Einführung der Gesundheitskarte

Certificate Policy

Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL

|  |  |
| --- | --- |
| Version: | 2.1.0 |
| Revision: | \main\rel\_online\rel\_ors1\rel\_opb1\rel\_ors2\24 |
| Stand: | 18.12.2017 |
| 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

Änderungen zum Ausbau von LE-AdV

Dokumentenhistorie

| **Version** | **Stand** | **Kap./ Seite** | **Grund der Änderung, besondere Hinweise** | **Bearbeitung** |
| --- | --- | --- | --- | --- |
| 2.0.0 | 02.08.17 |  | Überarbeitung zum Online-Produktivbetrieb (Stufe 2.1) | gematik |
| 2.1.0 | 18.12.17 |  | freigegeben | gematik |
|  |  |  |  |  |
|  |  |  |  |  |

Inhaltsverzeichnis

[1 Einordnung des Dokumentes 9](#_Toc501699693)

[1.1 Zielsetzung 9](#_Toc501699694)

[1.2 Zielgruppe 9](#_Toc501699695)

[1.3 Geltungsbereich 9](#_Toc501699696)

[1.4 Abgrenzung des Dokuments 9](#_Toc501699697)

[1.5 Methodik 10](#_Toc501699698)

[2 Einleitung fachlicher Teil 11](#_Toc501699699)

[2.1 Überblick 11](#_Toc501699700)

[2.1.1 Teilnehmer in der PKI 11](#_Toc501699701)

[2.1.2 Ziel dieser Richtlinie 11](#_Toc501699702)

[2.1.3 Rahmen dieser Richtlinie 12](#_Toc501699703)

[3 Allgemeine Maßnahmen 13](#_Toc501699704)

[3.1 Verzeichnisse 13](#_Toc501699705)

[3.2 Veröffentlichung von Zertifikaten 13](#_Toc501699706)

[3.3 Zeitpunkt und Häufigkeit von Veröffentlichungen 13](#_Toc501699707)

[3.4 Zugriffskontrollen auf Verzeichnisse 14](#_Toc501699708)

[4 Identifizierung und Authentifizierung 15](#_Toc501699709)

[4.1 Namensregeln 15](#_Toc501699710)

[4.1.1 Arten von Namen 15](#_Toc501699711)

[4.1.2 Namensform 15](#_Toc501699712)

[4.1.3 Aussagekraft von Namen 15](#_Toc501699713)

[4.1.4 Notwendigkeit für aussagefähige und eindeutige Namen 15](#_Toc501699714)

[4.1.5 Anonymität oder Pseudonyme von Zertifikatsnehmern 16](#_Toc501699715)

[4.1.6 Regeln für die Interpretation verschiedener Namensformen 16](#_Toc501699716)

[4.2 Erstmalige Überprüfung der Identität 16](#_Toc501699717)

[4.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels 16](#_Toc501699718)

[4.2.2 Authentifizierung von Organisationszugehörigkeiten 17](#_Toc501699719)

[4.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikatsantragstellers 17](#_Toc501699720)

[4.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer 17](#_Toc501699721)

[4.2.5 Prüfung der Berechtigung zur Antragstellung 17](#_Toc501699722)

[4.2.6 Kriterien für den Einsatz interoperabler Systeme 18](#_Toc501699723)

[4.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (Rekeying) 18](#_Toc501699724)

[4.3.1 Identifizierung und Authentifizierung von routinemäßigen Anträgen zur Schlüsselerneuerung 18](#_Toc501699725)

[4.3.2 Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen 18](#_Toc501699726)

[4.4 Identifizierung und Autorisierung von Sperranträgen 18](#_Toc501699727)

[5 Betriebliche Maßnahmen 19](#_Toc501699728)

[5.1 Zertifikatsantrag durch TSP-X.509 19](#_Toc501699729)

[5.1.1 Autorisierung für die Beantragung von Zertifikaten 19](#_Toc501699730)

