument richtet sich an die Trust Service Provider.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des deutschen Gesundheitswesens. Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungsverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z. B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzung des Dokuments

Die vorliegende Certificate Policy ist auf Zertifikate für HBAs in der Produktivumgebung nicht anwendbar. Für diese gilt die „Gemeinsame Policy für die Ausgabe der HPC“ [CP-HPC].

Für sämtliche Zertifikate der HBA (nonQES, Pseudo-QES) in der Test- und Referenzumgebung gelten die Festlegungen dieser Certificate Policy gemäß Anhang B.

Anforderungen an den Anbieter des TSL-Dienstes (in Vorversionen des Dokumentes als „TSL-SP“ bezeichnet) werden in der Spezifikation des TSL-Dienstes [gemSpec_TSL] beschrieben.

Anforderungen an die Vertrauensdiensteanbieter (VDA) qualifizierter X.509-Zertifikate (TSP-X.509 QES) werden in [eIDAS] festgelegt.

Anforderungen an die Anbieter von CV-Zertifikaten (TSP-CVC) werden in der Spezifikation des TSP CVC beschrieben [gemSpec_CVC_TSP]

1.5 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID und die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

⌦ **GS-A_0000 <Titel der Afo>**

Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

2 Einleitung fachlicher Teil

2.1 Überblick

Alle an der Telematikinfrastruktur (TI) beteiligten Trustcenter, die nicht-qualifizierte X.509-Zertifikate für Aussteller oder Endbenutzer erstellen (gematik Root-CA und TSP-X.509 nonQES), müssen aus Gründen der Informationssicherheit ein Mindestsicherheitsniveau einhalten.

Der Nachweis dieses Sicherheitsniveaus erfolgt u. a. durch die Umsetzung der Anforderungen aus dieser Richtlinie (vgl. Abschnitt 2.1.1). Zum Nachweis der Umsetzung erstellen die Anbieter ein betreiberspezifisches Sicherheitskonzept.

Die Erfüllung der Mindestanforderungen muss gegenüber der gematik durch die Vorlage eines Sicherheitsgutachtens bestätigt werden. Das Gutachten muss die Wirksamkeit des betreiberspezifischen Sicherheitskonzepts bestätigen.

Diese Bestätigung durch einen Gutachter und die Vorlage des Gutachtens bei der gematik stellen die Voraussetzung für die Aufnahme der gematik Root-CA oder eines TSP-X.509 nonQES in den TI-Vertrauensraum dar, der durch eine Trust-Service Status List (TSL) abgebildet wird (vgl. [gemKPT_PKI_TIP#2.3.3, 7.2.1]).

Die Vorlage des Gutachtens ist im Regelfall im Rahmen eines Zulassungsverfahrens oder einer Abnahme relevant. Der Ablauf des Zulassungs- oder Abnahmeverfahrens wird durch das Zulassungskonzept beschrieben.

2.1.1 Teilnehmer in der PKI

Die Definition und Abgrenzung der Teilnehmer in der PKI erfolgt im Rahmen von [gemKPT_PKI_TIP#2.7.1], [gemSpec_PKI#8.1]. Die in diesem Dokument definierten Teilnehmer werden im Rahmen dieser Richtlinie als Adressaten für Anforderungen verwendet.

2.1.2 Ziel dieser Richtlinie

Der Prozess der Aufnahme der gematik Root-CA oder eines TSP-X.509 nonQES in die gematik-TSL orientiert sich grundsätzlich an den Wertmaßstäben

- technische Konformität und
- angemessener und vergleichbarer Sicherheitslevel.

Das vorliegende Dokument adressiert vorrangig den zweiten Wertmaßstab, da die entsprechenden Vorgaben zur technischen Konformität durch andere Dokumente vorgegeben werden.

2.1.3 Rahmen dieser Richtlinie

Diese Richtlinie trifft Vorgaben sowohl für TSPs, die als Root-Instanz (gematik Root-CA) fungieren, als auch für TSPs, die innerhalb einer Zertifizierungshierarchie nachgeordnet sind (TSP-X.509 nonQES). Für den TSP-X509 nonQES werden zudem Anforderungen bzgl. der Erstellung von Endnutzer-Zertifikaten gestellt.

Sofern in dieser Richtlinie Anforderungen an einzelne Sicherheitsmaßnahmen nicht spezifiziert werden und nicht durch andere normative Dokumente der gematik gefordert werden, sind diese mindestens an die entsprechenden Maßnahmenkataloge des [BSI_2005] oder international vergleichbarer Rahmenwerke wie [ISO17799] und [ISO27001] anzulehnen.

3 Allgemeine Maßnahmen

Die Verzeichnisdienstleistungen und Veröffentlichung von Verzeichnisinformationen stehen im Verantwortungsbereich der gematik Root-CA oder eines TSP-X.509 nonQES.

3.1 Verzeichnisse

GS-A_4173 Erbringung von Verzeichnisdienstleistungen

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN eine ordnungsgemäße Erbringung der Verzeichnisdienstleistungen im Rahmen ihres Sicherheitskonzepts gewährleisten und sich am aktuellen Stand der Technik orientieren.

Die Bereitstellung eines Zugriffs auf den Verzeichnisdienst, z. B. für die Suche nach Zertifikaten, wird ggf. durch die Fachanwendungen motiviert. Ein Zugriff auf die Verzeichnisdienste soll perspektivisch realisiert werden.

3.2 Veröffentlichung von Zertifikaten

GS-A_4174 Veröffentlichung von CA- und Signer-Zertifikaten

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN einer Veröffentlichung ihrer Teilnahme an der TSL der TI und der Weitergabe seines Ausstellerzertifikats, im Rahmen der Vorgaben der gematik, zustimmen.

3.3 Zeitpunkt und Häufigkeit von Veröffentlichungen

GS-A_4175 Veröffentlichungspflicht für kritische Informationen

Die gematik Root-CA und TSP-X.509 nonQES MÜSSEN kritische Informationen, wie eine Betriebseinstellung oder Störungen des Betriebsablaufes, unverzüglich der gematik anzeigen.

GS-A_4176 Mitteilungspflicht bei Änderungen

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN rechtzeitig Änderungen an der Architektur und den organisatorischen Abläufen der PKI gegenüber der gematik bekannt geben, sofern die Sicherheit verringert oder das Außenverhalten verändert wird.

3.4 Zugriffskontrollen auf Verzeichnisse

GS-A_4177 Zugriffskontrolle auf Verzeichnisse

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN eine geeignete Zugriffskontrolle auf die entsprechenden Verzeichnisse gewährleisten.

4 Identifizierung und Authentifizierung

4.1 Namensregeln

4.1.1 Arten von Namen

⌦ **GS-A_4178 Standardkonforme Namensvergabe in Zertifikaten**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN für die Namensvergabe in Zertifikaten den Standard [X.501] beachten. Die Angabe eines subject.distinguishedName ist obligatorisch. ⌫

⌦ **GS-A_4179 Format von E-Mail-Adressen in Zertifikaten**

Die gematik Root-CA und ein TSP-X.509 nonQES SOLLEN E-Mail-Adressen in Zertifikaten unter der X.509-Extension *subjectAltNames* im Format nach [RFC822] hinterlegen, sofern die Angabe einer E-Mail-Adresse im jeweiligen Profil vorgesehen ist. ⌫

4.1.2 Namensform

⌦ **GS-A_4180 Gestaltung der Struktur der Verzeichnisdienste**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die Namensform der jeweiligen Zertifikate bei der Gestaltung der Struktur der Verzeichnisdienste beachten und sicherstellen, dass der Aufbau des *distinguishedName* im Feld *Subject* und die Struktur des Verzeichnisdienstes zueinander konsistent sind. ⌫

4.1.3 Aussagekraft von Namen

Vorgaben für die Zertifikate der eGK und für Zertifikate der SMC sind im Dokument „Spezifikation PKI der TI-Plattform“ [gemSpec_PKI] beschrieben.

4.1.4 Notwendigkeit für aussagefähige und eindeutige Namen

⌦ **GS-A_4181 Eindeutigkeit der Namensform des Zertifikatsnehmers**

Die ausstellende gematik Root-CA und ein ausstellender TSP-X.509 nonQES MÜSSEN bei der Vergabe von Namen (Endnutzer- oder CA-Zertifikate) die Eindeutigkeit der gewählten *distinguishedName* des Zertifikatsnehmers umsetzen und sicherstellen, dass die Daten spezifikationsgemäß aufbereitet werden.⌫

Siehe auch Kapitel 4.1.2. Die Integrität und Vollständigkeit der Daten liegt in der Hoheit der Herausgeber der Zertifikate.

⌦ **GS-A_4182 Kennzeichnung von personen- bzw. organisationsbezogenen Zertifikaten**

Ein TSP-X.509 nonQES MUSS personen- bzw. organisationsbezogene Zertifikate entsprechend den Zertifikatsprofilen eindeutig als solche kenntlich machen. ⌫

⌦ **GS-A_4183 Kennzeichnung von maschinen-, rollenbezogenen oder pseudonymisierten (nicht personenbezogenen) Zertifikaten**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN maschinen-, rollenbezogene oder pseudonymisierte (nicht personenbezogene) Zertifikate als solche kenntlich machen, um Verwechslungsfreiheit zu garantieren.⌫

4.1.5 Anonymität oder Pseudonyme von Zertifikatsnehmern

⌦ **GS-A_4184 Eindeutigkeit von pseudonymen Zertifikaten**

Der Kartenherausgeber MUSS die Eindeutigkeit der pseudonymen Zertifikate sicherstellen.⌫

4.1.6 Regeln für die Interpretation verschiedener Namensformen

⌦ **GS-A_4185 Unterscheidung von Zertifikaten**

Ein TSP-X.509 nonQES MUSS zur Unterscheidung von Zertifikaten die Kennzeichnung des Zertifikattyps in die Extension *certificatePolicies* schreiben.⌫

Der Inhalt des Kennzeichens wird definiert in [gemSpec_OID#3.5.3].

4.2 Erstmalige Überprüfung der Identität

4.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

⌦ **GS-A_4186 Prüfung auf den Besitz des privaten Schlüssels bei dem Zertifikatsnehmer**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN Prozesse und Vorgaben entsprechend des betreiberspezifischen Sicherheitskonzepts definieren, die eine Prüfung auf den Besitz des privaten Schlüssels bei dem Zertifikatsnehmer gewährleisten, bevor das jeweilige Zertifikat im Verzeichnisdienst freigeschaltet und veröffentlicht wird.⌫

Bei Authentisierungs- und Verschlüsselungszertifikaten der Endanwender (Versicherte) des TSP-X.509 nonQES können die bestehenden Vorgaben bezüglich der Übermittlung der Karten beibehalten werden.

⌦ **GS-A_4187 Nutzung bestehender SGB-Datensätze bei Registrierung für Endanwender (Versicherte)**

Der TSP-X.509 nonQES (eGK) SOLL für die Registrierung der Endanwender die bestehenden Datensätze der Endanwender (Versicherte) beim Kostenträger verwenden, so wie sie im Rahmen der Vorgaben des Sozialgesetzbuches erhoben wurden.⌫

Der Kostenträger verantwortet die Korrektheit dieser Daten. Eine erneute Identifizierung der Versicherten, nur für die Erstellung von AUT- und ENC-Zertifikaten, ist aufgrund der datenschutzrechtlichen Vorgaben nicht geboten.

4.2.2 Authentifizierung von Organisationszugehörigkeiten

Keine Vorgaben

4.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikatsantragstellers

GS-A_4188 Zuverlässige Identifizierung und vollständige Prüfung der Antragsdaten

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um den Antragsteller gemäß Herausgeber-Policy zu identifizieren und den Schutz der Antragsdaten zu gewährleisten.

4.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

GS-A_4189 Prüfungspflicht für Person, Schlüsselpaar, Schlüsselaktivierungsdaten und Name

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN gewährleisten, dass ungeprüfte Angaben nicht die Verbindung der Person zu Schlüsselpaar, Schlüsselaktivierungsdaten und Name betreffen.

4.2.5 Prüfung der Berechtigung zur Antragstellung

GS-A_4190 Regelung für die Berechtigung zur Antragstellung

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN konkrete Prüfregeln für die Berechtigung zur Antragsstellung in ihrem CP (bzw. CPS) definieren und diese konsistent zu den Anforderungen der zuständigen Kartenherausgeber gestalten, sofern die Antragstellung durch diesen bzw. durch einen verantwortlichen Mitarbeiter des Kartenherausgebers erfolgt.

4.2.6 Kriterien für den Einsatz interoperabler Systeme

GS-A_4191 Einsatz interoperabler Systeme durch einen externen Dienstleister

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass bei der Interoperation von Diensten, die Integritäts-, Authentizitäts- und Vertraulichkeitsanforderungen erfüllt bleiben.

Siehe auch Kapitel 5.3. Dies gilt insbesondere, wenn die Registrierung durch einen externen Dienstleister erfolgt, während andere PKI-Betriebsprozesse ganz oder teilweise im Hause der gematik Root-CA oder eines TSP-X.509 nonQES stattfinden (so kann z. B. die inkonsistente Umwandlung von deutschen Umlauten verhindert werden).

4.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (Rekeying)

4.3.1 Identifizierung und Authentifizierung von routinemäßigen Anträgen zur Schlüsselerneuerung

⌦ GS-A_4192 Prüfung der Berechtigung zur Antragstellung auf Schlüsselerneuerung

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN konkrete Prüfregeln für die Berechtigung zur Antragsstellung auf Schlüsselerneuerung in ihrer Certificate Policy (CP) bzw. ihrem Certification Practice Statement (CPS) definieren. ⌫

4.3.2 Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen

Siehe Abschnitt 4.2.3

4.4 Identifizierung und Autorisierung von Sperranträgen

⌦ GS-A_4193 Zuverlässige Identifizierung und Autorisierung des Sperrantragstellers

Die Registrierungsstellen der gematik Root-CA und eines TSP-X.509 nonQES MÜSSEN eine zuverlässige Identifizierung und Autorisierung des Sperrantragstellers gewährleisten, die sich an den Vorgaben des betreiberspezifischen Sicherheitskonzepts orientiert.⌫

5 Betriebliche Maßnahmen

5.1 Zertifikatsantrag durch TSP-X.509

GS-A_4194 Identifikation des Antragstellers und Dokumentation bei der Beantragung eines CA-Zertifikats

Die gematik Root-CA MUSS sicherstellen, dass der Zertifikatsantrag eines TSP-X.509 nonQES die zweifelsfreie Identifizierung des Antragstellers unterstützt und das Ergebnis des Antragsprozesses dokumentieren.⌫

GS-A_4195 Schriftform für Aufnahme eines Zertifikats in die TSL

TSP-X.509 nonQES MÜSSEN schriftlich die Aufnahme ihres CA-Zertifikats in die TSL beantragen. ⌫

GS-A_4196 Vorlage zulassungsrelevanter Dokumentationen und des Betriebskonzepts bei der gematik vor Aufnahme in die TSL

Der TSP-X.509 nonQES MUSS nach Aufforderung der gematik zulassungsrelevante Dokumentationen und das Betriebskonzept zur Prüfung durch die gematik vorlegen, bevor eine Aufnahme in die TSL erfolgt.⌫

5.1.1 Autorisierung für die Beantragung von Zertifikaten

GS-A_4199 Berechtigung für Beantragung von CA-Zertifikaten

Ein TSP-X.509 nonQES MUSS festlegen, wer in seinem Namen einen Zertifikatsantrag stellen darf und benennt diese Personen gegenüber der gematik Root-CA. ⌫

5.1.2 Registrierungsprozess und Zuständigkeiten

GS-A_4201 Dokumentation des Registrierungsprozesses

Die Registrierungsstellen einer gematik Root-CA und eines TSP-X.509 nonQES MÜSSEN den Registrierungsprozess dokumentieren, der die Anforderungen der Identifikation des Antragstellers erfüllt.⌫

Siehe Abschnitt 4.2.

