Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Spezifikation

Trust Service Provider X.509

Version:	1.5.0
Revision:	\main\rel_online\rel_ors1\15
Stand:	17.06.2014
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemSpec_X.509_TSP]

Dokumentinformationen

Änderungen zur Vorversion

Es wurden die Serverzertifikate C.ZD.TLS-S in Tabelle 6 und in Tabelle 10 ergänzt, "Kontaktperson" wurden zum besseren Verständnis auf "Antragsteller" umbenannt, redundante Daten wurden gestrichen, statt "Verlängerung von Zertifikaten" wurde die korrekte Formulierung „Folgezertifikate“ eingesetzt, die falschen Bezeichner C.GEM.RCA1 bzw. C.GEM.RCA2 für die Root-CAs in den Erläuterungen zur Cross-Zertifizierung wurden korrigiert.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.5.0	10.08.12		zur Abstimmung freigegeben	PL P77
			Überarbeitung nach Kommentierung und Workshop	P77
1.0.0	15.10.12		freigegeben	gematik
			Einarbeitung Kommentare aus der übergreifenden Konsistenzprüfung	P77
1.1.0	12.11.12		freigegeben	gematik
	15.02.13		Überarbeitung anhand interner Änderungsliste (Fehlerkorrekturen, Inkonsistenzen)	P77
1.1.9	22.04.13		zur Abstimmung freigegeben	PL P77
			Einarbeitung Kommentare aus Kommentierung Gesamtpaket	P77
1.2.0 RC	30.05.13		zur Freigabe empfohlen	PL P77
1.2.0	06.06.13		freigegeben	gematik
			Einarbeitung lt. Änderungsliste vom 08.08.13	P77
1.3.0	15.08.13		freigegeben	gematik
			Losübergreifende Synchronisation	P77
1.4.0	21.02.14		freigegeben	gematik
	17.04.14		Es wurden die Serverzertifikate C.ZD.TLS-S in Tabelle 6 und in Tabelle 10 ergänzt, "Kontakt-person" wurden zum besseren Verständnis auf "Antragsteller" umbenannt, redundante Daten wurden gestrichen, statt "Verlängerung von Zerti-fikaten" wurde die korrekte Formulierung „Folge-zertifikate“ eingesetzt, die falschen Bezeichner C.GEM.RCA1 bzw. C.GEM.RCA2 für die Root-CAs in den Erläuterungen zur Cross-Zertifizierung wurden korrigiert.	P77
1.5.0	17.06.14		freigegeben	gematik

Inhaltsverzeichnis

Dokumentinformationen 2

Inhaltsverzeichnis 3

1 Einordnung des Dokumentes 6

1.1 Zielsetzung 6

1.2 Zielgruppe 6

1.3 Geltungsbereich 6

1.4 Abgrenzung 6

1.5 Methodik 7

2 Systemüberblick 8

2.1 Hierarchie der PKI für X.509-Zertifikate 8

2.2 Begriffsverwendung 8

3 Systemkontext 9

3.1 Akteure und Rollen 9

3.1.1 gematik 9
3.1.2 TSP-X.509 QES und TSP-X.509 nonQES 9
3.1.3 gematik-Root-CA 10
3.1.4 Kartenherausgeber 10
3.1.5 Kartenhersteller 11
3.1.6 Zertifikatsnehmer 11
3.1.7 Hersteller 11
3.1.8 Anbieter 12

3.2 Nachbarsysteme 12

4 Zerlegung des Produkttyps 14

4.1 Produkttypen TSP-X.509 QES und TSP-X.509 nonQES 14

4.2 Produkttyp gematik-Root-CA 18

4.3 Statusprüfdienst 19

5 Übergreifende Festlegungen 20

5.1 Ausstellung von X.509-Zertifikaten 20

5.1.1 Erstellung Sicherheitskonzept Zertifikatsprozess durch TSP-X.509 20
5.1.2 Zulassung 21
5.1.3 Datenschutz 21
5.1.4 Unterscheidung produktive TSP-X.509 und Test-TSP-X.509 22

5.2 Sperrung von X.509-Zertifikaten 22
5.3 Schutzbedarfsfeststellung 23
5.4 Sichere Kommunikation zwischen Rollen und Diensten 24
5.5 Schutz der gematik Root-CA 24

6 Funktionsmerkmale 25
6.1 Ausstellung von Personen- und Organisationszertifikaten 25
6.1.1 Schnittstelle P_Cert_Provisioning_nonQES_Registration 27
6.1.1.1 Schnittstellendefinition 27
6.1.1.2 Umsetzung 30
6.1.2 Schnittstelle P_Cert_Provisioning_QES_Registration 31
6.1.2.1 Schnittstellendefinition 31
6.1.2.2 Umsetzung 33
6.1.3 Schnittstelle P_Cert_Provisioning_Erstellung 34
6.1.3.1 Schnittstellendefinition 34
6.1.3.2 Umsetzung 36
6.2 Ausstellung von X.509-Zertifikaten über die zentrale PKI 37
6.2.1 Schnittstelle I_Cert_Provisioning_Registration 41
6.2.1.1 Schnittstellendefinition 41
6.2.1.2 Umsetzung 45
6.2.1.3 Nutzung 48
6.2.2 Schnittstelle I_Cert_Provisioning_Erstellung 49
6.2.2.1 Schnittstellendefinition 49
6.2.2.2 Umsetzung 51
6.2.3 Testunterstützung 51
6.3 Sperren von X.509-Zertifikaten 52
6.3.1 Schnittstelle P_Cert_Revocation 54
6.3.1.1 Schnittstellendefinition 54
6.3.1.1.1 Prozess zur Sperrung nonQES-Personen- und Organisationszertifikate 54
6.3.1.1.2 Prozess zur Sperrung QES-Zertifikate 55
6.3.1.2 Umsetzung 56
6.3.2 Schnittstelle I_Cert_Revocation 57
6.3.2.1 Schnittstellendefinition 57
6.3.2.1.1 Sperrung von Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikaten 57
6.3.2.2 Umsetzung 60
6.4 Ausstellung von X.509-Sub-CA-Zertifikaten 62
6.4.1 P_Sub_CA_Cert_Certification_X.509 63
6.4.1.1 Schnittstellendefinition 63
6.4.1.2 Umsetzung 65
6.5 Statusprüfdienst 67

Anhang A – Verzeichnisse 68
A1 – Abkürzungen 68

A2 – Glossar 69

A3 – Abbildungsverzeichnis 69

A4 – Tabellenverzeichnis 70

A5 – Referenzierte Dokumente 71

A5.1 – Dokumente der gematik 71

A5.2 – Weitere Dokumente 72

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen an den Produkttyp TSP-X.509 einschließlich der durch ihn bereitgestellten Schnittstellen für den Online-Rollout (Stufe 1).

1.2 Zielgruppe

Das Dokument richtet sich Trust Service Provider X.509 QES und nonQES, Anbieter einer gematik-Root-CA, Hersteller von Kartenterminals und Konnektoren, Anbieter von zentralen Diensten der TI sowie Kartenhersteller und Kartenherausgeber.

1.3 Geltungsbereich

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

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzung

Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang A5).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in den Produkttypsteckbrief der Produkttypen TSP-X.509 QES, TSP-X.509 nonQES und gematik-Root-CA verzeichnet.

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zum Themenbereich

- Verfahrensbeschreibung für Zulassungs- und Registrierung TSP-X.509 QES und TSP-X.509 nonQES sowie
- Anforderungen an die Sicherheit eines TSP-X.509 QES, TSP-X.509 nonQES und der gematik-Root-CA.
- Prozesse und Verfahren zur Personalisierung der Karten selbst.

Die Sicherheitsanforderungen, die an einen TSP-X.509 nonQES bzw. an die gematik-Root-CA gestellt werden, sind Gegenstand der „Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL“ [gemRL_TSL_SP_CP].

Anforderungen an den Produkttyp TSP-X.509 QES sind durch das Signaturgesetz (SigG) und die Signaturverordnung (SigV) festgelegt.

Die Spezifikation der Schnittstelle des OCSP-Responders ist nicht Bestandteil dieses Dokumentes, sondern ist in [gemSpec_PKI#9] beschrieben.

1.5 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern sowie 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:

⌦ **TIP1-A_nnnn <Titel der Afo>**

Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

2 Systemüberblick

2.1 Hierarchie der PKI für X.509-Zertifikate

Eine Darstellung der CA-Strukturen für den Aufbau und Betrieb der PKI für X.509-Zertifikate befindet sich im Konzept PKI der TI-Plattform [gemKPT_PKI_TIP].

Gemäß [gemKPT_PKI_TIP] ist der Herausgeber eines Zertifikats für die Bereitstellung von Sperrinformationen zu jedem Zertifikat über den Zeitraum der Zertifikatslaufzeit sowie über einen zu definierenden Zeitraum nach Ablauf der Gültigkeit des Zertifikates für Zwecke der Zertifikats- und Signaturprüfung verantwortlich. Diese Sperrinformationen werden über eine server-basierte Statusprüfung (OCSP) zur Verfügung gestellt. Analog zu den drei Domänen von Zertifikatsherausgebern (Kostenträger, Leistungserbringer und gematik) lassen sich auch die Verantwortlichkeiten für den Betrieb der OCSP-Responder diesen Domänen bzw. Herausgebern zuordnen.

Die gematik als Policy-Authority für die Telematikinfrastruktur (TI) hat eine übergeordnete Certificate Policy [gemRL_TSL_SP_CP], die die Mindestanforderungen für die Anwendungsbereiche Vertraulichkeit, Authentisierung und elektronischer Signatur mit nicht-qualifizierten X.509-Zertifikaten enthält, erstellt. Alle beteiligten TSP-X.509, die X.509-Zertifikate für den nicht-qualifizierten Bereich ausgeben, sowie die gematik-Root-CA müssen die relevanten Anforderungen dieser Policy erfüllen. Regelungen eines TSP-X.509 sind in seiner eigenen Certificate Policy sowie in seinem „Certification Practice Statement“ zu treffen [gemKPT_PKI_TIP#2.7.1].

TSP-X.509 QES, die qualifizierte X.509-Zertifikate ausgeben, unterliegen den Anforderungen des deutschen Signaturgesetzes [SigG01] und der Signaturverordnung [SigV01].

Für die Bereitstellung von Diensten im Zusammenhang mit HBA-Zertifikaten gilt die HPC-Policy [HPC-CP]. Sowohl für HBA- wie auch für SMC-B-Zertifikate können durch die jeweils zuständige berufsständische Organisation weitere, aufbauende oder detaillierende Anforderungen gestellt werden.

2.2 Begriffsverwendung

Die gSMC kann in den technischen Ausprägungen gSMC-K als Sicherheitsmodul für den Konnektor und als gSMC-KT als Sicherheitsmodul für das Kartenterminal vorliegen. In der weiteren Darstellung wird i.d.R. der Oberbegriff „gSMC“ verwendet. Eine Unterscheidung zwischen gSMC-K und gSMC-KT wird jedoch vorgenommen, wenn sie für die konkrete inhaltliche Betrachtung relevant ist.

3 Systemkontext

3.1 Akteure und Rollen

Bei der folgenden Beschreibung wird von einer Trennung der Organisationen bzw. Personen bei der Ausübung der Rollen ausgegangen. Eine Organisation bzw. Person kann jedoch mehrere Rollen übernehmen.

Übernimmt eine Organisation/Person eine Rolle, so kann sie Teile der zu dieser Rolle gehörenden Zuständigkeiten/Aufgaben an eine andere Organisation/Person übergeben. Hiervon unabhängig bleiben aber die im Folgenden genannten Verantwortlichkeiten bei der die Rolle ausübenden Organisation/Person.

3.1.1 gematik

Die gematik ist verantwortlich für die Gestaltung der PKI der X.509-Zertifikate. Sie übernimmt unter anderem die folgenden Aufgaben:

- Zulassung TSP-X.509 QES und TSP-X.509 nonQES,
- Bereitstellung einer zentralen PKI (TSP-X.509 nonQES) zur Erstellung von
    - Komponentenzertifikaten,
    - OCSP-Signerzertifikate,
    - CRL-Signerzertifikate,
    - nonQES-HBA-Zertifikate und
    - Organisationszertifikate.
- Die zentrale PKI (TSP-X.509 nonQES) umfasst dazu
    - Komponenten- und Dienste-CA
    - OCSP-Signer-CA
    - CRL-Signer-CA
- Verantwortung von Spezifikationen und übergreifende Policies.

3.1.2 TSP-X.509 QES und TSP-X.509 nonQES

Herausgeber von X.509-Zertifikaten, die innerhalb der TI eingesetzt werden sollen, werden als Trust Service Provider X.509 (TSP-X.509 QES und TSP-X.509 nonQES) bezeichnet.

Zur Aufnahme in die TSL der gematik müssen TSP-X.509 QES und TSP-X.509 nonQES nachweisen, dass die durch die gematik vorgegebenen Mindestanforderungen an die

Sicherheit des TSP-X.509 erfüllt werden. In der Rolle als TSP-X.509 QES und TSP-X.509 nonQES können ZDAs, Kartenherausgeber, Kartenhersteller, berechtigte Anbieter eines Fachdienstes oder eines zentralen Dienstes sowie Hersteller oder durch sie beauftragte Dienstleister auftreten.

TSP-X.509 QES und TSP-X.509 nonQES generieren Zertifikate auf Antrag berechtigter Stellen.

TSP-X.509 QES und TSP-X.509 nonQES, die Zertifikate für HBA und SMC-B bereitstellen, müssen OCSP-Responder in der TI und im Internet betreiben, über den Zertifikatsstatusabfragen zu allen von diese TSP-X.509 QES und TSP-X.509 nonQES generierten X.509-Zertifikaten beantwortet werden.

TSP-X.509 QES und TSP-X.509 nonQES führen Sperrungen von X.509-Zertifikaten auf Veranlassung berechtigter Stellen durch.

TSP-X.509 nonQES können für ihren Statusinformationsdienst die notwendigen X.509-nonQES OCSP- und CRL-Signerzertifikate bei dem TSP-X.509 nonQES für OCSP- und CRL-Signerzertifikate (OCSP-Signer-CA bzw. CRL-Signer-CA) beantragen (vgl. gemKPT_PKI_TIP#3.2.1). Unabhängig davon können die TSP-X.509 nonQES auch eine eigene OCSP-Signer-CA bzw. CRL-Signer-CA betreiben, die jedoch ebenfalls von der gematik Root-CA abgeleitet sein müssen.

3.1.3 gematik-Root-CA

Die gematik als Verantwortlicher Anbieter der gematik-Root-CA beauftragt einen Dienstleister, der diese im Auftrag der gematik betreibt.

Zur Etablierung einer einheitlich geregelten PKI für nonQES-Zertifikate stellt die gematik als Policy-Authority eine zentrale Root-CA für alle zertifikatsausgebenden TSP-X.509 nonQES bereit. Entsprechend werden alle nonQES-X.509 Sub-CA-Zertifikate in der TI durch die „gematik-Root-CA“ signiert. Ausnahmen bilden hierbei die CA-Zertifikate für eGK, die auf eigenen PKI-Strukturen der Herausgeber basieren können.

Die gematik Root-CA muss einen Statusinformationsdienst im Internet betreiben, über den Zertifikatsstatusabfragen zu allen von dieser ausgestellten X.509 nonQES Sub-CA-Zertifikaten im Internet beantwortet werden. Für die Nutzung dieser X.509 nonQES Sub-CA-Zertifikate in der TI wird die Statusinformation durch die TSL abgebildet.

Sperrungen von ausgestellten X.509 nonQES Sub-CA-Zertifikaten in der TI werden durch entfernen des nonQES-X.509 Sub-CA-Zertifikates aus der TSL bzw. der in der TSL-enthaltenen Statusinformation abgebildet.

Im Internet werden Sperrungen von ausgestellten X.509 nonQES Sub-CA-Zertifikaten über den OCSP-Responder bereitgestellt.

3.1.4 Kartenherausgeber

Der Kartenherausgeber beantragt bei einem durch die gematik zugelassenen TSP-X.509 QES oder TSP-X.509 nonQES die benötigten X.509-Zertifikate.

Der Kartenherausgeber ist verantwortlich für die Zusammenstellung der korrekten semantischen und syntaktischen Feldinhalte zur Einbringung in die Zertifikate und muss

für den Karteninhaber verbindliche Vorgaben treffen, wie die Chipkarten nach Lebensende dauerhaft unbrauchbar gemacht werden.

Verantwortlichkeiten der Kartenherausgeber sind in [gemRL_TSL_SP_CP] beschrieben.

3.1.5 Kartenhersteller

Der Kartenhersteller ist bei der Produktion der Chipkarte für die sichere Einbringung der korrekten Schlüsselmaterialien und Zertifikate in die Karte verantwortlich. Dazu gehören:

- Ein oder mehrere X.509-Zertifikate
- zu den X.509-Zertifikaten zugehörige private Schlüssel

Es liegt in der Verantwortung des Kartenherausgebers, dass hierbei die korrekten Werte in die Chipkarte bzw. das Sicherheitsmodul eingebracht werden.

Chipkarten bzw. Module, die vor Weitergabe als fehlerhaft erkannt werden, werden durch den Kartenhersteller ordnungsgemäß vernichtet und entsorgt. Die Karten und ihre Vernichtung werden dokumentiert.

Der Kartenhersteller kann bei der Produktion einer Chipkarte Dienstleistungen anderer Organisationen in Anspruch nehmen. Typische Dienstleistungen sind die Durchführung der Karteninitialisierung und Kartenpersonalisierung sowie der Versand der produzierten Karten (Lettershop). Die genannten Dienstleistungen können aber auch durch den Kartenhersteller selbst vorgenommen werden. Ein konkretes Modell wird durch diese Spezifikation nicht vorgegeben.

3.1.6 Zertifikatsnehmer

Zertifikatsnehmer können Personen (z. B. Versicherter, Leistungserbringer) oder Organisationen (z. B. medizinische Institution) sein. Diese Zertifikate werden als Personen- und Organisationszertifikate bezeichnet.

Zertifikatsnehmer können auch technische Komponenten (z. B. Konnektor, fachanwendungsspezifischer Dienst) sein. Diese Zertifikate werden als Komponentenzertifikate bezeichnet.

Zertifikatsnehmer können auch technische Signaturdienste (z. B. OCSP-Responder, CRL, TSL-Dienst) sein. Diese Zertifikate werden als Signerzertifikate bezeichnet.

3.1.7 Hersteller

Die Hersteller von Konnektoren und Kartenterminals beantragen bei einem zugelassenen TSP-X.509 nonQES die entsprechenden X.509-Komponentenzertifikate. Die erstellten X.509-Zertifikate werden auf die erforderlichen gerätespezifischen Sicherheitsmodule (gSMC) aufgebracht. Die gSMCs werden in die entsprechenden Konnektoren und Kartenterminals verbaut bzw. eingesteckt.

Der Hersteller tritt als Sperrberechtigter auf und nutzt dafür die vorgesehenen Schnittstellen (s. Kapitel 6.3) des TSP-X.509 nonQES.

3.1.8 Anbieter

Anbieter zentraler Dienste (Betreiber_ZD) und fachanwendungsspezifischer Dienste (Betreiber_FD) beantragen bei einem zugelassenen TSP-X.509 nonQES für jede Komponente bzw. jeden in der TI etablierten Dienst die notwendigen X.509-Zertifikate (vgl. gemKPT_PKI_TIP#3.2.1).

Der Anbieter tritt als Sperrberechtigter auf und nutzt dafür die vorgesehenen Schnittstellen (s. Abschnitt 6.3) des TSP-X.509 nonQES.

3.2 Nachbarsysteme

Für die gematik-Root-CA sind die folgenden Nachbarsysteme relevant:

- TSL-Dienst (bzw. TSL-Signer-CA) bei Ausstellung des X.509-Zertifikats der CA, die das X.509-Zertifikat des TSL-Signers ausstellt (Schritte 1 und 2),
- TSP-X.509 nonQES mit nachgeordneter CA (Schritte 3 und 4).

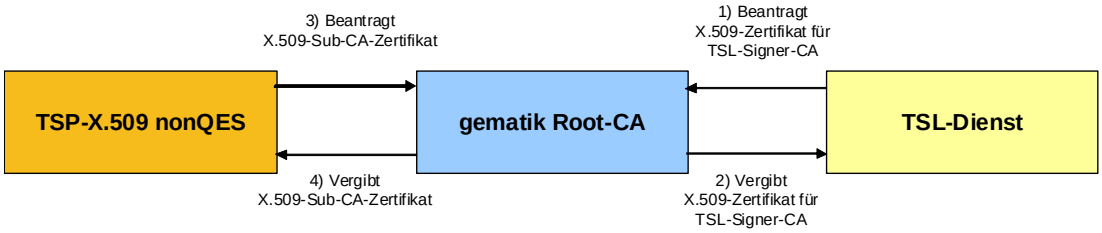

Abbildung 1: Abb_PKI_502 Nachbarsysteme der gematik-Root-CA

Die folgenden Nachbarsysteme sind für TSP-X.509 QES und TSP-X.509 nonQES zu berücksichtigen:

- gematik als verantwortliche Zulassungs- und Registrierungsstelle (Schritte 1 und 2),
- gematik-Root-CA (Schritte 3 und 4 nur für TSP-X.509 nonQES),
- Leistungserbringer, Kartenherausgeber, Hersteller zugelassener technischer Komponenten, Anbieter von Fachanwendungsspezifischen Diensten und Anbieter von zentralen Diensten als Zertifikatsnehmer (Ausgabe von X.509-Zertifikaten) bzw. als Initiator einer Sperrung von X.509-Zertifikaten (Schritte 5 und 6),
- Attributsbestätigende Stellen bei Beantragung der Ausgabe bzw. Sperrung von X.509-Zertifikaten
- Fachanwendungen und technische Komponenten, die Statusauskünfte zu den X.509-Zertifikaten anfragen (Schritte 9 und 10).

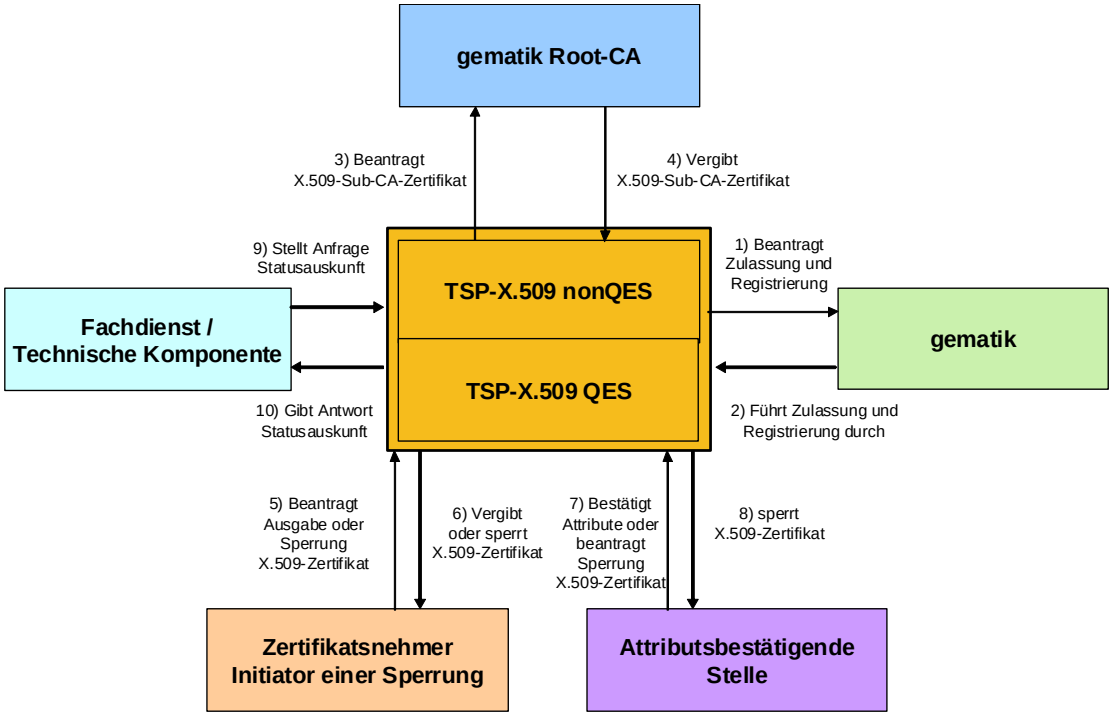

Abbildung 2: Abb_PKI_503 Nachbarsysteme TSP-X.509 QES und TSP-X.509 nonQES

Die Erstellung und Ausgabe von X.509-Zertifikaten für eGK, HBA, SMC-B und gSMC erfolgt im Auftrag der jeweils verantwortlichen Kartenherausgeber.