[5.1.2 Registrierungsprozess und Zuständigkeiten 19](#_Toc501699731)

[5.2 Verarbeitung des Zertifikatsantrags 20](#_Toc501699732)

[5.2.1 Durchführung der Identifizierung und Authentifizierung 20](#_Toc501699733)

[5.2.2 Annahme oder Ablehnung von Zertifikatsanträgen 20](#_Toc501699734)

[5.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen 20](#_Toc501699735)

[5.3 Zertifikatsausgabe 20](#_Toc501699736)

[5.3.1 Ausgabe eines Zertifikats für einen nachgeordneten TSP (TSP-X.509 nonQES) 20](#_Toc501699737)

[5.3.2 Erstellen eines TSP-Zertifikats (self signed Root) 21](#_Toc501699738)

[5.3.3 Ausgabe eines Zertifikats für Zertifikatsnehmer (an Endnutzer) 21](#_Toc501699739)

[5.3.4 Aktionen des TSP-X.509 nonQES bei der Ausgabe von Zertifikaten 21](#_Toc501699740)

[5.3.5 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats 22](#_Toc501699741)

[5.4 Zertifikatsannahme 22](#_Toc501699742)

[5.4.1 Verhalten für eine Zertifikatsannahme 22](#_Toc501699743)

[5.4.2 Veröffentlichung des TSP-Zertifikats 22](#_Toc501699744)

[5.4.3 Benachrichtigung anderer Zertifikatsnutzer über die Zertifikatsausgabe 22](#_Toc501699745)

[5.5 Verwendung des Schlüsselpaars und des Zertifikats 23](#_Toc501699746)

[5.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer 23](#_Toc501699747)

[5.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer 23](#_Toc501699748)

[5.6 Zertifikatserneuerung 23](#_Toc501699749)

[5.7 Zertifizierung nach Schlüsselerneuerung 24](#_Toc501699750)

[5.8 Zertifikatsänderung 24](#_Toc501699751)

[5.8.1 Bedingungen für eine Zertifikatsänderung 24](#_Toc501699752)

[5.8.2 Autorisierung einer Zertifikatsänderung 24](#_Toc501699753)

[5.8.3 Bearbeitung eines Antrags auf Zertifikatsänderung 24](#_Toc501699754)

[5.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats 25](#_Toc501699755)

[5.8.5 Verhalten für die Annahme einer Zertifikatsänderung 25](#_Toc501699756)

[5.8.6 Veröffentlichung der Zertifikatsänderung 25](#_Toc501699757)

[5.8.7 Benachrichtigung anderer Zertifikatsnutzer über die Ausgabe eines neuen Zertifikats 25](#_Toc501699758)

[5.8.8 Sperrung und Suspendierung von Zertifikaten 25](#_Toc501699759)

[5.8.9 Bedingungen für eine Sperrung 25](#_Toc501699760)

[5.8.10 Autorisierung der Sperrung eines Endanwenderzertifikats 27](#_Toc501699761)

[5.8.11 Verfahren für einen Sperrantrag 28](#_Toc501699762)

[5.8.12 Fristen für einen Sperrantrag 28](#_Toc501699763)

[5.8.13 Fristen/Zeitspanne für die Bearbeitung des Sperrantrags 28](#_Toc501699764)

[5.8.14 Verfügbare Methoden zum Prüfen von Sperrinformationen 28](#_Toc501699765)

[5.8.15 Aktualisierung und Veröffentlichung von Sperrlisten (CRL) 28](#_Toc501699766)

[5.8.16 Gültigkeitsdauer von Sperrlisten (CRL) 29](#_Toc501699767)

[5.8.17 Online-Verfügbarkeit von Sperrinformationen 29](#_Toc501699768)

[5.8.18 Anforderungen zur Online-Prüfung von Sperrinformationen 29](#_Toc501699769)

