

Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Trust Service Provider X.509

Version: 1.1516.0 CC
Revision: 192694231770
Stand: 02.10.201930.04.2020
Status: zur Abstimmung freigegeben
Klassifizierung: öffentlich_Entwurf
Referenzierung: gemSpec_X.509_TSP

22

Dokumentinformationen

Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

26

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.5.0	10.08.12		zur Abstimmung freigegeben	gematik
1.0.0	15.10.12		Überarbeitung nach Kommentierung und Workshop	gematik
1.1.0	12.11.12		Einarbeitung Kommentare aus der übergreifenden Konsistenzprüfung	gematik
1.2.0	06.06.13		Überarbeitung anhand interner Änderungsliste (Fehlerkorrekturen, Inkonsistenzen), Einarbeitung Kommentare aus Kommentierung Gesamtpaket	gematik
1.3.0	15.08.13		Einarbeitung lt. Änderungsliste vom 08.08.13	gematik
1.4.0	21.02.14		Losübergreifende Synchronisation	gematik
1.5.0	17.06.14		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.	gematik

1.6.0	12.08.16		Anpassungen zum Online-Produktivbetrieb (Stufe 1)	gematik
1.7.0	28.10.16		Aufnahme SMC-B für Organisationen der Gesellschafter, Anpassungen gemäß Änderungsliste	gematik
1.8.0	21.04.17		Einarbeitung Anpassungen Kartengeneration G2.1 sowie lt. Änderungsliste	gematik
1.9.0	18.12.17		Übernahme in OPB2.1, Änderungsliste P14.15	gematik
1.10.0	14.05.18		freigegeben	gematik
1.12.0	18.12.18		Ergänzung der ePA-Inhalte	gematik
1.13.0	15.05.19		Änderungen gemäß Änderungsliste P18.1	gematik
1.14.0	28.16.19		Einarbeitung P19.1	gematik
1.15.0	02.10.19		Einarbeitung P16.1	gematik
1.1516.0 CC	30.04.2020 02.10.19		freigegeben Anpassungen gemäß Änderungsliste P22.1	gematik

Inhaltsverzeichnis

29	1 Einordnung des Dokumentes	8
30	1.1 Zielsetzung	8
31	1.2 Zielgruppe	8
32	1.3 Geltungsbereich	8
33	1.4 Abgrenzung	8
34	1.5 Methodik	9
35	2 Systemüberblick	10
36	2.1 Hierarchie der PKI für X.509-Zertifikate	10
37	2.2 Begriffsverwendung	10
38	3 Systemkontext	11
39	3.1 Akteure und Rollen	11
40	3.1.1 gematik	11
41	3.1.2 TSP X.509 QES und TSP X.509 nonQES	11
42	3.1.3 gematik-Root-CA	12
43	3.1.4 Kartenherausgeber	12
44	3.1.5 Kartenpersonalisierer	12
45	3.1.6 Kartenhersteller	12
46	3.1.7 Zertifikatsnehmer	13
47	3.1.8 Hersteller	13
48	3.1.9 Anbieter	13
49	3.2 Nachbarsysteme	13
50	4 Zerlegung des Produkttyps	16
51	4.1 Produkttypen TSP X.509 QES und TSP X.509 nonQES	16
52	4.2 Produkttyp gematik-Root-CA	20
53	4.3 Statusprüfdienst	21
54	5 Übergreifende Festlegungen	22
55	5.1 Ausstellung von X.509-Zertifikaten	22
56	5.1.1 Erstellung Sicherheitskonzept Zertifikatsprozess durch TSP X.509	22
57	5.1.2 Zulassung	23
58	5.1.3 Datenschutz	23
59	5.1.4 Unterscheidung produktive TSP X.509 und Test TSP X.509	24
60	5.2 Sperrung von X.509-Zertifikaten	24
61	5.3 Schutzbedarfsfeststellung	25
62	5.4 Sichere Kommunikation zwischen Rollen und Diensten	26
63	5.5 Schutz der gematik-Root-CA	27
64	6 Funktionsmerkmale	28

65	6.1 Ausstellung von Personen- und Organisationszertifikaten	28
66	6.1.1 Schnittstelle P_Cert_Provisioning_nonQES_Registration	31
67	6.1.1.1 Schnittstellendefinition	31
68	6.1.1.2 Umsetzung	34
69	6.1.2 Schnittstelle P_Cert_Provisioning_QES_Registration	35
70	6.1.2.1 Schnittstellendefinition	35
71	6.1.2.2 Umsetzung	37
72	6.1.3 Schnittstelle P_Cert_Provisioning_Erstellung	38
73	6.1.3.1 Schnittstellendefinition	38
74	6.1.3.2 Umsetzung	40
75	6.1.4 Schnittstelle I_Cert_Provisioning	41
76	6.1.4.1 AUT_ALT	41
77	6.2 Ausstellung von X.509-Zertifikaten über die zentrale PKI	42
78	6.2.1 Schnittstelle I_Cert_Provisioning_Registration	46
79	6.2.1.1 Schnittstellendefinition	46
80	6.2.1.2 Umsetzung	50
81	6.2.1.3 Nutzung	53
82	6.2.2 Schnittstelle I_Cert_Provisioning_Erstellung	54
83	6.2.2.1 Schnittstellendefinition	54
84	6.2.2.2 Umsetzung	55
85	6.2.3 Testunterstützung	56
86	6.3 Sperren von X.509-Zertifikaten	57
87	6.3.1 Schnittstelle P_Cert_Revocation	59
88	6.3.1.1 Schnittstellendefinition	59
89	6.3.1.1.1 Prozess zur Sperrung nonQES Personen- und Organisationszertifikate	59
90	6.3.1.1.2 Prozess zur Sperrung QES-Zertifikate	61
91	6.3.1.2 Umsetzung	61
92	6.3.2 Schnittstelle I_Cert_Revocation	62
93	6.3.2.1 Schnittstellendefinition	62
94	6.3.2.1.1 Sperrung von Komponenten-, Signer-, nonQES-HBA- und	
95	Organisationszertifikaten	62
96	6.3.2.2 Umsetzung	65
97	6.4 Ausstellung von X.509-Sub-CA-Zertifikaten	68
98	6.4.1 P_Sub_CA_Cert_Certification_X.509	68
99	6.4.1.1 Schnittstellendefinition	68
100	6.4.1.2 Umsetzung	70
101	6.5 Statusprüfdienst	72
102	7 Anhang A – Verzeichnisse	73
103	7.1 Abkürzungen	73
104	7.2 Glossar	75
105	7.3 Abbildungsverzeichnis	75
106	7.4 Tabellenverzeichnis	77
107	7.5 Referenzierte Dokumente	78
108	7.5.1 Dokumente der gematik	78
109	7.5.2 Weitere Dokumente	79
110		