4 Zerlegung des Produkttyps

4.1 Produkttypen TSP-X.509 QES und TSP-X.509 nonQES

Die Produkttypen TSP-X.509 QES und TSP-X.509 nonQES können (logisch) in die Teilsysteme

- Registrierungsdienst
- Erstellungsdienst,
- Sperrdienst und
- Statusprüfdienst

untergliedert werden. Zur Umsetzung der Dienste sind gemäß [gemKPT_Arch_TIP#5.4] folgende Schnittsellen und Prozesse durch den TSP-X.509 QES und TSP-X.509 nonQES zu implementieren:

- P_Cert_Provisioning

  Die Prozessschnittstelle zur Veranlassung der Erzeugung eines X.509-Personen- oder Organisationszertifikates durch den berechtigten Akteur mit anschließender Bereitstellung des Zertifikats durch die CA.

- P_Cert_Revocation

  Die Prozessschnittstelle zur Veranlassung der Sperrung eines X.509- Personen- oder Organisationszertifikates durch den berechtigten Akteur.

- I_Cert_Provisioning

  Die technische Schnittstelle zur Veranlassung der Erzeugung eines X.509-Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikates durch den berechtigten Akteur mit anschließender Bereitstellung des Zertifikats durch die Zentrale PKI.

- I_Cert_Revocation

  Die technische Schnittstelle zur Veranlassung der Sperrung eines X.509-Komponenten- oder Signer-, nonQES-HBA- oder Organisationszertifikates durch den berechtigten Akteur bei der Zentralen PKI.

- I_OCSP_Status_Information

  Die technische Schnittstelle zur Bereitstellung der Zertifikatsstatusinformation für Personen-, Organisations-, Komponenten- und Signerzertifikate.

Die folgenden Umsetzungen der Schnittstellen sind zu berücksichtigen.

Für Personen- und Organisationszertifikate müssen TSP-X.509 QES und TSP-X.509 nonQES die Schnittstellen P_Cert_Provisioning, P_Cert_Revocation und I_OCSP_Status_Information umsetzen.

Für Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate muss der Anbieter der zentralen PKI (TSP-X.509 nonQES) die Schnittstellen I_Cert_Provisioning, I_Cert_Revocation und I_OCSP_Status_Information umsetzen.

Die folgende Abbildung Abb_PKI_504 zeigt eine Zuordnung der Schnittstellen zu den Teilsystemen des TSP-X.509.

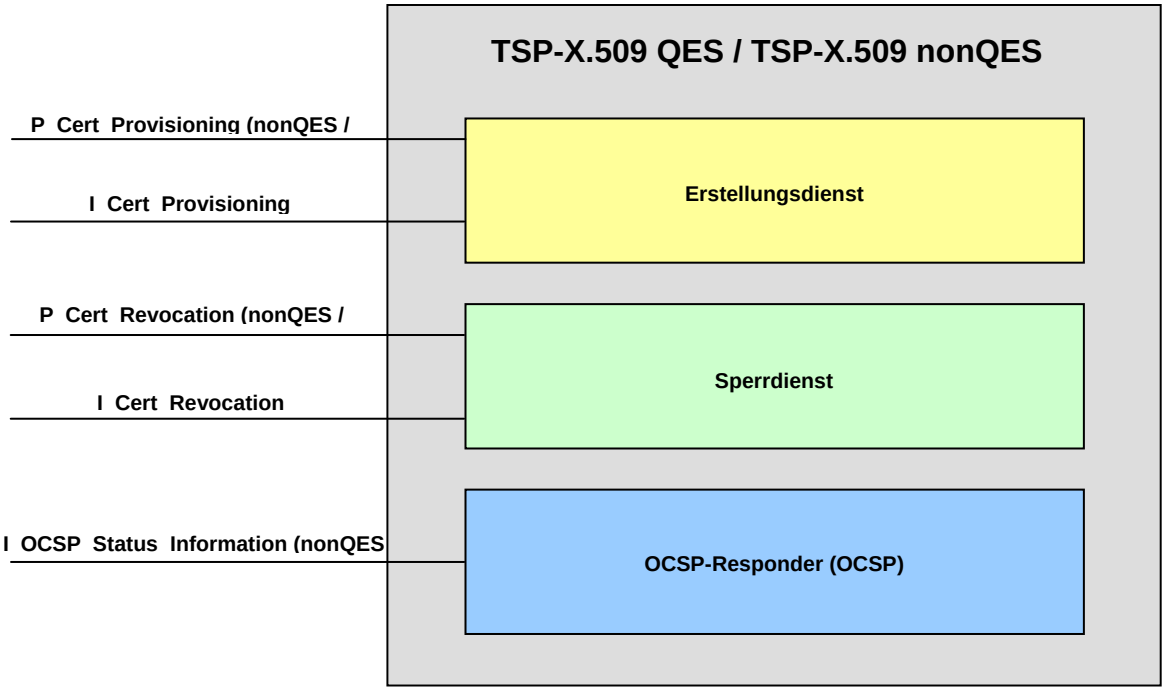

Abbildung 3: Abb_PKI_504 Schnittstellen TSP-X.509 QES und TSP-X.509 nonQES

Zur Umsetzung werden die Schnittstellen P_Cert_Provisioning und I_Cert_Provisioning internen Schnittstellen logisch zugeordnet, um den funktionalen Anteil der Registrierung von Antragstellern im Prozess des Erstellungsdienstes geeignet zu berücksichtigen. Hierzu werden die folgenden internen Schnittstellen verwendet:

- P_Cert_Provisioning_nonQES_Registration

  Schnittstelle zur Registrierung von nonQES-X.509-Personen- und Organisationszertifikaten durch den berechtigten Akteur mit anschließender Bereitstellung des Zertifikats.

- P_Cert_Provisioning_QES_Registration

  Schnittstelle zur Registrierung von QES-X.509-Zertifikaten durch den berechtigten Akteur mit anschließender Bereitstellung des Zertifikats.

- P_Cert_Provisioning_Erstellung

Schnittstelle zur Erstellung von nonQES-Personen- und Organisationszertifikaten und QES-X.509-Zertifikate durch die X.509-CA.

- I_Cert_Provisioning _Registration

  Schnittstelle zur Registrierung der Zentralen PKI von X.509-Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate.

- I_Cert_Provisioning_Erstellung

  Schnittstelle zur Erstellung der Zentralen PKI von X.509-Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate.

Abbildung Abb_PKI_504 zeigt die Zuordnung der umzusetzenden Schnittstellen für die Registrierung und Erstellung von X.509-Zertifikaten gemäß [gemKPT_Arch_TIP] und den zugehörigen internen Schnittstellen.

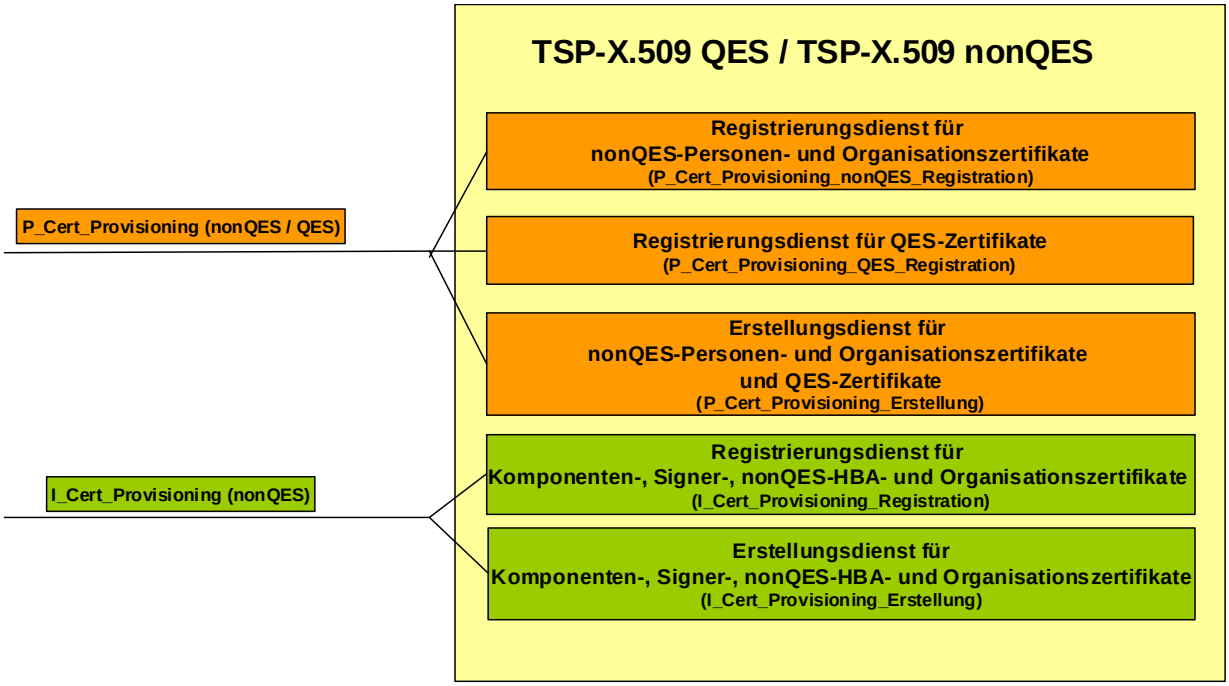

Abbildung 4: Abb_PKI_504 Schnittstellen Registrierungs- und Erstellungsdienst TSP-X.509 QES und TSP-X.509 nonQES

Die nachfolgende Abbildung Abb_PKI_506 integriert zusätzlich den berechtigten Antragsteller für Personen- und Organisationszertifikate bzw. an der Zentralen PKI für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate. Weiterhin wird dargestellt, dass der funktionale Anteil der Registrierung vor der eigentlichen Erstellung des X.509-Zertifikates erfolgt. D.h. aus Sicht TSP-X.509 QES und TSP-X.509 nonQES die Schnittstellen P_Cert_Provisioning_Erstellung und I_Cert_Provisioning Erstellung rein interne Schnittstellen sind. Die Schnittstellen

- P_Cert_Provisioning_nonQES_Registration,
- P_Cert_Provisioning_QES_Registration und
- I_Cert_Provisioning_Registration

sind Schnittstellen nach außen zum Antragsteller.

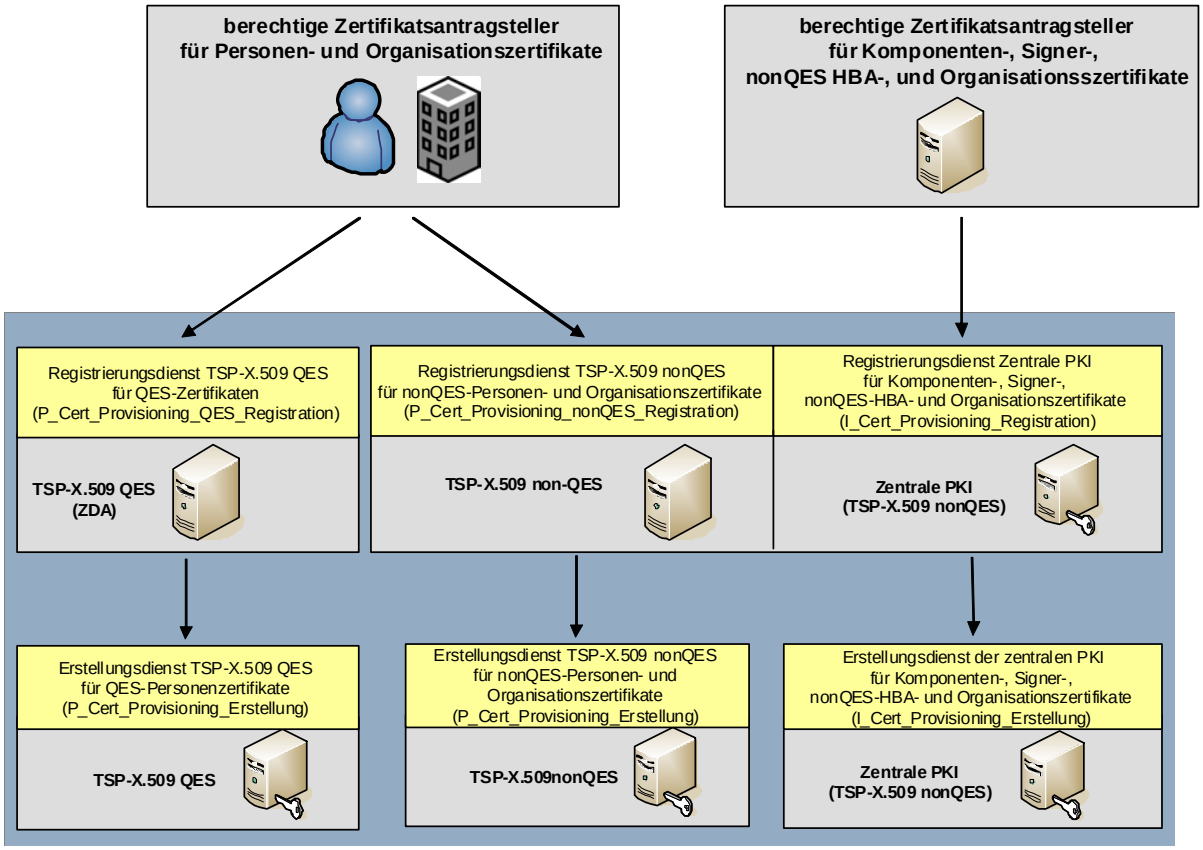

Abbildung 5: Abb_PKI_506 Organisatorische Anordnung der Schnittstelle Registrierungs- und Erstellungsdienst TSP-X.509 QES und TSP-X.509 nonQES

Für die Schnittstellen zur Veranlassung einer Sperrung (Teilsystem Sperrdienst) eines X.509-Zertifikates ist eine entsprechende Aufteilung nicht erforderlich. Es sind die folgenden Schnittstellen zu berücksichtigen.

- P_Cert_Revocation

  Schnittstelle zur Veranlassung einer Sperrung von X.509-Personen- und Organisationszertifikaten durch den berechtigten Akteur.

- I_Cert_Revocation

  Schnittstelle zur Veranlassung einer Sperrung bei der Zentralen PKI von X.509-Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikaten durch den berechtigten Akteur.

Eine Zuordnung der Schnittstelle zu Personen- und Organisationszertifikaten bzw. der Schnittstelle der Zentralen PKI zu Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikaten wird in der Abbildung Abb_PKI_507 dargestellt. Weiterhin ist angegeben, ob die Schnittstelle für den TSP-X.509 nonQES oder TSP-X.509 QES umzusetzen ist.

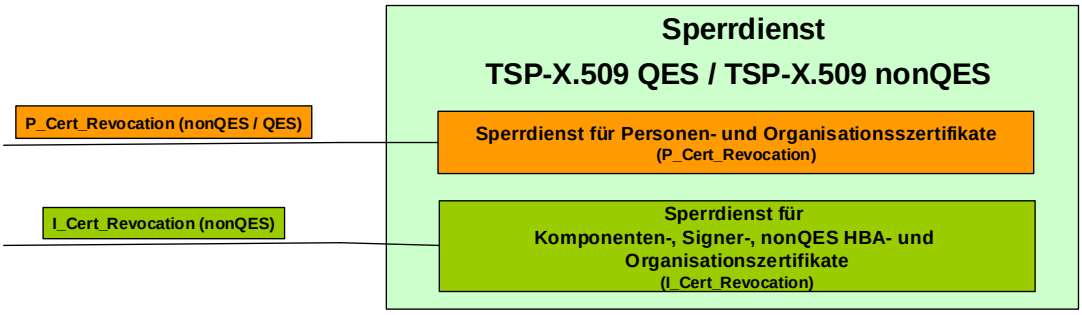

Abbildung 6: Abb_PKI_507 Schnittstellen Sperrdienst des TSP-X.509

Die nachfolgende Abbildung Abb_PKI_508 integriert zusätzlich den berechtigten Sperrantragsteller für Personen- und Organisationszertifikate bzw. an der Zentralen PKI für Komponenten- Signer-, nonQES-HBA- und Organisationszertifikate.

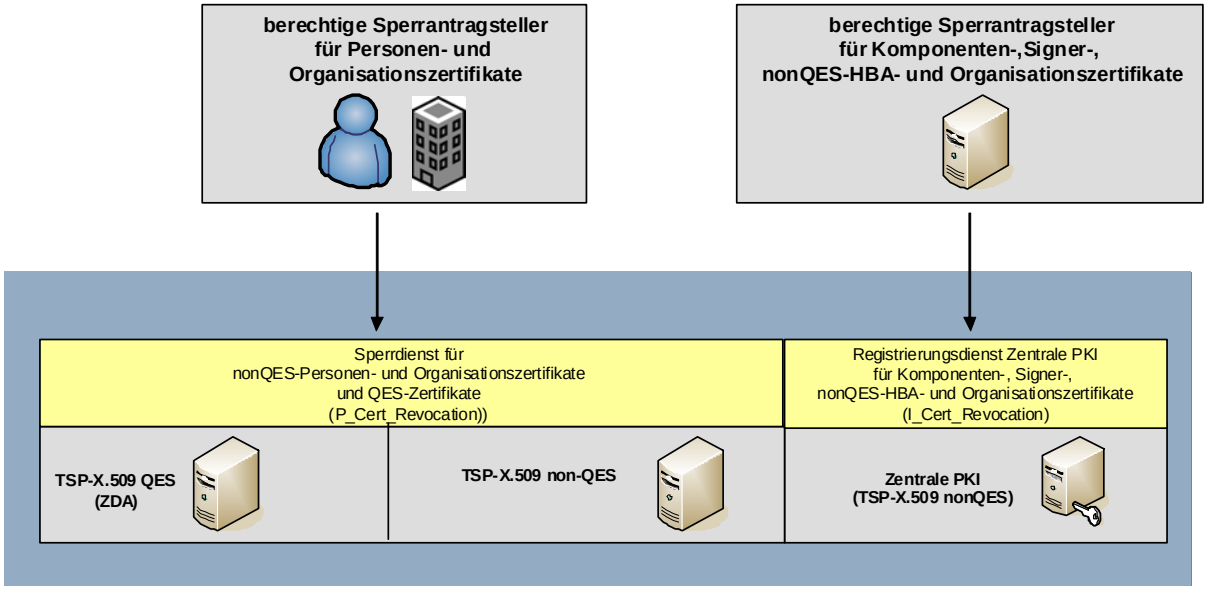

Abbildung 7: Abb_PKI_508 Organisatorische Anordnung Sperrdienst

4.2 Produkttyp gematik-Root-CA

Der Produkttyp gematik-Root-CA bietet die Schnittstelle P_Sub_CA_Certification_X.509 zur Ausstellung und Sperrung von X.509-Zertifikaten nachgeordneter TSP-X.509 nonQES an. Der Produkttyp übernimmt keine weiteren Funktionen.

Eine weitere Untergliederung der Aufbaustruktur des Produkttyps gematik-Root-CA ist nicht erforderlich.

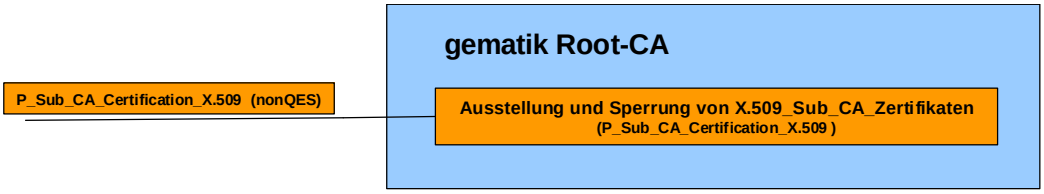

Abbildung 8: Abb_PKI_510 Schnittstellen Erstellung und Sperrung der gematik-Root-CA

4.3 Statusprüfdienst

Für die Schnittstelle I_OCSP_Status_Information zur Ausgabe von Statusauskünften (Teilsystem OCSP-Responder) ist eine Aufteilung ebenfalls nicht erforderlich. Sie ist durch den TSP-X.509 QES, TSP-X.509 nonQES und die gematik Root-CA umzusetzen.

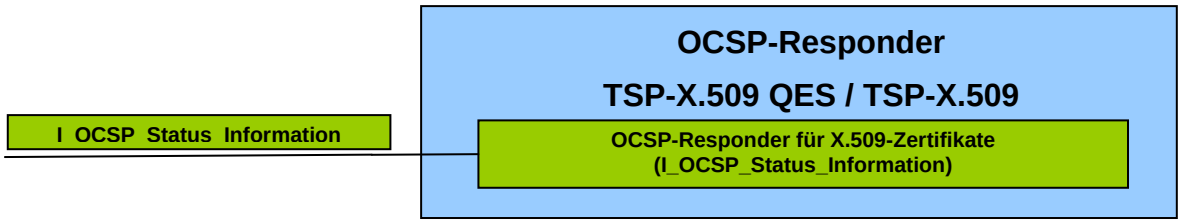

Abbildung 9: Abb_PKI_509 Schnittstellen OCSP-Responder TSP-X.509 QES und TSP-X.509 nonQES

Die Schnittstelle des OCSP-Responder ist nicht Bestandteil dieses Dokumentes sondern ist in [gemSpec_PKI#9.1] beschrieben.

5 Übergreifende Festlegungen

5.1 Ausstellung von X.509-Zertifikaten

Auf Grundlage übergreifender Festlegungen wurde zur Nutzung von PKI-Komponenten eine übergreifende gematik-Policy entwickelt [gemRL_TSL_SP_CP].

⌦ **TIP1-A_3547 Erstellung einer Ausgabepolicy**

TSP-X.509 MÜSSEN für die Produktion von X.509-Zertifikaten eine Ausgabepolicy erstellen, die nicht im Widerspruch zu den übergeordneten Ausgabepolicies stehen darf und mindestens folgende Inhalte beschreibt: a)Festlegungen für Identifizierung, Registrierung, Ausgabe und Sperrung von Zertifikaten sowie Ausstellung von Folgezertifikaten b)Angaben zu organisatorischen (z.B. Rollen, Personal) und technischen Sicherheitsanforderungen (z.B. Schlüsselerzeugung, Backup c)Wirtschaftliche und Rechtliche Angelegenheiten sowie Angaben zur Haftung.⌫

⌦ **TIP1-A_5087 Berücksichtigung und Umsetzung übergeordneter Herausgeber-policies**

TSP-X.509 QES und TSP X.509 nonQES MÜSSEN die übergeordneten Herausgeberpolicies in ihrer Ausgabepolicy berücksichtigen und explizit umsetzen.⌫

Alle Zertifikatsherausgeber stellen sicher, dass im Rahmen der Zertifikatserstellung für den Antragsteller nur genau die Zertifikate erstellt werden, für die der Antragsteller gemäß Ausgabepolicy berechtigt ist.