5.2 Verarbeitung des Zertifikatsantrags

5.2.1 Durchführung der Identifizierung und Authentifizierung

GS-A_4202 Identifikation des Zertifikatsnehmers im Rahmen der Registrierung

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN den Zertifikatsnehmer und den Antragsteller vor der Registrierung nach einem dokumentierten Prozess gemäß Herausgeber-Policy identifizieren.⌫

GS-A_5083 Zertifikatsantragstellung im Vier-Augen-Prinzip

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass die Zertifikatseingangsdaten im Vier-Augen-Prinzip entgegengenommen werden und die durchgeführten Prozessschritte bei der Antragstellung (z. B. Identifizierung und Authentifizierung von Zertifikatsantragstellern und Prüfung der Autorisierung) protokolliert werden.⌫

5.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

GS-A_4203 Dokumentationspflichten für die Beantragung von Zertifikaten

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass das Vorgehen zur Annahme oder Ablehnung eines Zertifikatsantrages vollständig dokumentiert wird und eine Annahme nur für identifizierte Antragsteller mit berechtigtem Antrag erfolgen darf.⌫

5.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Keine Vorgaben

5.3 Zertifikatsausgabe

Ausgabe- und Ausstellungsprozess für ein TSP-Zertifikat sind unmittelbar miteinander verbunden. Für Zertifikate für Zertifikatsnehmer sind dieses getrennte Prozesse.

5.3.1 Ausgabe eines Zertifikats für einen nachgeordneten TSP (TSP-X.509 nonQES)

Die gematik Root-CA erzeugt im Rahmen ihrer Verpflichtungen, nach Vorliegen eines vollständigen und geprüften Antrags und nach erfolgter Identifizierung Zertifikate für ihre nachgeordneten TSP-X.509 nonQES.

GS-A_4204 Bearbeitung von Zertifikatsanträgen eines TSP-X.509 nonQES durch die gematik Root-CA

Die gematik Root-CA MUSS bei der Bearbeitung eines durch den nachgeordneten TSP-X.509 nonQES korrekt signierten Zertifikatsantrages sicherstellen, dass
(a) der Antrag hinsichtlich der Vollständigkeit kontrolliert und die Integrität mit dem vorgelegten öffentlichen Signaturschlüssel geprüft wird,
(b) die vertretende Person des TSP-X.509 nonQES sicher authentifiziert wird; hierfür kommt alternativ ein persönliches Erscheinen, das Postident-Verfahren oder eine qualifizierte Signatur in Betracht.⌫

GS-A_4206 Prüfung auf Korrektheit des Schlüsselpaares eines TSP-X.509 nonQES

Die gematik Root-CA MUSS bei der Erzeugung von Zertifikaten für einen TSP-X.509 nonQES sicherstellen, dass
(a) der dabei zertifizierte öffentliche Schlüssel authentisch ist und
(b) der TSP-X.509 nonQES den zugehörigen privaten Schlüssel besitzt.⌫

5.3.2 Erstellen eines TSP-Zertifikats (self signed Root)

Für die Ausgabe gelten die gleichen Sicherheitsbedingungen wie für die Ausgabe von TSP-X.509 nonQES-Zertifikaten.

5.3.3 Ausgabe eines Zertifikats für Zertifikatsnehmer (an Endnutzer)

⌦ **GS-A_4207 Vorgaben für die Ausgabe von Endnutzerzertifikaten**

Ein TSP-X.509 nonQES MUSS die Anforderungen an die Ausgabe von Zertifikaten für Zertifikatsnehmer in seinem CPS beschreiben.⌫

5.3.4 Aktionen des TSP-X.509 nonQES bei der Ausgabe von Zertifikaten

⌦ **GS-A_4208 Ausgabe von Zertifikaten**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass eine Ausgabe eines Zertifikats nur dann erfolgen kann, wenn der Zertifikatsantrag gültig ist.⌫

⌦ **GS-A_4209 Sicherstellung der Verbindung von Zertifikatsnehmer und privatem Schlüssel**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die eindeutige Verbindung von Zertifikatsnehmer und privatem Schlüssel sicherstellen.⌫

⌦ **GS-A_4394 Dokumentation der Zertifikatsausgabeprozesse**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die Aktionen bei den Zertifikatsausgabeprozessen und die Benachrichtigung des Zertifikatsnehmers über die Ausgabe seiner Zertifikate dokumentieren.⌫

⌦ **GS-A_4906 Zuordnung von Schlüsseln zu Identitäten**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass ein Schlüssel nicht zwei verschiedenen Identitäten zugeordnet wird. ⌫

5.3.5 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats

⌦ **GS-A_4395 Benachrichtigung des Zertifikatsnehmer**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN den Zertifikatsnehmer über die Ausgabe seiner Zertifikate informieren. ⌫

5.4 Zertifikatsannahme

Ein Zertifikat gilt als angenommen, wenn der gesamte Prozess für Antragstellung, Ausstellung des Zertifikats und Zertifikatsausgabe erfolgreich durchlaufen und von der gematik Root-CA oder vom TSP-X.509 nonQES geprüft ist.

5.4.1 Verhalten für eine Zertifikatsannahme

⌦ **GS-A_4210 Dokumentation der Annahme eines Zertifikatsantrags und der sicheren Ausgabe des Zertifikats**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN den Prozess für die sichere Ausgabe und die Bedingungen, die zu einer Annahme des Zertifikats führen, dokumentieren. ⌫

5.4.2 Veröffentlichung des TSP-Zertifikats

⌦ **GS-A_4211 Bereitstellung von CA-Zertifikaten bei Aufnahme in die TSL**

Der TSP-X.509 nonQES MUSS seine CA-Zertifikate im Rahmen der Aufnahme in die TSL dem Anbieter des TSL-Dienstes zur Verfügung stellen.⌫

5.4.3 Benachrichtigung anderer Zertifikatsnutzer über die Zertifikatsausgabe

Keine Vorgaben

5.5 Verwendung des Schlüsselpaars und des Zertifikats

5.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

⌦ **GS-A_4212 Verwendung des privaten Schlüssels durch den Zertifikatsnehmer**

Ein TSP-X.509 nonQES MUSS die Verantwortlichkeiten des Zertifikatsnehmers dokumentieren und dem Zertifikatsnehmer mitteilen, dass der private Schlüssel nur für Anwendungen benutzt werden darf, die in Übereinstimmung mit den im Endnutzerzertifikat angegebenen Nutzungsarten (*keyUsage*) stehen. ⌫

⌦ **GS-A_4213 Zulässige Nutzungsarten**

Ein TSP-X.509 nonQES DARF NICHT andere Nutzungsarten für Endbenutzerzertifikate als die nachfolgend aufgeführten unterstützen:
(a) Authentifizierung von Benutzer- oder Anwendungsdaten (Nutzungsart *digitalSignature*),
(b) Entschlüsselung von Benutzer- oder Anwendungsdaten oder von symmetrischen Schlüsseln, welche in dem so genannten Hybridverfahren für die Verschlüsselung solcher Daten dienen (Nutzungsarten *dataEncipherment* bzw. *keyEncipherment*),
(c) Kennzeichnung der Verbindlichkeit (Nutzungsart *nonRepudiation*) einer elektronischen Signatur durch den Zertifikatsnehmer
(d) Authentifizierung und Verschlüsselung von symmetrischen Schlüsseln für AUT-Zertifikate im Anwendungskontext TLS (Nutzungsart *digitalSignature* und *keyEncipherment*). ⌫

5.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

⌦ **GS-A_4214 Veröffentlichung der öffentlichen Schlüssel durch den TSP-X.509 nonQES**

Der TSP-X.509 nonQES DARF NICHT den Schlüssel eines Zertifikatsnehmers veröffentlichen, sofern der Zertifikatsnehmer der Veröffentlichung nicht zugestimmt hat.⌫

5.6 Zertifikatserneuerung

Die Erneuerung von Zertifikaten ist in der Telematikinfrastruktur nicht vorgesehen.

⌦ **GS-A_4348 Verbot der Erneuerung von Zertifikaten**

Die gematik Root-CA und ein TSP-X.509 nonQES DÜRFEN NICHT Zertifikate erneuern.⌫

5.7 Zertifizierung nach Schlüsselerneuerung

⌦ **GS-A_4215 Bedingungen für eine Zertifizierung nach Schlüsselerneuerung**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN Bedingungen beschreiben, unter welchen Umständen ein neu erzeugtes Schlüsselpaar zusammen mit den bisherigen Nutzerdaten zertifiziert wird. Mögliche Voraussetzungen sind:
a) Zertifikatsrücknahme aufgrund einer Schlüsselkompromittierung,
b) Ablauf des bestehenden Zertifikats,
c) Ablauf des Schlüssels, oder der Schlüsselparameter.⌫

Keine Vorgaben bestehen für die Abschnitte

- Autorisierung von Zertifikatsanträgen für Schlüsselerneuerungen
- Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen
- Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats
- Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen
- Veröffentlichung von Zertifikaten für Schlüsselerneuerungen
- Benachrichtigung anderer Zertifikatsnehmer über die Ausgabe eines Nachfolgezertifikats

5.8 Zertifikatsänderung

5.8.1 Bedingungen für eine Zertifikatsänderung

⌦ **GS-A_4216 Bedingungen für eine Zertifikatsänderung**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN Bedingungen beschreiben, unter welchen Umständen eine Zertifikatsänderung durchgeführt wird.⌫

5.8.2 Autorisierung einer Zertifikatsänderung

⌦ **GS-A_4217 Autorisierung einer Zertifikatsänderung**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass ausschließlich der Zertifikatsnehmer und von dem Zertifikatsnehmer autorisierte Personen eine Zertifikatsänderung beantragen können. ⌫

5.8.3 Bearbeitung eines Antrags auf Zertifikatsänderung

Keine Vorgaben

5.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Siehe Abschnitt 5.3.5.

5.8.5 Verhalten für die Annahme einer Zertifikatsänderung

Siehe Abschnitt 5.3.4.

5.8.6 Veröffentlichung der Zertifikatsänderung

Keine Vorgaben

5.8.7 Benachrichtigung anderer Zertifikatsnutzer über die Ausgabe eines neuen Zertifikats

Keine Vorgaben

5.9 Sperrung und Suspendierung von Zertifikaten

Suspendierungen (vorübergehende Sperrungen) von Zertifikaten werden für Endanwenderzertifikate der Typen AUT, ENC, AUTN und ENCV auf der eGK auf Grundlage des Bestandsschutzes vorgesehen. Für das optional auf der eGK befindliche QES-Zertifikat ist eine Suspendierung/Desuspendierung nicht möglich (siehe auch [gemKPT_PKI_TIP# 2.9.1]).

5.9.1 Bedingungen für eine Sperrung

⌦ **GS-A_4218 Beschreibung der Bedingungen für die Sperrung eines Anwenderzertifikats**

Der TSP-X.509 nonQES MUSS Bedingungen beschreiben, unter welchen Umständen eine Sperrung eines Anwenderzertifikates durchgeführt wird. ⌫

⌦ **GS-A_4219 Sperrung von Anwenderzertifikaten**

Ein TSP-X.509 nonQES MUSS für die von ihm herausgegebenen Anwenderzertifikate Sperraufträge umsetzen, unter Anwendung der Berechtigungen gemäß Tab_PKI_305 sowie nach Authentifizierung und Berechtigungsprüfung der beauftragenden Person oder Organisationseinheit.⌫

Tabelle 1: Tab_PKI_305 Übersicht der PKI-spezifischen Sperrgründe

	Zertifikate der Kartenarten						
Sperrberechtigte Stellen *)	eGK	HBA nonQES	SMC-B LEI	SMC-B ORG	SMC-B KTR	gSMC-K	FD, ZD
LE		1a	1a				
med. Institution			1a				
Hersteller						1b	
Anbieter **)							1b, 3
Herausgebende LEO **)		2,5	2,5	2			
Zertifikatsnehmende LEO				1a			
GKV-Spitzenverband **)				2	2		
KTR **)	1a, 2			1a	1a		
gematik		3	3	3	3	3	3

1a) Jederzeit ohne Angabe von Gründen

1b) Eventgetriggert im Rahmen eines definierten Incident-Prozesses mit den zuständigen und betroffenen Parteien

2) Wegfall oder Entzug geforderter Eigenschaften des Antragstellers gemäß Ausgabepolicy

3) Wegfall oder Entzug geforderter Eigenschaften des TSP gemäß gematik-Zulassung

5) Wegfall oder Entzug geforderter Eigenschaften des VDA/TSP gemäß Sektor-Zulassung

*) Berechtigung für organisatorische Sperrungen gilt nur für den jeweiligen Herausgeber der

Zertifikate

**) In herausgeberspezifischen Policies können weitere Sperrgründe definiert sein.

Die Bedingungen für die Suspendierung/Desuspendierung von Anwenderzertifikaten der Typen AUT, ENC, AUTN und ENCV auf der eGK sind im Abschnitt 5.9.13 beschrieben.

Die maximale Dauer von Suspendierungen ist aus Abschnitt 5.9.16 zu entnehmen.

⌦ **GS-A_4221 Anzeige der Kompromittierung des privaten Signaturschlüssels**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die Kompromittierung ihres privaten Signaturschlüssels der gematik unverzüglich anzeigen.⌫

⌦ **GS-A_4222 Beschreibung der Bedingungen für die Sperrung des Zertifikat eines TSP-X.509 nonQES**

Die gematik Root-CA MUSS Bedingungen beschreiben, unter welchen Umständen eine Sperrung des Zertifikats eines TSP-X.509 nonQES durchgeführt wird. ⌫

⌦ **GS-A_4223 Obligatorische Gründe für die Sperrung des Zertifikats eines TSP-X.509 nonQES durch die gematik Root-CA**

Die gematik Root-CA MUSS das Zertifikat eines TSP-X.509 nonQES sperren, wenn
a) nach dem Wirksamwerden der Kündigung des Vertrages durch eine der Vertragsparteien die Deaktivierung des zugehörigen privaten Schlüssels nicht gewährleistet werden kann,
b) der TSP-X.509 nonQES die Sperrung seines Zertifikats beantragt, c) der geheime Signaturerstellungsschlüssel nicht mehr verfügbar ist oder kompromittiert wurde,
d) das Zertifikat des TSP-X.509 nonQES Angaben enthält, die nicht oder nicht mehr gültig sind,
e) erhebliche Schwächen (nach Einschätzung des BSI) eines verwendeten Kryptoalgorithmus samt zugehörigem Schlüssel bekannt werden oder
f) erhebliche Schwächen (nach Einschätzung des BSI) der eingesetzten Hard- oder Software bekannt werden.⌫

⌦ **GS-A_4349 Obligatorische Gründe für die Sperrung eines selbst signierten Zertifikats eines TSP-X.509 nonQES**

Ein TSP-X.509 nonQES MUSS ein selbst signiertes Zertifikat der eigenen CA sperren, wenn
a) nach dem Wirksamwerden der Kündigung des Vertrages durch eine der Vertragsparteien die Deaktivierung des zugehörigen privaten Schlüssels nicht gewährleistet werden kann,
b) der geheime Signaturerstellungsschlüssel nicht mehr verfügbar ist oder kompromittiert wurde,
c) das Zertifikat des TSP-X.509 nonQES Angaben enthält, die nicht oder nicht mehr gültig sind,
d) erhebliche Schwächen (nach Einschätzung des BSI) eines verwendeten Kryptoalgorithmus samt zugehörigem Schlüssel bekannt werden oder
e) erhebliche Schwächen (nach Einschätzung des BSI) der eingesetzten Hard- oder Software bekannt werden.⌫

GS-A_4224 Optionale Gründe für die Sperrung des Zertifikats eines TSP-X.509 nonQES

Die gematik Root-CA KANN das Zertifikat eines TSP-X.509 nonQES sperren, wenn der TSP-X.509 nonQES seinen vertraglichen Verpflichtungen in wesentlichen Punkten nicht nachkommt.