111	1 Einordnung des Dokumentes	8
112	1.1 Zielsetzung	8
113	1.2 Zielgruppe	8
114	1.3 Geltungsbereich	8
115	1.4 Abgrenzung	8
116	1.5 Methodik	9
117	2 Systemüberblick	10
118	2.1 Hierarchie der PKI für X.509-Zertifikate	10
119	2.2 Begriffsverwendung	10
120	3 Systemkontext	11
121	3.1 Akteure und Rollen	11
122	3.1.1 gematik	11
123	3.1.2 TSP-X.509 QES und TSP-X.509 nonQES	11
124	3.1.3 gematik-Root-CA	12
125	3.1.4 Kartenherausgeber	12
126	3.1.5 Kartenpersonalisierer	12
127	3.1.6 Kartenhersteller	12
128	3.1.7 Zertifikatsnehmer	13
129	3.1.8 Hersteller	13
130	3.1.9 Anbieter	13
131	3.2 Nachbarsysteme	13
132	4 Zerlegung des Produkttyps	16
133	4.1 Produkttypen TSP-X.509 QES und TSP-X.509 nonQES	16
134	4.2 Produkttyp gematik-Root-CA	20
135	4.3 Statusprüfdienst	21
136	5 Übergreifende Festlegungen	22
137	5.1 Ausstellung von X.509-Zertifikaten	22
138	5.1.1 Erstellung Sicherheitskonzept Zertifikatsprozess durch TSP-X.509	22
139	5.1.2 Zulassung	23
140	5.1.3 Datenschutz	23
141	5.1.4 Unterscheidung produktive TSP-X.509 und Test-TSP-X.509	24
142	5.2 Sperrung von X.509-Zertifikaten	24
143	5.3 Schutzbedarfsfeststellung	25
144	5.4 Sichere Kommunikation zwischen Rollen und Diensten	26
145	5.5 Schutz der gematik Root-CA	27
146	6 Funktionsmerkmale	28
147	6.1 Ausstellung von Personen- und Organisationszertifikaten	28
148	6.1.1 Schnittstelle P_Cert_Provisioning_nonQES_Registration	31
149	6.1.1.1 Schnittstellendefinition	31

150	6.1.1.2 Umsetzung	34
151	6.1.2 Schnittstelle P_Cert_Provisioning_QES_Registration	35
152	6.1.2.1 Schnittstellendefinition	35
153	6.1.2.2 Umsetzung	37
154	6.1.3 Schnittstelle P_Cert_Provisioning_Erstellung	38
155	6.1.3.1 Schnittstellendefinition	38
156	6.1.3.2 Umsetzung	40
157	6.1.4 Schnittstelle I_Cert_Provisioning	41
158	6.1.4.1 AUT_ALT	41
159	6.2 Ausstellung von X.509-Zertifikaten über die zentrale PKI	42
160	6.2.1 Schnittstelle I_Cert_Provisioning_Registration	46
161	6.2.1.1 Schnittstellendefinition	46
162	6.2.1.2 Umsetzung	50
163	6.2.1.3 Nutzung	53
164	6.2.2 Schnittstelle I_Cert_Provisioning_Erstellung	54
165	6.2.2.1 Schnittstellendefinition	54
166	6.2.2.2 Umsetzung	55
167	6.2.3 Testunterstützung	56
168	6.3 Sperren von X.509-Zertifikaten	57
169	6.3.1 Schnittstelle P_Cert_Revocation	59
170	6.3.1.1 Schnittstellendefinition	59
171	6.3.1.1.1 Prozess zur Sperrung nonQES-Personen- und Organisationszertifikate	59
172	6.3.1.1.2 Prozess zur Sperrung QES-Zertifikate	61
173	6.3.1.2 Umsetzung	61
174	6.3.2 Schnittstelle I_Cert_Revocation	62
175	6.3.2.1 Schnittstellendefinition	62
176	6.3.2.1.1 Sperrung von Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikaten	62
177	6.3.2.2 Umsetzung	65
178	6.4 Ausstellung von X.509-Sub-CA-Zertifikaten	68
179	6.4.1 P_Sub_CA_Cert_Certification_X.509	68
180	6.4.1.1 Schnittstellendefinition	68
181	6.4.1.2 Umsetzung	70
182	6.5 Statusprüfdienst	72
183	7 Anhang A – Verzeichnisse	73
184	7.1 Abkürzungen	73
185	7.2 Glossar	75
186	7.3 Abbildungsverzeichnis	75
187	7.4 Tabellenverzeichnis	77
188	7.5 Referenzierte Dokumente	78
189	7.5.1 Dokumente der gematik	78
190	7.5.2 Weitere Dokumente	79
191		
192		
193		

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.

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 7.5: Referenzierte Dokumente).

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

- 229 • Verfahrensbeschreibung für Zulassungs- und Registrierung TSP-X.509 QES
- 230 und TSP-X.509 nonQES sowie
- 231 • Anforderungen an die Sicherheit eines TSP-X.509 QES, TSP-X.509 nonQES
- 232 und der gematik-Root-CA.
- 233 • Prozesse und Verfahren zur Personalisierung der Karten selbst.
- 234 Die Sicherheitsanforderungen, die an einen TSP-X.509 nonQES bzw. an die gematik-
- 235 Root-CA gestellt werden, sind Gegenstand der „Certificate Policy Gemeinsame
- 236 Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL“ [gemRL_TSL_SP_CP].
- 237 Anforderungen an den Produkttyp TSP-X.509 QES sind durch [eIDAS] festgelegt.
- 238 Die Spezifikation der Schnittstelle des OCSP-Responders ist nicht Bestandteil dieses
- 239 Dokumentes, sondern ist in [gemSpec_PKI#9] beschrieben.

240 1.5 Methodik

- 241 Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in
- 242 eckigen Klammern sowie die dem RFC 2119 [RFC2119] entsprechenden, in
- 243 Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL,
- 244 SOLL NICHT, KANN gekennzeichnet.
- 245 Sie werden im Dokument wie folgt dargestellt:
- 246 **<AFO-ID> - <Titel der Afo>**
- 247 Text / Beschreibung
- 248 [**<=**]
- 249
- 250 Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und der Textmarke [**<=**]
- 251 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].