5.1.1 Erstellung Sicherheitskonzept Zertifikatsprozess durch TSP-X.509

Ein TSP-X.509 muss für den Betrieb einer TSP-X.509 in einem Sicherheitskonzept den Gesamtprozess der X.509-(CA) und die Einhaltung der beschriebenen Maßnahmen auf Verlangen der TI-Plattform nachweisen [gemKPT_PKI_TIP#TIP1-A_2086]. Sind mehrere Organisationen an diesem Prozess beteiligt, sind die technischen- und organisatorischen Schnittstellen sowie deren Absicherung zu beschreiben – ggf. auch durch Referenzierung der Sicherheitskonzepte der beteiligten Organisationen.

⌦ **TIP1-A_3877 Darstellung der Zusammenarbeit von Kartenherausgeber, Kartenhersteller und TSP-X.509 im Sicherheitskonzept**

In dem Sicherheitskonzept des TSP-X.509 MUSS der TSP-X.509 beschreiben, wie die Zusammenarbeit von Kartenherausgeber, Kartenhersteller sowie TSP-X.509 organisiert ist und wie die entsprechenden Sicherheitsmaßnahmen bei den einzelnen Organisationen greifen. Es sind alle im Verantwortungsbereich des TSP-X.509 befindlichen Schnittstellen zu beschreiben. ⌫

5.1.2 Zulassung

⌦ **TIP1-A_3879 Ausstellung von X.509-Zertifikate für zugelassene TSP-X.509**

Die gematik Root-CA MUSS sicherstellen, dass ein X.509-Sub-CA-Zertifikat nur dann erzeugt wird, wenn der beantragende TSP.X.509 aktuell bei der gematik zugelassen ist.⌫

⌦ **TIP1-A_5088 Sektorzulassung für zugelassene TSP-X.509**

TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN sicherstellen, dass ein X.509-Zertifikat für einen HBA oder eine SMC-B in der Produktivumgebung nur dann erzeugt wird, wenn dieser eine Sektorzulassung von dem jeweiligen Kartenherausgeber erhalten hat (gilt nicht für die Produktion von HBA und SMC-B für die Personalisierungsvalidierung).⌫

⌦ **TIP1-A_3880 Bestätigung Auflagen bei Widerruf der Zulassung**

Der TSP-X.509 MUSS bei Widerruf der TSP-X.509-Zulassung durch die gematik den Widerruf sowie die korrekte Durchführung der Auflagen schriftlich gegenüber der gematik dokumentieren und die Umsetzung bestätigen. ⌫

⌦ **TIP1-A_3894 Obligatorisch abzuleitende Sub-CAs unterhalb der „gematik-Root-CA“**

Der TSP-X.509 nonQES MUSS Sub-CA-Zertifikate zur Erstellung von X.509-Zertifikate von der „gematik-Root-CA“ ableiten.
Von dieser Anforderung ausgenommen ist der TSP-X.509nonQES der eGK. ⌫

5.1.3 Datenschutz

Es gelten folgende Datenschutzanforderungen an die gematik-Root-CA und den TSP-X.509 nonQES.

⌦ **TIP1-A_4230 Datenschutzgerechte Antrags- und Sperrprozesse**

TSP-X.509 nonQES und gematik-Root-CA MÜSSEN die Antrags- und Sperrprozesse datenschutzgerecht ausgestalten, d.h. insbesondere ist für die Erhebung, Verarbeitung und Nutzung der Antrags- und Sperrauftragsdaten das Prinzip der Datensparsamkeit und Zweckbindung zu berücksichtigen sowie die technischen und organisatorischen Maßnahmen nach Anlage zu § 9 BDSG sind zu treffen.⌫

⌦ **TIP1-A_4231 Löschung gespeicherter X.509-Zertifikate**

TSP-X.509 MÜSSEN die auf ihren Diensten gespeicherten Zertifikate beim TSP-X.509 nonQES unverzüglich löschen, sobald die gesetzlichen oder vertraglichen Aufbewahrungsfristen erreicht sind.⌫

⌦ **TIP1-A_4232 Löschung von TSP-X.509 nonQES-Zertifikatstatusinformationen, Zertifikats- und Sperranträge**

Der TSP-X.509 nonQES MUSS die Zertifikatsanträge, die Zertifikatstatusinformationen und die Sperraufträge zu einem X.509-Zertifikat unverzüglich löschen, sobald die gesetzlichen oder vertraglichen Aufbewahrungsfristen erreicht sind.⌫

⌦ **TIP1-A_4233 Löschung von gematik-Root-CA Zertifikats- und Sperraufträge**

Die gematik-Root-CA MUSS die Zertifikats- und Sperraufträge zu einem ausgestellten X.509-Zertifikat unverzüglich löschen, sobald die gesetzlichen oder vertraglichen Aufbewahrungsfristen erreicht sind.⌫

⌦ **TIP1-A_4234 Protokollierung von OCSP-Anfragen**

Der TSP-X.509 nonQES und die gematik Root-CA DÜRFEN OCSP-Anfragen NICHT protokollieren. ⌫

⌦ **TIP1-A_4235 Fehlerprotokollierung**

Falls es erforderlich sein sollte, dass TSP-X.509 nonQES und gematik-Root-CA eine Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung durchführen, MÜSSEN die Protokolldaten entsprechend des Prinzips der Datenvermeidung und Datensparsamkeit nach §3a BDSG derart gestaltet sein, dass nur personenbezogene Daten in der Art und dem Umfang enthalten sein, wie sie zur Behebung erforderlich sind.⌫

5.1.4 Unterscheidung produktive TSP-X.509 und Test-TSP-X.509

Bei den TSP-X.509 wird zwischen einem Produktiv-TSP-X.509 und einem Test-TSP-X.509 unterschieden.

Der Anbieter der gematik-Root-CA stellt sowohl eine produktive gematik-Root-CA als auch eine gematik Test-Root-CA zur Verfügung. Anbieter einer TSP-X.509 QES stellen sowohl eine produktive TSP-X.509 QES als auch eine Test-TSP-X.509 QES zur Verfügung. Anbieter einer TSP-X.509 nonQES stellen sowohl eine produktive TSP-X.509 nonQES als auch eine Test-TSP-X.509 nonQES zur Verfügung.

⌦ **TIP1-A_4427 Betrieb einer Test-TSP-X.509**

Jeder TSP-X.509 MUSS neben einer produktiven TSP-X.509-CA ebenfalls eine Test-TSP-X.509-CA betreiben. ⌫

⌦ **TIP1-A_3660 Trennung der TSP-X.509-Betriebsumgebungen**

TSP-X.509 MÜSSEN sicherstellen, dass das Testsystem von dem Produktivsystem technisch, organisatorisch und betrieblich so getrennt werden, dass keine gegenseitige Beeinflussung und keine Verwechslung möglich sind.⌫

⌦ **TIP1-A_4428 Registrierung eines Test-TSP-X.509**

Der TSP-X.509 MUSS eine Test-TSP-X.509 bei der gematik registrieren.⌫

5.2 Sperrung von X.509-Zertifikaten

⌦ **TIP1-A_3630 Implementierung eines Sperrdienstes für nonQES-Personen- und Organisationszertifikate**

Der TSP-X.509 nonQES MUSS einen Sperrdienst für nonQES-Zertifikate implementieren und die geforderten organisatorischen Schnittstellen für die Sperrung implementieren.⌫

TIP1-A_3643 Implementierung eines Sperrdienstes für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS einen Sperrdienst für Komponenten- und Signer-, nonQES-HBA- und Organisationszertifikate sowie die geforderten technischen und organisatorischen Schnittstellen für die Sperrung implementieren.

TIP1-A_5376 Erreichbarkeit des Sperrdienstes von TSP-X.509 nonQES und gematik Root-CA

Der TSP-X.509 nonQES und der Anbieter der gematik Root-CA MÜSSEN mindestens in der Zeit von Mo.-So. 6-22 Uhr für die Annahme von Sperraufträgen der Sperrberechtigten erreichbar sein.

5.3 Schutzbedarfsfeststellung

TIP1-A_3548 Schützenswerte Objekte

TSP-X.509 QES, TSP-X.509 nonQES und die gematik Root-CA MÜSSEN die folgenden kryptographischen Objekte als schützenswerte Objekte in ihrem Sicherheitskonzept berücksichtigen: (a) Private Schlüssel (Erstellungsdienst und OCSP-Responder), (b) Öffentlicher Schlüssel (Erstellungsdienst und OCSP-Responder), (c) Öffentlicher Schlüssel von Antragstellern, (d) Anträge zur Ausstellung von X.509-Zertifikaten, (e) Authentisierungsinformationen von Sperrberechtigten, (f) Dokumentation über beauftragte und durchgeführte Sperrungen, (g) Statusinformationen, (h) Zulassungsdokumente, (i) Registrierungsdokumente, (j) Authentisierungsinformationen zur Authentisierung von internen Akteuren bzw. Rollen, (k) Protokolldaten, (l) Konfigurationsdaten.

TIP1-A_3549 Vorgaben zum Schutzbedarf durch die gematik

TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN die Vorgaben der gematik hinsichtlich der Einstufung des Schutzbedarfs gemäß dem Ergebnis der Schutzbedarfsfeststellung der TI berücksichtigen.

TIP1-A_3550 Spezifische Erhöhung des Schutzbedarfs ist zulässig

Der TSP-X.509 KANN die durch die gematik festgelegte Einstufung des Schutzbedarfs spezifisch erhöhen.

TIP1-A_3881 Schutzbedarf darf nicht verringert werden

Der TSP-X.509 DARF die durch die gematik festgelegte Einstufung des Schutzbedarfs NICHT verringern.

TIP1-A_3883 Sicherstellung TSP-X.509 OCSP-Responder und Sperrdienst bei nicht-sicherheitskritischen Incidents

Die TSP-X.509 MÜSSEN sicherstellen, dass im Falle nicht-sicherheitskritischer Incidents der OCSP-Responder und Sperrdienst in der vereinbarten Dienstgüte für die bereits ausgegebenen nonQES-CA- und EE-Zertifikate bis zu ihrem regulären Ablauf in der TI bereitgestellt werden.

5.4 Sichere Kommunikation zwischen Rollen und Diensten

⌦ **TIP1-A_3554 Gesicherte interne Schnittstellen des TSP-X.509 QES und TSP-X.509 nonQES**

TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN für den internen Datenaustausch einen Mechanismus zur Sicherung der Datenintegrität, der Authentizität und zur Vertraulichkeit der Daten zur Verfügung stellen. ⌫

⌦ **TIP1-A_3555 Datenaustausch zwischen gematik und TSP-X.509 nonQES und gematik Root-CA**

TSP-X.509 nonQES und gematik Root-CA MÜSSEN für den Datenaustausch zwischen gematik und TSP-X.509 nonQES bzw. zwischen gematik und gematik Root-CA einen Mechanismus zur Sicherung der Datenintegrität, der Authentizität und zur Vertraulichkeit der Daten zur Verfügung stellen. ⌫

⌦ **TIP1-A_3557 Gesicherte externe Schnittstellen des TSP-X.509 nonQES**

TSP-X.509 nonQES MUSS für den Datenaustausch mit anderen Rollen und Diensten einen Mechanismus zur Sicherung der Datenintegrität, der Authentizität und zur Vertraulichkeit der Daten zur Verfügung stellen. Hierzu gehören die Schnittstellen des TSP-X.509 nonQES a) zum berechtigten Zertifikatsantragsteller zur Beantragung und Ausstellung von X.509-Personen- und Organisationszertifikaten, b) zum berechtigten Hersteller oder Anbieter zur Beantragung und Ausstellung von X.509-Komponentenzertifikaten, c) zum berechtigten TSP-X.509 nonQES zur Beantragung und Ausstellung von Signerzertifikaten, d) zum berechtigten TSP-X.509 QES zur Beantragung und Ausstellung von nonQES-HBA-Zertifikaten e) zum berechtigten Kartenherausgeber zur Beantragung und Ausstellung von Organisationszertifikaten f) zum Sperrantragsteller für die automatisierte Sperrung von X.509-Komponenten-, Signer-, nonQES- und Organisationszertifikaten. ⌫

Hierbei sind die Anforderungen zur Verwendung kryptographischer Algorithmen in der Telematikinfrastrukur zu berücksichtigen [gemSpec_Krypt].

5.5 Schutz der gematik Root-CA

⌦ **TIP1-A_5371 Systemtechnische Trennung bei Aufbau und Betrieb der gematik Root-CA**

Der Anbieter der gematik Root-CA MUSS sicherstellen, dass die gematik Root-CA hinsichtlich der Signaturidentitäten vollständig getrennt von anderen Systemen und deren Signaturidentitäten aufgebaut und betrieben wird. ⌫

6 Funktionsmerkmale

⌦ **TIP1-A_3558 Schnittstellen TSP-X.509 nonQES für Personen- und Organisationszertifikate**

Der TSP-X.509 nonQES MUSS zur Ausstellung von Personen- und Organisationszertifikaten die Schnittstellen P_Cert_Provisioning, P_Cert_Revocation und I_OCSP_Status_Information umsetzen.⌫

⌦ **TIP1-A_3559 Schnittstellen TSP-X.509 nonQES für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate**

Der Anbieter der Zentralen PKI (TSP-X.509 nonQES) MUSS zur Ausstellung von Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikaten die Schnittstellen I_Cert_Provisioning, I_Cert_Revocation und I_OCSP_Status_Information umsetzen.⌫

⌦ **TIP1-A_3560 Obligatorische Schnittstellen TSP-X.509 QES**

Der TSP-X.509 QES MUSS die Schnittstellen P_Cert_Provisioning, P_Cert_Revocation und I_OCSP_Status_Information umsetzen.⌫

⌦ **TIP1-A_3562 Schnittstellen gematik-Root-CA**

Der Anbieter der gematik-Root-CA MUSS die Schnittstelle P_Sub_CA_Certification_X.509 zur Ausstellung von X.509-Zertifikaten für nachgeordnete CAs umsetzen.⌫

6.1 Ausstellung von Personen- und Organisationszertifikaten

TSP-X.509 QES und TSP-X.509 nonQES muss sicherstellen, dass nur für berechtigte Antragsteller Personen- und Organisationszertifikate erstellt werden.

Der Registrierungsdienst registriert, identifiziert und authentisiert den berechtigten Zertifikatsantragsteller, empfängt dazu die Antragsdaten und sendet die für die Zertifikatserstellung erforderlichen Daten an den Erstellungsdienst. Nach Erstellung der beantragten X.509-Zertifikate durch den Erstellungsdienst, liefert der Registrierungsdienst die Zertifikate an den Kartenherausgeber aus.

Die Beantragung zur Zertifikatserstellung wird von Antragsberechtigten durchgeführt und von den Berechtigungsprüfenden Stellen bestätigt.

Der Erstellungsdienst des TSP-X.509 erstellt mit seiner X.509-CA die Personen- und Organisationszertifikate und liefert die X.509-Zertifikate an den Registrierungsdienst zur Übermittlung an den Zertifikatsantragsteller zurück.

Für die Prüfung der Antragsberechtigung muss eine Berechtigungsprüfende Stelle übergreifend festlegen, wer welche Zertifikate (Komponenten, Versicherte, etc.) beantragen darf und Berufsgruppenattribute bestätigen darf.

Zur Erstellung der Personen- und Organisationszertifikate werden die in Tab_PKI_501 zusammengefassten Rollen zur Berechtigungsprüfung definiert.

Tabelle 1: Tab_PKI_501 Allgemeine Übersicht der Rollen und deren Aufgaben beim Registrierungsdienst

Rolle	Aufgabe/Funktion
TSP-X.509 QES, TSP-X.509 nonQES	nimmt Anfragen entgegen und liefert Zertifikate nach Erstellung aus
Antragsberechtigter	beantragt Zertifikat und setzt dieses nach Auslieferung ein
Berechtigungsprüfende Stelle	verwaltet wer die Berechtigung besitzt, einen bestimmten Zertifikatstyp zu beantragen und teilt diese Berechtigungen dem TSP-X.509 mit

Gemäß Tab_PKI_502 gelten folgende Zuständigkeiten für die berechtigte Antragstellung von nonQES-Zertifikaten für Leistungserbringer, LEO- bzw. KTR-Organisationen und Versicherte.

Tabelle 2: Tab-PKI_502 Berechtigte Zertifikatsantragsteller für non-QES Leistungserbringer-, LEO bzw. KTR-Organisation und Versichertenzertifikate

Zertifikatstyp	Berechtigte Zertifikatsantragsteller	Berechtigungsprüfende Stelle	Zertifikatsnehmer
C.HP.AUT C.HP.ENC	Leistungserbringer	herausgebende LEO	Leistungserbringer
C.HCI.AUT C.HCI.ENC C.HCI.OSIG	Leistungserbringer der med. Institution	herausgebende LEO	med. Institution
	KTR-Organisation	KTR-Organisation	Kostenträger-Geschäftsstelle
C.CH.AUT C.CH.ENC C.CH.AUTN C.CH.ENCV	herausgebender Kostenträger	herausgebender Kostenträger	Versicherter

Gemäß Tab_PKI_503 gelten folgende Zuständigkeiten für die berechtigte Antragstellung von QES-Zertifikate für Leistungserbringer.

Tabelle 3: Tab_PKI_503 Berechtigte Zertifikatsantragsteller für QES Leistungserbringerzertifikate

Zertifikatstyp	Berechtigte Zertifikatsantragsteller	Berechtigungsprüfende Stelle	Zertifikatsnehmer
C.HP.QES	Leistungserbringer selbst	herausgebende LEO	Leistungserbringer

Die Abbildung Abb_PKI_511 stellt die Zuständigkeiten der Rollen bei der Antragsstellung der Personen- und Organisationszertifikate dar.

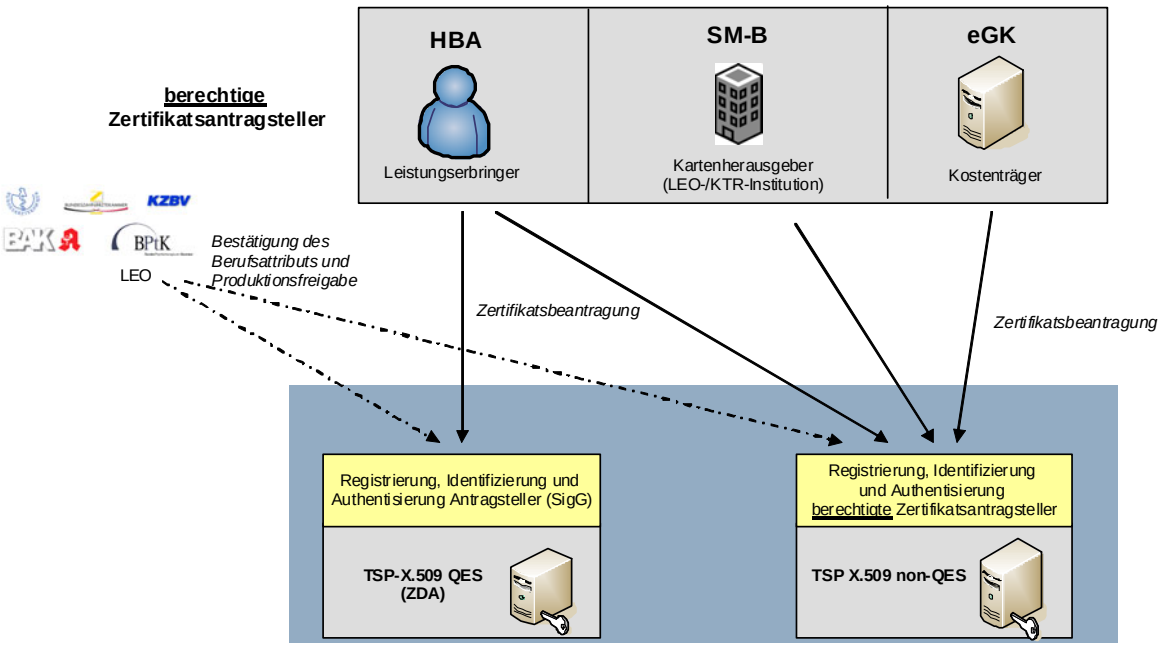

Abbildung 10: Abb_PKI_511 Zuständigkeiten der Rollen bei Zertifikatsantragstellung der Personen- und Organisationszertifikate

Bei der Ausstellung von Zertifikaten wird zwischen folgenden Schnittstellen unterschieden:

- Registrierungsdienst für nonQES-Personen- und Organisationszertifikate (P_Cert_Provisioning_nonQES_Registration)
- Registrierungsdienst für QES-Zertifikate (P_Cert_Provisioning_QES_Registration)
- Erstellungsdienst für QES-Personen sowie non-QES-Personen- und Organisationszertifikaten (P_Cert_Provisioning_Erstellung)

6.1.1 Schnittstelle P_Cert_Provisioning_nonQES_Registration

6.1.1.1 Schnittstellendefinition

⌦ **TIP1-A_3564 Bereitstellung eines Registrierungsdienstes**

Der TSP-X.509 nonQES MUSS die technischen und organisatorischen Voraussetzungen schaffen, um die Anforderungen an den Registrierungsdienst für nonQES-Zertifikate für Leistungserbringer, LEO und KTR-Institutionen sowie Versicherte zu erfüllen. ⌫

Gemäß [gemRL_TSL_SP_CP#4.2.3] muss der TSP-X.509 nonQES einen Zertifikatsantragssteller identifizieren und eine vollständige Prüfung der Antragsdaten gewährleisten.

⌦ **TIP1-A_3565 Certificate Policy des TSP-X.509 nonQES**

Der TSP-X.509 nonQES MUSS in seiner CP (bzw. CPS) festlegen, a) welche Stellen für die Zertifikatsbeantragung von nonQES-Personen- und Organisations-

zertifikate berechtigt sind und b) wie die Registrierung zur eindeutigen Identifikation und Authentisierung der berechtigten Zertifikatsantragsteller durchzuführen ist.⌫

⌦ **TIP1-A_3567 Abgestimmtes Antragsverfahren zwischen TSP-X.509 nonQES und Kartenherausgeber**

Der TSP-X.509 nonQES MUSS das Antragsverfahren mit den Kartenherausgebern für HBAs, eGKs, und SMC-Bs abstimmen und bereitstellen.⌫

⌦ **TIP1-A_3569 Weiterleitung von Zertifikatsanträgen an Registrierungsdienst**

Der TSP-X.509 nonQES MUSS bei Eingang eines Zertifikatsantrags zur Erstellung von Personen- und Organisationszertifikaten sicherstellen, dass der Zertifikatsantrag an den Erstellungsdienst des TSP-X.509 nonQES nur weitergeleitet wird, wenn a) der berechtigte Zertifikatsantragssteller erfolgreich identifiziert und authentisiert wurde, b) der Antrag vollständig war und erfolgreich geprüft werden konnte, c) die Berechtigungsprüfende Stelle die Berechtigung der Antragsstellung und das Berufsgruppenattribut bestätigt, d) alle für die Erstellung des beauftragten X.509-Zertifikats obligatorischen Zertifikatsdaten übermittelt wurden.⌫

⌦ **TIP1-A_5089 Negative Prüfung von nonQES-Zertifikatsanträgen**

Ist die Überprüfung des Zertifikatsantrags negativ verlaufen, MUSS der TSP-X.509 nonQES sicherstellen, dass keine Zertifikatsanträge an Bestätigungsprüfende Stellen zur Bestätigung des Berufsgruppenattributs und Produktionsfreigabe weitergeleitete werden.⌫

⌦ **TIP1-A_5086 Eingangsdaten der Bestätigungsprüfende Stelle für Produktion von nonQES-Zertifikaten für Leistungserbringer**

Der TSP-X.509 nonQES MUSS sicherstellen, dass die folgenden Daten für die Erstellung von X.509-Zertifikaten für Leistungserbringer von der Bestätigungsprüfende Stellen zur Bestätigung des Berufsgruppenattributs und Produktionsfreigabe vorliegen.