[5.8.19 Andere Formen zur Anzeige von Sperrinformationen 29](#_Toc501699770)

[5.8.20 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels 29](#_Toc501699771)

[5.8.21 Bedingungen für eine Suspendierung (Endanwender) 29](#_Toc501699772)

[5.8.22 Autorisierung für eine Suspendierung 30](#_Toc501699773)

[5.8.23 Verfahren für Anträge auf Suspendierung 30](#_Toc501699774)

[5.8.24 Begrenzungen für die Dauer von Suspendierungen (Endanwender) 30](#_Toc501699775)

[5.9 Statusabfragedienst für Zertifikate 31](#_Toc501699776)

[5.9.1 Funktionsweise des Statusabfragedienstes 31](#_Toc501699777)

[5.9.2 Verfügbarkeit des Statusabfragedienstes 31](#_Toc501699778)

[5.9.3 Optionale Leistungen 31](#_Toc501699779)

[5.10 Kündigung durch den Zertifikatsnehmer 31](#_Toc501699780)

[5.11 Schlüsselhinterlegung und Wiederherstellung 31](#_Toc501699781)

[5.11.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater CA-Schlüssel 31](#_Toc501699782)

[5.11.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln 32](#_Toc501699783)

[5.12 Grundlagen für die Sicherheit der Zertifikatserstellung 32](#_Toc501699784)

[5.12.1 Technische Vorgaben 32](#_Toc501699785)

[5.12.2 Organisatorische Vorgaben 32](#_Toc501699786)

[5.12.3 Betriebliche Vorgaben 33](#_Toc501699787)

[6 Allgemeine Sicherheitsmaßnahmen 35](#_Toc501699788)

[6.1 Bauliche Sicherheitsmaßnahmen 35](#_Toc501699789)

[6.2 Verfahrensvorschriften 36](#_Toc501699790)

[6.2.1 Rollenkonzept 36](#_Toc501699791)

[6.2.2 Involvierte Mitarbeiter pro Arbeitsschritt 38](#_Toc501699792)

[6.2.3 Rollenausschlüsse 40](#_Toc501699793)

[6.3 Personalkontrolle 41](#_Toc501699794)

[6.3.1 Anforderungen an Qualifikation, Erfahrung und Zuverlässigkeit 41](#_Toc501699795)

[6.3.2 Methoden zur Überprüfung der Rahmenbedingungen 41](#_Toc501699796)

[6.3.3 Anforderungen an Schulungen 41](#_Toc501699797)

[6.3.4 Häufigkeit von Schulungen und Belehrungen 42](#_Toc501699798)

[6.3.5 Häufigkeit und Folge von Job-Rotation 42](#_Toc501699799)

[6.3.6 Maßnahmen bei unerlaubten Handlungen 42](#_Toc501699800)

[6.3.7 Anforderungen an freie Mitarbeiter 42](#_Toc501699801)

[6.3.8 Einsicht in Dokumente für Mitarbeiter 42](#_Toc501699802)

[6.4 Überwachungsmaßnahmen 42](#_Toc501699803)

[6.4.1 Arten von aufgezeichneten Ereignissen 42](#_Toc501699804)

[6.4.2 Häufigkeit der Bearbeitung der Aufzeichnungen 43](#_Toc501699805)

[6.4.3 Aufbewahrungszeit von Aufzeichnungen 43](#_Toc501699806)

[6.4.4 Schutz der Aufzeichnungen 44](#_Toc501699807)

[6.4.5 Datensicherung der Aufzeichnungen 44](#_Toc501699808)

[6.4.6 Speicherung der Aufzeichnungen (intern/extern) 44](#_Toc501699809)

[6.4.7 Benachrichtigung der Ereignisauslöser 44](#_Toc501699810)

[6.4.8 Verwundbarkeitsabschätzungen 44](#_Toc501699811)