Um einen reibungslosen Wechsel der Schlüsselgenerationen zu ermöglichen, werden zeitweise verschiedene Schlüsselgenerationen parallel unterstützt (vgl. [gemKPT_PKI_TIP#TIP1-A_6878]).

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 von [eIDAS].

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 bzw. die Gesellschafterorganisationen 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 (für gSMC und Dienste),
 - OCSP-Signerzertifikaten,
 - CRL-Signerzertifikaten,
- 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 (Zulassung) 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 kann dabei nur ein Vertrauensdiensteanbieter (VDA) für QES gemäß [eIDAS] auftreten.

TSP-X.509 QES und TSP-X.509 nonQES generieren Zertifikate auf Antrag berechtigter Stellen. Wenn es sich bei TSP-X.509 nonQES, TSPX.509 QES (und TSP-CVC) um denselben Anbieter handelt, verwendet dieser – wo zulässig – auch dieselben Schnittstellen für die verschiedenen Produkttypen.

TSP-X.509 nonQES, die Zertifikate für den VPN-Zugangsdienst bereitstellen, müssen Sperrinformation über OCSP und CRL im Internet bereitstellen.

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.

324 TSP-X.509 nonQES eGK stellen neben den Zertifikaten für die eGK auch die Zertifikate
325 für die alternativen Versichertenidentitäten bereit. Für diese gelten im Wesentlichen die
326 gleichen Anforderungen wie für die Zertifikate der eGK, aber sie werden über eine
327 dedizierte CA generiert.

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

330 **3.1.3 gematik-Root-CA**

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

333 Zur Etablierung einer einheitlich geregelten PKI für nonQES-Zertifikate stellt die gematik
334 als Policy-Authority eine zentrale Root-CA für alle zertifikatsausgebenden TSP-X.509
335 nonQES bereit. Entsprechend werden alle nonQES-X.509 Sub-CA-Zertifikate in der TI
336 durch die gematikRoot-CA signiert.

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

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

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

346 **3.1.4 Kartenherausgeber**

347 Der Begriff des Kartenherausgebers wird in [gemGlossar] definiert. Siehe dazu auch
348 [gemKPT_PKI_TIP#2.7.3].

349 Leistungserbringerorganisationen (LEOs), Kostenträger (KTR) und Gerätehersteller treten
350 als Kartenherausgeber auf.

351 Verantwortlichkeiten der Kartenherausgeber sind in [gemRL_TSL_SP_CP] beschrieben.

352 **3.1.5 Kartenpersonalisierer**

353 Wird ein Unternehmen mit der Personalisierung beauftragt, dann arbeitet dieses
354 Unternehmen im Sinne eines Betreibers für den Herausgeber der Karte.

355 Der Begriff des Kartenpersonalisierers wird in [gemGlossar] definiert.

356 **3.1.6 Kartenhersteller**

357 Der Kartenhersteller ist für die Produktion der Chipkarten, für die Entwicklung, die
358 Produktzulassung und Installation des COS und für die Entwicklung, die Produktzulassung
359 und Installation des Objektsystems verantwortlich. Der Kartenhersteller kann identisch
360 mit dem Kartenpersonalisierer sein.

3.1.7 Zertifikatsnehmer

Zertifikatsnehmer können Personen (z. B. Versicherter, Leistungserbringer) oder Organisationen des Gesundheitswesens (z. B. medizinische Institution oder Gesellschafterorganisationen) sein. Diese Zertifikate werden als Personen- und Organisationszertifikate bezeichnet (s. auch [gemGlossar].)

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

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

3.1.8 Hersteller

Der Begriff des Herstellers wird in [gemGlossar] definiert.

Die Hersteller von Konnektoren und Kartenterminals verwenden gerätespezifische Sicherheitsmodule (gSMC). Auf diesen sind vom jeweiligen Hersteller beantragte X.509-Komponentenzertifikate (und auch CV-Gerätezertifikate) aufgebracht. Diese gSMCs werden in die entsprechenden Konnektoren und Kartenterminals verbaut bzw. eingesteckt.

Der TSP-X.509 nonQES muss die Konnektor-Zertifikate (C.NK.VPN, C.AK.AUT, C.SAK.AUT) einer gSMC-K auf Antrag hin sperren können (für gSMC-KT ausgestellte Zertifikate ist Sperrbarkeit nicht vorgeschrieben, vgl. [gemSpec_PKI#5.5]). Der TSP-X.509 nonQES kommuniziert im Sperrprozess aber nicht mit dem Besitzer eines Konnektors, sondern nur mit dem Konnektor-Hersteller. Dieser tritt dem TSP-X.509 nonQES gegenüber als Sperrberechtigter auf und nutzt die dafür vorgesehenen Schnittstellen.

Der Hersteller protokolliert deshalb die Zuordnung der Konnektor-Geräte

- zu den darin verbauten gSMC-K (bzw. zu den darauf enthaltenen Zertifikaten) und
- zu den Konnektor-Besitzern.

3.1.9 Anbieter

Der Begriff des Anbieters wird in [gemGlossar] definiert.

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

Anbieter sind Sperrberechtigte für ihren Dienst und nutzen dafür die vorgesehenen Schnittstellen 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).

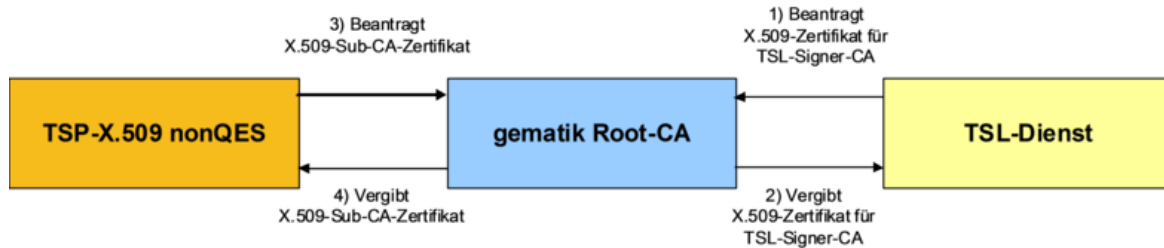


Abbildung 1: Abb_PKI_502 Nachbarsysteme der gematik-Root-CA

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).