- Produktionsfreigabe
- UID des Antragsstellers (optional)
- Telematik-ID⌫

⌦ **TIP1-A_3570 Eingangsdaten Leistungserbringerzertifikat**

Die TSP-X.509 nonQES MUSS sicherstellen, dass mindestens die in den Zertifikatsprofilen der HBA-Kartenherausgeber als Pflichtfelder festgelegten spezifischen Daten des Zertifikatsnehmers für die Erstellung von X.509-Zertifikaten für Leistungserbringer zu jedem Zertifikatsantrag vorliegen.⌫

⌦ **TIP1-A_3571 professionItem und professionOID für LE**

Der TSP-X.509 nonQES MUSS für Leistungserbringer die Berufsbezeichnung für das Feld professionItem sowie die vorgegebene OID zu der angegeben Berufsbezeichnung für das Attribut Admission des X.509-Personen- und Organisationszertifikates als professionOID gemäß [gemSpec_OID#Tab_PKI_402] zu den Zertifikatserstellungsdaten hinzufügen.⌫

Die Object Identifier sind im Dokument [gemSpec_OID] angegeben.

⌦ **TIP1-A_3572 Eingangsdaten Organisationszertifikate**

Die TSP-X.509 nonQES MUSS sicherstellen, dass mindestens die in [gemSpec_PKI#Tab_PKI_238], [gemSpec_PKI#Tab_PKI_239] und [gemSpec_PKI#Tab_PKI_240] mit der Kardinalität 1 festgelegten spezifischen Daten des Zertifikatsnehmers für die Erstellung von X.509-Organistationszertifikate für LEO- und KTR-Institutionen zu jedem Zertifikatsantrag vorliegen. ⌫

⌦ **TIP1-A_3573 professionOID für LEO- und KTR-Organisationszertifikate**

Der TSP-X.509 nonQES MUSS die von dem Kartenherausgeber für das Feld professionItem sowie die vorgegebene OID zu der angegebene Institutionsbezeichnung (professionItem) des X.509-Organisationszertifikates als professionOID gemäß [gemspec_OID#Tab_PKI_403] zu den Zertifikatserstellungsdaten hinzufügen.⌫

⌦ **TIP1-A_3574 Eingangsdaten Versichertenzertifikate ohne Pseudonym**

Der TSP-X.509 nonQES MUSS sicherstellen, dass mindestens die in [gemSpec_PKI#Tab_PKI_232] und [gemSpec_PKI#Tab_PKI_233] mit der Kardinalität 1 festgelegten spezifischen Daten des Zertifikatsnehmers für die Erstellung von X.509-Personenzertifikaten für Versicherte zu jedem Zertifikatsantrag vorliegen. ⌫

⌦ **TIP1-A_3575 Eingangsdaten Versichertenzertifikate AUTN und ENCV**

Der TSP-X.509 nonQES MUSS sicherstellen, dass mindestens die in [gemSpec_PKI#Tab_PKI_235] und [gemSpec_PKI#Tab_PKI_236] mit der Kardinalität 1 festgelegten spezifischen Daten des Zertifikatsnehmers für die Erstellung der X.509-Zertifikate vom Typ AUTN und ENCV für Versicherte zu jedem Zertifikatsantrag vorliegen. ⌫

⌦ **TIP1-A_3576 professionItem und professionOID für Versichertenzertifikate**

Der TSP-X.509 nonQES MUSS für alle Versichertenzertifikate die zu „oid_versicherter“ zugeordnete Beschreibung in das Feld professionItem sowie die zugehörige OID in das Feld professionOID gemäß [gemSpecOID#Tab_PKI_402] für das Attribut Admission des X.509-Zertifikates zu den Zertifikatsdaten hinzufügen.⌫

⌦ **TIP1-A_3577 Optionale Eingangsdaten**

Der TSP-X.509 nonQES MUSS die in den Zertifikatsprofilen [gemSpec_PKI#5] als optional gekennzeichneten Daten an den Erstellungsdienst des TSP-X.509 nonQES übermitteln, wenn diese vom berechtigten Zertifikatsantragssteller für Personen- und Organisationszertifikate im Rahmen des Antragsverfahrens übermittelt werden. ⌫

⌦ **TIP1-A_3580 Übermittlung der Antragsdaten an Erstellungsdienst**

Der Registrierungsdienst des TSP-X.509 nonQES MUSS für die Erstellung der X.509-Personen- und Organisationszertifikate mindestens alle notwendigen Zertifikatsdaten an den Erstellungsdienst weiterleiten.⌫

⌦ **TIP1-A_3581 Ausgangsdaten für Personen- und Organisationszertifikate**

Der Registrierungsdienst des TSP-X.509 nonQES MUSS pro Zertifikatsantrag mindestens das erstellte X.509-Personen- und Organisationszertifikat als Ausgabedatum sowie weitere Daten, die eine eindeutigen Bezug zur Bestellung ermöglichen, bereitstellen. ⌫

⌦ **TIP1-A_5090 Rückmeldung Zertifikatsinformationen (nonQES) an Bestätigende Stelle**

TSP-X.509 nonQES MUSS der Bestätigenden Stelle des Berufgruppenattributes über die Ausstellung des Zertifikats informieren und die folgenden Daten zurückliefern:

- das erzeugte nonQES-Zertifikat
- Ablaufdatum des Zertifikates ⌫

⌦ **TIP1-A_3884 Umgang mit nicht-sicherheitskritischen Incidents für nonQES-Personen- und Organisationszertifikate**

Der TSP-X.509 nonQES MUSS sicherstellen, dass ab dem Zeitpunkt der Feststellung eines nicht-sicherheitskritischen Incidents, bis zum Entscheid des Incident-Managements über das weitere Vorgehen, keine Zertifikatsanträge für X.509-Personen- und Organisationszertifikate der betroffenen CA entgegengenommen oder an den Erstellungsdienst des TSP-X.509 nonQES weitergeleitet wird. ⌫

6.1.1.2 Umsetzung

⌦ **TIP1-A_3582 Umsetzung Registrierungsdienst TSP-X.509 nonQES für Personen- und Organisationszertifikate**

Der TSP-X.509 nonQES MUSS in seinem Registrierungsdienst für X.509-Personen- und Organisationszertifikate die folgenden Schritte durchführen:

(1) Der TSP-X.509 nonQES MUSS dem berechtigten Zertifikatsantragsteller eine Schnittstelle zur Beantragung, Identifizierung und Ausgabe eines X.509-Personen- und Organisationszertifikats bereitstellen

(2) Der TSP-X.509 nonQES MUSS eine Schnittstelle zur Bestätigenden Stelle einrichten, um die Berechtigung des Antragstellers sowie die Berufsgruppenattributbestätigung zu erhalten.

(3) Der TSP-X.509 nonQES MUSS nach dem Eingang des Antrags diesen auf Vollständigkeit prüfen und den Zertifikatsantragssteller registrieren, identifizieren und authentisieren.

(4) Der TSP-X.509 nonQES, MUSS den Zertifikats-Request an den Erstellungsdienst weiterleiten, wenn dieser den Zertifikatsantragsteller eindeutig identifiziert und die Prüfung des Antrags, dass dieser berechtigt ist X.509-Zertifikate zu beantragen, zu einem positiven Ergebnis geführt hat. Konnte der Zertifikatsantragsteller nicht identifiziert werden oder hat die Prüfung des Antrags zu einem negativem Ergebnis geführt, wird der Zertifikatsantrag abgelehnt.

(5) Der Registrierungsdienst des TSP-X.509 nonQES erhält vom Erstellungsdienst des TSP-X.509 das erstellte Personen- und Organisationszertifikat zurück.

(6) Der Registrierungsdienst des TSP-X.509 nonQES MUSS das Zertifikat an den berechtigten Zertifikatsantragssteller ausliefern.

(7) Der Registrierungsdienst des TSP-X.509 nonQES MUSS der Bestätigen Stelle des Berufgruppenattributes das Zertifikat und zertifikatsrelevante Informationen zurückliefern. ⌫

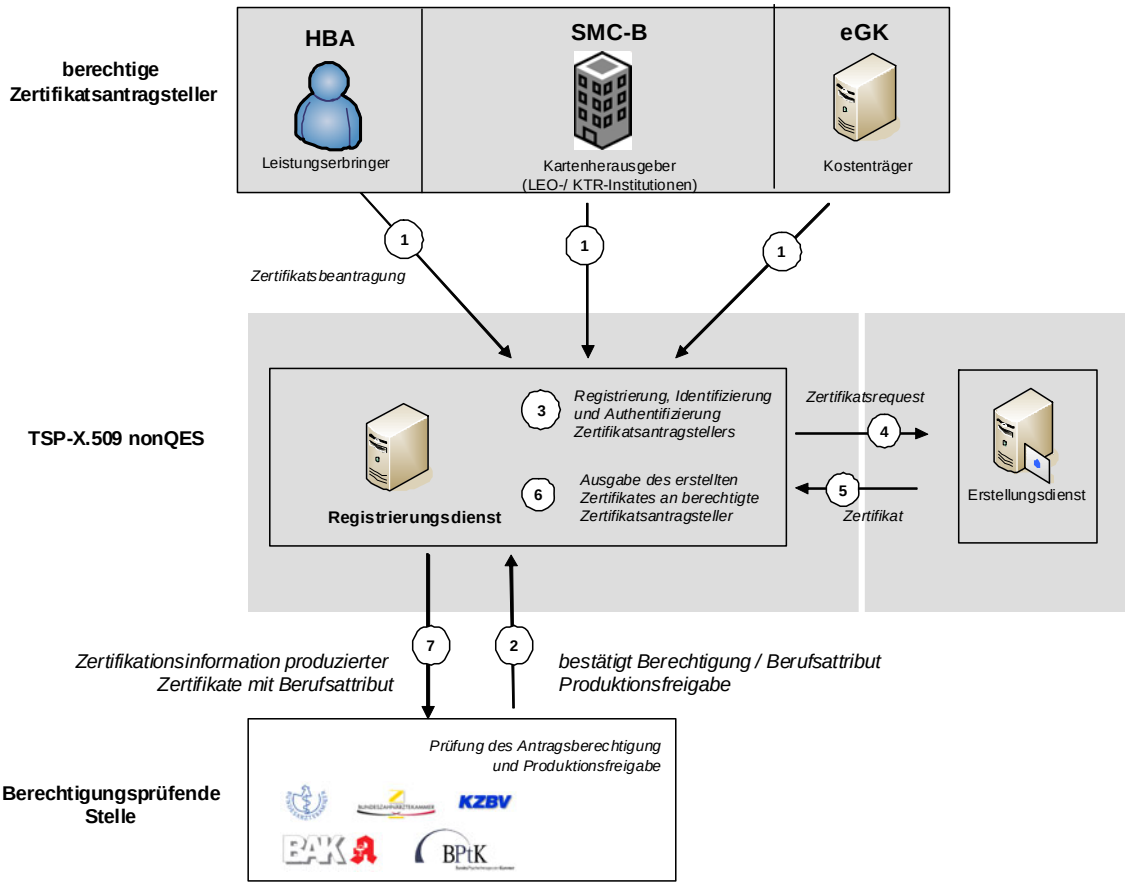

Abbildung 11: Abb_PKI_512 Prozessablauf Registrierungsdienst nonQES-Personen- und Organisationszertifikate

6.1.2 Schnittstelle P_Cert_Provisioning_QES_Registration

6.1.2.1 Schnittstellendefinition

Dieser Abschnitt enthält spezifische Ausprägungen des Registrierungsprozess der Leistungserbringer zur Bereitstellung von qualifizierten X.509-Zertifikaten durch TSP-X.509 QES.

⌦ **TIP1-A_3584 Prozessgestaltung für QES-Zertifikat nach SigG/SigV**

Der TSP-X.509 QES MUSS seine Antrags- und Ausgabeprozesse sowie Registrierungs-, Erstellungs- und Statusprüfdienst OCSP-Responder für QES-Zertifikate gemäß den Vorgaben aus SigG/SigV durchführen. ⌫

⌦ **TIP1-A_5091 KammerIdentverfahren**

Sollte die Bestätigende Stelle über ein nach SigG bestätigtes Sicherheitskonzept „KammerIdent“ zur Identifizierung von Antragstellern verfügen, MUSS der TSP-X.509 QES dieses – auf Wunsch der bestätigenden Stelle – in seinem Sicherheitskonzept einbinden und die (kostenlose) Identifizierung des Antragstellers durch die Bestätigende Stelle ermöglichen. ⌫

⌦ **TIP1-A_5092 Negative Prüfung von QES-Zertifikatsanträgen**

Ist die Überprüfung des Zertifikatsantrags negativ verlaufen, MUSS der TSP-X.509 QES sicherstellen, dass keine Zertifikatsanträge an Bestätigungsprüfende Stellen zur Bestätigung des Berufsgruppenattributs und Produktionsfreigabe weitergeleitete werden.⌫

⌦ **TIP1-A_5093 Eingangsdaten der Bestätigungsprüfende Stelle für Produktion von QES-Zertifikaten für Leistungserbringer**

Der TSP-X.509 QES MUSS sicherstellen, dass die folgenden Daten für die Erstellung von X.509-Zertifikaten für Leistungserbringer von der Bestätigungsprüfende Stellen zur Bestätigung des Berufsgruppenattributs und Produktionsfreigabe vorliegen.

- Produktionsfreigabe
- UID des Antragsstellers (optional)
- Telematik-ID⌫

⌦ **TIP1-A_3585 Eingangsdaten Leistungserbringerzertifikat (QES)**

Die Registrierungsstelle des TSP-X.509 QES MUSS sicherstellen, dass mindestens die in gemSpec_PKI#Tab_PKI_218 mit der Kardinalität 1 festgelegten spezifischen Daten des Zertifikatsnehmers für die Erstellung von X.509-Zertifikaten für Leistungserbringer zu jedem Zertifikatsantrag vorliegen.⌫

⌦ **TIP1-A_3586 professionItem und der professionOID für LE (QES)**

Der TSP-X.509 QES MUSS für den Leistungserbringer die Berufsbezeichnung in das Feld professionItem sowie die vorgegebene OID zu der angegeben Berufsbezeichnung in das Attribut Admission des X.509-QES-Zertifikates als professionOID gemäß [gemSpec_OID#Tab_PKI_402] zu den Zertifikatserstellungsdaten hinzufügen.⌫

Die Object Identifier sind im Dokument [gemSpec_OID] angegeben.

⌦ **TIP1-A_3587 Ausgabe von nonQES-Zertifikate**

Der TSP-X.509 QES KANN auch als TSP-X.509 nonQES für berechtigte Zertifikatsantragssteller agieren. ⌫

⌦ **TIP1-A_3588 Abstimmung des Antragsverfahrens**

Der TSP-X.509 QES MUSS mit dem Kartenherausgeber die Antragsverfahren festlegen und in seiner CP (bzw. CPS) beschreiben, wenn der TSP-X.509 QES im

Rahmen der Zertifikatserstellung für einen HBA mit der Erstellung von QES und nonQES-Zertifikaten beauftragt wird.⌫

⌦ **TIP1-A_5094 Rückmeldung Zertifikatsinformationen (QES) an Bestätigende Stelle**

TSP-X.509 QES MUSS die Bestätigende Stelle des Berufgruppenattributes über die Ausstellung des Zertifikats informieren und dazu die folgenden Daten zurückliefern:

- das erzeugte nonQES-Zertifikat
- Ablaufdatum des Zertifikates ⌫

⌦ **TIP1-A_3885 Umgang mit nicht-sicherheitskritischen Incidents für QES-Zertifikate**

Der TSP-X.509 QES MUSS sicherstellen, dass ab dem Zeitpunkt der Feststellung nicht-sicherheitskritischen Incidents, bis zum Entscheid des Incident-Managements über das weitere Vorgehen, keine Zertifikatsanträge für QES-X.509-Zertifikate der betroffenen CA entgegengenommen oder an den Erstellungsdienst des TSP-X.509 QES weitergegeben werden. ⌫

6.1.2.2 Umsetzung

⌦ **TIP1-A_3589 Umsetzung Registrierungsdienst TSP-X.509 QES**

Der TSP-X.509 QES MUSS in seinem Registrierungsdienst für QES-Zertifikate die folgenden Schritte durchführen:

(1) Der Registrierungsdienst des TSP-X.509 QES MUSS dem berechtigten Zertifikatsantragsteller eine Schnittstelle zur Beantragung und Erstellung eines X.509-Zertifikats bereitstellen und den Antragsteller identifizieren.

(2) Der TSP-X.509 QES MUSS eine Schnittstelle zur Bestätigenden Stelle einrichten, um die Berechtigung des Antragstellers sowie die Berufsgruppenattributbestätigung zu erhalten.

(3) Der Registrierungsdienst des TSP-X.509 QES MUSS den Antragsteller gemäß den Vorgaben aus SigG/SigV identifizieren und den Zertifikats-Request an den Erstellungsdienst weiterleiten, wenn dieser den Zertifikatsantragsteller eindeutig identifiziert und die Prüfung des Antrags, dass dieser berechtigt ist ein qualifiziertes X.509-Zertifikat zu beantragen, zu einem positiven Ergebnis geführt hat.

(4) Konnte der Zertifikatsantragsteller nicht identifiziert werden oder hat die Prüfung des Antrags zu einem negativem Ergebnis geführt, wird der Zertifikatsantrag abgelehnt.

(5) Der Registrierungsdienst des TSP-X.509 QES MUSS vom Erstellungsdienst des TSP-X.509 QES das erstellte QES-X.509-Zertifikat erhalten.

(6) Der Registrierungsdienst des TSP-X.509 QES MUSS nach Erhalt des Zertifikates dieses an den berechtigten Zertifikatsantragssteller ausliefern.

(7) Der Registrierungsdienst des TSP-X.509 nonQES MUSS der Bestätigen Stelle das Zertifikat und zertifikatsrelevante Informationen zurückliefern. ⌫

In Abbildung Abb_PKI_513 ist der Prozessablauf des Registrierungsdienstes des TSP-X.509 QES für QES-Zertifikate von Leistungserbringern und dessen Schnittstellen im Überblick dargestellt.

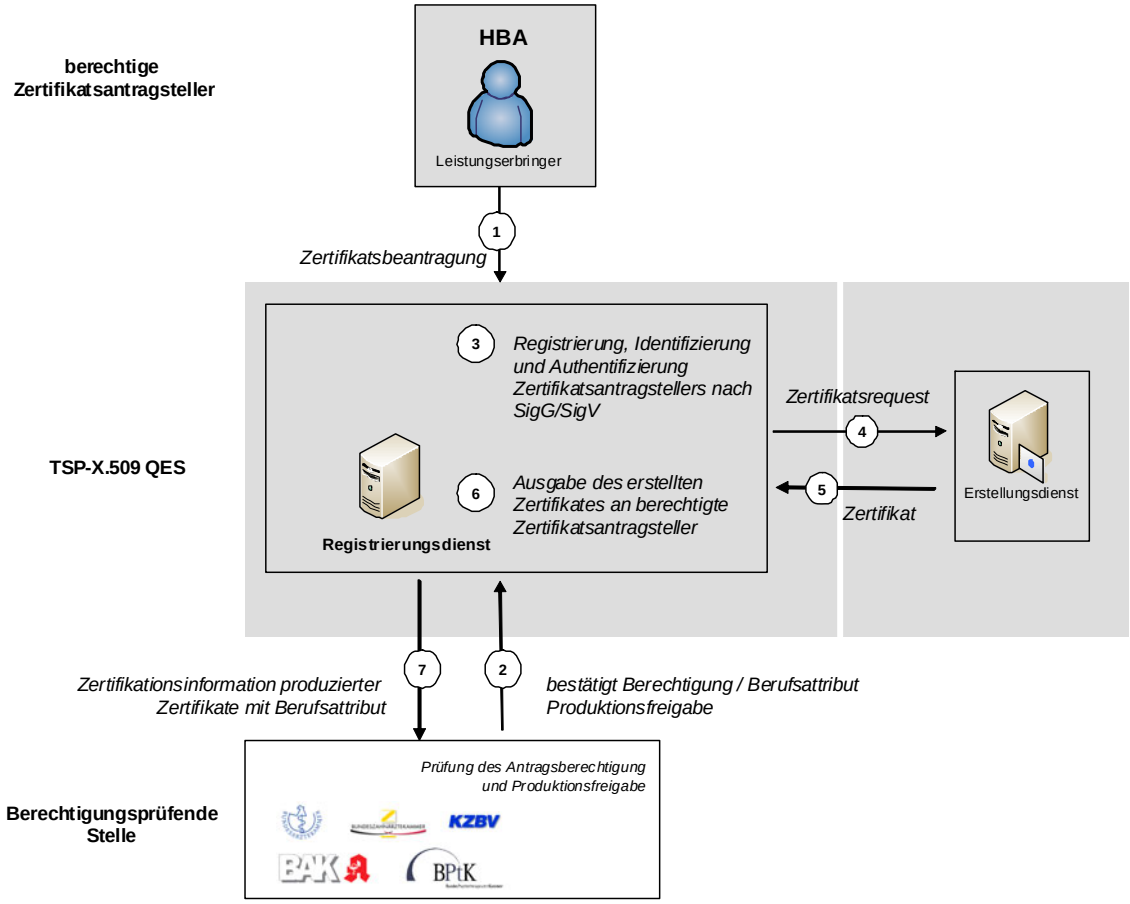

Abbildung 12: Abb_PKI_513 Prozessablauf Registrierungsdienst QES-Zertifikate

6.1.3 Schnittstelle P_Cert_Provisioning_Erstellung

6.1.3.1 Schnittstellendefinition

TSP-X.509 QES und TSP-X.509 nonQES stellen einen Erstellungsdienst für X.509-Personen- und Organisationszertifikate bereit.

⌦ **TIP1-A_3590 Eindeutige Verbindung Personen- und Organisationszertifikatsnehmer und privater Schlüssel**

TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN sicherstellen, dass der öffentliche Schlüssel, dem die Attribute des Zertifikatsnehmers in einem X.509-Personen- und Organisationszertifikat zugeordnet werden, und der private Schlüssel des Zertifikatsnehmers zusammengehören. ⌫

⌦ **TIP1-A_3591 Eindeutigkeit von X.509-Personen- und Organisationszertifikaten**

TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN die TI-weite Eindeutigkeit des SubjectDN eines X.509-Personen- und Organisationszertifikates durch die Attributsinhalte im SubjectDN sicherstellen. Dies gilt unabhängig davon, ob die Attribute optional oder obligatorisch sind.⌫

Für die Erzeugung des X.509-Personen- und Organisationszertifikats sind die Festlegungen gemäß [gemSpec_PKI] hinsichtlich der Zertifikatsprofile sowie der Kodierung von Identitäten zu berücksichtigen.