5.9.2 Autorisierung der Sperrung eines Endanwenderzertifikats

GS-A_4225 Festlegung eines Sperrberechtigten für Endanwenderzertifikate

Der TSP-X.509 nonQES MUSS in seinem CPS beschreiben, wer Sperrberechtigter ist und sicherstellen, dass nur Sperrberechtigte eine Sperrung von Endanwenderzertifikaten vornehmen dürfen.

Grundsätzlich sind immer der Zertifikatsnehmer und der ausstellende TSP-X.509 nonQES Sperrberechtigte.

5.9.3 Verfahren für einen Sperrantrag

GS-A_4226 Verfahren für einen Sperrantrag

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN ein Verfahren für einen Sperrantrag definieren und dokumentieren, welches folgende Schritte umfasst:
(a) Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN den Sperrantragsteller hinreichend identifizieren und seine Sperrberechtigung entsprechend dem CPS der gematik Root-CA bzw. des TSP-X.509 nonQES legitimieren.
(b) Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN den Sperrantragsteller auf die Konsequenzen einer Sperrung hinweisen.
(c) Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN den Zertifikatsnehmer über die Sperrung seines Zertifikats informieren.

5.9.4 Fristen für einen Sperrantrag

GS-A_4227 Dokumentation der Fristen für einen Sperrantrag

Die gematik Root-CA und ein TSP-X.509 nonQES SOLLEN Fristen für einen Sperrantrag gegenüber dem Zertifikatsnehmer dokumentieren.

5.9.5 Fristen/Zeitspanne für die Bearbeitung des Sperrantrags

GS-A_4228 Unverzügliche Bearbeitung eines Sperrantrags

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN eine Zertifikatssperrung nach Antragstellung zu den allgemeinen Geschäftszeiten unverzüglich durchführen.

5.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

⌦ **GS-A_4229 Methoden zum Prüfen von Sperrinformationen**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die verfügbaren Methoden zum Prüfen von Sperrinformationen definieren, die den Konformitätskriterien der gematik entsprechen.⌫

5.9.7 Aktualisierung und Veröffentlichung von Sperrlisten (CRL)

Die CRL für VPN-Zugangsdienstzertifikate wird mindestens einmal täglich aktualisiert und unmittelbar darauf im Internet zum Download bereitgestellt.

5.9.8 Gültigkeitsdauer von Sperrlisten (CRL)

CRL für VPN-Zugangsdienstzertifikate der TI werden mit einer Gültigkeitsdauer von 7 Tagen ab Erstellungszeitpunkt ausgestellt.

5.9.9 Online-Verfügbarkeit von Sperrinformationen

⌦ **GS-A_4230 Gewährleistung der Online-Verfügbarkeit von Sperrinformationen**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN Sperrinformationen online zur Verfügung stellen und die Verfügbarkeit dieser Online-Dienstleistung im Certification Practice Statement dokumentieren.⌫

5.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen

⌦ **GS-A_4231 Anforderungen zur Online-Prüfung von Sperrinformationen**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN gegenüber den Zertifikatsnutzern eine Beschreibung des Nutzens und der Notwendigkeit einer Online-Prüfung abgeben.⌫

5.9.11 Andere Formen zur Anzeige von Sperrinformationen

⌦ **GS-A_4232 Informationspflicht der gematik Root-CA bei Sperrung der Zertifikats eines TSP-X.509 nonQES**

Die gematik Root-CA MUSS sicherstellen, dass die gematik unverzüglich über die Sperrung des Zertifikats eines TSP-X.509 nonQES informiert wird.⌫

Die gematik informiert dann die anderen TSP-X.509 nonQES (Teilnehmer der TSL) und veranlasst die unverzügliche Aktualisierung der TSL. Über weitere Maßnahmen wird im Einzelfall entschieden.

5.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Keine Vorgaben

5.9.13 Bedingungen für eine Suspendierung (Endanwender)

Suspendierung ist in der TI nur für eGK-Zertifikate erlaubt. Siehe dazu auch [gemSpec_PKI#GS-A_4965].

⌦ **GS-A_4233 Zertifikatsuspendierung für Kartenzertifikate**

Der zuständige Kartenherausgeber MUSS Bedingungen beschreiben, unter welchen Umständen und durch wen eine Zertifikatssperrung und ggf. eine Zertifikatssuspendierung durchgeführt wird.⌫

⌦ **GS-A_4234 Zusammenhang zwischen Zertifikatssperrung und -suspendierung**

Ein TSP-X.509 nonQES (eGK) KANN eine Suspendierung anstelle einer Sperrung durch den Sperrberechtigten des Zertifikats einer eGK unterstützen, falls
a) der Versicherte seine eGK verloren hat,
b) die eGK des Versicherten entwendet wurde
und in beiden Fällen eine Wiederbeschaffung der eGK mitsamt Zertifikaten möglich erscheint.⌫

Siehe auch Abschnitt 5.9.15.

5.9.14 Autorisierung für eine Suspendierung

⌦ **GS-A_4235 Festlegung zu Verantwortlichkeit für Suspendierung**

Der TSP-X.509 nonQES (eGK) MUSS, falls er Zertifikatssuspendierung unterstützt, in seinem CPS festlegen, dass nur Sperrberechtigte eine Suspendierung vornehmen dürfen. Grundsätzlich sind immer der Zertifikatsnehmer und der ausstellende TSP-X.509 nonQES Sperrberechtigte.⌫

5.9.15 Verfahren für Anträge auf Suspendierung

⌦ **GS-A_4236 Verfahren für Anträge auf Suspendierung**

Der TSP-X.509 nonQES (eGK) MUSS, falls er Zertifikatssuspendierung unterstützt, in seinem CPS Verfahren für Anträge auf Suspendierung definieren; dies umfasst,
a) dass der Antragsteller durch den TSP-X.509 nonQES hinreichend identifiziert werden und seine Berechtigung zur Suspendierung legitimieren muss,
b) dass der TSP-X.509 nonQES den Antragsteller auf die Konsequenzen einer Suspendierung hinweisen muss und
c) dass der Zertifikatsnehmer über die Suspendierung seines Zertifikats informiert wird.⌫

5.9.16 Begrenzungen für die Dauer von Suspendierungen (Endanwender)

⌦ **GS-A_4237 Festlegung zu maximaler Dauer von Suspendierungen**

Ein TSP-X.509 nonQES (eGK) MUSS, falls er Zertifikatssuspendierung unterstützt, für Zertifikate der eGK eine durch die Kartenherausgeber frei wählbare, gemeinsame Festlegung der maximalen Dauer einer Suspendierung bis zu maximal 14 Tagen unterstützen.⌫

Die maximale Dauer von Suspendierungen ist auf 14 Tagen begrenzt. Ist das suspendierte Zertifikat nicht innerhalb dieser Frist wieder aktiviert worden (Desuspendierung), wird es automatisch gesperrt.

5.10 Statusabfragedienst für Zertifikate

5.10.1 Funktionsweise des Statusabfragedienstes

GS-A_4238 Funktionsbeschreibung des Statusabfragedienstes

Ein TSP-X.509 nonQES MUSS die Funktionsweise des Statusabfragedienstes im Certification Practice Statement beschreiben, welcher den Konformitätskriterien der gematik für OCSP-Responder entspricht.

5.10.2 Verfügbarkeit des Statusabfragedienstes

Die Anforderungen an die Verfügbarkeit und Performance des Statusabfragedienstes eines TSP-X.509 nonQES werden in [gemSpec_Perf] beschrieben.

5.10.3 Optionale Leistungen

Keine Vorgaben

5.11 Kündigung durch den Zertifikatsnehmer

GS-A_4241 Sperrung von Zertifikaten bei Kündigung durch den Zertifikatsnehmer

Der TSP-X.509 nonQES MUSS im Fall einer Kündigung durch den Zertifikatsnehmer die Sperrung des Zertifikates am Ende der Kündigungsfrist durchführen.

5.12 Schlüsselhinterlegung und Wiederherstellung

5.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater CA-Schlüssel

GS-A_5075 Schlüsselbackup bei der gematik

Der Anbieter der gematik Root-CA MUSS im Rahmen des mit dem BSI im Kontext CVC-Root-CA abgestimmten Konzepts "Verfahren zur Sicherung der CVC-Root-CA" die im Konzept definierten Mitwirkungspflichten erfüllen. Er muss im Rahmen des Konzeptes das für das Erzeugen von X.509-Sub-CA-Zertifikaten verwendete Schlüsselpaar für die Übergabe an die gematik exportieren.

GS-A_4242 Dokumentationspflicht für Prozesse der Schlüsselhinterlegung

Im Fall einer Schlüsselhinterlegung von Root- bzw. CA-Schlüsseln MÜSSEN die gematik Root-CA und ein TSP-X.509 nonQES die Prozesse der Schlüsselhinterlegung, die dem betreiberspezifischen Sicherheitskonzept und dem aktuellen Stand der Technik entsprechen, dokumentieren.

GS-A_4396 Speicherung hinterlegter Root- und CA-Schlüssel

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN für die Schlüsselhinterlegung von Root- bzw. CA-Schlüsseln ein geeignetes HSM verwenden.

Anforderungen an Standards und Sicherheitsmaßnahmen für kryptographische Module sind im Abschnitt 7.2.1 enthalten.

5.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Keine Vorgaben

5.13 Grundlagen für die Sicherheit der Zertifikatserstellung

5.13.1 Technische Vorgaben

Die technischen Vorgaben für die Erstellung von Zertifikaten wurden in dieser Version des Dokuments in den Abschnitt 7.1.1 verschoben.

5.13.2 Organisatorische Vorgaben

GS-A_4245 Anzeige von Änderung an der Gesellschafterstruktur des Betreibers

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN jede wesentliche Änderung an ihrer Gesellschafterstruktur und jede Änderung an der Gesellschaftsform unverzüglich der gematik anzeigen.

GS-A_4246 Bereitstellung aktueller Liste registrierter TSP

Die gematik Root-CA MUSS zu jedem Zeitpunkt über eine aktuelle Liste der bei ihm registrierten TSP-X.509 nonQES verfügen und diese Liste initial und nach jeder erfolgten Änderung der gematik zur Verfügung stellen.

GS-A_4247 Obligatorische Vorgaben für das Rollenkonzept

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN das Rollenkonzept der übergeordneten Certificate Policy umsetzen und die operative Umsetzung der Vorgaben im Rahmen ihres betreiberspezifischen Sicherheitskonzepts darlegen.

GS-A_4248 Bereitstellung der Protokollierungsdaten

Auf Antrag MÜSSEN die gematik Root-CA und ein TSP-X.509 nonQES der gematik Einblick in die revisionssichere Protokollierung der Zertifikatserzeugung im Kontext der TI gewähren.⌫

5.13.3 Betriebliche Vorgaben

⌦ **GS-A_4249 Standort für Backup-HSM**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN das Backup-HSM an einem sicheren Ort außerhalb des primären Standorts aufbewahren.⌫

⌦ **GS-A_4250 Verwendung des Backup-HSM gemäß Vier-Augen-Prinzip**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN in ihrem betreiberspezifischen Sicherheitskonzept beschreiben, wie sichergestellt wird, dass ein Zugriff auf das Backup-HSM und sein Freischalten im Rahmen des Einbringens in das eigentliche Produktivsystem nur unter Wahrung des Vier-Augen-Prinzips möglich ist. ⌫

⌦ **GS-A_4251 Backup-Konzept**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN für die im Rahmen des Betriebs benötigte Hardware, Software und den Datenbestand ein Backup-Konzept erstellen und umsetzen. ⌫

⌦ **GS-A_5123 Verfahrensbeschreibung Datensicherung der gematik Root-CA**

Die gematik Root-CA MUSS eine Verfahrensbeschreibung zur Datensicherung des gematik-Root-CA-Schlüsselpaars erstellen und mit der gematik abstimmen. Die Verfahrensbeschreibung beinhaltet mindestens die folgenden Punkte:

Beschreibung des zu sichernden Schlüsselmaterials

Erzeugung

Speicherung

Lagerung

(Wieder-) Einbringung

Organisatorische Maßnahmen

Beteiligte Rollen

Übergabe des Schlüsselmaterials zur Datensicherung bei der gematik ⌫

⌦ **GS-A_4252 Besetzung von Rollen und Informationspflichten**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN eine Rollenzuordnung nach den Vorgaben der übergreifenden Certificate Policy derart umsetzen, dass zu jeder der relevanten Rollen mindestens ein verantwortlicher Mitarbeiter sowie ein Stellvertreter benannt werden und die Rollenzuordnung initial und fortlaufend bei Änderungen der gematik mitgeteilt wird. ⌫

Siehe Kapitel 6.2.1 und 6.2.2.

GS-A_4253 Durchgängige Verfügbarkeit spezifischer Rollen

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN eine Rollenzuordnung derart umsetzen, dass zu jedem Zeitpunkt der festgelegten Betriebszeit für jede der relevanten Rollen mindestens ein für diese Rolle verantwortlicher Mitarbeiter bzw. sein Stellvertreter kurzfristig erreichbar sind. ⌫

Siehe Kapitel 6.2.1 und 6.2.2.

GS-A_4254 Rollenzuordnung unter Wahrung der Vier-Augen-Prinzips

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN bei der Zuordnung von Rollen zu Personen gewährleisten, dass eine einzelne Person nicht zwei miteinander unverträgliche Rollen ausübt und somit Zugriffe auf das HSM unter Umgehung des Vier-Augen-Prinzips für diese einzelne Person ermöglicht werden.⌫

Siehe Kapitel 6.2.2.

GS-A_4255 Nutzung des HSM im kontrollierten Bereich

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass das zu realisierende System einschließlich der HSM in einem kontrollierten Bereich der Betriebsstätte untergebracht ist und dass der Zugang zu diesem Bereich nur für berechtigte Personen möglich ist.⌫

Die Definition der Sicherheitsbereiche erfolgt gemäß [gemSpec_SiBetrUmg#2].