419

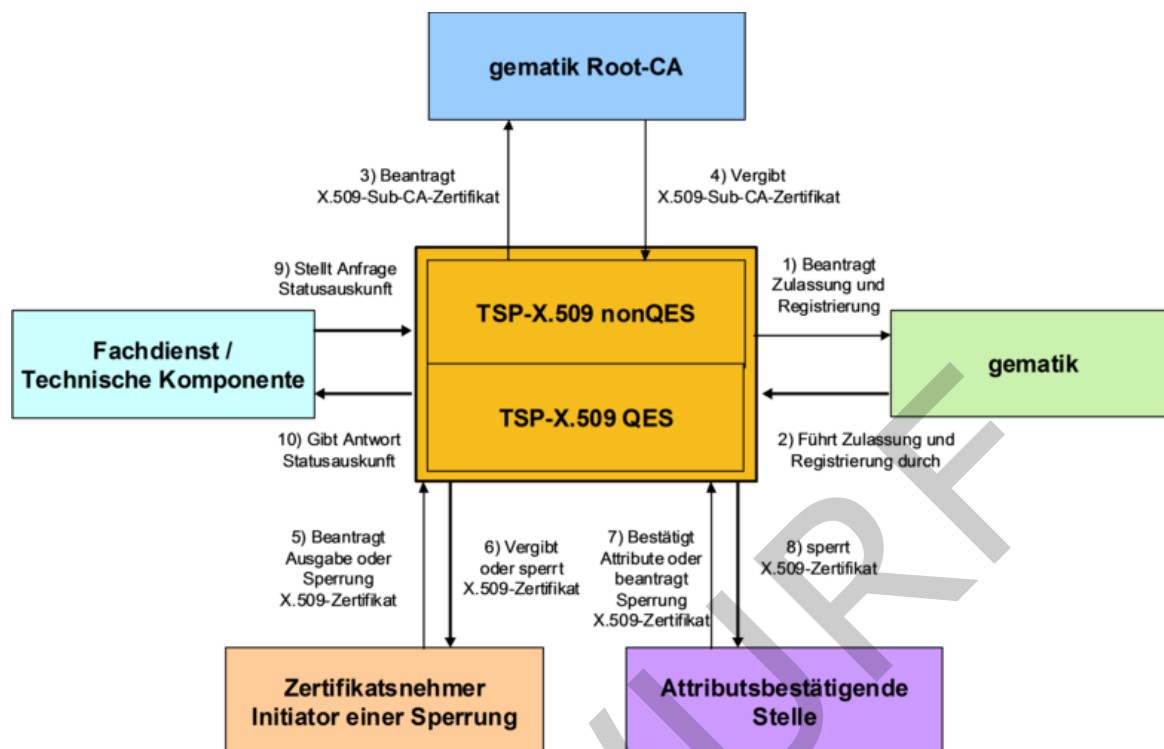


Abbildung 2: Abb_PKI_503 Nachbarsysteme TSP-X.509 QES und TSP-X.509 nonQES

Die Erstellung und Ausgabe von X.509-Zertifikaten für eGK, alternative Versichertenidentitäten, 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 Schnittstellen 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.

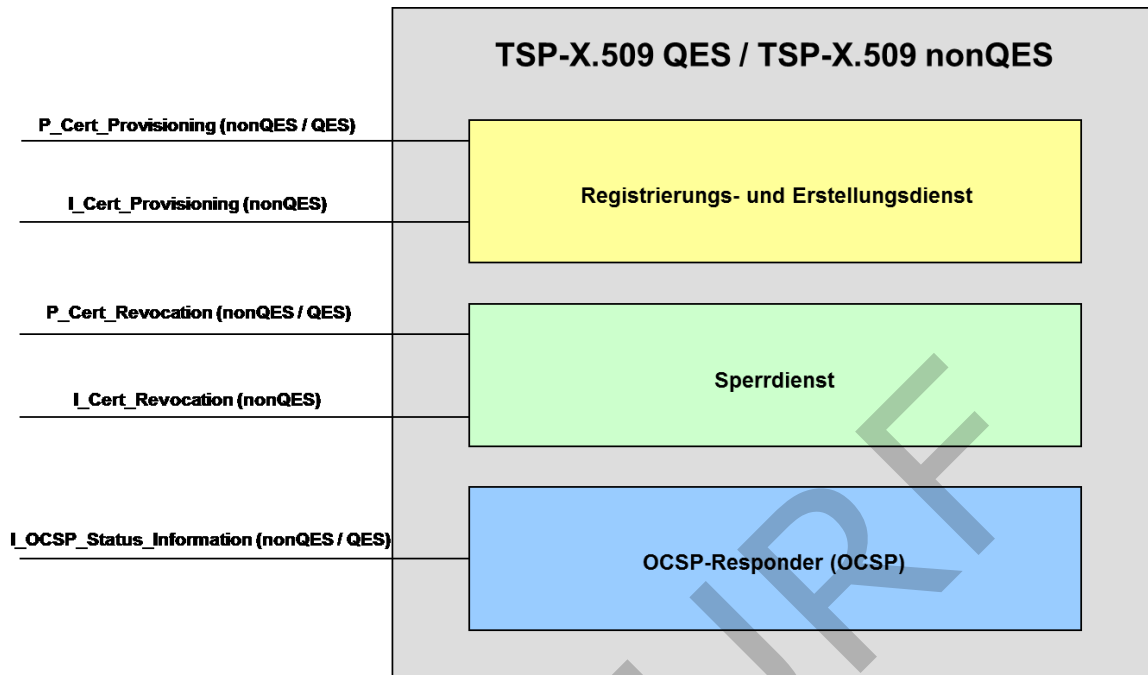
Die folgenden Umsetzungen der Schnittstellen sind zu berücksichtigen.

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.