⌦ **TIP1-A_3886 OCSP-Adresse im X.509-Zertifikate**

Die TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN im Feld AIA der ausgegebenen X.509-Zertifikate den URL des zugeordneten OCSP-Responders eintragen. ⌫

⌦ **TIP1-A_3592 Erstellung von X.509-Personen- und Organisationszertifikaten**

TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN mit Hilfe der X.509-CA zur Erzeugung von X.509-Personen- und Organisationszertifikaten das X.509-Zertifikat erstellen und das erstellte X.509-Zertifikat an den Registrierungsdienst TSP-X.509 QES bzw. TSP-X.509 nonQES zurückliefern. ⌫

⌦ **TIP1-A_3583 Erstellung QES-Zertifikat nach SigG/SigV**

Der TSP-X.509 QES MUSS die Erstellung von QES-X.509-Zertifikaten gemäß den Vorgaben von SigG/SigV durchführen. ⌫

⌦ **TIP1-A_3887 Verarbeitung von Anträgen bei einem nicht-sicherheitskritischen Incidents von X.509-Personen- und Organisationszertifikaten**

TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN sicherstellen, dass ab dem Zeitpunkt der Feststellung eines nicht-sicherheitskritischen Incidents, bis zur Klärung des Sachverhaltes über das weitere Vorgehen im Rahmen des Incident Managements, keine Zertifikatsanträge für Personen- und Organisationszertifikate der betroffenen CA von dem Registrierungsdienst des TSP-X.509 QES und TSP-X.509 nonQES entgegennehmen oder bereits entgegengenommene verarbeiten werden. ⌫

⌦ **TIP1-A_3888 Zertifikatsstatusinformationen der Personen- und Organisationszertifikate**

TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN die Statusinformation für die erstellten Personen- und Organisationszertifikat dem OCSP-Responder in der TI und im Internet zur Verfügung stellen. ⌫

⌦ **TIP1-A_3594 Bereitstellungszeitpunkt der Zertifikatsstatusinformation für Personen- und Organisationszertifikate**

TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN die Zertifikatsstatusinformation für die erstellten Personen- und Organisationszertifikate dem OCSP-Responder in der TI und im Internet gemäß den in Tabelle Tab_PKI_509 definierten Bereitstellungszeitpunkten zur Verfügung stellen. ⌫

Tabelle 4: Tab_PKI_509 Bereitstellungszeitpunkt der Zertifikatsstatusinformation durch den Erstellungsdienst

Zertifikatstyp	Bereitstellungszeitpunkt der Zertifikatsstatusinformation
C.HP.AUT C.HP.ENC	Nach Bestätigung des Zertifikatsnehmers über den gesicherten Besitz des privaten Schlüssels
C.HP.QES C.CH.QES	Nach Bestätigung des Zertifikatsnehmers über den gesicherten Besitz des privaten Schlüssels
C.HCI.AUT C.HCI.ENC C.HCI.OSIG	Nach Bestätigung des Zertifikatsnehmers über den gesicherten Besitz des privaten Schlüssels
C.CH.AUT C.CH.ENC C.CH.AUTN C.CH.ENCV	Unmittelbar nach Erstellung des X.509-Zertifikates

⌦ **TIP1-A_3595 Anforderungen von LEO- und KTR-Institutionen**

TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN weitere Anforderungen und Konkretisierungen an den Erstellungsdienst für Personen- und Organisationszertifikate durch die jeweiligen LEO- und KTR-Organisationen in ihren Prozessen berücksichtigen. ⌫

6.1.3.2 Umsetzung

⌦ **TIP1-A_3596 Umsetzung Erstellungsdienst TSP-X.509 QES und TSP-X.509 nonQES für Personen- und Organisationszertifikate**

TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN in Ihrem Erstellungsdienst für Personen- und Organisationszertifikate die folgenden Schritte durchführen:

(1) TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN nach erfolgreicher Identifizierung des Antragstellers die erforderlichen Angaben zur Zertifikatserstellung an den Erstellungsdienst des TSP-X.509-CA weiterleiten.

(2) TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN auf Grund der übermittelten Angaben die Personen- und Organisationszertifikate erzeugen und diese mit dem privaten Schlüssel der ausstellenden X.509-CA signieren.

(3) TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN die erzeugten Personen- und Organisationszertifikate an den Registrierungsdienst TSP-X.509 QES bzw. TSP-X.509 nonQES zurückliefern.

(4) TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN dem OCSP-Responder die Zertifikatsstatusinformationen nach den in Tabelle Tab_PKI_509 definiertem Zeitpunkten zur Verfügung stellen. ⌫

In der Abbildung Abb_PKI_514 ist der Prozessablauf des Erstellungsdienstes TSP-X.509 QES und TSP-X.509 nonQES sowie dessen Schnittstellen im Überblick dargestellt.

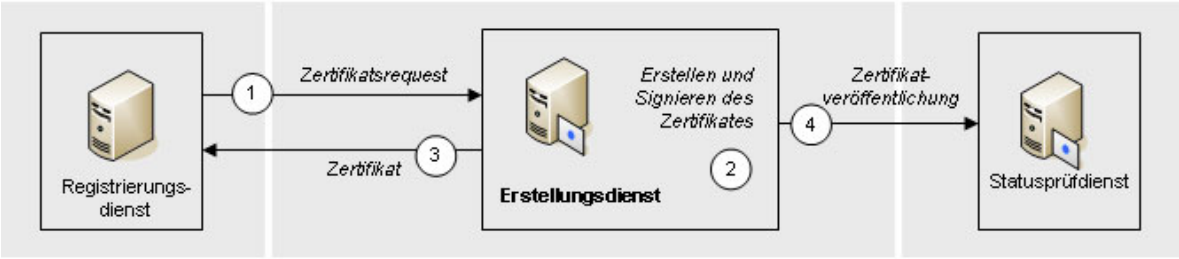

Abbildung 13: Abb_PKI_514 Prozessablauf Erstellungsdienstes des TSP-X.509-CA

6.2 Ausstellung von X.509-Zertifikaten über die zentrale PKI

Die gematik hat die Verantwortung für die Ausgabe von Komponenten- sowie Signerzertifikaten und beauftragt einen Anbieter als TSP-X.509 nonQES mit der Wahrnehmung und operativen Durchführung des Betriebs der zentralen PKI für die Erstellung und Ausgabe von

- nonQES-X.509-Komponentenzertifikaten
- nonQES-X.509-OCSP-Signerzertifikaten und
- nonQES-X.509-CRL-Signerzertifikaten

OCSP- und CRL-Signer werden als Signerzertifikate bezeichnet.

Berechtigt für die Antragsstellung eines X.509-Komponentenzertifikates sind Hersteller der durch die gematik zugelassenen Produkte.

Berechtigt für die Antragsstellung von X.509-Signerzertifikaten sind die durch die gematik zugelassenen TSP-X.509 nonQES.

Darüber hinaus beauftragt die gematik den Anbieter der zentralen PKI mit der Wahrnehmung und operativen Durchführung des Betriebs einer X.509-Sub-CA für die Erstellung und Ausgabe von

- nonQES-HBA-X.509-Zertifikate (C.HP.AUT/C.HP.ENC)
- X.509-Organisationszertifikate (C.HCI.AUT/C.HCI.ENC/C.HCI.OSIG)

Berechtigt für die Antragsstellung von X.509-Zertifikaten sind die zuständigen Kartenherausgeber bzw. deren Dienstleister.

Die Zulassungsinformationen der gematik (Berechtigungsinformation) enthalten die relevanten Informationen über zugelassene TSPs und zugelassene Produkte von Herstellern und Anbietern. Diese Zulassungsinformationen sind die Entscheidungsgrundlage, ob ein Hersteller oder Anbieter antragsberechtigt ist und ein Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikat für das von ihm beantragte Produkt generiert wird.

Gemäß Tabelle Tab_PKI_510 gelten folgende Zuständigkeiten:

Tabelle 5: Tab_PKI_510 Zuständigkeiten Rollen beim Registrierungsdienst der zentralen PKI für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate

Rolle	Aufgabe/Funktion
Anbieter der zentralen PKI (TSP-X.509 nonQES)	Durch gematik beauftragter TSP-X.509 nonQES
Antragsberechtigter Komponentenzertifikate	Hersteller und Anbieter eines durch die gematik zugelassenen Produktes
Antragsberechtigter Signerzertifikate	durch die gematik zugelassene TSP-X.509 nonQES
Antragsberechtigter nonQES-HBA-Zertifikate	Kartenherausgeber oder vom Kartenherausgeber beauftragter Dienstleister
Antragsberechtigter Organisationszertifikate	Kartenherausgeber oder vom Kartenherausgeber beauftragter Dienstleister
Berechtigungsprüfende Stelle	Berechtigungsprüfende Stelle ist die gematik

Gemäß Tabelle Tab_PKI_511 gelten folgende Zuständigkeiten für die berechtigte Antragstellung der X.509-Zertifikatstypen:

Tabelle 6: Tab_PKI_511 Berechtigte Zertifikatsantragsteller für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate

Zertifikatstyp	Berechtigte Zertifikatsantragsteller	Berechtigungs-prüfende Stelle	Zertifikatsnehmer
C.NK.VPN	Hersteller	gematik	Konnektor
C.SAK.AUT	Hersteller	gematik	Konnektor
C.AK.AUT	Hersteller	gematik	Konnektor
C.SMKT.AUT	Hersteller	gematik	Kartenterminal
C.FD.TLS-C	Diensteanbieter	gematik	Fachanwendungsspezifischer Dienst
C.FD.TLS-S	Diensteanbieter	gematik	Fachanwendungsspezifischer Dienst
C.ZD.AUT	Diensteanbieter	gematik	Fachanwendungsspezifischer Dienst
C.ZD.TLS-C	Diensteanbieter	gematik	Zentraler Dienst
C.ZD.TLS-S	Diensteanbieter	gematik	Zentraler Dienst
C.VPNK.VPN	Diensteanbieter	gematik	VPN-Zugangsdienst

Zertifikatstyp	Berechtigte Zertifikatsantragsteller	Berechtigungs-prüfende Stelle	Zertifikatsnehmer
C.VPNK.VPN-SIS	Diensteanbieter	gematik	VPN-Zugangsdienst
C.GEM.OCSP	TSP-X.509 nonQES	gematik	TSP-X.509 nonQES
C.GEM.CRL	TSP-X.509 nonQES	gematik	TSP-X.509 nonQES
C.HP.AUT	TSP-X.509 QES	gematik Kartenherausgeber	Leistungserbringer
C.HP.ENC	TSP-X.509 QES	gematik Kartenherausgeber	Leistungserbringer
C.HCI.AUT	Kartenherausgeber	gematik Kartenherausgeber	med. Institution Kostenträgergeschäftsstelle
C.HCI.ENC	Kartenherausgeber	gematik Kartenherausgeber	med. Institution Kostenträgergeschäftsstelle
C.HCI.OSIG	Kartenherausgeber	gematik Kartenherausgeber	med. Institution Kostenträgergeschäftsstelle

Die Abbildung Abb_PKI_515 stellt die Zuständigkeiten der Rollen bei der Antragsstellung der Komponenten- und Signerzertifikate dar.

© gematik – öffentlich

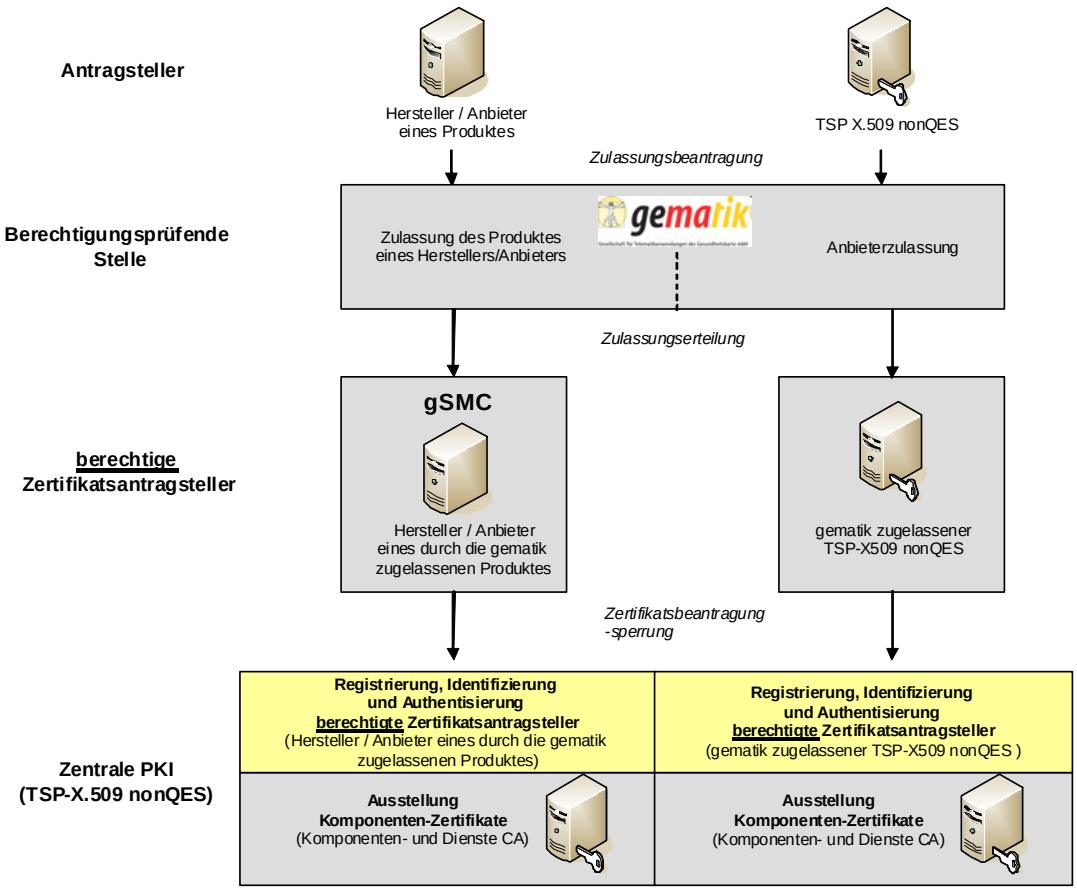

Abbildung 14: Abb_PKI_515 Zuständigkeiten der Rollen bei der Beantragung von Komponenten- und Signerzertifikaten

Die Abbildung Abb_PKI_520 stellt die Zuständigkeiten der Rollen bei der Antragsstellung der nonQES-HBA- und Organisationszertifikate dar.

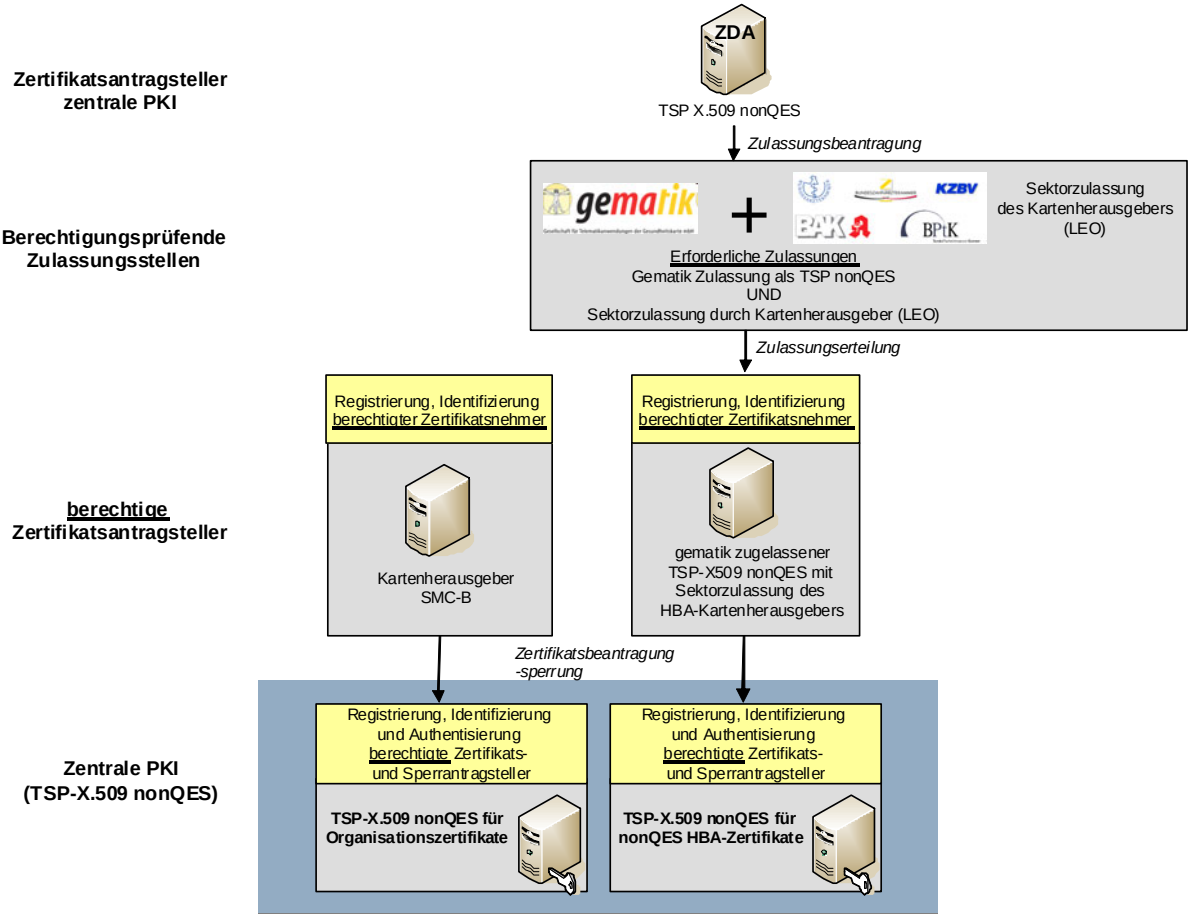

Abbildung 15: Abb_PKI_520 Zuständigkeiten der Rollen bei nonQES-HBA- und Organisationszertifikatsantragstellung

Bei der technischen Schnittstelle zur Ausstellung von Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikaten sind die Schnittstellen

- Registrierungsdienst (I_Cert_Provisioning_Registration)
- Erstellungsdienst (I_Cert_Provisioning_Erstellung)

zu unterscheiden.

6.2.1 Schnittstelle I_Cert_Provisioning_Registration

6.2.1.1 Schnittstellendefinition

Die gematik muss Hersteller, Anbieter, TSP-X.509 nonQES und Kartenherausgeber zulassen und diesen die Berechtigung erteilen für deren zugelassene Produkte Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate bei dem beauftragten Anbieter der zentralen PKI zu beantragen.

Die gematik übermittelt dem Anbieter der zentralen PKI alle notwendigen Berechtigungsinformationen der Hersteller und Anbieter von zugelassenen Produkten, TSP-X.509 nonQES, und Kartenherausgeber, die berechtigt sind Zertifikate bei dem Anbieter der zentralen PKI zu beantragen oder zu sperren.

⌦ **TIP1-A_3597 Eingangsprüfung Berechtigungsinformationen für Komponenten- und Signerzertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS bei Eingang einer neuen Berechtigungsinformation zugelassener Hersteller, Anbieter und TSP-X.509 nonQES (Berechtigungsinformation) den Empfang an die gematik authentisch und integer bestätigen und die folgenden Überprüfungen durchführen: 1) Stammen die Berechtigungsinformationen von der gematik? 2) Ist die Berechtigungsinformation von einer berechtigten Stelle bzw. einem berechtigtem Mitarbeiter der gematik ausgestellt? ⌫

⌦ **TIP1-A_4464 Eingangsprüfung Berechtigungsinformationen für nonQES-HBA- und Organisationszertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS bei Eingang einer neuen Berechtigungsinformation zugelassener TSP-X.509 nonQES oder Kartenherausgeber (Berechtigungsinformation) den Empfang an die gematik authentisch und integer bestätigen und die folgenden Überprüfungen durchführen: 1) Stammen die Berechtigungsinformationen von der gematik? 2) Ist die Berechtigungsinformation von einer berechtigten Stelle bzw. Mitarbeiter der gematik ausgestellt? 3) Hat der TSP-X.509 nonQES oder Kartenherausgeber die Berechtigung (Sektorzulassung) zur Ausgabe einer HBA bzw. SMC-B durch den jeweiligen Kartenherausgeber.⌫

⌦ **TIP1-A_3598 Verbindliche Nutzung der Berechtigungsinformationen**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS nach positiver Überprüfung der Berechtigungsliste für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate die neue Berechtigungsinformation ab dem angegebenen Gültigkeitszeitraum verbindlich verwenden. ⌫

⌦ **TIP1-A_3599 Registrierungsverfahren Antragsberechtigter**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS eine Schnittstelle zur Verfügung stellen, die Antragsberechtigten von Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate die Registrierung durch den Anbieter der zentralen PKI (TSP-X.509 nonQES) ermöglicht.⌫

⌦ **TIP1-A_3889 Festlegung des Registrierungsverfahrens**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die Ausgestaltung des Antrags und des Prozesses für die Registrierung Antragsberechtigter von Komponenten- und Signer-, nonQES-HBA- und Organisationszertifikate festlegen. ⌫

⌦ **TIP1-A_3601 Regelung des Registrierungsverfahrens für Hersteller , Anbieter und TSP-X.509 nonQES**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die genauen Regelungen für das Registrierungsverfahren sowie Prüfregeln für die Berechtigung zur

Antragsstellung von Komponenten- und Signerzertifikaten in seiner CP (bzw. CPS) definieren. ⌫

⌦ **TIP1-A_3603 Überprüfung bei Registrierung der Antragsteller für Komponenten- und Signerzertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS bei der Registrierung von Antragsberechtigten für Komponenten- und Signerzertifikaten prüfen, ob a) der Antragsteller berechtigt ist, Komponenten- oder Signerzertifikat zu beziehen und b) eine Zulassung des Produkts durch die gematik erfolgt ist⌫

⌦ **TIP1-A_4465 Überprüfung bei Registrierung der Antragsteller für nonQES-HBA- und Organisationszertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS bei der Registrierung von Antragsberechtigten für nonQES-HBA- und Organisationszertifikate prüfen, ob a) der Antragsteller berechtigt ist, nonQES-HBA- bzw. Organisationszertifikate zu beziehen, b) eine Zulassung durch die gematik erfolgt ist und c) eine Sektorzulassung vorliegt. ⌫

⌦ **TIP1-A_3605 Registrierungsdienst für Komponenten- und Signer-, nonQES-HBA- und Organisationszertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS einen Registrierungsdienst für Komponenten- und Signer-, nonQES-HBA- und Organisationszertifikate zur Verfügung stellen, der aus dem Zertifikatsantragsdienst und der Zertifikatsausgabe besteht. ⌫

⌦ **TIP1-A_3606 Automatisierter Registrierungsdienst für Komponentenzertifikate**

Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS eine vollständig automatisierte Authentisierung, Berechtigungsprüfung, Anlieferung und Bearbeitung der Requests sowie Ausgabe der erstellten Komponenten, Signer-, nonQES-HBA- und Organisationszertifikate ermöglichen. ⌫

⌦ **TIP1-A_3607 Request-Inhalte**

Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS prüfen, ob in dem eingereichten Zertifikatsantrag alle obligatorisch geforderten Inhalte für die Erstellung eines Komponenten-, Signer-, nonQES-HBA oder Organisationszertifikats enthalten sind. ⌫

⌦ **TIP1-A_3608 Überprüfung Zertifikatsantrag für Komponentenzertifikate**

Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS bei Eingang eines Zertifikatsantrags folgende Überprüfungen durchführen: a) Ist der Hersteller oder Anbieter von der gematik berechtigt Zertifikatsanträge für Komponentenzertifikate zu stellen? b) Ist der Hersteller oder Anbieter durch den TSP-X.509 nonQES registriert? c) Ist das Produkt für den der Zertifikatsantrag des zugelassenen Herstellers oder Anbieters bei dem TSP-X.509 nonQES eingereicht wurde, von der gematik zugelassen? d) Ist die angegebene Seriennummer so gewählt, dass der SubjectDN des zu erstellenden Komponentenzertifikats eindeutig ist? e) Sind alle Inhalte für die Erstellung eines Komponentenzertifikats enthalten?⌫

⌦ **TIP1-A_3609 Überprüfung Hersteller, Anbieter und TSP-X.509 nonQES zu Produktangaben**

Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS bei den Überprüfungen eines Zertifikatsantrags sicherstellen, dass die Angaben des Antragsberechtigten für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate in dem Zertifikatsantrag genau mit den entsprechenden Angaben der Berechtigungsinformationen der gematik zu den Herstellern, Anbietern, TSP-X.509 nonQES oder Kartenherausgebern und den zugelassenen Produkten übereinstimmen. ⌫

⌦ **TIP1-A_3611 Eindeutige Zuordnung Zertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS sicherstellen, dass ein Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikat einem Hersteller oder Anbieter, einem TSP-X.509 nonQES oder Kartenherausgeber eindeutig zugeordnet werden kann. ⌫

⌦ **TIP1-A_4240 professionItem und professionOID für Komponenten- und Signerzertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS für Komponenten- und Signerzertifikate die dem Typ und Verwendungszweck entsprechende technische Rolle gemäß gemSpec_OID#Tab_PKI_406 den Zertifikatserstellungsdaten hinzufügen und in die Admission-Extension des Zertifikats einbringen. Ist für einen Zertifikatstyp keine technische Rolle definiert, bleibt die Admission-Extension leer.⌫

Die Object Identifier sind im Dokument [gemSpec_OID] angegeben.