[6.5 Archivierung von Aufzeichnungen 44](#_Toc501699812)

[6.5.1 Arten von archivierten Aufzeichnungen 44](#_Toc501699813)

[6.5.2 Aufbewahrungsfristen für archivierte Daten 45](#_Toc501699814)

[6.5.3 Sicherung des Archivs 45](#_Toc501699815)

[6.5.4 Datensicherung des Archivs 45](#_Toc501699816)

[6.5.5 Anforderungen zum Zeitstempeln von Aufzeichnungen 45](#_Toc501699817)

[6.5.6 Archivierung (intern/extern) 45](#_Toc501699818)

[6.5.7 Verfahren zur Beschaffung und Verifikation von Archivinformationen 45](#_Toc501699819)

[6.6 Schlüsselwechsel beim TSP 45](#_Toc501699820)

[6.7 Kompromittierung und Geschäftsweiterführung 45](#_Toc501699821)

[6.8 Schließung eines TSP oder einer Registrierungsstelle 46](#_Toc501699822)

[7 Technische Sicherheitsmaßnahmen 48](#_Toc501699823)

[7.1 Erzeugung und Installation von Schlüsselpaaren 48](#_Toc501699824)

[7.1.1 Erzeugung von Schlüsselpaaren und Zertifikaten 48](#_Toc501699825)

[7.1.2 Übergabe privater Schlüssel an Zertifikatsnehmer 50](#_Toc501699826)

[7.1.3 Übergabe öffentlicher Schlüssel an Zertifikatsherausgeber 50](#_Toc501699827)

[7.1.4 Lieferung öffentlicher Schlüssel des TSP an Zertifikatsnutzer 50](#_Toc501699828)

[7.1.5 Schlüssellängen 51](#_Toc501699829)

[7.1.6 Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle 51](#_Toc501699830)

[7.1.7 Schlüsselverwendungen 51](#_Toc501699831)

[7.2 Sicherung des privaten Schlüssels und Anforderungen an krypto-graphische Module 51](#_Toc501699832)

[7.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module 52](#_Toc501699833)

[7.2.2 Mehrpersonen-Zugriffssicherung zu privaten Schlüsseln (n von m) 52](#_Toc501699834)

[7.2.3 Hinterlegung privater Schlüssel 52](#_Toc501699835)

[7.2.4 Sicherung privater Schlüssel 53](#_Toc501699836)

[7.2.5 Archivierung privater Schlüssel 53](#_Toc501699837)

[7.2.6 Transfer privater Schlüssel in oder aus kryptographischen Modulen 53](#_Toc501699838)

[7.2.7 Speicherung privater Schlüssel in kryptographischen Modulen 53](#_Toc501699839)

[7.2.8 Aktivierung privater Schlüssel 53](#_Toc501699840)

[7.2.9 Deaktivierung privater Schlüssel 53](#_Toc501699841)

[7.2.10 Vernichtung privater Schlüssel 54](#_Toc501699842)

[7.2.11 Beurteilung kryptographischer Module 54](#_Toc501699843)

[7.3 Andere Aspekte des Managements von Schlüsselpaaren 54](#_Toc501699844)

[7.3.1 Archivierung öffentlicher Schlüssel 54](#_Toc501699845)

[7.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren 54](#_Toc501699846)

[7.4 Aktivierungsdaten 55](#_Toc501699847)

[7.4.1 Aktivierungsdaten 55](#_Toc501699848)

[7.4.2 Schutz von Aktivierungsdaten 56](#_Toc501699849)

[7.4.3 Andere Aspekte von Aktivierungsdaten 56](#_Toc501699850)

[7.5 Sicherheitsmaßnahmen in den Rechneranlagen 56](#_Toc501699851)

[7.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen 56](#_Toc501699852)

[7.5.2 Beurteilung der Systemsicherheit 56](#_Toc501699853)