465



466

467

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

468

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

473

- P_Cert_Provisioning_nonQES_Registration

474

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

475

476

477

- P_Cert_Provisioning_QES_Registration

478

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

479

480

- P_Cert_Provisioning_Erstellung

481

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

482

483

- I_Cert_Provisioning_Registration

484

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

485

486

- I_Cert_Provisioning_Erstellung

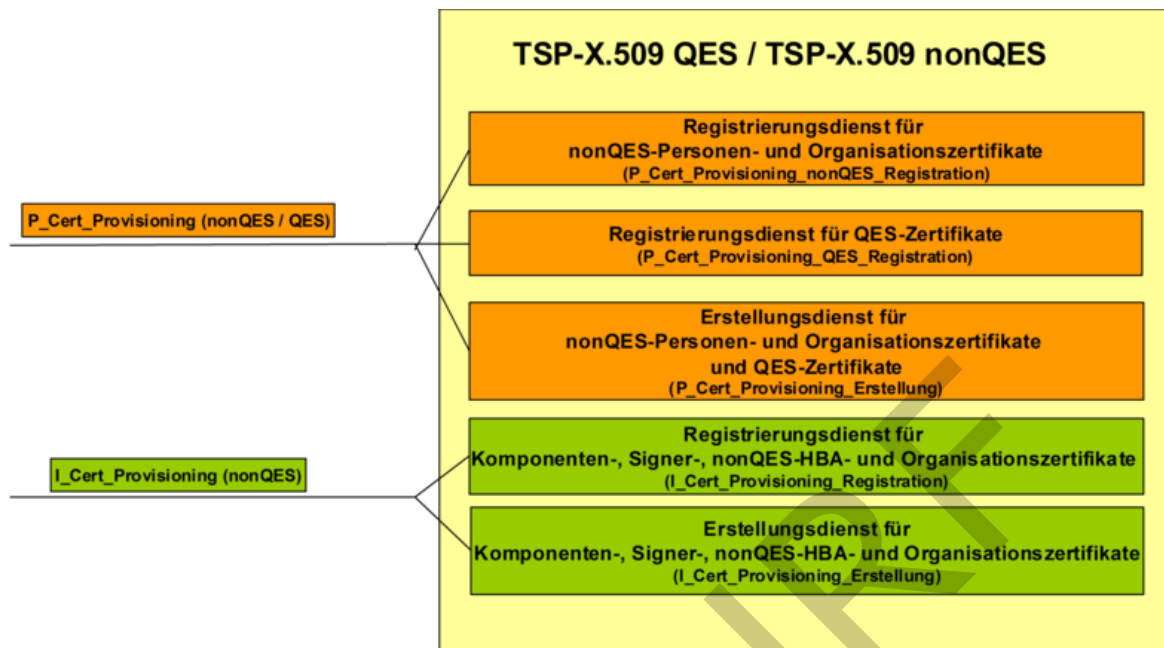
487

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

488

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

492



493

494

495

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

496

497

498

499

500

501

502

503

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

504

- P_Cert_Provisioning_nonQES_Registration,

505

- P_Cert_Provisioning_QES_Registration und

506

- I_Cert_Provisioning_Registration

507

sind Schnittstellen nach außen zum Antragsteller.

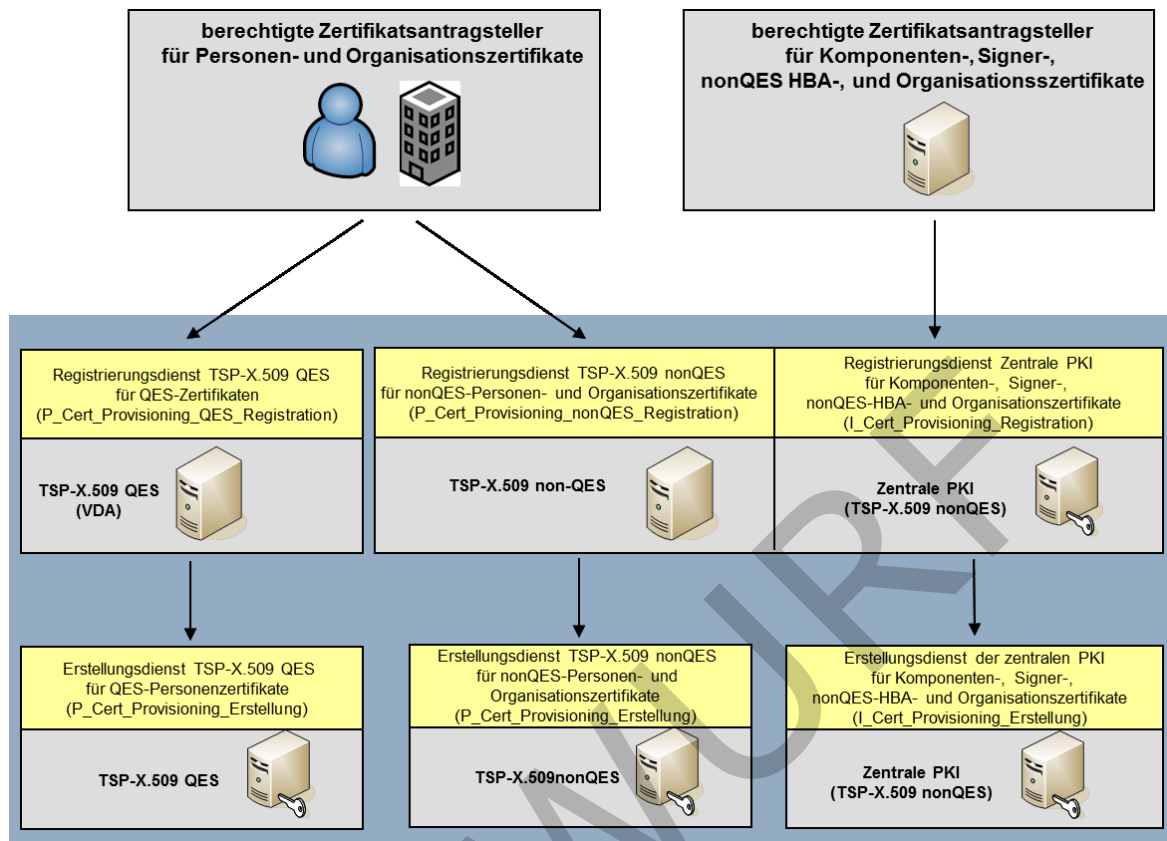


Abbildung 5: Abb_PKI_506 Organisatorische Anordnung der Schnittstelle Registrierungs- und Erstellungsdienst TSP-X.509 QES und TSP-X.509 nonQES

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.