Für nonQES-HBA- und Organisationszertifikate der LEO sind professionItem und –OID gemäß [gemSpec_OID#Tab_PKI_402] bzw. [gemSpec_OID#Tab_PKI_403] zu den Zertifikatserstellungsdaten hinzuzufügen (vgl. [TIP1-A_3571] bzw. [TIP1-A_3573]).

⌦ **TIP1-A_3612 Erstellung von Zertifikaten**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) DARF ein Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikat NICHT ausstellen, wenn mindestens eine der Überprüfungen des Antragsteller oder der Zertifikatsantragsdaten negativ war. ⌫

⌦ **TIP1-A_3613 Widerruf der Registrierung von Antragsberechtigten**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS auf Aufforderung der gematik unmittelbar die Berechtigung eines Herstellers, Anbieters, TSP-X.509 nonQES oder Kartenherausgebers zur Antragstellung von Komponenten- Signer-, nonQES-HBA- oder Organisationszertifikaten widerrufen. ⌫

⌦ **TIP1-A_3614 Widerrufsverfahren der Zertifikatsantragsberechtigung**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS das Verfahren zum Widerruf der Berechtigung der Zertifikatsantragstellung für Komponenten-, Signer- nonQES-HBA- und Organisationszertifikat eines Antragsberechtigten mit der gematik abstimmen. ⌫

⌦ **TIP1-A_3615 Ausstellung von Zertifikaten nach Widerruf eines Hersteller oder Anbieters**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) DARF Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate für einen widerrufenen Hersteller, Anbieter, TSP-X.509 nonQES oder Kartenherausgeber NICHT mehr erzeugen. ⌫

Auswirkungen auf die Gültigkeit bereits ausgestellter X.509-Zertifikate hat der Vorgang nicht.

⌦ **TIP1-A_3616 Weiterleitung der Daten an den Registrierungsdienst des TSP-X.509**

Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS nach erfolgreicher Authentifizierung und Prüfung des Zertifikatsantrags die Daten zur Zertifikatserstellung von Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate an den Erstellungsdienst weiterleiten. ⌫

⌦ **TIP1-A_3890 Umgang mit nicht-sicherheitskritischen Incidents für Komponentenzertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS sicherstellen, dass ab dem Zeitpunkt der Feststellung eines nicht-sicherheitskritischen Incidents, bis zur Klärung des Sachverhaltes über das weitere Vorgehen im Rahmen des Incident Managements, keine Zertifikatsanträge für Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate der betroffenen CA entgegengenommen oder an den Erstellungsdienst des TSP-X.509 nonQES weitergeleitet werden. ⌫

⌦ **TIP1-A_5095 Schnittstelle zur Beantragung von EE-Zertifikaten**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS eine automatisierte Schnittstelle zur Verfügung stellen, über die berechtigte TSP-X.509 nonQES Endnutzer-Zertifikate beantragen können. ⌫

⌦ **TIP1-A_5096 Statusinformationen der nonQES-HBA- und Organisationszertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die von berechtigten TSP-X.509 nonQES eingegangenen Informationen hinsichtlich der Empfangsbestätigung des Zertifikatsnehmers über die betreffende Karte, unmittelbar umsetzen und Zertifikatsstatusinformationen in der TI und im Internet veröffentlichen gemäß Tab_PKI_509. ⌫

6.2.1.2 Umsetzung

Voraussetzung für den Bezug von X.509-Zertifikaten über die zentrale PKI der TI ist die erfolgreiche Zulassung des Herstellers (Komponentenzertifikate) oder TSP-X.509 nonQES (Signerzertifikate, HBA- und SMC-B Zertifikate) durch

- den beauftragenden Sektor (LEO, KTR) und die gematik für nonQES X.509-Zertifikate für HBA und SMC-B
- die gematik für nonQES X.509-Zertifikate für Signer- und Komponentenzertifikate.

Nachfolgend werden kurz Zulassungsablauf sowie spezifische Anforderungen an den Anbieter der zentralen PKI aufgezeigt. Eine grafische Übersicht dieser Zusammenhänge erfolgt in der Abb_PKI_516.

Zuständigkeiten und Ablauf für die Zulassung:

(a) TSP-X.509 nonQES und Hersteller von Komponenten beantragen eine Zulassung bei der gematik in ihrer Eigenschaft als Herausgeber von Zertifikaten.

(b) TSP-X.509 nonQES beantragen eine Sektorzulassung bei der zuständigen LEO / KTR, sofern sie nonQES-Zertifikate für HBA oder SMC-B anbieten wollen.

⌦ **TIP1-A_3618 Umsetzung Registrierungsdienst für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS sicherstellen, dass zur Bearbeitung einer Registrierung und eines Antrags auf die Ausstellung eines Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikat die folgenden Schritte durchgeführt werden:

(1) Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS der gematik eine Schnittstelle zur Verfügung stellen, über die die gematik dem beauftragtem TSP-X.509 nonQES Berechtigungsinformationen authentisch, integritätsgeschützt und vertraulich übermitteln kann.

(2) Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die von der gematik übermittelten Berechtigungsinformationen auf Authentizität und Integrität prüfen und in dem eigenen Registrierungssystem übernehmen.

(3) Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS nach erfolgreicher Prüfung aus (2) die Antragsberechtigten zur Zertifikatsantragstellung für zugelassene Produkte autorisieren und ihnen geeignete Authentifizierungsmittel vertraulich zustellen, mit deren Hilfe sie sich an der Schnittstelle I_Cert_Provisioning authentifizieren können.

(4) Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS über einen vertraulichkeitsgeschützten Kanal der bereitgestellten Schnittstelle den Antragsteller sicher authentifizieren und den Request des Zertifikatsantragstellers entgegennehmen.

(5) Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS im Rahmen der Prüfung des Zertifikatsantrags die eindeutige Identität und die Berechtigung des Antragsberechtigten anhand der gematik-Berechtigungsinformationen sowie die Korrektheit und Vollständigkeit des eingereichten Zertifikats-Requests prüfen

(6) Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS nach erfolgreicher Überprüfung den Zertifikatsantrag an den Erstellungsdienst des TSP-X.509 nonQES weiterleiten.

(7) Der Erstellungsdienst des TSP-X.509 nonQES produziert das X.509-Zertifikat und liefert dies an den Registrierungsdienst zurück.

(8) Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS das erzeugte X.509-Zertifikat an den Antragsberechtigten ausliefern. ⌫

In der Abbildung Abb_PKI_516 ist der Prozessablauf des Registrierungsdienstes für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate und dessen Schnittstellen im Überblick dargestellt.

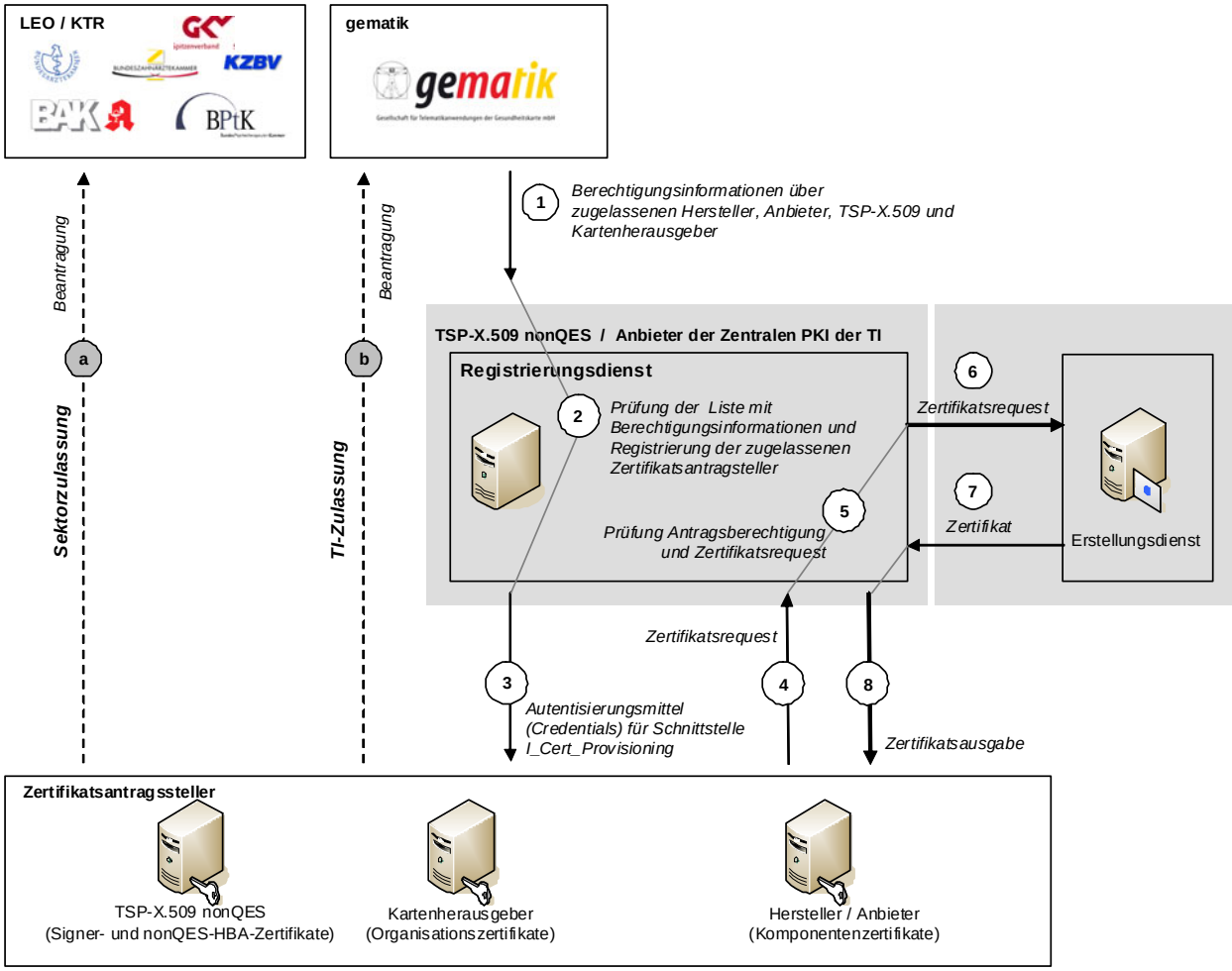

Abbildung 16: Abb_PKI_516 Prozessabläufe der zentralen PKI

Logische Operation I_Cert_Provisioning::provide_Certificate

Die Schnittstelle I_Cert_Provisioning enthält genau eine logische Operation provide_Certificate, die als Ausgabe ein Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikat liefert.

⌦ TIP1-A_4429 I_Cert_Provisoning::provide_Certificate

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS für die Schnittstelle I_Cert_Provisioning die logische Operation provide_Certificate implementieren.⌫

⌦ TIP1-A_4430 I_Cert_Provisoning::provide_Certificate:SEND_REQUEST

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die logische Operation I_Cert_Provisoning::provide_Certificate so implementieren, dass sie durch den SEND-REQUEST-Befehl angestoßen werden und alle zur Zertifikatsbeantragung und –erzeugung erforderlichen Daten enthält. ⌫

⌦ **TIP1-A_4466 I_Cert_Provisoning::provide_Certificate: AUTHENTICATE_REQUESTOR**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die logische Operation I_Cert_Provisoning::provide_Certificate::AUTHENTICATE_REQUESTOR so implementieren, dass sie durch den AUTHENTICATE_REQUEST-Befehl angestoßen werden und den Zertifikatsantragssteller authentifiziert sowie die Berechtigung zur Zertifikatsantragsstellung und des angeforderten Zertifikatstyps überprüft. ⌫

⌦ **TIP1-A_4431 Cert_Provisoning::provide_Certificate: GET_CERTIFICATE**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die logische Operation I_Cert_Provisoning::GET_CERTIFICATE so implementieren, dass sie durch den Befehl GET-CERTIFICATE angestoßen wird und zum zuvor übermittelten Zertifikats-Request das erstellte X.509-Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikat zurück erhält.⌫

6.2.1.3 Nutzung

⌦ **TIP1-A_3619 Voraussetzungen zur Umsetzung Registrierungsdienst TSP-X.509 nonQES für Komponenten-, Signer, nonQES-HBA- und Organisationszertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS alle Voraussetzungen schaffen, dass die durchzuführenden Schritte von der Berechtigungsprüfung bis zur Rückgabe des erzeugten X.509-Zertifikats an den Antragsteller vollautomatisiert ablaufen können.⌫

Die Nutzung erfolgt, wenn die Schritte (1) bis (4) aus [TIP1-A_3618] erfolgreich abgeschlossen wurden.

⌦ **TIP1-A_3620 Technische Umsetzung Registrierungsdienst TSP-X.509 nonQES für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikat**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die technische Umsetzung der Schnittstelle zur Beantragung und Auslieferung der Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate so realisieren, dass eine beidseitige Authentisierung (Zertifikatsantragsteller und TSP-X.509 nonQES) realisiert wird sowie die Daten verschlüsselt übertragen werden.⌫

Die Durchführung kann auf unterschiedliche Weisen realisiert werden, wie z. B.

- Beantragung über Web-GUI mit sicherer beidseitiger Authentisierung,
- Automatisierte Beantragung über SOAP nach sicherer beidseitiger Authentisierung

⌦ **TIP1-A_5097 Zertifikatsbeantragung über SOAP-Schnittstelle**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS für die Beantragung und Ausgabe von Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate eine SOAP-Schnittstelle zur Verfügung stellen.⌫

⌦ **TIP1-A_5098 Zertifikatsbeantragung über Web-Portal**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS für die Beantragung und Ausgabe von Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate ein Web-Portal zur Verfügung stellen.⌫

⌦ **TIP1-A_3621 Zertifikatsmanagementprotokolle des Registrierungsdienstes für Komponenten-, Signer, nonQES-HBA- und Organisationszertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) für die Ausstellung von Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate MUSS mindestens das Zertifikatsmanagementprotokoll CMP [RFC4210] unterstützen.⌫

6.2.2 Schnittstelle I_Cert_Provisioning_Erstellung

6.2.2.1 Schnittstellendefinition

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) stellt einen Erstellungsdienst für Komponenten-, Signer-, nonQES- und Organisationszertifikate bereit.

⌦ **TIP1-A_3622 Eindeutige Verbindung Zertifikatsnehmer und privater Schlüssel**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS sicherstellen, dass der öffentliche Schlüssel, dem die Attribute des Zertifikatsnehmers in einem Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate zugeordnet werden, und der private Schlüssel des Zertifikatsnehmers zusammengehören. ⌫

⌦ **TIP1-A_3623 Eindeutigkeit des Zertifikats für den Produkttyp gSMC-KT**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS bei der Erstellung eines Komponentenzertifikats für den Produkttyp gSMC-KT prüfen, ob der Wert der ICCSN im *commonName* die Eindeutigkeit des *SubjectDN* herstellt. ⌫

⌦ **TIP1-A_3624 Verwendung des Host- und Domänenname**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS sicherstellen, dass für die Erstellung eines TLS-Zertifikats der Host- und Domänenname verwendet wird, der durch die gematik für diesen Anbieter und für den angegebenen Zweck autorisiert wurde.⌫

Für die Erzeugung des Zertifikats sind die Festlegungen gemäß [gemSpec_PKI] hinsichtlich der Zertifikatsprofile sowie der Kodierung von Identitäten zu berücksichtigen.

⌦ **TIP1-A_3626 Erstellung von X.509-Komponten-, Signer-, nonQES-HBA- oder Organisationszertifikaten**

Der Erstellungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS mit Hilfe der entsprechenden X.509-CA die Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate erstellen und diese an den zugehörigen Registrierungsdienst des TSP-X.509 nonQES zurückliefern.⌫

⌦ **TIP1-A_3891 Verarbeitung von Anträgen bei nicht-sicherheitskritischen Incidents von Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikaten**

Der Erstellungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS sicherstellen, dass ab dem Zeitpunkt der Feststellung eines nicht-sicherheitskri-

tischen Incidents, bis zur Klärung des Sachverhaltes über das weitere Vorgehen im Rahmen des Incident Managements, keine Zertifikatsanträge für Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate der betroffenen CA von dem zugehörigen Registrierungsdienst des TSP-X.509 nonQES entgegengenommen oder bereits entgegengenommene verarbeiten werden. ⌫

⌦ **TIP1-A_3627 Bereitstellung der Zertifikatsstatusinformationen der Komponenten- und Signerzertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die Statusinformation für Komponenten- und Signerzertifikate gemäß den in Tabelle Tab_PKI_512 definierten Bereitstellungszeitpunkten dem zugehörigen OCSP-Responder in der TI zur Verfügung stellen. ⌫

Tabelle 7: Tab_PKI_512 Bereitstellungszeitpunkte der Zertifikatsstatusinformation durch den Erstellungsdienst

Zertifikatstyp	Bereitstellungszeitpunkt der Zertifikatsstatusinformation
C.NK.VPN	unmittelbar nach Erstellung
C.SAK.AUT	Nie (Veröffentlichung nicht erforderlich)
C.AK.AUT	Nie (Veröffentlichung nicht erforderlich)
C.SMKT.AUT	Nie (Veröffentlichung nicht erforderlich)
C.FD.AUT	unmittelbar nach Erstellung
C.FD.TLS-C	unmittelbar nach Erstellung
C.FD.TLS-S	unmittelbar nach Erstellung
C.ZD.AUT	unmittelbar nach Erstellung
C.ZD.TLS-C	unmittelbar nach Erstellung
C.ZD.TLS-S	unmittelbar nach Erstellung
C.VPNK.VPN	unmittelbar nach Erstellung
C.VPNK.VPN-SIS	unmittelbar nach Erstellung
C.GEM.OCSP	unmittelbar nach Erstellung

Die Bereitstellung von Statusinformation für nonQES-HBA- und Organisationszertifikaten erfolgt gemäß Tab_PKI_509.

6.2.2.2 Umsetzung

⌦ **TIP1-A_3629 Umsetzung Erstellungsdienst für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikaten**

Der Erstellungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS für die Erzeugung von Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikaten die folgenden Schritte durchführen:

(1) Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS eine Schnittstelle bereitstellen über die der Registrierungsdienst des TSP-X.509 nonQES-Zertifikats-Requests für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate an den Erstellungsdienst des TSP-X.509 nonQES weiterleiten kann.

(2) Der Erstellungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS das beantragte Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikat erstellen und es mit Hilfe der entsprechenden X.509-CA signieren.

(3) Der Erstellungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS das erstellte Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikat an den Registrierungsdienst übermitteln. Die Übermittlung der erstellten X.509-Zertifikate an den Zertifikatantragsteller wird aufgrund der automatisierten Prozesse dem Registrierungsdienst zugerechnet.

(4) Der Erstellungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS dem OCSP-Responder die Zertifikatsstausinformation des erstellten Zertifikates bereitstellen. ⌫

In der Abb_PKI_517 sind der Prozessablauf des Erstellungsdienstes und dessen Schnittstellen im Überblick dargestellt.

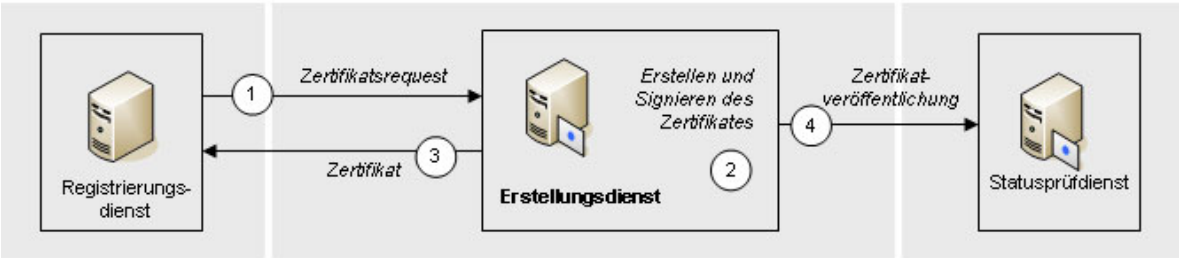

Abbildung 17: Abb_PKI_517 Prozessablauf Erstellungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate

6.2.3 Testunterstützung

Das Vorgehen ist bei TSP-X.509 nonQES und Test-TSP-X.509-TSP nonQES identisch. Mit dem Antrag muss jedoch angegeben werden, dass ein Test-X.509-Zertifikat erzeugt werden soll und TSP-X.509 nonQES müssen zur Erzeugung des X.509-Zertifikats eine Test-X.509-CA einsetzen.

⌦ **TIP1-A_4242 Signierung des Test-nonQES-X.509-Zertifikats**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die zusammengestellten Daten für das Test-nonQES-X.509-Zertifikat mit dem zugehörigen privaten Schlüssel der Test-X.509-CA des signieren. ⌫

6.3 Sperren von X.509-Zertifikaten

Die Sperrdienste von TSP-X.509 QES und TSP-X.509 nonQES nehmen Sperraufträge von sperrberechtigten Personen bzw. Stellen entgegen und leiten die Änderung des Zertifikatsstatus an den OCSP-Responder weiter.