[7.6 Technische Maßnahmen während des Lebenszyklus 56](#_Toc501699854)

[7.6.1 Sicherheitsmaßnahmen bei der Entwicklung 56](#_Toc501699855)

[7.6.2 Sicherheitsmaßnahmen beim Systemmanagement 57](#_Toc501699856)

[7.6.3 Sicherheitsmaßnahmen während der Lebenszyklus 57](#_Toc501699857)

[7.7 Sicherheitsmaßnahmen für Netze 57](#_Toc501699858)

[7.8 Zeitstempel 57](#_Toc501699859)

[8 Format der Zertifikate 58](#_Toc501699860)

[9 Weitere finanzielle und rechtliche Angelegenheiten 59](#_Toc501699861)

[9.1 Gebühren 59](#_Toc501699862)

[9.2 Finanzielle Zuständigkeiten 59](#_Toc501699863)

[9.2.1 Versicherungsdeckung 59](#_Toc501699864)

[9.2.2 Andere Posten 59](#_Toc501699865)

[9.2.3 Versicherung oder Gewährleistung für Endnutzer 59](#_Toc501699866)

[9.3 Vertraulichkeitsgrad von Geschäftsdaten 59](#_Toc501699867)

[9.3.1 Definition von vertraulichen Informationen 60](#_Toc501699868)

[9.3.2 Informationen, die nicht zu den vertraulichen Informationen gehören 60](#_Toc501699869)

[9.3.3 Zuständigkeiten für den Schutz vertraulicher Informationen 60](#_Toc501699870)

[9.4 Datenschutz von Personendaten 60](#_Toc501699871)

[9.5 Geistiges Eigentumsrecht 60](#_Toc501699872)

[9.6 Zusicherungen und Garantien 61](#_Toc501699873)

[9.7 Haftungsausschlüsse 61](#_Toc501699874)

[9.8 Haftungsbeschränkungen 61](#_Toc501699875)

[9.9 Schadenersatz 61](#_Toc501699876)

[9.10 Gültigkeitsdauer und Beendigung 61](#_Toc501699877)

[9.11 Individuelle Absprachen zwischen Vertragspartnern 62](#_Toc501699878)

[9.12 Ergänzungen 62](#_Toc501699879)

[9.13 Verfahren zur Schlichtung von Streitfällen 62](#_Toc501699880)

[9.14 Zugrunde liegendes Recht 62](#_Toc501699881)

[9.15 Einhaltung geltenden Rechts 62](#_Toc501699882)

[9.16 Sonstige Bestimmungen 63](#_Toc501699883)

[10 Anhang A – Certificate Policy für Komponentenzertifikate 64](#_Toc501699884)

[11 Anhang B – Certificate Policy für Testzertifikate 67](#_Toc501699885)

[11.1 B1 – Geltungsbereich 67](#_Toc501699886)

[11.2 B2 – Allgemeine Maßnahmen 67](#_Toc501699887)

[11.2.1 B2.1 Rahmen der Policy 67](#_Toc501699888)

[11.2.2 B2.2 Verzeichnisse und Veröffentlichungen 68](#_Toc501699889)

[11.3 B3 – Identifizierung und Authentifizierung 68](#_Toc501699890)

[11.3.1 B3.1 Namensregeln 68](#_Toc501699891)

[12 B3.1.1 Arten von Namen 69](#_Toc501699892)

[13 B3.1.2 Namensform 70](#_Toc501699893)

[14 B3.1.3 Aussagekraft von Namen 71](#_Toc501699894)

[15 B3.1.4 Notwendigkeit für aussagefähige und eindeutige Namen 72](#_Toc501699895)

[15.1.1 B3.2 Erstmalige Überprüfung der Identität 72](#_Toc501699896)

[16 B3.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels 73](#_Toc501699897)

[16.1 B4 – Betriebliche Maßnahmen 73](#_Toc501699898)