GS-A_4256 Zugang zu Systemen für die Zertifikatserzeugung

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN im Rahmen der Zugangskontrolle gewährleisten, dass den Mitarbeitern der gematik bzw. durch die gematik beauftragten Personen nach Ankündigung (ggf. in Begleitung eines Mitarbeiters des Betreibers der gematik Root-CA oder des TSP-X.509 nonQES) Zugang zu den für die Zertifikatserzeugung im Kontext der TI-relevanten Systemen gewährt wird und genaue Regelungen (Vorlaufzeit für die Ankündigung, Mitteilung der berechtigten Personen) festlegen. ⌫

6 Allgemeine Sicherheitsmaßnahmen

⌦ **GS-A_4259 Vorgaben für die informationstechnische Trennung sicherheitskritischer Bestandteile der Systemumgebung**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherheitskritische Bestandteile der Systemumgebung – wie z. B. die technischen Einrichtungen der Registrierungsstelle - informationstechnisch trennen. Falls eine Onlineverbindung zu den sicherheitskritischen Bestandteilen der Systemumgebung besteht, muss durch technische Maßnahmen sichergestellt werden, dass Zugriffe auf sicherheitskritische Systembestandteile unterbunden werden. ⌫

⌦ **GS-A_4260 Manipulationsschutz veröffentlichter Daten**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass die Internetseite zur Bereitstellung der öffentlichen Schlüssel sowie der Fileserver für den Download der Dateien vor Manipulationen entsprechend dem BSI-Grundschutz-Baustein B 5.4 "Webserver" geschützt wird.⌫

⌦ **GS-A_4261 Vorgaben zur Betriebsumgebung für sicherheitskritische Bestandteile des Systems**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass sicherheitskritische Bestandteile des Systems in einem kontrollierten Bereich betrieben werden.⌫

⌦ **GS-A_4262 Gewährleistung des Zugangs zur Betriebsstätte**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass Vertreter der gematik auf Antrag uneingeschränkten Zugang zu den Teilen der Betriebsstätte haben, die für den Betrieb im Kontext der TI relevant sind.⌫

⌦ **GS-A_5084 Zugang zu HSM-Systemen im Vier-Augen-Prinzip**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass alle Zugriffe auf das HSM und die direkt zur Administration des HSM verwendeten IT-Systeme im Vier-Augen-Prinzip erfolgen.⌫

Die Anforderungen an die Erstellung des betreiberspezifischen Sicherheitskonzepts und eines betreiberspezifischen Betriebskonzepts werden in [gemSpec_SiBetrUmg#B1] beschrieben. Diese Richtlinie enthält keine darüber hinaus gehenden Anforderungen.

6.1 Bauliche Sicherheitsmaßnahmen

Die Anforderungen an bauliche Sicherheitsmaßnahmen sind in [gemSpec_SiBetrUmg#2] enthalten. Diese Spezifikation enthält keine darüber hinausgehenden Anforderungen.

Diese Richtlinie enthält keine Anforderungen für die Abschnitte:

- Lage und Gebäude
- Zugang
- Strom, Heizung und Klimaanlage

- Wassergefährdung
- Brandschutz
- Lager und Archiv
- Müllbeseitigung

Anforderungen an die Notfallvorsorge werden in [gemSpec_SiBetrUmg#B1.5] beschrieben. Diese Richtlinie enthält keine darüber hinaus gehenden Anforderungen.

6.2 Verfahrensvorschriften

Der Betrieb der Zertifizierungsstelle bzw. Registrierungsstelle erfolgt anhand von dokumentierten Verfahrensvorschriften im Rahmen des Sicherheitskonzepts.

6.2.1 Rollenkonzept

Um einen ordnungsgemäßen und revisionssicheren Betrieb einer Zertifizierungsstelle zu gewährleisten, ist u. a. eine entsprechende Aufgabenverteilung und Funktionstrennung vorzunehmen.

⌦ **GS-A_4263 Rollenunterscheidung im organisatorischen Konzept**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN in ihrem Organisationskonzept mindestens die Rollen gemäß der Tabelle Tab_PKI_301 unterscheiden.

Tabelle 2 Tab_PKI_301 – Beschreibung der einzelnen Rollen

Rolle	Funktion	Kürzel
Registrierungsdienst	Schnittstelle zum Zertifikatsnehmer. Annahme von Zertifikatsanträgen, Prüfung der notwendigen Unterlagen und Annahme von Sperranträgen	
Teilnehmerservice	Entgegennahme von Zertifikatsanträgen und Sperranträgen Identifizierung, Authentifizierung und Prüfung der Autorisierung der Zertifikatsnehmer Verifikation der Dokumente Belehrung der Zertifikatsnehmer	TS
Registrator	Prüfung des Zertifikatsantrags hinsichtlich Vollständigkeit und Korrektheit Archivierung von Dokumenten falls erforderlich Freigabe, Übermittlung von Zertifikatsanträgen und Sperr-/Widerrufsanträgen an die zuständige Zertifizierungsstelle	RG
Zertifizierung	Ausstellen von Zertifikaten und Widerrufslisten, Erzeugung und Verwahrung der TSP-Schlüssel	

Rolle	Funktion	Kürzel
TSP-Mitarbeiter	verantwortlich für die Anwendung und Lagerung von elektronischen Datenträgern, auf denen die privaten Schlüssel der Zertifizierungsstelle gespeichert sind	CAO1
PIN-Geber	Kenntnis eines Geheimnisses (z. B. Passwort) zur Anwendung der privaten Schlüssel der Zertifizierungsstelle	CAO2
Systembetreuung	Administration der IT-Systeme und des täglichen Betriebs (Backups usw.)	
System- und Netzwerk-Administrator	Installation, Konfiguration, Administration und Wartung der IT- und Kommunikationssysteme. vollständige Kontrolle über die eingesetzte Hard- und Software, jedoch kein Zugriff auf und keine Kenntnis von kryptographischen Schlüsseln und deren Passwörtern für Zertifizierungsprozess, Zertifikats- und Sperrmanagement ausschließliche Kenntnis der Boot- und Administrator-Passwörter der Systeme	SA
Systemoperator	Betreuung der Anwendungen (Datensicherung und -wiederherstellung, Web-Server, Zertifikats- und Sperrmanagement)	SO
Überwachung des Betriebs	keine Funktion im operativen Betrieb, zuständig für die Durchsetzung der in der CP, dem CPS und dem Sicherheitskonzept festgelegten Grundsätze	
Revision	Durchführung der betriebsinternen und externen Audits, Überwachung und Einhaltung der Datenschutzbestimmungen	R
Sicherheitsbeauftragter	Definition und Einhaltung der Sicherheitsbestimmungen Überprüfung der Mitarbeiter Vergabe von Berechtigungen Ansprechpartner für sicherheitsrelevante Fragen	ISO
Datenschutzbeauftragter	Definition und Einhaltung der Datenschutzbestimmungen Ansprechpartner für datenschutzrelevante Fragen	DSO

⌫

In der Tabelle 2 sind in vier Gruppen die sicherheitsrelevanten Rollen definiert, die im Rahmen des Zertifizierungsprozesses erforderlich sind. Jeder Rolle sind dabei bestimmte Tätigkeiten, Verantwortungen und Kompetenzen zugeordnet. Die vollständige oder teilweise Kenntnis von PINs und Passwörtern und die Erlaubnis zum Zugriff auf bestimmte Teile der Betriebsinfrastruktur (z. B. Sicherheitsbereiche, Tresore, abgesicherte Betriebsräume) werden anhand der Rollen vorgenommen.

Ein Mitarbeiter kann auch in mehr als einer Rolle auftreten. Dabei ist jedoch zu beachten, dass es Rollenunverträglichkeiten (Abschnitt 6.2.3) gibt. Ebenso ist es möglich, dass Funktionen einer Rolle auf mehrere Mitarbeiter mit dieser Rolle verteilt werden.

⌦ **GS-A_4264 Mitteilungspflicht für Zuordnung der Rollen**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die Belegung der Rollen mit ihren benannten Mitarbeitern der gematik mitteilen.⌫

6.2.2 Involvierte Mitarbeiter pro Arbeitsschritt

In der Tabelle 3 werden die sicherheitsrelevanten Tätigkeiten beschrieben und den entsprechenden Rollen zugeordnet. Aus der Tabelle ist ebenso zu entnehmen, für welche Tätigkeiten das Vier-Augen-Prinzip eingehalten werden muss**.**

⌦ **GS-A_4265 Obligatorische Rollen für sicherheitsrelevante Tätigkeiten**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die Rollenzuordnung sicherheitsrelevanter Tätigkeiten gemäß dem Vier-Augen-Prinzip auf der Grundlage der Tabelle Tab_PKI_302 umsetzen.

Tabelle 3 Tab_PKI_302 - Involvierte Mitarbeiter pro Arbeitsschritt

Tätigkeit	Rollen	Vier-Augen-Prinzip	Erläuterung
Annahme von Zertifikatsanträgen	TS		
Identifizierung und Authentifizierung von Zertifikatsnehmern	TS		
Prüfung der Autorisierung von Zertifikatsnehmern	TS		
Verifikation von Dokumenten	TS		
Belehrung von Zertifikatsnehmern	TS		
Prüfung des DN	TS		
Generierung von Autorisierungs-informationen	TS		kann auch durch CAO1 wahrgenommen werden
Annahme und Prüfung von Sperranträgen	TS		TS nimmt den Sperrauftrag entgegen und prüft Autorisierungsinformation
Prüfung der Anträge hinsichtlich Vollständigkeit und Korrektheit	RG		
Archivierung von Dokumenten sofern erforderlich	RG		
Freigabe und Übermittlung von Zertifikats- und Sperranträgen an die zuständige Zertifizierungsstelle	RG		

Tätigkeit	Rollen	Vier-Augen-Prinzip	Erläuterung
Erzeugung von Schlüsselpaaren für selbst betriebene TSPs, RAs und Datenverarbeitungssysteme	CAO1, CAO2	x	
Starten von Prozessen zur Erzeugung von Schlüsselpaaren für Zertifikatsnehmer und PIN-Briefen	CAO1, CAO2	x	
Zertifizierung; Starten von Prozessen zum Ausstellen von Zertifikaten und Widerrufslisten	CAO1, CAO2	x	
Übertragen von Zertifikats-Requests zum Zertifizierungsrechner	CAO1		
Veröffentlichen von Zertifikaten und Widerrufslisten	CAO1		
Schlüsselhinterlegung von privaten TSP-Schlüsseln für selbst betriebene TSPs	CAO1, CAO2	x	
Kenntnis von Boot- und Administrator-Passwörtern	SA		
Starten und Stoppen von Prozessen (z. B. Web-Server, Datensicherung)	SO		
Datensicherung	SO, CAO1		CAO1 ermöglicht physikalischen Zugang
Austausch von Soft- und Hardware-Komponenten für			
Zertifizierung	SA, CAO1	x	
andere Systeme	SA, CAO1		CAO1 ermöglicht physikalischen Zugang
Wiedereinspielung von Datensicherungen			
Zertifizierung	SA, CAO1	x	
andere Systeme	SA, CAO1		CAO1 ermöglicht physikalischen Zugang
Überprüfung von Protokolldateien	SA, R		Wird regelmäßig durch SA wahrgenommen, im Rahmen eines Audits durch R
Audit	R		

Tätigkeit	Rollen	Vier-Augen-Prinzip	Erläuterung
Vergabe von physikalischen Berechtigungen	ISO		
Technische Vergabe von Berechtigungen	SA, ISO	x	ISO überwacht
Fortschreibung des Betriebs- bzw. Sicherheitskonzepts	ISO		
Fortschreibung des Betriebs- bzw. Datenschutzkonzepts	DSO		

⌫

6.2.3 Rollenausschlüsse

⌦ **GS-A_4266 Ausschluss von Rollenzuordnungen**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN bei der Aufteilung der Rollen auf Mitarbeiter gemäß der Tabelle Tab_PKI_303 sicherstellen, dass einer Person keine miteinander unverträglichen Rollen zugewiesen werden. In der Tabelle ist aufgeführt, welche Rollen miteinander unverträglich sind.

Tabelle 4 Tab_PKI_303 - Rollenausschlüsse

Rolle	Unverträglich mit
R - Revision	TS, RG, CAO1, CAO2, SA, SO
ISO - Sicherheitsbeauftragter	TS, RG, CAO1, CAO2, SA, SO
TS - Teilnehmerservice	R, ISO, SA, SO
RG - Registrator	R, ISO, SA, SO
SA - Systemadministrator	R, ISO, TS, RG, CAO1
SO - Systemoperator	R, ISO, TS, RG, CAO1
CAO1 TSP-Mitarbeiter	R, ISO, CAO2, SA, SO
CAO2 PIN-Geber	R, ISO, CAO1

⌫

⌦ **GS-A_4267 Rollenaufteilung auf Personengruppen**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN für ihren Betrieb die folgende Aufteilung der Rollen auf Personengruppen gemäß der Tabelle Tab_PKI_304 wählen.

Tabelle 5 Tab_PKI_304 - Rollenaufteilung auf Personengruppen

Personengruppe	Aufgabengebiet	Rollen
1	Überwachung des Betriebs	R, ISO
2	Registrierungsdienst (Teilnehmerservice)	TS
3	Registrierungsdienst (Registrator) und Zertifizierung	RG, CAO1
4	Systembetreuung und PIN-Geber für Zertifizierung	CAO2, SA, SO

⌫

6.3 Personalkontrolle

6.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit

Die Anforderungen an die Qualifikation und Zuverlässigkeit der Mitarbeiter der gematik Root-CA oder eines TSP-X.509 nonQES sind in denjenigen von [gemSpec_SiBetrUmg#2] enthalten. Diese Richtlinie enthält keine darüber hinaus gehenden Anforderungen.

6.3.2 Methoden zur Überprüfung der Rahmenbedingungen

Siehe Abschnitt 6.3.1.

6.3.3 Anforderungen an Schulungen

Siehe Abschnitt 6.3.1.

6.3.4 Häufigkeit von Schulungen und Belehrungen

Siehe Abschnitt 6.3.1.

6.3.5 Häufigkeit und Folge von Job-Rotation

Keine Vorgaben

6.3.6 Maßnahmen bei unerlaubten Handlungen

Die Anforderungen an das Vorgehen beim Missbrauch von Berechtigungen durch Mitarbeiter der gematik Root-CA oder eines TSP-X.509 nonQES werden in [gemSpec_SiBetrUmg#2] beschrieben. Diese Richtlinie enthält keine darüber hinaus gehenden Anforderungen.

6.3.7 Anforderungen an freie Mitarbeiter

⌦ **GS-A_4268 Anforderungen an den Einsatz freier Mitarbeiter**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass freie Mitarbeiter die gleichen Sicherheitsanforderungen erfüllen, wie festangestellte Mitarbeiter.⌫

6.3.8 Einsicht in Dokumente für Mitarbeiter

⌦ **GS-A_4269 Einsicht in Dokumente für Mitarbeiter**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass seine Mitarbeiter in
a) die Zertifizierungsrichtlinie,
b) die Erklärung zum Zertifikatsbetrieb (CPS),
c) das betreiberspezifische Betriebskonzept,
d) das Rollenkonzept,
e) das betreiberspezifische Sicherheitskonzept,
f) die Prozessbeschreibungen und Formulare für den regulären Betrieb,
g) die Verfahrensanweisungen für den Notfall,
h) die Dokumentation der IT-Systeme,
i) die Bedienungsanleitungen für die eingesetzte Software und
j) die Datenschutzerklärung Einsicht erhalten.⌫

6.4 Überwachungsmaßnahmen

6.4.1 Arten von aufgezeichneten Ereignissen

⌦ **GS-A_4270 Aufzeichnung von technischen Ereignissen**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die folgenden technischen Ereignisse protokollieren:
a) Bootvorgänge der Hardware,
b) Installation und Konfiguration von Software,
c) Fehlgeschlagene Login-Versuche,
d) Durchführung von Änderungen an Zugriffsrechten,
e) Erstellung von Schlüsseln,
f) Erstellung von Zertifikaten,
g) Änderung von Sperrinformationen im OCSP-Dienst ⌫

⌦ **GS-A_4271 Aufzeichnung von organisatorischen Ereignissen**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die folgenden organisatorischen Ereignisse protokollieren:
a) Vergabe und Entzug von Berechtigungen,
b) Bearbeitung von Zertifikatsanträgen,
c) Auslieferung von Zertifikaten,
d) Veröffentlichung von Zertifikaten,
e) Sperrung von Zertifikaten,
f) Änderungen des betreiberspezifischen Betriebshandbuches und der korrespondierenden Richtlinien,
g) Änderungen an Rollendefinitionen,
h) Änderungen an Prozessbeschreibungen,
i) Wechsel von Verantwortlichkeiten,
j) Ausscheiden von Mitarbeitern ⌫

- Siehe auch Abschnitt 6.5.4.