Gemäß Tab_PKI_514 gelten die folgenden Berechtigungen für die Sperrantragstellung von nonQES-Personen- und Organisationszertifikate sowie die jeweils zulässigen Sperrgründe:

Tabelle 8: Tab_PKI_514 Berechtigte Sperrantragsteller für nonQES-Personen- und Organisationszertifikate

Zertifikatstyp	Berechtigte Sperrantragsteller	zulässiger Sperrgrund
C.HP.AUT C.HP.ENC	Leistungserbringer selbst	zu jeder Zeit ohne Angabe von Gründen
	herausgebende LEO	bei Entzug oder Wegfall des Berufsattributes in einem geregelten Verfahren gemäß Ausgabepolicy
C.HCI.AUT C.HCI.ENC C.HCI.OSIG	Zertifikatsnehmende med. Institution oder Kostenträgergeschäftsstelle	zu jeder Zeit ohne Angabe von Gründen
	herausgebende LEO bzw. KTR-Institutionen	festgestellter Wegfall der Voraussetzungen für den Betrieb einer SMC-B gemäß deren Ausgabepolicy
	herausgebender Kostenträger	gemäß Ausgabepolicy des herausgebenden Kosträgers

Gemäß Tab_PKI_515 gelten folgenden Berechtigungen für die Sperrantragstellung von QES-Zertifikaten für Leistungserbringer sowie die jeweils zulässigen Sperrgründe:

Tabelle 9: Tab_PKI_515 Berechtigte Sperrantragsteller für QES-Zertifikat für Leistungserbringer

Zertifikatstyp	Berechtigte Sperrantragsteller	zulässiger Sperrgrund
C.HP.QES	Leistungserbringer selbst	zu jeder Zeit ohne Angabe von Gründen

Zertifikatstyp	Berechtigte Sperrantragsteller	zulässiger Sperrgrund
	Berufsattributvergebene LEO	bei Entzug oder Wegfall des Berufsattributes in einem geregelten Verfahren gemäß Ausgabepolicy
	Alle gemäß SigG/SigV berechtigten Sperrantragsteller	Sperrgrund gemäß SigG/SigV

Gemäß Tab_PKI_516 gelten folgenden Berechtigungen für die Sperrantragstellung von Komponenten- und Signerzertifikaten sowie die jeweils zulässigen Sperrgründe:

Tabelle 10: Tab_PKI_516 Berechtigte Sperrantragsteller für Komponenten- und Signerzertifikate

Zertifikatstyp	Berechtigte Sperrantragsteller	zulässiger Sperrgrund
C.NK.VPN C.SAK.AUT C.AK.AUT C.SMKT.AUT C.FD. TLS-C C.FD. TLS-S C.ZD.AUT C.ZD.TLS-C C.ZD.TLS-S C.VPNK.VPN C.VPNK.VPN-SIS	Zertifikatsnehmender Hersteller und Anbieter,	zu jeder Zeit ohne Angabe von Gründen
	gematik	Wegfall der Voraussetzung für den Betrieb gemäß Ausgabepolicy
C.GEM.OCSP	Zertifikatsnehmender TSP-X.509 nonQES	zu jeder Zeit ohne Angabe von Gründen
	gematik	Wegfall der Voraussetzung für den Betrieb gemäß Ausgabepolicy
C.GEM.CRL	Zertifikatsnehmender TSP-X.509 nonQES	zu jeder Zeit ohne Angabe von Gründen
	gematik	Wegfall der Voraussetzung für den Betrieb gemäß Ausgabepolicy

Bei der organisatorischen Schnittstelle P_Cert_Revocation zur Sperrung von X.509-Zertifikaten wird zwischen

- nonQES-X.509-Zertifikate und
- QES-X.509-Zertifikate

unterschieden.

6.3.1 Schnittstelle P_Cert_Revocation

6.3.1.1 Schnittstellendefinition

6.3.1.1.1 Prozess zur Sperrung nonQES-Personen- und Organisationszertifikate

⌦ **TIP1-A_3631 Prüfung der Berechtigung des Antragstellers für nonQES-Personen- und Organisationszertifikate**

Der TSP-X.509 nonQES MUSS Sperranträge für Personen- und Organisationszertifikate des Antragsberechtigten entgegennehmen und prüfen, ob der Sperrantragsteller für Personen- und Organisationszertifikate gemäß Tab_PKI_514 sperrberechtigt ist ⌫

Für die Identifizierung und Autorisierung eines Sperrantragstellers gelten die Anforderungen gemäß [gemRL_TSL_SP_CP#4.2.3]

⌦ **TIP1-A_3632 Angaben des Sperrantrags für nonQES-Personen- und Organisationszertifikate**

Der TSP-X.509 nonQES MUSS die Angaben des Sperrantrags prüfen, ob diese dem Anspruch auf zweifelsfreie Identifizierung des Sperrberechtigten für Personen- und Organisationszertifikate entsprechen.⌫

⌦ **TIP1-A_3633 Identifizierung des zu sperrenden nonQES-Personen- und Organisationszertifikates**

Der TSP-X.509 nonQES MUSS nach erfolgreicher Identifizierung und Authentisierung des Sperrantragstellers das zu sperrende Personen- und Organisationszertifikat eindeutig identifizieren.⌫

⌦ **TIP1-A_3634 Eingangsdaten zur Identifizierung des nonQES-Personen- und Organisationszertifikates**

Der TSP-X.509 nonQES SOLL zur Identifizierung des zu sperrenden Personen- und Organisationszertifikates mindestens die Eingangsdaten gemäß Tabelle Tab_PKI_517 abfragen.⌫

Tabelle 11: Tab_PKI_517 Eingangsdaten zur Sperrung von nonQES-Personen- und Organisationszertifikaten

Daten	Bezeichnung
Zertifikatsseriennummer	Zertifikatsseriennummer des zu sperrenden X.509-Zertifikates
CA	ausstellende X.509-CA
Name	Name des Personen- oder Organisationszertifikatnehmers
Sperrgrund	Grund, warum Zertifikat gesperrt werden soll

⌦ **TIP1-A_3635 Regelungen zum Sperrprozess für nonQES-Personen- und Organisationszertifikate**

Der TSP-X.509 nonQES MUSS die genauen Regelungen für den Sperrprozess für Personen- und Organisationszertifikate sowie Prüfregeln für die berechtigte Sperrantragsstellung in seiner Certificate Policy und in seinem Certification Practice Statement definieren.⌫

⌦ **TIP1-A_3637 Regelungen zur Suspendierung und Desuspendierung von Versichertenzertifikaten**

Der TSP-X.509 nonQES MUSS die genauen Regelungen für den Suspendierungs- bzw. Desuspendierungsprozess für Versichertenzertifikate sowie Prüfregeln für die berechtigte Sperrantragsstellung in seiner Certificate Policy und in seinem Certification Practice Statement definieren.⌫

⌦ **TIP1-A_3638 Unmittelbare Ausführung der Sperrung von nonQES-Personen- und Organisationszertifikaten**

Der TSP-X.509 nonQES MUSS nach eindeutiger Identifizierung des berechtigten Sperrantragstellers und des nonQES-Personen- und Organisationszertifikates die Sperrung sowie die Suspendierung bzw. Desuspendierung von eGK-Zertifikaten, unmittelbar ausführen.⌫

⌦ **TIP1-A_3639 Weitergabe der Zertifikatsstatusinformationen von Personen- und Organisationszertifikaten an den OCSP-Responder**

Der TSP-X.509 nonQES MUSS nach erfolgreicher Sperrung, Suspendierung bzw. Desuspendierung die Änderung des Zertifikatstatus der nonQES-Personen- und Organisationszertifikate dem OCSP-Responder in der TI und im Internet unmittelbar zur Verfügung stellen. ⌫

Für nonQES-Personen- und Organisationszertifikate gelten die Bereitstellungsinformationen gemäß Tabelle Tab_PKI_509.

⌦ **TIP1-A_3640 Information an den Sperrantragsteller für nonQES-Personen- und Organisationszertifikate**

Der Sperrdienst des TSP-X.509 nonQES MUSS dem berechtigten Sperrantragsteller für nonQES-Personen- und Organisationszertifikate eine Rückinformation zur erfolgreichen Sperrung zurückgeben.⌫

6.3.1.1.2 Prozess zur Sperrung QES-Zertifikate

⌦ **TIP1-A_3641 Sperrdienst gemäß den Vorgaben von SigG/SigV**

Ein TSP-X.509 QES MUSS den Sperrdienst für QES-Zertifikate betreiben und Sperrungen gemäß den Vorgaben aus SigG/SigV durchführen.⌫

⌦ **TIP1-A_4243 Prüfung der Berechtigung des Antragstellers für QES-Zertifikate**

Der TSP-X.509 QES MUSS Sperrantrag für QES-Zertifikate des Antragsberechtigten entgegennehmen und prüfen, ob der Sperrantragsteller gemäß Tab_PKI_515 sperrberechtigt ist.⌫

6.3.1.2 Umsetzung

⌦ **TIP1-A_3642 Umsetzung der Schnittstelle des Sperrdienstes für Personen- und Organisationszertifikate**

TSP X.509 QES und TSP-X.509 nonQES MÜSSEN zur Umsetzung der Schnittstelle bzw. zur Durchführung des Sperrdienstes für Personen- und Organisationszertifikate die folgenden Schritte durchführen:

(5) TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN eine Schnittstelle bereitstellen über die ein Sperrberechtigter einen Sperrantrag für Personen- und Organisationszertifikate stellen kann.

(6) TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN den Sperrantragsteller von Personen- und Organisationszertifikate eindeutig identifizieren.

(7) TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN nach positiver Prüfung des Sperrantrags und eindeutiger Identifizierung des zu sperrenden Personen- und Organisationszertifikates dieses auf Grund der übermittelten Angaben sperren und die aktuellen Statusinformationen der Personen- und Organisations-zertifikate dem OCSP-Responder in der TI und im Internet unmittelbar bereitstellen.

(8) TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN dem Sperrantragsteller von Personen- und Organisationszertifikaten eine Rückinformation zur erfolgreichen Sperrung mitteilen. ⌫

In der Abbildung Abb_PKI_518 sind der Prozessablauf des Sperrdienstes und dessen Schnittstellen im Überblick dargestellt.

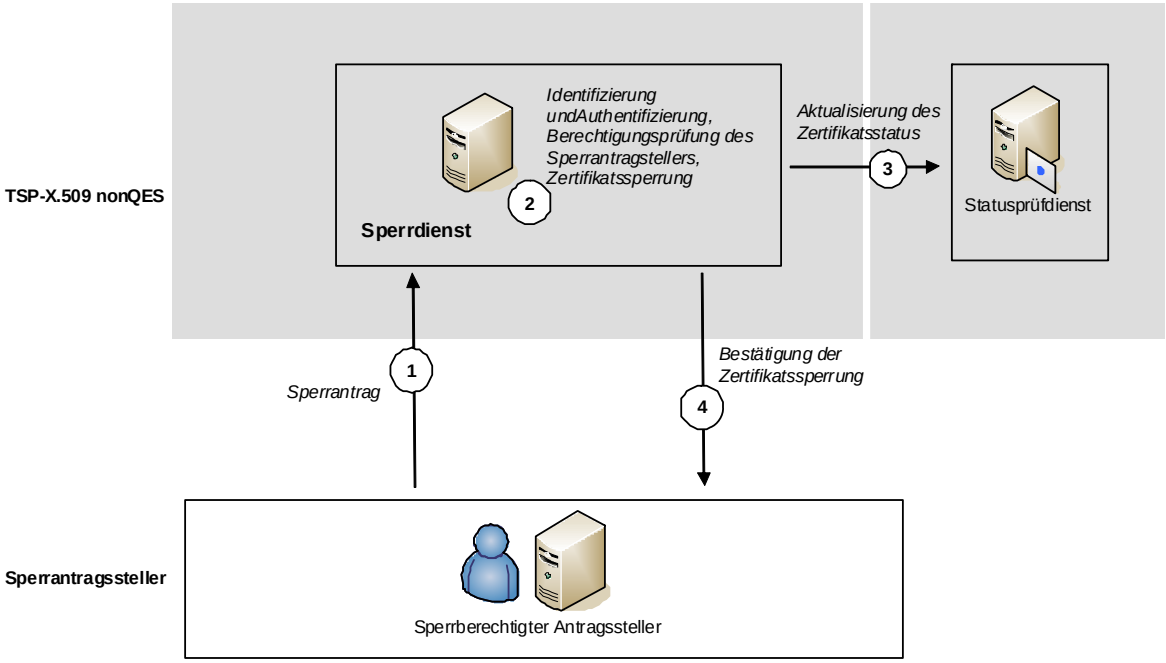

Abbildung 18: Abb_PKI_518 Prozessablauf Sperrdienst Personen- und Organisationszertifikate

6.3.2 Schnittstelle I_Cert_Revocation

6.3.2.1 Schnittstellendefinition

6.3.2.1.1 Sperrung von Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikaten

Die Übermittlung und Überprüfung der Berechtigungsinformationen und Überprüfung der Angaben wird gemäß [TIP1-A_3597], [TIP1-A_4464] und [TIP1-A_3598] durchgeführt.

Die Registrierung der Sperrberechtigten erfolgt analog zur Registrierung von Zertifikatsantragstellern [TIP1-A_3599].

⌦ **TIP1-A_3644 Abgleich der Registrierungsdaten mit vorhandenen Daten aus der Berechtigungsinformation**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die für die Registrierung gemachten Angaben des Sperrantragsteller von Komponenten- und Signerzertifikaten durch einen Abgleich mit den im Rahmen der Zulassung vorgenommenen Angaben überprüfen.⌫

⌦ **TIP1-A_3645 Prüfung der Sperrberechtigung für Komponenten- und Signerzertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS anhand der bei der Registrierung gemachten Angaben entscheiden, ob der Sperrantragsteller für Komponenten- und Signerzertifikate gemäß Tab_PKI_516 sperrberechtigt ist.⌫

⌦ **TIP1-A_4467 Prüfung der Sperrberechtigung für nonQES-HBA- und Organisationszertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS anhand der bei der Registrierung gemachten Angaben entscheiden, ob der Sperrantragsteller für nonQES- und Organisationszertifikate gemäß Tab_PKI_514 sperrberechtigt ist.⌫

Für die Identifizierung und Autorisierung eines Sperrantragstellers gelten die Anforderungen gemäß [gemRL_TSL_SP_CP #4.4]

⌦ **TIP1-A_3648 Angaben zur Identifizierung des zu sperrenden Zertifikats**

Der Sperrdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS sicherstellen, dass im Sperrantrag für ein Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikat alle Informationen zur eindeutigen Identifikation des zu sperrenden Zertifikates enthalten sind.⌫

⌦ **TIP1-A_3649 Prüfungen bei Eingang eines Sperrantrags**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS bei Eingang eines Sperrantrags folgende Überprüfungen durchführen: a) Ist der Sperrantragsteller von der gematik berechtigt Sperranträge für Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate zu stellen? b) Ist der Sperrantragsteller berechtigt einen Sperrantrag für das zu sperrende Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikat zu stellen? c) Konnte das zu sperrende Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikat eindeutig identifiziert werden? ⌫

⌦ **TIP1-A_3650 Prüfung der Sperrantragsangaben**

Der Sperrdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS bei den Überprüfungen eines Sperrantrags sicherstellen, dass die Angaben Sperrberechtigten in dem Sperrantrag genau mit den entsprechenden Angaben der Berechtigungsinformationen für Komponenten, Signer-, nonQES-HBA- oder Organisationszertifikate der gematik übereinstimmen. ⌫

⌦ **TIP1-A_3651 Eingangsdaten zur Identifizierung des zu sperrenden Zertifikats**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) SOLL zur Identifizierung des zu sperrenden Komponenten- oder Signerzertifikates mindestens die in Tabelle Tab_PKI_518 angegebenen Eingangsdaten zur Sperrung eines Komponentenzertifikates abfragen: ⌫

Tabelle 12: Tab_PKI_518 Eingangsdaten zur Sperrung von Komponenten- und Signerzertifikaten

Daten	Bezeichnung
Zertifikatsseriennummer	Zertifikatsseriennummer des zu sperrenden X.509-Zertifikates
CA	ausstellende X.509-CA
Name	Name des Herstellers, Anbieters (Komponentenzertifikate) oder TSP-X.509 nonQES (Signerzertifikate)

Daten	Bezeichnung
Sperrgrund	Grund, warum das X.509-Zertifikat gesperrt werden soll
FQDN	FQDN des Dienstes gemäß Festlegung aus Dienstzulassung (nur für Zertifikate von Zentralen Diensten oder Fachanwendungsspezifischen Diensten)
ICCSN	ICCSN des SMC-KT oder SMC-K (nur für Zertifikate der SMC-KT oder SMC-K)

Zur Sperrung von nonQES-HBA- und Organisationszertifikaten gelten die Eingangsdaten aus Tab_PKI_517.

⌦ **TIP1-A_3652 Regelungen zum Sperrprozess**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die genauen Regelungen für den Sperrprozess für Komponenten, Signer-, nonQES-HBA- oder Organisationszertifikate sowie Prüfregeln für die berechtigte Sperrantragsstellung in seiner Certificate Policy und in seinem Certification Practice Statement definieren. ⌫

⌦ **TIP1-A_3653 Keine Bearbeitung von Sperranträgen bei nicht berechtigter Beantragung**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS sicherstellen, dass keine Sperranträge bearbeitet werden, die von einem nicht registrierten oder nicht zugelassenen Hersteller und Anbieter, TSP-X.509 nonQES oder Kartenherausgeber zu einem nicht zugelassenen Produkt gestellt wurden.⌫

⌦ **TIP1-A_3646 Automatisierte Anlieferung und Bearbeitung von Sperranträgen für Komponenten- und Signerzertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS eine vollständig automatisierte Anlieferung und Bearbeitung der Sperranträge von Komponenten, Signer-, nonQES-HBA- oder Organisationszertifikate ermöglichen.⌫

⌦ **TIP1-A_4244 Unmittelbare Ausführung der Sperrung für Komponenten, Signer-, nonQES-HBA- oder Organisationszertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS nach eindeutiger Identifizierung des berechtigten Sperrantragstellers und des Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikates die Sperrung ausführen.⌫

⌦ **TIP1-A_4246 Erzeugung einer CRL für Zertifikate von VPN-Zugangsdiensten**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS zur Bereitstellung der Sperrinformationen für VPN-Zugangsdienstzertifikate eine CRL erzeugen.⌫

⌦ **TIP1-A_4247 Bereitstellung der Sperrinformationen per CRL**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die Sperrinformation für VPN-Zugangsdienstzertifikate nach erfolgreicher Sperrung in die CRL aufnehmen und diese unmittelbar bereitstellen.⌫

⌦ **TIP1-A_4248 CRL im Internet**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS sicherstellen, dass die CRL für VPN-Zugangsdienstzertifikate im Internet über das Protokoll HTTP zur Verfügung gestellt wird.⌫

⌦ **TIP1-A_4468 Aktualisierung der CRL**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS sicherstellen, dass die CRL für VPN-Zugangsdienstzertifikate mindestens einmal täglich mit einer Gültigkeitsdauer von 7 Tagen aktualisiert und unmittelbar darauf im Internet zum Download bereitgestellt wird.⌫

⌦ **TIP1-A_3647 Rückmeldung zur Sperrung an den Antragsteller**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS dem berechtigen Sperrantragsteller eine Rückinformation zur erfolgreichen Sperrung von Komponenten- und Signer-, nonQES-HBA- und Zertifikaten geben.⌫

6.3.2.2 Umsetzung

⌦ **TIP1-A_3654 Umsetzung der Schnittstelle zur Sperrung von Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikaten**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS zur Umsetzung der Schnittstelle bzw. zur Durchführung des Sperrdienstes für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikaten die folgenden Schritte durchführen (vgl. Abb_PKI_519):

(1) Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS der gematik eine geeignete Schnittstelle zur Verfügung stellen, über die die Berechtigungsinformationen der Sperrberechtigten übermittelt werden können.

(2) Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS den Sperrberechtigten eine geeignete technische und organisatorische Schnittstelle zur Verfügung stellen, um die Sperranträge an den Sperrdienst zu übermitteln.

(3) Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS gewährleisten, dass nur die von der gematik benannten Sperrberechtigten Sperranträge stellen können und den Sperrantragsteller identifizieren und authentisieren.

(4) Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS nach erfolgreicher Prüfung des Sperrantrags das entsprechende Zertifikat sperren und die geänderte Zertifikatstatusinformation an den OCSP-Responder in der TI und im Internet übermitteln.

(5) Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS dem Sperrantragsteller in geeigneter Art eine Rückinformation zur erfolgreichen Sperrung des Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikates mitteilen. ⌫

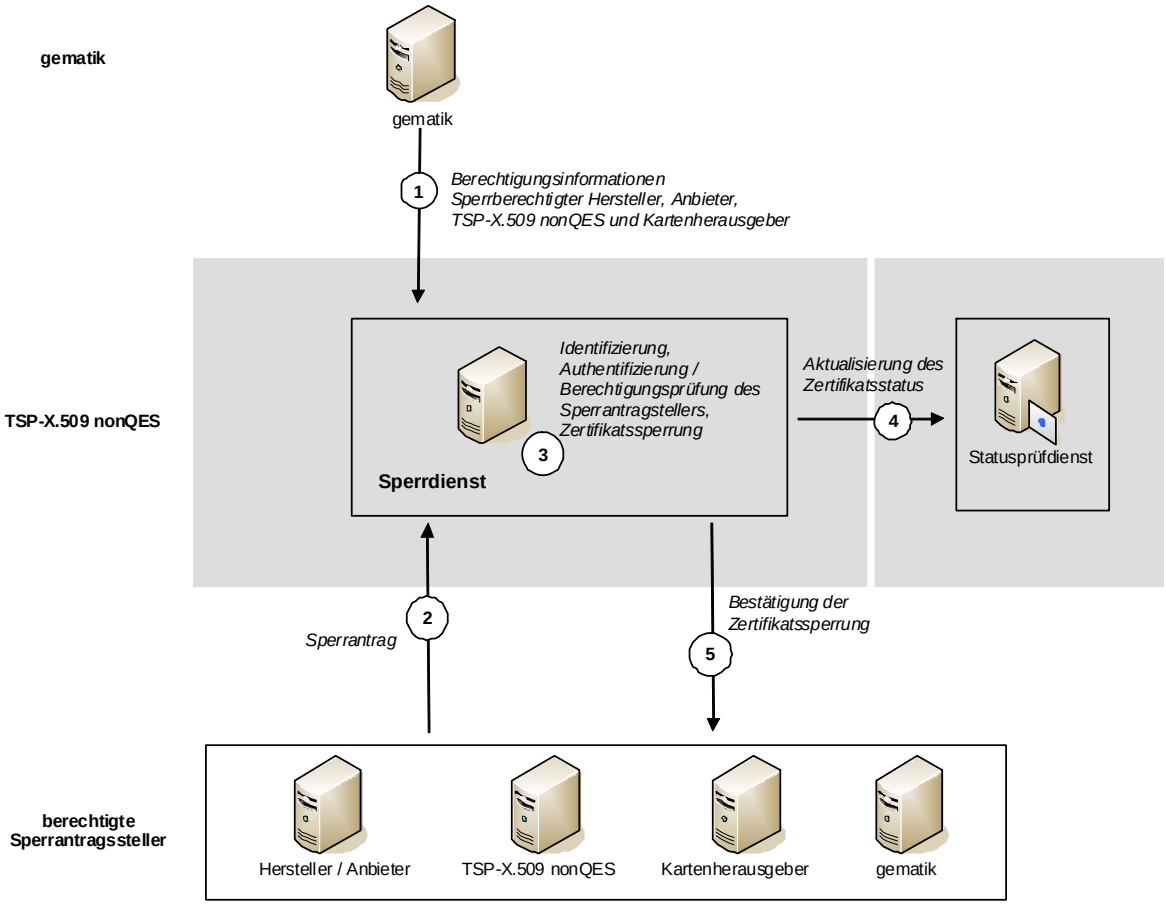

Abbildung 19: Abb_PKI_519 Prozessablauf Sperrdienst des TSP-X.509 nonQES

Schnittstelle Logische Operation I_Cert_Revocation::revoke_Certificate

Die Schnittstelle I_Cert_Revocate enthält genau eine logische Operation revoke_Certificate, welche die Durchführung der Sperrung eines Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikates initiiert.