[16.1.1 B4.1 Zertifikatsausgabe 73](#_Toc501699899)

[16.1.2 B4.2 Sperrung und Suspendierung von Testzertifikaten (Endanwender) 74](#_Toc501699900)

[16.1.3 B4.3 Statusabfragedienst für Testzertifikate 74](#_Toc501699901)

[16.2 B5 – Allgemeine Sicherheitsmaßnahmen 74](#_Toc501699902)

[16.3 B6 – Technische Sicherheitsmaßnahmen 75](#_Toc501699903)

[16.4 B7 – Formate der Zertifikate 75](#_Toc501699904)

[17 Anhang C – Verzeichnisse 76](#_Toc501699905)

[17.1 C1 – Abkürzungen 76](#_Toc501699906)

[17.2 C2 – Glossar 76](#_Toc501699907)

[17.3 C3 – Tabellenverzeichnis 76](#_Toc501699908)

[17.4 C4 – Referenzierte Dokumente 77](#_Toc501699909)

[17.4.1 C4.1 Dokumente der gematik 77](#_Toc501699910)

[17.4.2 C4.2 Weitere Dokumente 78](#_Toc501699911)

# 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.

## 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.

## Zielgruppe

Das Dokument richtet sich an die Trust Service Provider.

## 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.

## 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]

## 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.

# 

# Einleitung fachlicher Teil

## 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.

### 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.

### 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.

### 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.

# 

# Allgemeine Maßnahmen

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

## 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.

## 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.

**⌫**

## 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.

**⌫**

## 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.

**⌫**

# 

# Identifizierung und Authentifizierung

## Namensregeln

### 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.

**⌫**

### 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.

**⌫**

### 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.

### 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.

**⌫**

### Anonymität oder Pseudonyme von Zertifikatsnehmern

**⌦ GS-A\_4184 Eindeutigkeit von pseudonymen Zertifikaten**

Der Kartenherausgeber MUSS die Eindeutigkeit der pseudonymen Zertifikate sicher­stellen.

**⌫**

### 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].

## Erstmalige Überprüfung der Identität

### 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.

### Authentifizierung von Organisationszugehörigkeiten

Keine Vorgaben

### 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.

**⌫**

### 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**.**

**⌫**

### 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.

**⌫**

### 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).

## Identifizierung und Authentifizierung von Anträgen auf Schlüssel­erneuerung (Rekeying)

### 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.

**⌫**

### Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen

Siehe Abschnitt 4.2.3

## 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.

**⌫**

# 

# Betriebliche Maßnahmen

## 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.

**⌫**

### 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.

**⌫**

### 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.

## Verarbeitung des Zertifikatsantrags

### 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.

**⌫**

### 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.

**⌫**

### Fristen für die Bearbeitung von Zertifikatsanträgen

Keine Vorgaben

## Zertifikatsausgabe

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

### 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.

**⌫**

### Erstellen eines TSP-Zertifikats (self signed Root)

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

### 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.

**⌫**

### 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.

**⌫**

### 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.

**⌫**

## 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.

### 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.

**⌫**

### 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.

**⌫**

### Benachrichtigung anderer Zertifikatsnutzer über die Zertifikatsausgabe

Keine Vorgaben

## Verwendung des Schlüsselpaars und des Zertifikats

### 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*).

**⌫**

### 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.

**⌫**

## 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.

**⌫**

## 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

## Zertifikatsänderung

### 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.

**⌫**

### 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.

**⌫**

### Bearbeitung eines Antrags auf Zertifikatsänderung

Keine Vorgaben

### Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Siehe Abschnitt 5.3.5.

### Verhalten für die Annahme einer Zertifikatsänderung

Siehe Abschnitt 5.3.4.