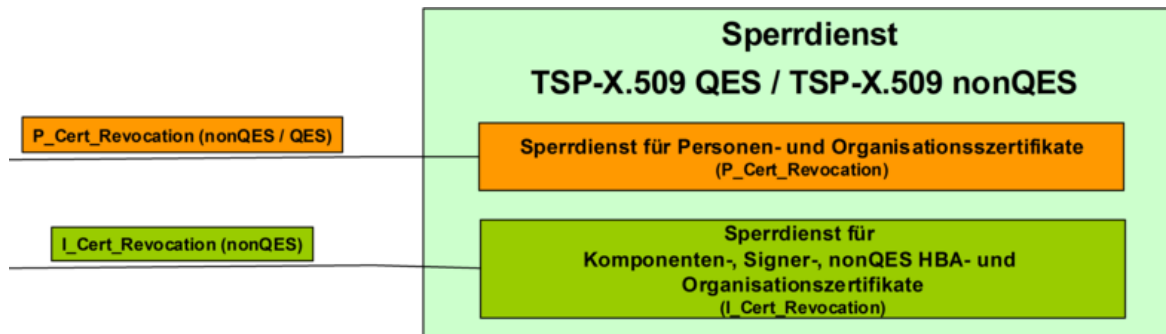


Abbildung 6: Abb_PKI_507 Schnittstellen Sperrdienst des TSP-X.509

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.

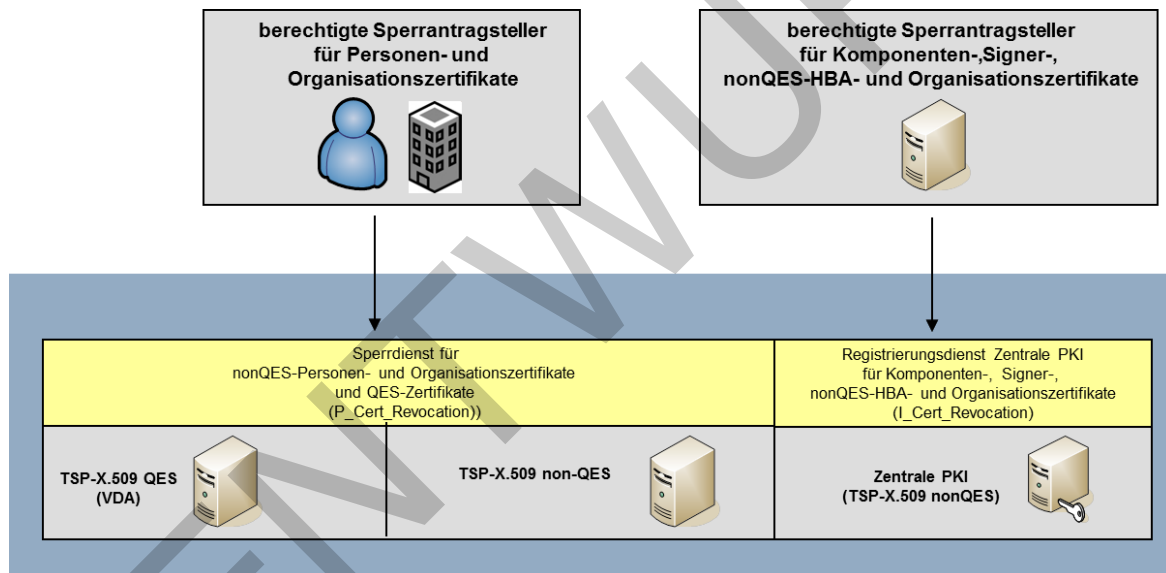


Abbildung 7: Abb_PKI_508 Organisatorische Anordnung Sperrdienst

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.

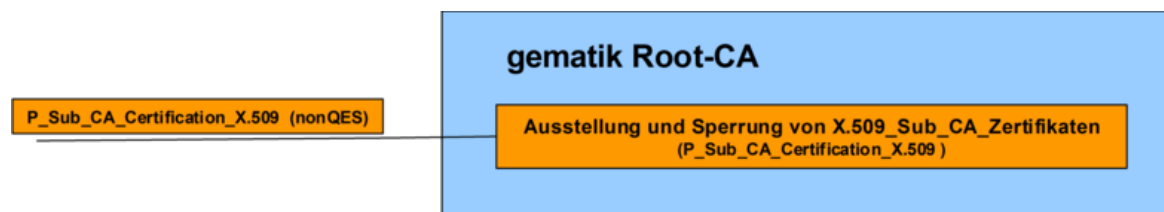


Abbildung 8: Abb_PKI_510 Schnittstellen Erstellung und Sperrung der gematik-Root-CA

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.

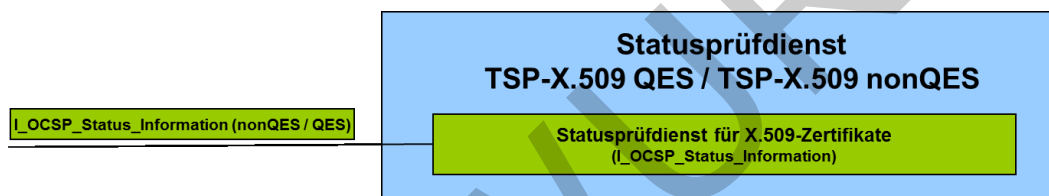


Abbildung 9: Abb_PKI_509 Schnittstellen OCSP-Responder TSP-X.509 QES und TSP-X.509 nonQES

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 Herausgeberpolicies

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. [\leq]

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. (Für die Produktion von HBA und SMC-B für die Personalisierungsvalidierung kann von den zuständigen Kartenherausgebern eine Ausnahmegenehmigung erteilt werden.) [\leq]

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. [\leq]

TIP1-A_3894 - Obligatorisch abzuleitende Sub-CAs unterhalb der gematikRoot-CA

Der TSP-X.509 nonQES MUSS Sub-CA-Zertifikate zur Erstellung von X.509-Zertifikaten von der gematikRoot-CA ableiten. [\leq]

A_17814 - TSP-X.509 nonQES eGK: Ableitung der Sub-CA der alternativen Versichertenidentitäten von der gematik-Root-CA

Der TSP-X.509 nonQES eGK MUSS Sub-CA-Zertifikate zur Erstellung von X.509-Zertifikaten der alternativen Versichertenidentitäten von der gematikRoot-CA ableiten. [\leq]

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 sind für die Verarbeitung der Antrags- und Sperrauftragsdaten die Datenschutzgrundsätze gemäß Art. 5 DSGVO zu berücksichtigen sowie die technischen und organisatorischen Maßnahmen nach Art. 25 und Art. 32 DSGVO zu treffen. [\leq]

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. [\leq]

TIP1-A_4232 - Löschung von TSP-X.509 nonQES-Zertifikatsstatusinformationen, Zertifikats- und Sperranträge

Der TSP-X.509 nonQES MUSS die Zertifikatsanträge, die Zertifikatsstatusinformationen und die Sperraufträge zu einem X.509-Zertifikat unverzüglich löschen, sobald die gesetzlichen oder vertraglichen Aufbewahrungsfristen erreicht sind. [\leq]