⌦ **TIP1-A_4432 I_Cert_Revocation::revoke_Certificate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS für die Schnittstelle I_Cert_Revocation die logische Operation revoke_Certificate implementieren ⌫

⌦ **TIP1-A_4433 I_Cert_Revocation::revoke_Certificate:SEND_REVOCATE_DATA**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die logische Operation I_Cert_Revocation::revoke_Certificate so implementieren, dass sie durch den SEND_REVOCATE_DATA-Befehl angestoßen wird und alle zur Zertifikatssperrung erforderlichen Daten gemäß Tab_PKI_518 enthält. ⌫

⌦ **TIP1-A_5099 I_Cert_Revocation::revoke_Certificate: AUTHENTICATE_REQUESTOR**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die logische Operation I_Cert_Revocation::revoke_Certificate::AUTHENTICATE_REQUESTOR so imple-

mentieren, dass sie durch den SEND_REVOCATE_DATA-Befehl angestoßen wird und den Zertifikatsantragssteller authentisiert sowie die Berechtigung zur Zertifikatssperrung des zu sperrenden Zertifikatstyps überprüft. ⌫

⌦ **TIP1-A_5100 I_Cert_Revocation::revoke_Certificate: GET_CERTIFICATE_STATUS**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die logische Operation I_Cert_Revocation::revoke_Certificate:GET_CERTIFICATE_STATUS so implementieren, dass sie durch den Befehl SEND_REVOCATE_DATA angestoßen wird und zur zuvor übermittelten Zertifikatssperrung den Zertifikatsstatus des X.509-Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikats zurück erhält.⌫

⌦ **TIP1-A_4469 Technische Umsetzung Sperrdienst TSP-X.509 nonQES für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die technische Umsetzung der Schnittstelle zur Sperrung der Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate so realisieren, dass eine beidseitige Authentisierung (Zertifikatsantragsteller und TSP-X.509 nonQES) realisiert wird sowie die Daten verschlüsselt übertragen werden.⌫

Die Durchführung kann auf unterschiedliche Weisen realisiert werden, wie z. B.

- Beantragung über Web-GUI mit sicherer beidseitiger Authentisierung,
- Automatisierte Beantragung über SOAP nach sicherer beidseitiger Authentisierung

⌦ **TIP1-A_5101 Zertifikatssperrung über Web-Schnittstelle**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS für die Sperrantragstellung von Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate eine Web-Schnittstelle mit SOAP-Protokoll zur Verfügung stellen. ⌫

⌦ **TIP1-A_5102 Zertifikatssperrung über Web-Portal**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS für die Sperrantragstellung von Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate ein Web-Portal zur Verfügung stellen.⌫

⌦ **TIP1-A_4470 Zertifikatsmanagementprotokolle des Sperrdienstes für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate**

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) für die Sperrung von Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate MUSS mindestens das Zertifikatsmanagementprotokoll CMP [RFC4210] unterstützen.⌫

6.4 Ausstellung von X.509-Sub-CA-Zertifikaten

Die gematik hat die Verantwortung für den Betrieb einer gematik-Root-CA für die Ausgabe von X.509-Sub-CA-Zertifikaten und beauftragt einen Anbieter mit der Wahrnehmung und operativen Durchführung der Aufgaben.

Die gematik-Root-CA generiert das X.509-Sub-CA-Zertifikat für zugelassenen TSP-X.509 nonQES und den Anbieter TSL-Dienst. Entscheidungsgrundlage hierfür sind entsprechende Zulassungsinformationen der gematik.

Gemäß Tab_PKI_519 gelten folgende Zuständigkeiten für die berechtigte Zertifikatsantragstellung von X.509-Sub-CA-Zertifikaten:

Tabelle 13: Tab_PKI_519 Berechtigte Zertifikatsantragsteller für X.509-Sub-CA-Zertifikate

Zertifikatstyp	Berechtigte Zertifikatsantragsteller	Berechtigungsprüfende Stelle	Zertifikatsnehmer
C.GEM.<usage>-CA<n>	zugelassene TSP-X.509 nonQES	gematik	zugelassene TSP-X.509 nonQES
C.GEM.TSL-CA	Anbieter TSL-Dienst	gematik	Beauftragter Anbieter TSL-Dienst

Gemäß Tabelle Tab_PKI_520 gelten folgende Zuständigkeiten für die berechtigte Sperrantragstellung von X.509-Sub-CA-Zertifikaten:

Tabelle 14: Tab_PKI_520 Berechtigte Sperrantragsteller für X.509-Sub-CA-Zertifikate

Zertifikatstyp	Berechtigte Zertifikatsantragsteller
C.GEM.<usage>-CA<n>	Zertifikatsnehmender TSP-X.509 nonQES und gematik
C.GEM.TSL-CA	Anbieter TSL-Dienst und gematik

Die Ausstellung von X.509-Sub-CA-Zertifikaten für berechtigte TSP-X.509 nonQES erfolgt über die Schnittstellen P_Sub_CA_Certification_X.509 (vgl. [gemKPT_Arch_TIP#5.7.5]).

6.4.1 P_Sub_CA_Cert_Certification_X.509

6.4.1.1 Schnittstellendefinition

⌦ **TIP1-A_3655 Certificate Policy des gematik-Root-CA**

Der Anbieter der gematik-Root-CA MUSS in seiner CP (bzw. CPS) festlegen, a) welche Stellen für die Zertifikatsbeantragung und –sperrung von X.509-Sub-CA-Zertifikaten berechtigt sind, b) wie die Registrierung zur eindeutigen Identifikation und Authentisierung der berechtigten Zertifikatsantragsteller durchzuführen ist und c) die vollständige Beschreibung der Regularien, wie die Zertifizierung von Sub-CA-Schlüsseln durch die „gematik-Root-CA“ erfolgt.⌫

Gemäß [gemRL_TSL_SP_CP#GS-A_4188] sind die konkreten Prüfregeln für die Berechtigung zur Antragsstellung vom gematik-Root-CA in seinem CP (bzw. CPS) zu definieren.

⌦ **TIP1-A_4250 Betriebskonzept gematik-Root-CA**

Der Anbieter der gematik-Root-CA MUSS ein Betriebskonzept auf Basis des Sicherheitskonzeptes erstellen, welches mindestens a) Root-Schlüsselerzeugung, b) Root-Zertifizierungszeremonie (self-signed) und c) die Ausstellungs- und Sperrprozesse der Sub-CA-Zertifikate beinhaltet.⌫

⌦ **TIP1-A_4434 Verfahren zur Zeitsynchronisierung gematik-Root-CA**

Der Anbieter der gematik-Root-CA MUSS ein Verfahren zur Zeitsynchronisierung einsetzen, das eine maximale Abweichung von einer Sekunde gegenüber der gesetzlichen Zeit der PTB gewährleistet. ⌫

⌦ **TIP1-A_4251 Auditierverfahren gematik-Root-CA**

Der Anbieter der gematik-Root-CA MUSS die Sicherheit des Betriebes und der Root-Schlüsselerzeugung in einem Auditierverfahren durch die gematik nachweisen.⌫

Das Audit der gematik-Root-CA kann auch durch einen von der gematik beauftragten Auditor erfolgen.

⌦ **TIP1-A_3656 abgestimmtes Antrags- und Sperrverfahren**

Der Anbieter der gematik-Root-CA MUSS das Antrags- und Sperrverfahren mit der gematik abstimmen und bereitstellen.⌫

⌦ **TIP1-A_3657 Gesicherte Zertifikatserstellung der X-509-Sub-CA-Zertifikate**

Der Anbieter der gematik-Root-CA MUSS sicherstellen, dass X.509-Sub-CA-Zertifikate nur generiert werden, wenn a) die Identifizierung und Authentifizierung des Zertifikatsantragstellers bzw. legitimierte Kontaktperson sowie b) der Zertifikatsantrag vollständig war und erfolgreich geprüft werden konnte, c) die gematik die Berechtigung der Antragsstellung bestätigt, d) alle für die Erstellung des beauftragten X.509-Zertifikats obligatorischen Antragsdaten übermittelt werden.⌫

⌦ **TIP1-A_3658 Antragsdaten X.509-Sub-CA-Zertifikat**

Der Anbieter der gematik-Root-CA MUSS sicherstellen, dass mindestens die in Tab_PKI_521 enthaltenen Angaben bei dem Zertifikatsantrag vorliegen. ⌫

Tabelle 15: Tab_PKI_521 Antragsdaten X.509-Sub-CA-Zertifikat

Daten	Beschreibung
TSP-X.509-CA	Name und Anschrift der TSP-X.509-CA,
CA-Name	CA-Name im Zertifikat gemäß [GS-A_4737],
Zertifikatstyp	Typ des gewünschten Zertifikats CA eines produktiven TSP-X.509 nonQES CA eines Test-TSP-X.509 nonQES TSL-Signer
Antragsteller	Name und Vorname einer Kontaktperson
Zertifikatsrequest	Zertifikatsantrag

Unterschriften	Unterschriften zweier bei der Zulassung bzw. einer Änderungsmitteilung genannten berechtigten Mitarbeiter des TSP-X.509

Bei der PKI für X.509-Sub-CA-Zertifikate wird zwischen einer gematik Produktiv-Root-CA und einer gematik Test-Root-CA unterschieden.

Der Betreiber der gematik-Root-CA stellt sowohl eine produktive gematik-Root-CA als auch eine gematik Test-Root-CA zur Verfügung.

⌦ **TIP1-A_3662 Registrierung einer Test-TSP-X.509-CA**

Der Anbieter der gematik-Root-CA MUSS ein mit der gematik abgestimmtes Antragsverfahren für Test-TSP-X.509-CA-Zertifikate abstimmen und bereitstellen.⌫

Für die Registrierung einer Test-TSP-X.509-CA ist ein verkürztes Verfahren vorgesehen.

⌦ **TIP1-A_3663 Dokumentation von Sperrungen**

Der Anbieter gematik-Root-CA MUSS sicherstellen, dass alle eingereichten Sperranträge von TSP-X.509 nonQES-CA-Zertifikate dokumentiert werden. ⌫

⌦ **TIP1-A_3664 Sperrinformationen**

Der Anbieter der gematik-Root-CA MUSS zu jeder Sperrung mindestens die folgenden Sperrinformationen dokumentieren: a) Sperrantragsteller, b) zu sperrende TSP-X.509 nonQES, c) zu sperrendes Zertifikat c) Sperrgrund, d) Zeitpunkt der Sperrannahme⌫

Eingereichte Sperrungen werden gemäß den definierten Incidents behandelt:

- sicherheitskritischer Incident gemäß [gemKPT_PKI_TIP#TIP1-A_2062]
- nicht-sicherheitskritischer Incident gemäß [gemKPT_PKI_TIP#TIP1-A_2065].

6.4.1.2 Umsetzung

Der Anbieter der gematik-Root-CA stellt eine Schnittstelle zur Verfügung über die zugelassene TSP-X.509 nonQES Sub-CA-Zertifikatsanträge und Sperranträge stellen können.

⌦ **TIP1-A_4252 Antragsverfahren Sub-CA-Zertifikate**

Für die Beantragung von Sub-CA-Zertifikats MUSS der Anbieter der gematik-Root-CA ein Antragsverfahren für die Ausstellung- und Sperrung eines Sub-CA-Zertifikates zur Verfügung stellen. ⌫

⌦ **TIP1-A_4253 Signierung des Sub-CA-Zertifikats für Produktivumgebung**

Die zusammengestellten Daten für das Sub-CA-Zertifikat, das für einen Einsatz in der Produktivumgebung vorgesehen ist, MÜSSEN durch die produktive gematik-Root-CA mit dem zugehörigen privaten Schlüssel signiert werden. ⌫

⌦ **TIP1-A_4254 Signierung des Sub-CA-Zertifikats für Testumgebung**

Die zusammengestellten Daten für das Sub-CA-Zertifikat, das für einen Einsatz in der Testumgebung vorgesehen ist, MÜSSEN durch die gematik Test-Root-CA mit dem zugehörigen privaten Schlüssel signiert werden. ⌫

⌦ **TIP1-A_4255 Ausgabe des Sub-CA-Zertifikats**

Die gematik-Root-CA MUSS das erzeugte Sub-CA-Zertifikat an eine vom TSP-X.509 nonQES autorisierte Person nach Erzeugung übergeben bzw. übermitteln. ⌫

Das erzeugte Sub-CA-Zertifikat wird dem TSP-X.509 nonQES zur Verfügung gestellt.

Die Vorgaben an die Zertifikatsprofile für gematik Root-CA und Sub-CA-Zertifikate sind in [gemSpec_PKI#5.10] festgelegt.

⌦ **TIP1-A_5164 Statusinformation erstellter X.509-Sub-CA-Zertifikate**

Der Anbieter der gematik Root-CA MUSS nach erfolgreicher Erstellung den Zertifikatsstatus für das erstellte X.509-Sub-CA-Zertifikat dem OCSP-Responder im Internet unverzüglich zur Verfügung stellen.⌫

⌦ **TIP1-A_5165 Statusinformation gesperrter X.509-Sub-CA-Zertifikate**

Der Anbieter der gematik Root-CA MUSS nach erfolgreicher Sperrung den Zertifikatsstatus für das gesperrte X.509-Sub-CA-Zertifikat dem OCSP-Responder im Internet unverzüglich zur Verfügung stellen.⌫

⌦ **TIP1-A_5166 Rückmeldung Sperrungen**

Der Anbieter der gematik Root-CA MUSS den TSP-X.509 nonQES des gesperrten X.509-Sub-CA-Zertifikatsnehmer und die gematik über die durchgeführte Sperrung informieren.⌫

⌦ **TIP1-A_5167 Crosszertifizierung gematik Root-CA-Zertifikate**

Um die Zertifikatshierarchie über mehrere gematik Root-CA-Zertifikate zu bilden MUSS der Anbieter der gematik Root-CA zugehörige Crosszertifikate zu dem jeweiligen Vorgänger- und Nachfolger-gematik-Root-CA-Zertifikat erstellen.⌫

Die Crosszertifizierung ist entsprechend dem Modell der Bundesnetzagentur zu erstellen. Beispiel:

- GEM.RCA1 auf GEM.RCA2 und
- GEM.RCA2 auf GEM.RCA1

⌦ **TIP1-A_5168 Bereitstellung gematik Root-CA- und Sub-Ca-Zertifikate und Fingerprints im Internet**

Der Anbieter der gematik Root-CA MUSS die erstellten X.509-gematik-Root-CA- und Sub-CA-Zertifikate sowie die zugehörigen Zertifikatsfingerprints im Internet publizieren.⌫

6.5 Statusprüfdienst

Die Schnittstelle des OCSP-Responder I_OCSP_Status_Information ist in [gem-Spec_PKI#9] vollständig beschrieben.

Die Algorithmen und Parameter für die Erstellung der Signaturen über die Antworten des OCSP werden in [gemSpec_Krypt] festgelegt.

© gematik – öffentlich

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
AUT	Authentisierung (Authentication)
AUTN	Technisches Authentisierungszertifikat für Nachrichten
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	certification authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
EE	End Entity
eGK	Elektronische Gesundheitskarte
ENC	Verschlüsselung (Encryption)
ENCV	Technisches Verschlüsselungszertifikat für Verordnungen
FQDN	Fully Qualified Domain Name
gSMC	Gerätebezogene Security Module Card
HBA	Heilberufsausweis
HCI	Health Care Institution
HP	Health Professional
HPC	Health Professional Card
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ICCSN	ICC Serial Number
ID	Identität (Identity)
IPSec	Internet Protocol Security
KT	Kartenterminal
KTR	Kostenträger
LEO	Leistungserbringer-Organisation
OCSP	Online Certificate Status Protocol
OCSP-R	OCSP-Responder
OID	Object Identifier

Kürzel	Erläuterung
OSIG	Organizational Signature
PKI	Public Key Infrastructure
PKIX	PKI nach X.509 Standard der IETF
PrK	Private Key
PuK	Public Key
QES	Qualifizierte elektronische Signatur
RCA	Root-CA
RFC	Request For Comment
SGB	Sozialgesetzbuch
SHA	Secure Hash Algorithm
SIG	Elektronische Signatur
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen
SigV	Signaturverordnung
SM	Security Module
SMC-B	Sicherheitsmodul vom Typ B <medizinische Institution>
SMC	Security Module Card
gSMC-K	Security Module Card Konnektor als <holder>
SM-K	Sicherheitsmodul für Konnektoren
SM-KT	Security Module Kartenterminal als <holder>
SM-KT-Zertifikat	X.509-Komponentenzertifikat zu einem SM-KT
SubjectDN	Subject Distinguished Name
TI	Telematikinfrastruktur
TLS	Transport Layer Security
TSL	Trust-service Status List
TSP	Trust Service Provider
VPN	Virtual Private Network
ZDA	Zertifizierungsdiensteanbieter

A2 – Glossar

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

A3 – Abbildungsverzeichnis

Abbildung 1: Abb_PKI_502 Nachbarsysteme der gematik-Root-CA 12

Abbildung 2: Abb_PKI_503 Nachbarsysteme TSP-X.509 QES und TSP-X.509 nonQES13

Abbildung 3: Abb_PKI_504 Schnittstellen TSP-X.509 QES und TSP-X.509 nonQES..... 15

Abbildung 4: Abb_PKI_504 Schnittstellen Registrierungs- und Erstellungsdienst TSP-X.509 QES und TSP-X.509 nonQES 16

Abbildung 5: Abb_PKI_506 Organisatorische Anordnung der Schnittstelle Registrierungs- und Erstellungsdienst TSP-X.509 QES und TSP-X.509 nonQES..... 17

Abbildung 6: Abb_PKI_507 Schnittstellen Sperrdienst des TSP-X.509 18

Abbildung 7: Abb_PKI_508 Organisatorische Anordnung Sperrdienst 18

Abbildung 8: Abb_PKI_510 Schnittstellen Erstellung und Sperrung der gematik-Root-CA 19

Abbildung 9: Abb_PKI_509 Schnittstellen OCSP-Responder TSP-X.509 QES und TSP-X.509 nonQES..... 19

Abbildung 10: Abb_PKI_511 Zuständigkeiten der Rollen bei Zertifikatsantragstellung der Personen- und Organisationszertifikate 27

Abbildung 11: Abb_PKI_512 Prozessablauf Registrierungsdienst nonQES-Personen- und Organisationszertifikate 31

Abbildung 12: Abb_PKI_513 Prozessablauf Registrierungsdienst QES-Zertifikate 34

Abbildung 13: Abb_PKI_514 Prozessablauf Erstellungsdienstes des TSP-X.509-CA 37

Abbildung 14: Abb_PKI_515 Zuständigkeiten der Rollen bei der Beantragung von Komponenten- und Signerzertifikaten 40

Abbildung 15: Abb_PKI_520 Zuständigkeiten der Rollen bei nonQES-HBA- und Organisationszertifikatsantragstellung..... 41

Abbildung 16: Abb_PKI_516 Prozessabläufe der zentralen PKI 47

Abbildung 17: Abb_PKI_517 Prozessablauf Erstellungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate 51

Abbildung 18: Abb_PKI_518 Prozessablauf Sperrdienst Personen- und Organisationszertifikate 57

Abbildung 19: Abb_PKI_519 Prozessablauf Sperrdienst des TSP-X.509 nonQES 61

A4 – Tabellenverzeichnis

Tabelle 1: Tab_PKI_501 Allgemeine Übersicht der Rollen und deren Aufgaben beim Registrierungsdienst..... 26

Tabelle 2: Tab-PKI_502 Berechtigte Zertifikatsantragsteller für non-QES Leistungserbringer-, LEO bzw. KTR-Organisation und Versichertenzertifikate..... 26

Tabelle 3: Tab_PKI_503 Berechtigte Zertifikatsantragsteller für QES Leistungserbringerzertifikate 26

Tabelle 4: Tab_PKI_509 Bereitstellungszeitpunkt der Zertifikatsstatusinformation durch den Erstellungsdienst 36

Tabelle 5: Tab_PKI_510 Zuständigkeiten Rollen beim Registrierungsdienst der zentralen PKI für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate 38

Tabelle 6: Tab_PKI_511 Berechtigte Zertifikatsantragsteller für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate 38

Tabelle 7: Tab_PKI_512 Bereitstellungszeitpunkte der Zertifikatsstatusinformation durch den Erstellungsdienst 50

Tabelle 8: Tab_PKI_514 Berechtigte Sperrantragsteller für nonQES-Personen- und Organisationszertifikate 52

Tabelle 9: Tab_PKI_515 Berechtigte Sperrantragsteller für QES-Zertifikat für Leistungserbringer 52

Tabelle 10: Tab_PKI_516 Berechtigte Sperrantragsteller für Komponenten- und Signerzertifikate 53

Tabelle 11: Tab_PKI_517 Eingangsdaten zur Sperrung von nonQES-Personen- und Organisationszertifikaten 54

Tabelle 12: Tab_PKI_518 Eingangsdaten zur Sperrung von Komponenten- und Signerzertifikaten 58

Tabelle 13: Tab_PKI_519 Berechtigte Zertifikatsantragsteller für X.509-Sub-CA-Zertifikate 63

Tabelle 14: Tab_PKI_520 Berechtigte Sperrantragsteller für X.509-Sub-CA-Zertifikate .. 63

Tabelle 15: Tab_PKI_521 Antragsdaten X.509-Sub-CA-Zertifikat 64

A5 – Referenzierte Dokumente

A5.1 – 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
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemKPT_PKI_TIP]	gematik: Konzept PKI der TI-Plattform
[gemRL_TSL_SP_CP]	gematik: Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastrukur

[Quelle]	Herausgeber: Titel
[gemSpec_OID]	gematik: Spezifikation OID
[gemSpec_PKI]	gematik: Spezifikation PKI

A5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[HPC-CP]	Bundesapothekerkammer, Bundesärztekammer, Bundespsychotherapeutenkammer, Bundeszahnärztekammer, Kassenzahnärztliche Bundesvereinigung Gemeinsame Policy für die Ausgabe der HPC, Zertifikatsrichtlinie HPC, Version: 1.0.5, 06.11.2012
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://www.ietf.org/rfc/rfc2119.txt
[RFC4210]	RFC 4210 (September 2005): Internet X.509 Public Key Infrastructure, Certificate Management Protocol (CMP); C. Adams, S. Farrell, T. Kause, T. Mononen
[SigG01]	Bundesgesetzblatt I (2001), S.876: Signaturgesetz vom 16. Mai 2001 (BGBl. I S. 876), zuletzt geändert durch Artikel 4 des Gesetzes vom 26. Februar 2007 (BGBl. I S. 179)
[SigV01]	Bundesgesetzblatt I (2001), S. 3074: Signaturverordnung vom 16. November 2001 (BGBl. I S. 3074), zuletzt geändert durch Artikel 9 Abs. 18 des Gesetzes vom 23. November 2007 (BGBl. I S. 2631)