### Veröffentlichung der Zertifikatsänderung

Keine Vorgaben

### Benachrichtigung anderer Zertifikatsnutzer über die Ausgabe eines neuen Zertifikats

Keine Vorgaben

### 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]).

### 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

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Sperrberechtigte  Stellen \*) | | | Zertifikate der Kartenarten | | | | | | | |
|  | HBA | SMC-B | SMC-B | SMC-B | SMC-B |  |  |
| eGK | non-QES | LEI | ORG | KTR | KTR-Adv | 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 | 2 |  |  |
| 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 5.8.21 beschrieben.

Die maximale Dauer von Suspendierungen ist aus Abschnitt 5.8.24 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.

**⌫**

### 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.

### 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.

**⌫**

### 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.

**⌫**

### 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.

**⌫**

### 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.

**⌫**

### Aktualisierung und Veröffentlichung von Sperrlisten (CRL)

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

### Gültigkeitsdauer von Sperrlisten (CRL)

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

### 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.

**⌫**

### 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.

**⌫**

### 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.

### Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Keine Vorgaben

### 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 5.8.23.

### 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.

**⌫**

### 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.

**⌫**

### 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.

## Statusabfragedienst für Zertifikate

### 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.

**⌫**

### Verfügbarkeit des Statusabfragedienstes

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

### Optionale Leistungen

Keine Vorgaben

## 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.

**⌫**

## Schlüsselhinterlegung und Wiederherstellung

### 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.

### Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Keine Vorgaben

## Grundlagen für die Sicherheit der Zertifikatserstellung

### Technische Vorgaben

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

### 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.

**⌫**

### 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.

**⌫**

# 

# 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.

## 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.

## Verfahrensvorschriften

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

### 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 |  |
| 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.

**⌫**

### 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 Autorisierungs­informationen | 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 |  |  |
| 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 |  |  |
| 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 |  |  |

**⌫**

### 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 |

**⌫**

## Personalkontrolle

### 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.

### Methoden zur Überprüfung der Rahmenbedingungen

Siehe Abschnitt 6.3.1.

### Anforderungen an Schulungen

Siehe Abschnitt 6.3.1.

### Häufigkeit von Schulungen und Belehrungen

Siehe Abschnitt 6.3.1.

### Häufigkeit und Folge von Job-Rotation

Keine Vorgaben

### 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.

### 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.

**⌫**

### 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.

**⌫**

## Überwachungsmaßnahmen

### 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.

### 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.

### 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.

**⌫**

### 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.

### 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.

### Speicherung der Aufzeichnungen (intern/extern)

Keine Vorgaben

### 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.

### 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.

## Archivierung von Aufzeichnungen

### 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.

### Aufbewahrungsfristen für archivierte Daten

Siehe Abschnitt 6.4.3.

### Sicherung des Archivs

Siehe Abschnitt 6.4.5.

### Datensicherung des Archivs

Siehe Abschnitt 6.4.5.

### Anforderungen zum Zeitstempeln von Aufzeichnungen

Keine Vorgaben

### Archivierung (intern/extern)

Siehe Abschnitt 6.4.5.

### Verfahren zur Beschaffung und Verifikation von Archivinformationen

Siehe Abschnitt 6.4.5.

## 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.

**⌫**

## 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

## 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.

**⌫**

# 

# Technische Sicherheitsmaßnahmen

## Erzeugung und Installation von Schlüsselpaaren

### 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 zweierhierfür 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 zweierhierfür 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.

**⌫**

### 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.

### Übergabe öffentlicher Schlüssel an Zertifikatsherausgeber

Keine Vorgaben

### 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].

### Schlüssellängen

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

### Festlegung der Parameter der öffentlichen Schlüssel und Qualitätskontrolle

Keine Vorgaben

### 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.

**⌫**

## Sicherung des privaten Schlüssels und Anforderungen an krypto-graphische 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.

**⌫**

### 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“.

**⌫**

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

Siehe Abschnitt 6.2.2.

### 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 5.11.1. Die gematik gilt dabei nicht als „Dritter“ gemäß Anforderung GS-A\_4311.