6.4.2 Häufigkeit der Bearbeitung der Aufzeichnungen

Die Anforderungen an die Sicherheitsstatusprüfung der gematik Root-CA oder eines TSP-X.509 nonQES bei irregulären Ereignissen werden in [gemSpec_SiBetrUmg#2] beschrieben. Diese Richtlinie enthält keine darüber hinaus gehenden Anforderungen.

6.4.3 Aufbewahrungszeit von Aufzeichnungen

⌦ **GS-A_4272 Aufbewahrungsfrist für sicherheitsrelevante Protokolldaten**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherheitsrelevante Protokolldaten mindestens entsprechend den gesetzlichen Regelungen aufbewahren. Die Aufbewahrungsdauer von Protokolldaten bezüglich des Schlüssel- und Zertifikatmanagements entspricht jeweils mindestens der Gültigkeitsdauer aller Zertifikate der gematik Root-CA oder des TSP-X.509 nonQES zuzüglich eines Jahres.⌫

6.4.4 Schutz der Aufzeichnungen

⌦ **GS-A_4273 Schutz vor Zugriff, Löschung und Manipulation elektronischer Protokolldaten**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass elektronische Protokolldaten trotz privilegierter Berechtigungen der System- und Netzadministratoren gegen unberechtigten Zugriff, Löschung und Manipulation dauerhaft geschützt werden.⌫

Durch die regelmäßige Speicherung nach Kapitel 6.4.5 können solche Daten dauerhaft geschützt werden.

6.4.5 Datensicherung der Aufzeichnungen

Die Anforderungen an die Datensicherung der gematik Root-CA oder eines TSP-X.509 nonQES sind in [gemSpec_SiBetrUmg#2] enthalten. Diese Richtlinie enthält keine darüber hinaus gehenden Anforderungen.

6.4.6 Speicherung der Aufzeichnungen (intern/extern)

Keine Vorgaben

6.4.7 Benachrichtigung der Ereignisauslöser

Die Anforderungen an Benachrichtigung von Akteuren, die ein sicherheitsrelevantes Ereignis bei der gematik Root-CA oder einem TSP-X.509 nonQES auslösen, werden in [gemSpec_SiBetrUmg#2] beschrieben. Diese Richtlinie enthält keine darüber hinaus gehenden Anforderungen.

6.4.8 Verwundbarkeitsabschätzungen

Die Anforderungen an Sicherheitsüberprüfungen bei der gematik Root-CA oder einem TSP-X.509 nonQES, werden in [gemSpec_SiBetrUmg#2] beschrieben. Diese Richtlinie enthält keine darüber hinaus gehenden Anforderungen.

6.5 Archivierung von Aufzeichnungen

6.5.1 Arten von archivierten Aufzeichnungen

⌦ **GS-A_4274 Archivierung von für den Zertifizierungsprozess relevanten Daten**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass folgende Daten, die für den Zertifizierungsprozess relevant sind, archiviert werden:
a) Zertifikatsanträge, diese enthalten persönliche Daten des Zertifikatsnehmers,
b) alle von dem TSP ausgestellten Zertifikate,
c) Widerrufsanträge/Widerruflisten.⌫

Siehe Abschnitt 6.4.5.

6.5.2 Aufbewahrungsfristen für archivierte Daten

Siehe Abschnitt 6.4.3.

6.5.3 Sicherung des Archivs

Siehe Abschnitt 6.4.5.

6.5.4 Datensicherung des Archivs

Siehe Abschnitt 6.4.5.

6.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen

Keine Vorgaben

6.5.6 Archivierung (intern/extern)

Siehe Abschnitt 6.4.5.

6.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen

Siehe Abschnitt 6.4.5.

6.6 Schlüsselwechsel beim TSP

GS-A_4275 Dokumentationspflicht für Prozesse zum Schlüsselwechsel

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass der Schlüsselwechsel anhand dokumentierter Prozesse erfolgt. ⌫

6.7 Kompromittierung und Geschäftsweiterführung

GS-A_4276 Aktionen und Verantwortlichkeit im Rahmen der Notfallplanung

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN im Rahmen der Notfallplanung gewährleisten, dass
a) für den Fall einer Kompromittierung oder eines Desasters Prozesse dokumentiert werden und
b) die Bewertung der Sicherheitslage durch den Sicherheitsbeauftragten vollzogen wird.⌫

Die Anforderungen an Notfallpläne und die Aufrechterhaltung des Regelbetriebs nach dem Eintreten eines Notfalls bei der gematik Root-CA oder einem TSP-X.509 nonQES werden in [gemSpec_SiBetrUmg#2] beschrieben. Diese Richtlinie enthält keine darüber hinaus gehenden Anforderungen.

Diese Richtlinie enthält keine Anforderungen für die Abschnitte:

- Rechnerressourcen-, Software- und/oder Datenkompromittierung
- Kompromittierung des privaten Schlüssels
- Möglichkeiten zur Geschäftsweiterführung nach einer Kompromittierung

6.8 Schließung eines TSP oder einer Registrierungsstelle

GS-A_4277 Anzeigepflicht bei Beendigung der Zertifizierungsdienstleistungen

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die Beendigung ihrer Zertifizierungsdienstleistungen im Kontext der TI als Prozess dokumentieren und die Beendigung der Zertifizierungsdienstleistungen der gematik anzeigen. ⌫

Die zu treffenden Maßnahmen und einzuhaltenden Pflichten sind in den folgenden Anforderungen beschrieben.

GS-A_4278 Maßnahmen zur Einstellung des Zertifizierungsbetriebs

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN folgende Aktivitäten bei der Einstellung von Zertifizierungsdienstleistungen im Kontext der TI durchführen:
a) Informieren aller Zertifikatsnehmer, Registrierungsstellen und betroffenen Organisationen mindestens drei Monate vor Einstellung der Tätigkeit,
b) Widerruf aller Zertifikate, sofern ein Statusauskunftsdienst per OCSP nicht aufrechterhalten werden kann,
c) sichere Zerstörung der privaten CA-Schlüssel.⌫

GS-A_4279 Fortbestand von Archiven und die Abrufmöglichkeit einer vollständigen Widerrufsliste

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN den Fortbestand der Archive und die Abrufmöglichkeit einer vollständigen Dokumentation der widerrufenen Zertifikate für den zugesicherten Aufbewahrungszeitraum sicherstellen.⌫

⌦ **GS-A_4280 Fristen bei Einstellung des Zertifizierungsbetriebs für die gematik Root-CA**

Die gematik Root-CA MUSS eine Ankündigungsfrist von sechs Monaten bei der Einstellung des Zertifizierungsbetriebs im Kontext der TI einhalten. ⌫

⌦ **GS-A_4281 Fristen bei der Einstellung des Zertifizierungsbetriebs für einen TSP-X.509 nonQES**

Ein TSP-X.509 nonQES MUSS eine Ankündigungsfrist ohne Angabe von Gründen von drei Monaten bei der Einstellung des Zertifizierungsbetriebs im Kontext der TI einhalten.⌫

⌦ **GS-A_4282 Erforderliche Form bei Einstellung des Zertifizierungsbetriebs**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die Einstellung des Zertifizierungsbetriebs schriftlich gegenüber der gematik ankündigen.⌫

⌦ **GS-A_4283 Gültigkeit der Zertifikate bei Einstellung des Zertifizierungsbetriebs**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die Gültigkeitsdauer aller neu erstellten Zertifikate nach erfolgter Ankündigung der Einstellung des Zertifizierungsbetriebs auf den Zeitpunkt der Einstellung des Zertifizierungsbetriebs beschränken. ⌫

⌦ **GS-A_4907 Beendigungsunterstützung bei Schließung eines TSP**

Bei Beendigung der Zertifizierungsdienstleistungen durch die gematik Root-CA oder eines TSP-X.509 nonQES MUSS die gematik die Dokumentation zu den ausgegebenen Zertifikaten und deren Status übernehmen sowie die Weiterführung des Betriebs sicherstellen, sofern diese Dienstleistungen nicht durch einen anderen Anbieter übernommen werden. ⌫

7 Technische Sicherheitsmaßnahmen

7.1 Erzeugung und Installation von Schlüsselpaaren

7.1.1 Erzeugung von Schlüsselpaaren und Zertifikaten

GS-A_4284 Beachtung des betreiberspezifischen Sicherheitskonzepts bei der Erzeugung von Schlüsselpaaren

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass die technischen Sicherheitsmaßnahmen zur Erzeugung und Installation von Schlüsselpaaren die Rahmenbedingungen des eigenen, betreiberspezifischen Sicherheitskonzeptes erfüllen und sich am aktuellen Stand der Technik orientieren.

GS-A_4285 Sicherheitsniveau bei der Generierung von Signaturschlüsseln

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN kryptographisch hinreichend sichere Signaturschlüssel in einem von einer allgemein anerkannten Evaluierungsstelle geprüften Hardwaresicherheitsmodul (HSM) oder alternativ in einer Chipkarte mit vergleichbarer geforderter Zertifizierungstiefe erzeugen.

Die für HSM geforderte Zertifizierungstiefe wird im Abschnitt 7.2.1 definiert.

GS-A_4287 Sichere Aufbewahrung des privaten Schlüssels einer CA

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass der private Schlüssel des Schlüsselpaars zum Signieren von Zertifikaten das HSM nicht im Klartext verlässt.

GS-A_4288 Verwendung eines Backup-HSM zum Im-/Export von privaten Schlüsseln

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN ein Backup-HSM zum sicheren Export bzw. Import von privaten Schlüsseln verwenden, wobei zu beachten ist, dass
a) primäres HSM und Backup-HSM die gleichen Sicherheitsanforderungen erfüllen,
b) zwischen primärem HSM und Backup-HSM MUSS ein kryptographisch gesicherter Transportkanal hergestellt wird, um den privaten Schlüssel der CA aus dem primären HSM sicher zu exportieren und in das Backup-HSM zu importieren.

GS-A_4289 Unterstützung des sicheren Löschen von Schlüsseln durch HSM

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass alle eingesetzten HSM eine Funktion unterstützen, mit der ein vorhandenes Schlüsselpaar innerhalb des HSM sicher gelöscht werden kann, wobei der sichere Löschvorgang durch ein Überschreiben mit einem vorgegebenen Wert oder durch das interne dauerhafte Sperren aller Zugriffe auf den Schlüssel realisiert werden kann.

⌦ **GS-A_4290 Generieren und Löschen von Schlüsselpaaren gemäß Vier-Augen-Prinzip**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass das Generieren eines neuen Schlüsselpaares und das Löschen eines Schlüsselpaares nur nach erfolgreicher, gemeinsamer Authentisierung zweier hierfür autorisierter Nutzer (Vier-Augen-Prinzip) durch das Verifizieren einer PIN oder ein gleichwertiges Verfahren ausführbar sind.⌫

⌦ **GS-A_4291 Berechnungen mit dem privaten Schlüssel gemäß Vier-Augen-Prinzip**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass alle kryptographischen Berechnungen mit dem privaten Schlüssel für das Erstellen eines Zertifikats innerhalb des HSM erfolgen, wobei das HSM diese Berechnungen nur nach erfolgreicher, gemeinsamer Authentisierung zweier hierfür autorisierter Nutzer (Vier-Augen-Prinzip) durch das Verifizieren einer PIN oder ein gleichartiges Verfahren durchführen darf.⌫

⌦ **GS-A_4292 Protokollierung der HSM-Nutzung**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass die Nutzung des HSM revisionssicher protokolliert wird, insbesondere welche Rolle/Person zu welchem Zeitpunkt für welche Funktion das HSM genutzt hat und für welche Profile das HSM konfiguriert ist.⌫

⌦ **GS-A_4294 Bedienung des Schlüsselgenerierungssystems**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass die Schlüsselgenerierung unter Beachtung des Vier-Augen-Prinzips erfolgt. ⌫

⌦ **GS-A_4295 Berücksichtigung des aktuellen Erkenntnisstands bei der Generierung von Schlüsseln**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass bei der Generierung von Schlüsseln jeweils der aktuelle Stand der Technik berücksichtigt wird. ⌫

⌦ **GS-A_4296 Anlass für den Wechsel von Schlüsselpaaren**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die verwendeten Schlüsselpaare auswechseln, wenn
a) organisatorische Regelungen der gematik dies erfordern,
b) die maximale Verwendungsdauer für ein Schlüsselpaar erreicht wurde und
c) wenn ein aktuell verwendetes Schlüsselpaar kompromittiert wurde.⌫

Anforderungen an Schlüsselverwaltungen finden sich in [gemSpec_Sich_DS#3.7], Vorgaben zur maximalen Verwendungsdauer von Schlüsseln in [gemSpec_Krypt#2].

⌦ **GS-A_4297 Behandlung einer Kompromittierung eines Schlüsselpaares**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN eine Abschätzung der Auswirkungen einer Kompromittierung eines Schlüsselpaares sowie die daraus folgenden Notfallprozesse in einer Risikoanalyse und Notfallplanung in einem gesonderten Dokument behandeln.⌫

⌦ **GS-A_4298 Vorgehen beim Schlüsselwechsel**

Kommt es bei der gematik Root-CA oder einem TSP-X.509 nonQES zu einem Wechsel des Schlüsselpaares für das Ausstellen von Zertifikaten, KANN dieser Fall logisch behandelt werden wie das Aufsetzen einer neuen gematik Root-CA oder eines neuen TSP-X.509 nonQES.⌫

⌦ **GS-A_4299 Zulassung/Abnahme und Aufnahme in den Vertrauensraum der TI**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN den öffentlichen Schlüssel ihres neuen Schlüsselpaares im Rahmen des Zulassungs- oder Abnahmeverfahrens in die TSL aufnehmen lassen. ⌫

⌦ **GS-A_4300 Zweckbindung von Schlüsselpaaren**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass das im Rahmen der Zulassung oder Abnahme registrierte Schlüsselpaar für die Zertifikatserzeugung verwendet wird.⌫

7.1.2 Übergabe privater Schlüssel an Zertifikatsnehmer

⌦ **GS-A_4302 Transportmedium für die Übergabe des privaten Schlüssels eines Schlüsselpaars**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN private Schlüssel an Zertifikatsnehmer ausschließlich unter Verwendung einer evaluierten Chipkarte transportieren.⌫

Dies geschieht bspw. bei der Kartenherausgabe.