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 - Protokollierungsverbot für 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 Datenschutzgrundsatzes der Datenminimierung gemäß Art. 5 Abs. 1 Satz 1 lit.c) DSGVO unter Berücksichtigung der Art. 25, 32 DSGVO derart gestaltet sein, dass nur personenbezogene Daten in der Art und dem Umfang enthalten sind, 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

Die TSP-X.509 nonQES MÜSSEN 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 von

- a) TSP-X.509 nonQES für HBA, SMC-B und eGK zum berechtigten Zertifikatsantragsteller zur Beantragung und Ausstellung von X.509-Personen- und Organisationszertifikaten,
- b) TSP-X.509 nonQES der Komponenten-PKI zum berechtigten Hersteller oder Anbieter zur Beantragung und Ausstellung von X.509-Komponentenzertifikaten,
- c) TSP-X.509 nonQES der Komponenten-PKI zum berechtigten TSP-X.509 nonQES zur Beantragung und Ausstellung von OCSP- und CRL-Signerzertifikaten,
- d) TSP-X.509 nonQES zum Sperrantragsteller für die Sperrung von X.509-Komponenten-, Signer-, nonQES-HBA-, nonQES-eGK- und Organisationszertifikaten.

[<=]

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

A_17234 - Personalisierung von HSMs der KTR-AdV (X.509)

Ein TSP-X.509 nonQES SMC-B MUSS, wenn er mit dem Betreiber einer KTR-AdV einen sicheren Prozess zur Personalisierung von HSMs definiert und etabliert, alle in [gemSpec_KTR-AdV#TAB_ADV_385] genannten Aspekte berücksichtigen.[<=]

A_17643 - Personalisierung von HSMs der Basis- und KTR-Consumer (X.509)

Ein TSP-X.509 nonQES SMC-B MUSS, wenn er mit dem Betreiber eines Basis- oder KTR-Consumer einen sicheren Prozess zur Personalisierung von HSMs definiert und etabliert, alle in [gemSpec_Basis_KTR_Consumer#Tab_Personalisierung_HSM] genannten Aspekte berücksichtigen.

[<=]

Falls für einen Prozess zur HSM-Personalisierung nur eine geringe Anzahl an Instanzen erwartet wird, kann es sinnvoll sein, Teile dieses Prozesses rein organisatorisch umzusetzen. Anstelle einer technischen Schnittstelle kann dann ein papierbasiertes Verfahren eingesetzt werden.

778 **5.5 Schutz der gematik Root-CA**

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

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

784 [\leq]

ENTWURF

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.

[<=]

A_17613 - Schnittstellen TSP-X.509 nonQES eGK für Zertifikate der alternativen Versichertenidentitäten

Der TSP-X.509 nonQES eGK MUSS für die Zertifikate der alternativen Versichertenidentitäten die Schnittstellen

- I_Cert_Provisioning, P_Cert_Revocation und I_OCSP_Status_Information für die AUT_ALT-Zertifikate

umsetzen.[<=]

A_17614 - Dedizierte CA für Zertifikate der alternativen Versichertenidentitäten

Ein TSP-X.509 nonQES eGK MUSS die Zertifikate der alternativen Versichertenidentitäten C.CH.AUT_ALT über eine dedizierte CA ausstellen (s. gemSpec_PKI#5.12.2).[<=]

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.

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

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

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

834 Zur Erstellung der Personen- und Organisationszertifikate werden die in Tab_PKI_501
835 zusammengefassten Rollen zur Berechtigungsprüfung definiert.
836

837 **Tabelle 1: Tab_PKI_501 Allgemeine Übersicht der Rollen und deren Aufgaben beim**
838 **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

839

840 Gemäß Tab_PKI_502 gelten folgende Zuständigkeiten für die berechtigte Antragstellung
841 von nonQES-Zertifikaten für Leistungserbringer, LEO- bzw. KTR-Organisationen und
842 Versicherte.
843

844 **Tabelle 2: Tab_PKI_502 Berechtigte Zertifikatsantragsteller für non-QES**
845 **Leistungserbringer-, LEO bzw. KTR-Organisation und Versicherten-zertifikate sowie**
846 **Prüfkartenzertifikate**

Zertifikatstyp	Berechtigte Zertifikatsantragsteller	Berechtigungsprüfende Stelle	Zertifikatsnehmer
C.HP.AUT C.HP.ENC	Leistungserbringer	herausgebende LEO	Leistungserbringer
	Leistungserbringer der med. Institution	herausgebende LEO	med. Institution

C.HCI.AUT C.HCI.ENC C.HCI.OSIG	Zeichnungsberechtigte r Mitarbeiter d. zertifi- katsnehmenden Ge- sellschafterorganisatio n	Herausgebende Organisation (z.B. Spitzenverband d. zertifikatsnehmenden Gesellschafterorganisa- tion)	Gesellschafterorganisat ion
	KTR-Organisation	KTR-Organisation	Kostenträger- Geschäftsstelle
C.CH.AUT C.CH.ENC C.CH.AUTN C.CH.ENCV C.CH.AUT_AL T	herausgebender Kos- tenträger	herausgebender Kos- tenträger	Versicherter
C.CH.AUT C.CH.ENC C.CH.AUTN C.CH.ENCV	gematik als Herausgeber der Prüfkarte eGK	gematik	gematik Prüfidetitität für Prüfkarte eGK

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

Zertifikatssty p	Berechtigte Zertifikatsantragstell er	Berechtigungsprüfend e Stelle	Zertifikatsnehme r
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.