### 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.

### Archivierung privater Schlüssel

Siehe Abschnitt 7.2.4.

### Transfer privater Schlüssel in oder aus kryptographischen Modulen

Siehe Abschnitt 7.2.4.

### Speicherung privater Schlüssel in kryptographischen Modulen

Siehe Abschnitt 7.2.4.

### 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.

### 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.

**⌫**

### 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.

### Beurteilung kryptographischer Module

Siehe Abschnitt 7.2.1.

## Andere Aspekte des Managements von Schlüsselpaaren

### 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.

### 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 Gütig­keits­dauer von 10 Jahren in dieser Richtlinie festgelegt, da eine kürzere Gültigkeit die maxi­male Gültigkeitsdauer der in dem Gültigkeitszeitraum des CA-Zertifikats ausge­stellten 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.

**⌫**

## Aktivierungsdaten

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

### 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.

**⌫**

### Schutz von Aktivierungsdaten

Siehe Abschnitt 6.2.1 und 6.2.2.

### Andere Aspekte von Aktivierungsdaten

Keine Vorgaben

## Sicherheitsmaßnahmen in den Rechneranlagen

### 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.

**⌫**

### 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.

**⌫**

## Technische Maßnahmen während des Lebenszyklus

### 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.

**⌫**

### 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\_SiBetr­Umg#AnhB] beschrieben. Diese Richtlinie enthält keine darüber hinaus gehenden Anforderungen.

### Sicherheitsmaßnahmen während der Lebenszyklus

Keine Vorgaben

## Sicherheitsmaßnahmen für Netze

Siehe Abschnitt 7.6.2.

## Zeitstempel

Keine Vorgaben.

# 

# Format der Zertifikate

Die Festlegung der Datenformate und Zertifikatsprofile erfolgt in [gemSpec\_PKI].

# 

# Weitere finanzielle und rechtliche Angelegenheiten

## Gebühren

Keine Vorgaben

## Finanzielle Zuständigkeiten

### Versicherungsdeckung

Keine Vorgaben

### Andere Posten

Keine Vorgaben

### 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.

**⌫**

## 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.

### 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.

### Informationen, die nicht zu den vertraulichen Informationen gehören

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

### Zuständigkeiten für den Schutz vertraulicher Informationen

Siehe Abschnitt 9.3.

## 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

## Geistiges Eigentumsrecht

Keine Vorgaben

## 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

## Haftungsausschlüsse

Keine Vorgaben

## Haftungsbeschränkungen

Keine Vorgaben

## Schadenersatz

Keine Vorgaben

## 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

## Individuelle Absprachen zwischen Vertragspartnern

Keine Vorgaben

## 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

## Verfahren zur Schlichtung von Streitfällen

Keine Vorgaben

## Zugrunde liegendes Recht

Es gelten die für Deutschland relevanten Rechtsnormen.

## Einhaltung geltenden Rechts

**⌦ GS-A\_4329 Konformität zum geltenden Recht**

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

**⌫**

## 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 5.8.9 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 5.8.11 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 5.8.10 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 5.8.12 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 5.9.1 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 5.11.1 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 MÜSSENbei 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 gene­rieren, 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

[Tabelle 1: Tab\_PKI\_305 Übersicht der PKI-spezifischen Sperrgründe 20](#_Toc485287838)

[Tabelle 2 Tab\_PKI\_301 – Beschreibung der einzelnen Rollen 30](#_Toc485287839)

[Tabelle 3 Tab\_PKI\_302 - Involvierte Mitarbeiter pro Arbeitsschritt 32](#_Toc485287840)

[Tabelle 4 Tab\_PKI\_303 - Rollenausschlüsse 34](#_Toc485287841)

[Tabelle 5 Tab\_PKI\_304 - Rollenaufteilung auf Personengruppen 34](#_Toc485287842)

## 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“) |
| [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 |