7.1.3 Übergabe öffentlicher Schlüssel an Zertifikatsherausgeber

Keine Vorgaben

7.1.4 Lieferung öffentlicher Schlüssel des TSP an Zertifikatsnutzer

Die Bereitstellung der CA- und Signer-Zertifikate in der TI erfolgt gemäß Vorgaben aus [gemSpec_TSL].

Die Bereitstellung der CA- und Signer-Zertifikate im Internet erfolgt gemäß Vorgaben aus [gemSpec_PKI] und [gemSpec_X.509_TSP].

7.1.5 Schlüssellängen

Die eingesetzten kryptographischen Algorithmen und deren Schlüssellängen orientieren sich an den Veröffentlichungen der Bundesnetzagentur [ALGCAT] und [gemSpec_Krypt].

7.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle

Keine Vorgaben

7.1.7 Schlüsselverwendungen

GS-A_4303 Festlegung der Schlüsselverwendung (*keyUsage)*

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN bei der Erzeugung von Zertifikaten die Schlüsselverwendung angeben, die den Verwendungszweck des Schlüssels und Beschränkungen im entsprechenden X.509 v3 Feld (*keyUsage)* festlegt.

7.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

GS-A_4304 Speicherung und Anwendung von privaten Schlüsseln

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN gewährleisten, dass
a) der private Schlüssel für die Erzeugung von Zertifikaten nicht auslesbar auf einem Hardware-Sicherheitsmodul (HSM) gespeichert wird und
(b) nach Verwendung des privaten Schlüssels keine Artefakte der Bearbeitung im System hinterlassen werden, die eine Kompromittierung des Schlüssels ermöglichen oder erleichtern.

GS-A_4305 Ordnungsgemäße Sicherung des privaten Schlüssels

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die ordnungsgemäße Sicherung des privaten Schlüssels nach dem aktuellen Stand der Technik gewährleisten und die Anforderungen an kryptographische Module im Rahmen ihres betreiberspezifischen Sicherheitskonzeptes definieren.

GS-A_4306 Verwendung von privaten Schlüsseln

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN gewährleisten, dass
a) alle kryptographischen Berechnungen mit einem privaten Schlüssel einer CA intern in einem Hardware-Sicherheitsmodul (HSM) durchgeführt werden und
b) private Schlüssel der gematik Root-CA oder des TSP-X.509 nonQES nicht im Klartext aus dem HSM exportiert werden.

GS-A_4307 Vorgaben an HSM-Funktionalität

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN Hardware-Sicherheitsmodule (HSM) einsetzen, die mindestens Funktionen
a) zur Generierung eines neuen Schlüsselpaares,
b) zur Aktivierung eines Schlüsselpaares,
c) zum (kryptographisch abgesicherten) Import eines privaten Schlüssels,
d) zum (physikalischen) Löschen eines Schlüsselpaares,
e) zur m von n Aktivierung und
f) zum Erstellen eines Zertifikats mit interaktiv einzugebenden Zertifikatsdaten beinhalten.

GS-A_4308 Speicherung und Auswahl von Schlüsselpaaren im HSM

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN ein Hardware-Sicherheitsmodul (HSM) einsetzen, das mehrere Schlüsselpaare speichern kann und über eine Funktion zur Aktivierung eines einzelnen, spezifischen Schlüsselpaares verfügt, dass nach erfolgter Auswahl zur Erzeugung von Zertifikaten verwendet wird.

7.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

⌦ **GS-A_4309 Verwendung von zertifizierten kryptographischen Modulen**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass die verwendeten kryptographischen Module eine anerkannte standardisierte Zertifizierung besitzen.⌫

⌦ **GS-A_4310 Vorgaben an die Prüftiefe der Evaluierung eines HSM**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN für alle eingesetzten Hardware-Sicherheitsmodule (HSM) sicherstellen, dass diese nach einer der folgenden Kombinationen aus Evaluierungsschema und Prüftiefe oder einem äquivalenten Zertifizierungsstandard evaluiert wurden:
a) FIPS 140-2 Level 3,
(b) CC EAL4+ mit Prüfung gegen hohes Angriffspotenzial oder
(c) ITSEC E3 der Stärke „hoch“. ⌫

7.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m)

Siehe Abschnitt 6.2.2.

7.2.3 Hinterlegung privater Schlüssel

⌦ **GS-A_4311 Hinterlegung des privaten Signaturschlüssels**

Die gematik Root-CA und ein TSP-X.509 nonQES DÜRFEN NICHT den privaten Schlüssel des Schlüsselpaars, das für die Signaturerstellung verwendet wird, bei Dritten hinterlegen.⌫

Aufgrund der besonderen Kritikalität der gematik Root-CA ist eine Hinterlegung des privaten Schlüssels bei der gematik umgesetzt, siehe Anforderung GS-A_5075, Abschnitt 5.12.1. Die gematik gilt dabei nicht als „Dritter“ gemäß Anforderung GS-A_4311.

7.2.4 Sicherung privater Schlüssel

Die Anforderungen an die Sicherung privater Schlüssel bei der gematik Root-CA oder einem TSP-X.509 nonQES werden als Teil der Anforderungen an die Schlüsselverwaltung in [gemSpec_Sich_DS#3.7] beschrieben. Diese Richtlinie enthält keine darüber hinaus gehenden Anforderungen.

7.2.5 Archivierung privater Schlüssel

Siehe Abschnitt 7.2.4.

7.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen

Siehe Abschnitt 7.2.4.

7.2.7 Speicherung privater Schlüssel in kryptographischen Modulen

Siehe Abschnitt 7.2.4.

7.2.8 Aktivierung privater Schlüssel

⌦ **GS-A_4312 Aktivierung privater Schlüssel**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass der private Schlüssel eines Schlüsselpaares, das zur Erstellung von Signaturen verwendet wird, durch ein Passwort bzw. eine PIN geschützt wird. ⌫

Bei privaten Schlüsseln der gematik Root-CA oder eines TSP-X.509 nonQES ist eine Aktivierung nur nach dem Vier-Augen-Prinzip durch die Rollen „CAO1“ und „CAO2“ möglich.

7.2.9 Deaktivierung privater Schlüssel

⌦ **GS-A_4313 Deaktivierung privater Schlüssel**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass der private Schlüssel eines Schlüsselpaares, das zur Erstellung von Signaturen verwendet wird, nach Beendigung der Erstellung einer Signatur oder eines Signaturstapels deaktiviert werden und durch technische Maßnahmen ausgeschlossen wird, dass eine weitere Verwendung ohne erneute Eingabe des Passwortes oder der PIN erfolgen kann. ⌫

7.2.10 Vernichtung privater Schlüssel

Verantwortlich für die Vernichtung sind die Rollen „ISO“ und „CAO1“.

Die Anforderungen an die Vernichtung privater Schlüssel bei der gematik Root-CA oder einem TSP-X.509 nonQES siehe unter Kap 7.1.1.

7.2.11 Beurteilung kryptographischer Module

Siehe Abschnitt 7.2.1.

7.3 Andere Aspekte des Managements von Schlüsselpaaren

7.3.1 Archivierung öffentlicher Schlüssel

Die Anforderungen an Archivierung öffentlicher Schlüssel bei der gematik Root-CA oder einem TSP-X.509 nonQES werden in [gemSpec_Sich_DS#3.7] beschrieben. Diese Richtlinie enthält keine darüber hinaus gehenden Anforderungen.

7.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Die Nutzungsdauer von Zertifikaten soll nach [gemSpec_Krypt] auf maximal 5 Jahre beschränkt werden. Diese Vorgabe wird für die Endbenutzerzertifikate umgesetzt.

Für die CA-Zertifikate der gematik Root-CA wird davon abweichend eine maximale Gültigkeitsdauer von 10 Jahren in dieser Richtlinie festgelegt, da eine kürzere Gültigkeit die maximale Gültigkeitsdauer der in dem Gültigkeitszeitraum des CA-Zertifikats ausge-

stellten CA-Zertifikate für TSP-X.509 nonQES und Endbenutzerzertifikate der TSP-X.509 nonQES einschränken kann.

Für die CA-Zertifikate der TSP-X.509 nonQES wird davon abweichend eine maximale Gültigkeitsdauer von 8 Jahren festgelegt, da eine kürzere Gültigkeit die maximale Gültigkeitsdauer der in dem Gültigkeitszeitraum des CA-Zertifikats des TSP-X.509 nonQES ausgestellten Endbenutzerzertifikate einschränken kann.

Die Gültigkeit von CA- und Endbenutzerzertifikaten kann zudem durch die Verwendung einer TSL während des laufenden Betriebs weiter eingeschränkt werden, da die TSL in diskreten Zeitabständen aktualisiert und veröffentlicht wird. Hierdurch kann ein zu einer kürzeren Gültigkeitsdauer der Zertifikate äquivalentes Sicherheitsniveau erreicht werden.

Die entsprechenden Rahmenbedingungen zur TSL werden in [gemKPT_PKI_TIP#6.3] beschrieben.

⌦ **GS-A_4350 Maximale Gültigkeitsdauer des Zertifikats der gematik Root-CA**

Die gematik Root-CA MUSS die Gültigkeitsdauer des eigenen CA-Zertifikats auf maximal zehn Jahre ab der Erstellung des Zertifikats begrenzen.⌫

⌦ **GS-A_4351 Maximale Gültigkeitsdauer des Zertifikats eines TSP-X.509 nonQES bei Erzeugung durch die gematik Root-CA**

Die gematik Root-CA MUSS die Gültigkeitsdauer der CA-Zertifikate der TSP-X.509 nonQES auf maximal acht Jahre ab der Erstellung des Zertifikats begrenzen. Die Realisierung kürzerer Gültigkeitsdauern MUSS dabei auch möglich sein.⌫

⌦ **GS-A_5468 Planmäßige Schlüsselerneuerung der gematik Root-CA**

Die gematik Root-CA MUSS spätestens 2 Jahre nach der Erstellung des letzten gematik Root-CA-Zertifikates eine planmäßige Schlüsselerneuerung durchführen.⌫

Hinweis: *Diese Schlüsselerneuerung beinhaltet auch die Erstellung eines neuen Root-Zertifikats. Der Schlüsselerneuerungs-Zeitraum von 2 Jahren ergibt sich aus der Differenz zwischen der maximalen Gültigkeitsdauer des Root-CA-Zertifikats (10 Jahre) und der maximalen Gültigkeitsdauer der von ihr ausgestellten Zertifikate (8 Jahre).*

⌦ **GS-A_5469 Verwendung des neuesten Schlüssels der gematik Root-CA**

Die gematik Root-CA MUSS bei der Ausstellung von Sub-CA-Zertifikaten das neueste Schlüsselpaar der jeweils festgelegten Schlüsselgeneration verwenden. ⌫

Hinweis: *Eine reguläre Schlüsselerneuerung, bei dem Schlüsselalgorithmus und Schlüssellänge unverändert bleiben, wird als Wechsel der Schlüsselversion bezeichnet. Durch veränderte kryptographische Vorgaben kann der Wechsel des Schlüsselalgorithmus oder Schlüssellänge notwendig werden. Dies wird als Wechsel der Schlüsselgeneration bezeichnet. In der TI werden in einer Übergangszeit mehrere Schlüsselgenerationen (RSA und ECDSA) unterstützt. Siehe dazu auch [gemKPT_PKI_TIP#TIP1-A_6878].*

⌦ **GS-A_4355 Maximale Gültigkeitsdauer des Zertifikats eines TSP-X.509 nonQES bei Erzeugung durch den TSP-X.509 nonQES**

Der TSP-X.509 nonQES (eGK) MUSS die Gültigkeitsdauer eines selbst erzeugten (nicht durch ein Zertifikat der gematik Root-CA bestätigten) CA-Zertifikats auf maximal acht Jahre ab der Erstellung des Zertifikats begrenzen. Die Realisierung kürzerer Gültigkeitsdauern MUSS dabei auch möglich sein.⌫

⌦ **GS-A_4352 Maximale Gültigkeitsdauer eines Endbenutzerzertifikats**

Ein TSP-X.509 nonQES MUSS die Gültigkeitsdauer der Endbenutzerzertifikate auf maximal fünf Jahre ab der Erstellung des Zertifikats begrenzen, wobei eine

Erweiterung der Gültigkeitsdauer des Endbenutzerzertifikats bis zum Ende des Monats, in welchem die fünf Jahre enden, zulässig ist. Die Realisierung kürzerer Gültigkeitsdauern MUSS dabei auch möglich sein.⌫

7.4 Aktivierungsdaten

Die Anforderungen an die Zuverlässigkeit von Kennwörtern und PINs werden in [gemSpec_SiBetrUmg#2] beschrieben. Diese Richtlinie enthält keine darüber hinaus gehenden Anforderungen.

7.4.1 Aktivierungsdaten

⌦ **GS-A_4314 Sichere Übermittlung von Aktivierungsdaten**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN geeignete Prozesse für die sichere Übermittlung von Aktivierungsdaten definieren.⌫

7.4.2 Schutz von Aktivierungsdaten

Siehe Abschnitt 6.2.1 und 6.2.2.

7.4.3 Andere Aspekte von Aktivierungsdaten

Keine Vorgaben

7.5 Sicherheitsmaßnahmen in den Rechneranlagen

7.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

⌦ **GS-A_4315 Konformität zum betreiberspezifischen Sicherheitskonzept**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass alle Systemkomponenten der PKI konform zu den Sicherheitsanforderungen ihres betreiberspezifischen Sicherheitskonzepts betrieben werden.⌫

⌦ **GS-A_4316 Härtung von Betriebssystemen**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN sicherstellen, dass alle sicherheitsrelevanten, technischen Abläufe innerhalb der PKI auf Basis gehärteter Betriebssysteme nach [BSI_2005#B3] ausgeführt werden.⌫

⌦ **GS-A_4317 Obligatorische Sicherheitsmaßnahmen**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN Maßnahmen für die Zugriffskontrolle, die Benutzerauthentisierung und die Intrusion Detection umsetzen.⌫

7.5.2 Beurteilung der Systemsicherheit

⌦ **GS-A_4318 Maßnahmen zur Beurteilung der Systemsicherheit**

Die gematik Root-CA und ein TSP-X.509 nonQES SOLLEN periodisch interne Audits zur Beurteilung der Systemsicherheit durchführen. ⌫

7.6 Technische Maßnahmen während des Lebenszyklus

7.6.1 Sicherheitsmaßnahmen bei der Entwicklung

⌦ **GS-A_4319 Prüfpflichten vor Nutzung neuer Software im Wirkbetrieb**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN neue oder geänderte Software in eigener Verantwortung prüfen und abnehmen oder freigeben, bevor diese im Wirkbetrieb eingesetzt wird. ⌫

7.6.2 Sicherheitsmaßnahmen beim Systemmanagement

Die Anforderungen an Sicherheitsmaßnahmen beim Systemmanagement ergeben sich aus den Inhalten des betreiberspezifischen Sicherheitskonzepts. Die Vorgaben für die Erstellung des betreiberspezifischen Sicherheitskonzepts sind in [gemSpec_SiBetr-Umg#AnhB] beschrieben. Diese Richtlinie enthält keine darüber hinaus gehenden Anforderungen.

7.6.3 Sicherheitsmaßnahmen während der Lebenszyklus

Keine Vorgaben

7.7 Sicherheitsmaßnahmen für Netze

Siehe Abschnitt 7.6.2.

7.8 Zeitstempel

Keine Vorgaben.

8 Format der Zertifikate

Die Festlegung der Datenformate und Zertifikatsprofile erfolgt in [gemSpec_PKI].

9 Weitere finanzielle und rechtliche Angelegenheiten

9.1 Gebühren

Keine Vorgaben

9.2 Finanzielle Zuständigkeiten

9.2.1 Versicherungsdeckung

Keine Vorgaben

9.2.2 Andere Posten

Keine Vorgaben

9.2.3 Versicherung oder Gewährleistung für Endnutzer

GS-A_4321 Bereitstellung eines Certificate Policy Disclosure Statements

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN eine Versicherung oder Gewährleistung für Endnutzer in Form eines Certificate Policy Disclosure Statements als Teil ihres Certification Practice Statements veröffentlichen.

Dieses dient als rechtsverbindliche Zusicherung der gematik Root-CA oder eines TSP-X.509 nonQES gegenüber dem auf das Zertifikat vertrauenden Dritten.

GS-A_4322 Zusicherung der Dienstqualität

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN als Teilnehmer des Vertrauensraums der TI versichern, dass ihre über den Anbieter des TSL-Dienstes bereitgestellten Dienste geeignet sind, Echtheit der Herkunft und Unversehrtheit des Inhaltes zu gewährleisten.

9.3 Vertraulichkeitsgrad von Geschäftsdaten

GS-A_4323 Wahrung der Vertraulichkeit

Die gematik Root-CA und ein TSP-X.509 nonQES als Teilnehmer des Vertrauensraums der TI MÜSSEN garantieren, dass die Vertraulichkeit ihnen zugänglicher, vertraulicher Dokumente Dritter gewahrt bleibt, sofern dies gefordert wird.

Diese Regelung kann beispielsweise die Certification Practice Statements (CPS) der gematik Root-CA oder eines TSP-X.509 nonQES betreffen. Regelungen zur Definition und zum Umgang mit vertraulichen Dokumenten sind jeweils bilateral zwischen den betroffenen Anbietern der gematik Root-CA oder eines TSP-X.509 nonQES abzustimmen.

9.3.1 Definition von vertraulichen Informationen

Vertrauliche Informationen sind Informationen, die lediglich im Rahmen der gematik TSL zugänglich gemacht werden und nicht für die Öffentlichkeit bestimmt sind.

9.3.2 Informationen, die nicht zu den vertraulichen Informationen gehören

Sperrlisten gehören nicht zu den vertraulichen Informationen und werden nicht in Basis-TI (Stufe 1) unterstützt.

9.3.3 Zuständigkeiten für den Schutz vertraulicher Informationen

Siehe Abschnitt 9.3.

9.4 Datenschutz von Personendaten

Die Anforderungen an den Schutz personenbezogener Daten werden in [gemSpec_Sich_DS] beschrieben. Diese Richtlinie enthält keine darüber hinaus gehenden Anforderungen.

Dies gilt auch für die Abschnitte:

- Datenschutzkonzept
- Personenbezogene Daten
- Nicht personenbezogene Daten
- Zuständigkeiten für den Datenschutz
- Hinweis und Einwilligung zur Nutzung persönlicher Daten
- Auskunft gemäß rechtlicher oder staatlicher Vorschriften
- Andere Bedingungen für Auskünfte

9.5 Geistiges Eigentumsrecht

Keine Vorgaben

9.6 Zusicherungen und Garantien

⌦ **GS-A_4324 Zusicherung der Dienstgüte**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN eine gleichbleibend hohe Güte in Datenqualität, Organisation und technischen Diensten zusichern. ⌫

⌦ **GS-A_4325 Zweckbindung von Zertifikaten**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN Nutzer von Zertifikaten im Kontext der TI darüber informieren, dass Zertifikate der TI nicht für sachfremde Zwecke genutzt werden dürfen. ⌫

Diese Richtlinie enthält keine Anforderungen für die Abschnitte:

- Zusicherungen und Garantien
- Zusicherungen und Garantien der Registrierungsstelle
- Zusicherungen und Garantien der Zertifikatsnehmer
- Zusicherungen und Garantien anderer PKI-Teilnehmer

9.7 Haftungsausschlüsse

Keine Vorgaben

9.8 Haftungsbeschränkungen

Keine Vorgaben

9.9 Schadenersatz

Keine Vorgaben

9.10 Gültigkeitsdauer und Beendigung

⌦ **GS-A_4326 Dokumentationspflicht für beschränkte Gültigkeit**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN die Zeiträume dokumentieren, in denen Dokumente, Prozesse oder Infrastrukturkomponenten genutzt werden können, sofern diese eine zeitlich beschränkte Gültigkeit aufweisen.⌫

Diese Richtlinie enthält keine darüber hinaus gehenden Anforderungen für die Abschnitte:

- Gültigkeitsdauer
- Beendigung

- Auswirkung der Beendigung und Weiterbestehen

9.11 Individuelle Absprachen zwischen Vertragspartnern

Keine Vorgaben

9.12 Ergänzungen

⌦ **GS-A_4327 Transparenz für Nachträge zum Certificate Policy Statement**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN Nachträge zum Certification Practice Statement (CPS) schriftlich ergänzen oder bei elektronischer Abrufbarkeit so ergänzend hinterlegen, dass sie dem Abrufenden unmittelbar als Ergänzung offensichtlich werden.⌫

⌦ **GS-A_4328 Informationspflicht bei Änderung des CPS**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN Vertragspartner über durchgeführte Änderungen an dem Certification Practice Statement (CPS) informieren.⌫

Diese Richtlinie enthält keine darüber hinausgehenden Anforderungen für die Abschnitte:

- Verfahren für Ergänzungen
- Benachrichtigungsmechanismen und –fristen
- Bedingungen für OID Änderungen

9.13 Verfahren zur Schlichtung von Streitfällen

Keine Vorgaben

9.14 Zugrunde liegendes Recht

Es gelten die für Deutschland relevanten Rechtsnormen.

9.15 Einhaltung geltenden Rechts

⌦ **GS-A_4329 Konformität zum geltenden Recht**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN geltendes Recht einhalten.⌫

9.16 Sonstige Bestimmungen

Diese Richtlinie enthält keine Anforderungen für die Abschnitte

- Vollständigkeitserklärung
- Abgrenzungen
- Vollstreckung (Anwaltsgebühren und Rechtsmittelverzicht)
- Höhere Gewalt
- Andere Bestimmungen

Anhang A – Certificate Policy für Komponentenzertifikate

In den folgenden Abschnitten werden die besonderen Regelungen für die gematik Root-CA und TSP-X.509 nonQES ausgeführt, die gelten, sofern es sich um Herausgeber von Komponentenzertifikaten handelt.

Die Darstellung fokussiert auf die Abweichung, d. h. zusätzliche Anforderungen oder den Entfall von Anforderungen für die Herausgeber von Komponentenzertifikaten. Die Anforderungen in diesem Anhang gelten also ausschließlich im Zusammenhang mit den Festlegungen aus dem Hauptdokument.

Ergänzend zu Abschnitt 5.3.4 gelten folgende Anforderungen bezogen auf die Zuordenbarkeit und Verwendung von Komponentenzertifikaten:

⌦ **GS-A_4330 Einbringung des Komponentenzertifikats**

Der Betreiber einer Produktinstanz oder der Hersteller eines Produkts MUSS das korrekte Einbringen des Komponentenzertifikats in die Produktinstanz sicherstellen. ⌫

⌦ **GS-A_5020 Einbringung des Komponentenzertifikats durch den Kartenherausgeber**

Der Kartenherausgeber MUSS das korrekte Einbringen des X.509-Komponentenzertifikats in die Karte sicherstellen. ⌫

Ergänzend zu Abschnitt 5.5.1 gelten zusätzlich folgende Anforderungen zu den Pflichten eines Antragstellers:

⌦ **GS-A_4331 Sicherstellungspflicht des Antragstellers eines Komponentenzertifikats**

Der Antragsteller MUSS sicherstellen, dass Zertifikatsnehmer den korrekten Umgang mit dem Komponentenzertifikat gewährleisten. Die entsprechenden Verantwortlichkeiten MÜSSEN durch den TSP-X.509 nonQES dokumentiert und dem Betreiber/Hersteller/Herausgeber mitgeteilt werden.⌫

⌦ **GS-A_4332 Dokumentation der Pflichten des Antragstellers eines Komponentenzertifikats**

Ein TSP-X.509 nonQES MUSS die Verantwortlichkeiten eines Antragstellers hinsichtlich des korrekten Umgangs mit den Komponentenzertifikaten durch den Zertifikatsnehmer dokumentieren und dem Antragsteller mitteilen.⌫

Ergänzend zu Abschnitt 5.8.4 gelten zusätzlich folgende Anforderungen hinsichtlich der Informationspflichten eines TSP-X.509 nonQES für Komponentenzertifikate:

⌦ **GS-A_4333 Informationspflicht gegenüber Antragsteller bei Sperrung eines Komponentenzertifikats**

Ein TSP-X.509 nonQES MUSS den Antragsteller informieren, falls ein bereits ausgestelltes Komponentenzertifikat gesperrt wird.⌫

Ergänzend zu Abschnitt 5.9.1 gelten zusätzlich folgende Anforderungen zur Sperrung von Komponentenzertifikaten:

⌦ **GS-A_4335 Keine Sperrung eines Zertifikats für den Produkttyp gSMC-KT**

Der TSP-X.509 nonQES der Komponenten-PKI SOLL NICHT die Sperrung eines Zertifikats unterstützen oder vornehmen, das für den Produkttyp gSMC-KT verwendet wird.
Der TSP-X.509 nonQES der Komponenten-PKI SOLL NICHT für die von ihm ausgestellten X.509-Zertifikate der gSMC-KT Statusinformationen bereitstellen. ⌫

Ergänzend zu Abschnitt 5.9.3 gelten zusätzlich folgende Anforderungen für den Umgang mit Sperranforderungen:

⌦ **GS-A_4336 Sperranträge der gematik für Komponentenzertifikate**

Ein TSP-X.509 nonQES MUSS es der gematik ermöglichen, alle Komponentenzertifikate sperren zu können, für die Statusinformationen bereitgestellt werden.⌫

⌦ **GS-A_4337 Sonderregelung für die Sperrung von Komponentenzertifikaten**

Ein TSP-X.509 nonQES MUSS ein Verfahren dokumentieren, dass die Sperrung von Komponentenzertifikaten regelt, falls
a) die eindeutige Zuordnung eines Zertifikats zu einer Produktinstanz nicht mehr gegeben ist,
b) sich die Verfügungsgewalt über die Produktinstanzen ändert und eine ordnungsgemäße Verwendung der Zertifikate nicht mehr sichergestellt werden kann oder
c) die Zulassung für den Produkttyp oder die Produktinstanz, widerrufen wird, in der das Komponentenzertifikat genutzt wird.⌫

Ergänzend zu Abschnitt 5.9.2 gilt zusätzlich folgende Anforderung hinsichtlich des autorisierten Personenkreises für Sperranforderungen:

⌦ **GS-A_4339 Autorisierung für die Sperrung von Komponentenzertifikaten**

Ein TSP-X.509 nonQES MUSS sicherstellen, dass Sperranträge für Komponentenzertifikate nur dann umgesetzt werden, wenn die Anträge entweder von der gematik, dem jeweiligen Konnektorbetreiber (Leistungserbringer) oder dem jeweiligen Hersteller bzw. Anbieter gestellt werden. ⌫

Ergänzend zu Abschnitt 5.9.4 gilt zusätzlich folgende Anforderung zur Befristung von Sperranträgen:

⌦ **GS-A_4340 Befristung von Sperranträgen für Komponentenzertifikate**

Ein TSP-X.509 nonQES DARF NICHT die Einhaltung von Fristen für die Beantragung einer Sperrung von Komponentenzertifikaten verlangen.⌫

Ergänzend zu Abschnitt 5.10.1 gelten zusätzlich folgende Anforderungen zur Bereitstellung einer Statusprüfung für Komponentenzertifikate:

⌦ **GS-A_4341 Entfall der Verpflichtung für die Bereitstellung einer Statusprüfung bestimmter Komponentenzertifikate**

Ein TSP-X.509 nonQES für gSMC SOLL NICHT einen Dienst zur Statusprüfung für die Komponentenzertifikate der Produkttypen gSMC-KT sowie die Komponentenzertifikate C.AK.AUT und C.SAK.AUT des Produkttyps Konnektor anbieten. ⌫

Ergänzend zu Abschnitt 5.12.1 gilt zusätzlich folgende Anforderung zur Schlüsselhinterlegung:

⌦ **GS-A_4342 Verbot einer Schlüsselhinterlegung für Komponentenzertifikate**

Ein TSP-X.509 nonQES DARF NICHT Schlüssel für Komponentenzertifikate hinterlegen und wiederherstellen.⌫

Ergänzend zu Abschnitt 6.8 gelten zusätzlich folgende Anforderungen zu den Pflichten eines TSP-X.509 nonQES bei Einstellung des Betriebs:

⌦ **GS-A_4343 Unterstützung der Übergabe bei Schließung eines TSP-X.509 nonQES für Komponentenzertifikate**

Ein TSP-X.509 nonQES für Komponentenzertifikate MUSS die Übergabe und Inbetriebnahme eines Statusabfragedienstes bei einem anderen Betreiber unterstützen, falls diese Übergabe aufgrund der Einstellung des Betriebs des TSP-X.509 nonQES erfolgt.⌫

⌦ **GS-A_4344 Sperrung von Komponentenzertifikate bei Schließung eines TSP-X.509 nonQES**

Ein TSP-X.509 nonQES DARF NICHT bei einer Einstellung des eigenen Betriebs die Komponentenzertifikate sperren, falls die für die Statusanfragen notwendigen Daten an einen anderen TSP-X.509 nonQES ordnungsgemäß übergeben wurden.⌫

Ergänzend zu Abschnitt 7.1.1 gilt zusätzlich folgende Anforderung für die Automatisierung von Zertifikatsanträgen:

⌦ **GS-A_4345 Automatisierte Zertifikatsanträge für Komponentenzertifikate**

Der TSP-X.509 nonQES SOLL die Vorgänge für Beantragung von Komponentenzertifikaten automatisieren, z. B. durch die Unterstützung eines signierten PKCS#10-Requests. ⌫

Anhang B – Certificate Policy für Testzertifikate

In diesem Anhang werden die besonderen Regelungen für die Produkttypen gematik Root-CA und TSP-X.509 nonQES ausgeführt, die für die Ausgabe von X.509-Zertifikaten für einen Einsatz in der Referenz- oder Testumgebung anzuwenden sind. Solche Zertifikate werden im Folgenden auch als „Testzertifikate“ bezeichnet. Dementsprechend werden Bezeichnungen weiterer Daten, die ebenfalls für einen Einsatz in der Referenz- oder Testumgebung vorgesehen sind, mit dem Präfix „Test“ versehen (z.B. Testschlüssel, Test-TSL).

Im Unterschied zu X.509-Zertifikaten für den Einsatz in der Produktivumgebung enthalten Testzertifikate Daten von fiktiven Personen bzw. Institutionen. Aufgrund dieser Nicht-Verwendung von Daten realer Personen und Institutionen ist die vorliegende Certificate Policy für Testzertifikate auf die absolut notwendigen Maßnahmen reduziert und entspricht nicht mehr in vollem Maß der üblichen Gliederung einer Certificate Policy gemäß [RFC3647].

B1 – Geltungsbereich

Die CP für Testzertifikate gilt für alle CA- und EE-X.509-Zertifikate der Test- und Referenzumgebungen der TI (siehe auch [gemSpec_PKI#3.2.2]):

- gematik Root-CA nonQES
- TSP-X.509 nonQES

Für diese Produkttypen ist eine von der Produktivumgebung vollständig separate Test-PKI zu implementieren, welche die nachfolgend definierten Anforderungen umsetzen muss.

Zusätzlich gilt diese CP für Testzertifikate auch für solche Zertifikate in den Test- und Referenzumgebungen, mit denen die Funktion der QES-Zertifikate des HBA getestet werden soll (siehe auch [gemSpec_PKI#3.2.3]):

- PseudoQES-CA

B2 – Allgemeine Maßnahmen

B2.1 Rahmen der Policy

⌦ **GS-A_4908 CP-Test, Erfüllung der Certificate Policy für Testzertifikate zur Aufnahme in die Test-TSL**

Die gematik Root-CA, ein TSP-X.509 QES und ein TSP-X.509 nonQES MÜSSEN die Vorgaben der Certificate Policy für Testzertifikate erfüllen, wenn das Testzertifikat (Testausstellerzertifikat der gematik Root-CA bzw. des TSP-X.509 nonQES) in die Test-TSL aufgenommen werden soll.⌫

Der organisatorische Prozess zur Aufnahme des Testausstellerzertifikats in die Test-TSL ist nicht Gegenstand der vorliegenden Certificate Policy für Testzertifikate.

B2.2 Verzeichnisse und Veröffentlichungen

⌦ **GS-A_4909 CP-Test, Erbringung von Verzeichnisdienstleistungen für Testzertifikate**

Die gematik Root-CA, ein TSP-X.509 QES und ein TSP.X.509 nonQES MÜSSEN eine ordnungsgemäße Erbringung der Verzeichnisdienstleistungen für Testzertifikate gewährleisten und sich am aktuellen Stand der Technik orientieren.⌫

⌦ **GS-A_4910 CP-Test, Zugriffskontrolle auf Verzeichnisse für Testzertifikate**

Die gematik Root-CA, ein TSP-X.509 QES und ein TSP-X.509 nonQES MÜSSEN eine geeignete Zugriffskontrolle auf die Verzeichnisse für Testzertifikate gewährleisten.⌫

Vergleiche hierzu auch Kapitel 3.1 und 3.4.

B3 – Identifizierung und Authentifizierung

B3.1 Namensregeln

B3.1.1 Arten von Namen

⌦ **GS-A_4911 CP-Test, Standardkonforme Namensvergabe in Testzertifikaten**

Die gematik Root-CA, ein TSP-X.509 QES und ein TSP-X.509 nonQES MÜSSEN für die Namensvergabe in Testzertifikaten den Standard [X.501] beachten. Die Angabe eines *distinguishedName* im Feld *Subject* ist für die Namensvergabe obligatorisch.⌫

⌦ **GS-A_4912 CP-Test, Format von E-Mail-Adressen in Testzertifikaten**

Ein TSP-X.509 nonQES und ein TSP-X.509 QES SOLLEN E-Mail-Adressen in Testzertifikaten unter der X.509-Extension *subjectAltNames* im Format nach [RFC822] hinterlegen, sofern die Angabe einer E-Mail-Adresse im jeweiligen Profil vorgesehen ist. ⌫

Vergleiche hierzu auch Kapitel 4.1.1.

B3.1.2 Namensform

⌦ **GS-A_4913 CP-Test, Gestaltung der Struktur der Verzeichnisdienste**

Die gematik Root-CA, ein TSP-X.509 QES und ein TSP-X.509 nonQES MÜSSEN die Namensform der jeweiligen Testzertifikate bei der Gestaltung der Struktur der Verzeichnisdienste beachten und sicherstellen, dass der Aufbau des *distinguishedName* im Feld *Subject* und die Struktur des Verzeichnisdienstes zueinander konsistent sind.⌫

Vergleiche hierzu auch Kapitel 4.1.2.

B3.1.3 Aussagekraft von Namen

Generelle Vorgaben an die Namensregeln und Formate sind im Dokument „Spezifikation PKI“ [gemSpec_PKI#4.1] beschrieben.

B3.1.4 Notwendigkeit für aussagefähige und eindeutige Namen

⌦ **GS-A_4914 CP-Test, Eindeutigkeit der Namensform des Zertifikatsnehmers**

Die ausstellende gematik Root-CA, ein ausstellender TSP-X.509 QES und ein ausstellender TSP-X.509 nonQES MÜSSEN bei der Vergabe von Namen für Testzertifikate (Endnutzer- oder Ausstellerzertifikate) die Eindeutigkeit der gewählten *distinguishedName* des Zertifikatsnehmers umsetzen und sicherstellen, dass die Daten spezifikationsgemäß aufbereitet werden.⌫

⌦ **GS-A_4915 CP-Test, Kein Bezug zu Echtdaten von Personen oder Organisationen**

Ein ausstellender TSP-X.509 nonQES und ein ausstellender TSP-X.509 QES MÜSSEN bei der Vergabe von Namen für Testzertifikate (Endnutzer- oder Ausstellerzertifikate) sicherstellen, dass der Name keinen Bezug zu Echtdaten von Personen oder Organisationen hat.⌫

Die Integrität und Vollständigkeit der Daten liegt in der Hoheit der Herausgeber der Testzertifikate.

⌦ **GS-A_4916 CP-Test, Kennzeichnung von personen- bzw. organisationsbezogenen Testzertifikaten**

Ein TSP-X.509 nonQES und ein TSP-X.509 QES MÜSSEN personen- bzw. organisationsbezogene Testzertifikate entsprechend den Zertifikatsprofilen eindeutig als solche kenntlich machen.⌫

⌦ **GS-A_4917 CP-Test, Kennzeichnung von maschinen-, rollenbezogenen oder pseudonymisierten (nicht personenbezogenen) Testzertifikaten**

Die gematik Root-CA und ein TSP-X.509 nonQES MÜSSEN maschinen-, rollenbezogene oder pseudonymisierte (nicht personenbezogene) Testzertifikate als solche kenntlich machen, um Verwechslungsfreiheit zu garantieren.⌫

⌦ **GS-A_4919 CP-Test, Testkennzeichen in Testzertifikaten**

Die gematik Root-CA, ein TSP-X.509 QES und ein TSP-X.509 nonQES MÜSSEN Testzertifikate eindeutig als solche kenntlich machen.⌫

B3.2 Erstmalige Überprüfung der Identität

B3.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

⌦ **GS-A_4920 CP-Test, Prüfung auf den Besitz des privaten Schlüssels bei dem Zertifikatsnehmer**

Die gematik Root-CA und ein TSP-X.509 nonQES KÖNNEN für die Ausgabe von Testzertifikaten auf Prozesse und Vorgaben, die eine Prüfung auf den Besitz des privaten Schlüssels bei dem Zertifikatsnehmer gewährleisten, verzichten.⌫

⌦ **GS-A_4922 CP-Test, Nutzung von Datensätzen mit frei wählbarem Inhalt**

Die gematik Root-CA und ein TSP-X.509 nonQES KÖNNEN zur Benennung von Zertifikatsnehmern von Testzertifikaten Datensätze mit frei wählbarem Inhalt gene-

rieren, sofern diese den Vorgaben der gematik entsprechen und keinen Bezug zu echten Personen oder Organisationen haben.⌫

Der Herausgeber des Zertifikates verantwortet die Korrektheit dieser Daten. Die Vorgaben der gematik an die Benennung von Zertifikatsnehmern sind in [gemSpec_PKI] enthalten.

B4 – Betriebliche Maßnahmen

B4.1 Zertifikatsausgabe

⌦ **GS-A_4923 CP-Test, Veröffentlichung von Testausstellerzertifikaten**

Für die Veröffentlichung von Testzertifikaten in der Test-TSL MUSS die gematik Root-CA die Test-Root-Zertifikate und ein TSP-X.509 nonQES bzw. TSP-X.509 QES die Testausstellerzertifikate der gematik zur Verfügung stellen. ⌫

⌦ **GS-A_4925 CP-Test, Keine Verwendung von Echtdaten**

Die gematik Root-CA, ein TSP-X.509 QES und ein TSP-X.509 nonQES DÜRFEN NICHT Echtdaten zur Ausstellung von Testzertifikaten verwenden.⌫

⌦ **GS-A_4926 CP-Test, Policy von Testzertifikaten**

Die gematik Root-CA und ein TSP-X.509 nonQES SOLLEN bei der Ausgabe von Testzertifikaten unter der Certificate Policy für Testzertifikate als Policy Object Identifier den Object Identifier der gemeinsamen Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL eintragen.⌫

B4.2 Sperrung und Suspendierung von Testzertifikaten (Endanwender)

⌦ **GS-A_4927 CP-Test, Bereitstellung eines Sperrdienstes**

Der TSP-X.509 nonQES und der TSP-X.509 QES MÜSSEN zur Sperrung von Testzertifikaten einen Sperrdienst betreiben. Der TSP-X.509 nonQES und der TSP-X.509 QES MÜSSEN Sperrberechtigte authentisieren, eine Sperrung darf nur durch hierzu berechtigte Personen initiiert werden.⌫

⌦ **GS-A_4928 CP-Test, Suspendierung und Desuspendierung von Testzertifikaten**

Der TSP-X.509 nonQES (eGK) KANN Testzertifikate suspendieren und wieder freischalten sofern Zertifikate dieses Zertifikatstyps auch in der Produktivumgebung suspendiert und wieder freigeschaltet werden können.⌫

B4.3 Statusabfragedienst für Testzertifikate

⌦ **GS-A_4929 CP-Test, Funktionsweise des Statusabfragedienst**

Ein TSP-X.509 nonQES und ein TSP-X.509 QES MÜSSEN den Zertifikatsnutzern Zugriff auf Statusinformationen zu Testzertifikaten in Form eines OCSP-Responders gewähren und die Schnittstelle des Statusabfragedienstes gemäß den technischen Vorgaben der gematik für den Statusabfragedienst von Zertifikaten für den Einsatz in der Produktivumgebung gestalten.⌫

Die Anforderungen an die Schnittstelle des Statusabfragedienstes sind in [gemSpec_PKI#9] enthalten.

⌦ **GS-A_4930 CP-Test, Verfügbarkeit des Statusabfragedienstes**

Im Rahmen des Testvorhabens MÜSSEN ein TSP-X.509 nonQES und ein TSP-X.509 QES sicherstellen, dass eine Vereinbarung hinsichtlich der Verfügbarkeit des Statusabfragedienstes zwischen gematik und TSP-X.509 nonQES bzw. TSP-X.509 QES getroffen wird.⌫

Für die Verfügbarkeit des Statusabfragedienstes für Testzertifikate werden keine übergreifenden Vereinbarungen getroffen.

B5 – Allgemeine Sicherheitsmaßnahmen

Da die Zertifikatsnehmer von Testzertifikaten keine realen Personen oder Organisationen sind, werden keine hohen Sicherheitsanforderungen, wie sie für Zertifikate zum Einsatz in der Produktivumgebung definiert sind, gestellt.

Um reale und aussagekräftige Testergebnisse zu erhalten, sollte sich die Testumgebung an der späteren Produktivumgebung orientieren.

B6 – Technische Sicherheitsmaßnahmen

⌦ **GS-A_4931 CP-Test, Maximale Gültigkeitsdauer von Testzertifikaten**

Die gematik Root-CA, ein TSP-X.509 QES und ein TSP-X.509 nonQES SOLLEN die Gültigkeitsdauer eines ausgestellten Testzertifikats gemäß den Vorgaben an die Gültigkeitsdauer von Zertifikaten, die für den Einsatz in der Produktivumgebung vorgesehen und vom gleichen Typ sind, begrenzen.⌫

B7 – Formate der Zertifikate

⌦ **GS-A_4933 CP-Test, Zertifikatsprofile für Testzertifikate**

Die gematik Root-CA, ein TSP-X.509 QES und ein TSP-X.509 nonQES MÜSSEN für die Ausstellung von Testzertifikaten das Zertifikatsprofil von Zertifikaten, die für den Einsatz in der Produktivumgebung vorgesehen und vom gleichen Typ sind, verwenden.⌫

Die Festlegung der Datenformate und Zertifikatsprofile erfolgt in [gemSpec_PKI].

Anhang C – Verzeichnisse

C1 – Abkürzungen

Kürzel	Erläuterung
CA	Certificate Autority
CP	Certificate Policy
CPS	Certification Practice Statement
CSR	Certificate Signing Request
eGK	Elektronische Gesundheitskarte
Root-CA	Trust-Service Provider für X.509-CA-Zertifikate
HSM	Hardware Security Module
OCSP	Online Certificate Status Protocol
PIN	Personal Identification Number
PKI	Publik Key Infrastructure
QES	Qualifizierte elektronische Signatur
RFC	Request For Comment
SLA	Service Level Agreement
TI	Telematikinfrastruktur
TSL	Trust-Service Status List
TSL-SP	Trust-Service Status List Service Provider
TSP	Trust-Service Provider
TSP-X.509 nonQES	Trust-Service Provider für nicht-qualifizierte X.509-Anwenderzertifikate

C2 – Glossar

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

C3 – Tabellenverzeichnis

C4 – Referenzierte Dokumente

C4.1 Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_PKI_TIP]	gematik: Konzept PKI der TI-Plattform
[gemSpec_CVC_TSP]	gematik: Spezifikation Trust Service Provider CVC
[gemSpec_Krypt]	gematik: Spezifikation Kryptographie (bis Release 0.5.3: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur)
[gemSpec_OID]	gematik: Spezifikation OID (bis Release 0.5.3: Spezifikation: Festlegung von OIDs)
[gemSpec_Perf]	gematik: Spezifikation Performance
[gemSpec_PKI]	gematik: Spezifikation PKI
[gemSpec_SiBetrUmg]	gematik: Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung für zentrale Produkte der TI
[gemSpec_Sich_DS]	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen
[gemSpec_TSL]	gematik: Spezifikation TSL-Dienst
[gemSpec_X.509_TSP]	gematik: Spezifikation Trust Service Provider X.509

C4.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ALGCAT]	Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen), Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, vom 11.12.2015 (auch online verfügbar: https://www.bundesanzeiger.de mit dem Suchbegriff „BAnz AT 01.02.2016 B5“)

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI_2005]	BSI (2005): IT-Grundschutz-Kataloge (11. Ergänzungslieferung 12/2008) https://www.bsi.bund.de/DE/Themen/weitereThemen/ITGrundschutzKataloge/itgrundschutzkataloge_node.html
[CP-HPC]	Bundesärztekammer et al (06.11.2012): Gemeinsame Policy für die Ausgabe der HPC – Zertifikatsrichtlinie HPC (Version 1.0.5) http://www.bundesaerztekammer.de/downloads/CP_HPC_v1.0.5.pdf
[eIDAS]	Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG
[ISO17799]	ISO/IEC 17799:2005 Information technology – Security techniques – Code of practice for information security management
[ISO27001]	ISO/IEC 27001:2005 Specification for an Information Security Management System, ISO/IEC JTC 1, Information technology, Subcommittee SC 27, IT Security techniques
[RFC822]	RFC 822 (August 1982): Standard for the format of ARPA internet text messages
[RFC2119]	RFC 2119 (März 1997): Key words for use in RfCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2109
[RFC3647]	RFC 3647 (November 2003) Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework http://tools.ietf.org/html/rfc3647
[X.501]	ITU-T (2008): Information Technology – Open Systems Interconnection – The Directory: Models