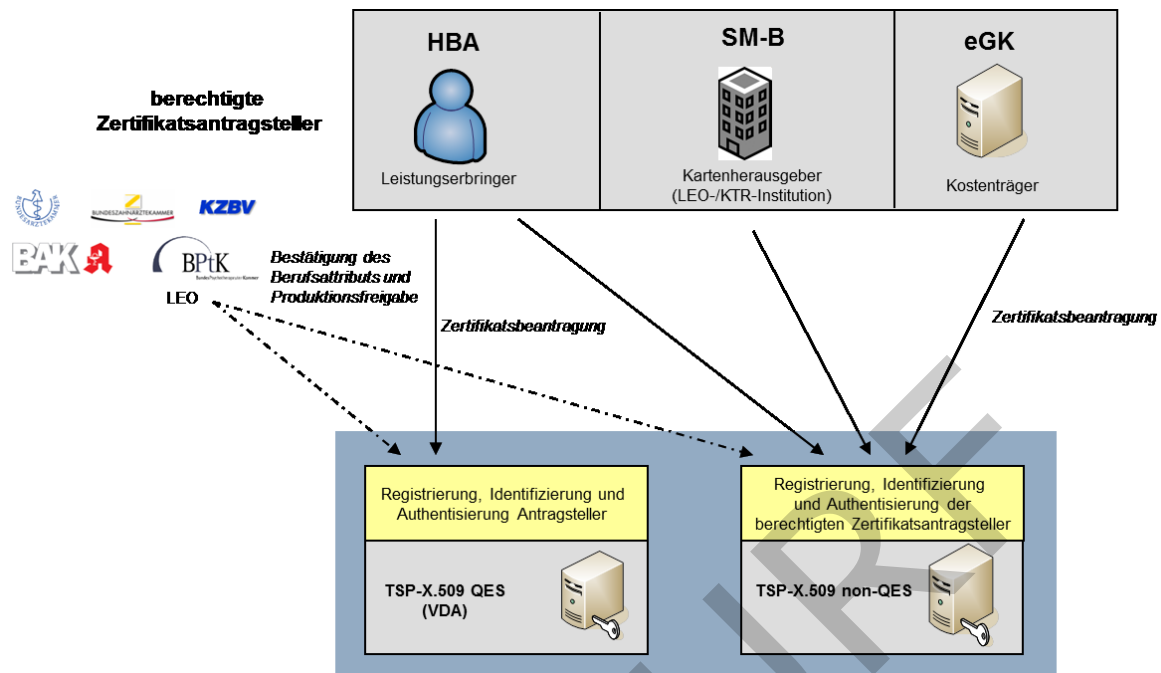


Abbildung 10: Abb_PKI_511 Zuständigkeiten der Rollen bei Zertifikatsantragstellung der Personen- und Organisationszertifikate

Hinweis: Die in der Abbildung aufgeführten Symbole für die Bundesorganisationen der Leistungserbringerorganisationen (LEO) stehen hier und in weiteren Abbildungen stellvertretend für die zuständigen Organisationen.

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)
- Schnittstelle zur Ausstellung von Zertifikaten der alternativen Versichertenidentitäten (I_Cert_Provisioning)

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.

[<=]

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

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

884 Der TSP-X.509 nonQES MUSS in seiner CP (bzw. CPS) festlegen, a) welche Stellen für die
885 Zertifikatsbeantragung von nonQES-Personen- und Organisationszertifikate berechtigt
886 sind und b) wie die Registrierung zur eindeutigen Identifikation und Authentisierung der
887 berechtigten Zertifikatsantragsteller durchzuführen ist.
888 [\leq]

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

891 Der TSP-X.509 nonQES MUSS das Antragsverfahren mit den Kartenherausgebern für
892 HBAs, eGKs, und SMC-Bs abstimmen und bereitstellen.
893 [\leq]

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

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

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

905 Ist die Überprüfung des Zertifikatsantrags negativ verlaufen, MUSS der TSP-X.509
906 nonQES sicherstellen, dass keine Zertifikatsanträge an Bestätigungsprüfende Stellen zur
907 Bestätigung des Berufsgruppenattributs und Produktionsfreigabe weitergeleitete werden.
908 [\leq]

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

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

- 914 • Produktionsfreigabe
- 915 • UID des Antragsstellers (optional)
- 916 • Telematik-ID

917 [\leq]

918 **TIP1-A_3570 - Eingangsdaten Leistungserbringerzertifikat**

919 Die TSP-X.509 nonQES MUSS sicherstellen, dass mindestens die in den Zertifikatsprofilen
920 der HBA-Kartenherausgeber als Pflichtfelder festgelegten spezifischen Daten des
921 Zertifikatsnehmers für die Erstellung von X.509-Zertifikaten für Leistungserbringer zu
922 jedem Zertifikatsantrag vorliegen.
923 [\leq]

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

925 Der TSP-X.509 nonQES MUSS für Leistungserbringer die Berufsbezeichnung für das Feld
926 professionItem sowie die vorgegebene OID zu der angegeben Berufsbezeichnung für das
927 Attribut Admission des X.509-Personen- und Organisationszertifikates als professionOID

928 gemäß [gemSpec_OID#Tab_PKI_402] zu den Zertifikatserstellungsdaten hinzufügen.
929 [=]

930 Die Object Identifier sind im Dokument [gemSpec_OID] angegeben.

931 **TIP1-A_3572 - Eingangsdaten Organisationszertifikate**

932 Die TSP-X.509 nonQES MUSS sicherstellen, dass mindestens die in
933 [gemSpec_PKI#Tab_PKI_238], [gemSpec_PKI#Tab_PKI_239] und
934 [gemSpec_PKI#Tab_PKI_240] mit der Kardinalität 1 festgelegten spezifischen Daten des
935 Zertifikatsnehmers für die Erstellung von X.509-Organisationszertifikate für LEO- und
936 KTR-Institutionen zu jedem Zertifikatsantrag vorliegen.
937 [=]

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

939 Der TSP-X.509 nonQES MUSS für Leistungserbringer- und Kostenträger-Organisationen
940 für die Erweiterung Admission im Feld professionItem die Beschreibung der Institution
941 sowie im Feld professionOID die OID der Institution gemäß
942 [gemSpec_OID#Tab_PKI_403] zu den Zertifikatserstellungsdaten hinzufügen.
943 [=]

944 Die Object Identifier sind im Dokument [gemSpec_OID] angegeben.

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

946 Der TSP-X.509 nonQES MUSS sicherstellen, dass mindestens die in
947 [gemSpec_PKI#Tab_PKI_232] und [gemSpec_PKI#Tab_PKI_233] mit der Kardinalität 1
948 festgelegten spezifischen Daten des Zertifikatsnehmers für die Erstellung von X.509-
949 Personenzertifikaten für Versicherte zu jedem Zertifikatsantrag vorliegen.
950 [=]

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

952 Der TSP-X.509 nonQES MUSS sicherstellen, dass mindestens die in
953 [gemSpec_PKI#Tab_PKI_235] und [gemSpec_PKI#Tab_PKI_236] mit der Kardinalität 1
954 festgelegten spezifischen Daten des Zertifikatsnehmers für die Erstellung der X.509-
955 Zertifikate vom Typ AUTN und ENCV für Versicherte zu jedem Zertifikatsantrag vorliegen.
956 [=]

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

958 Der TSP-X.509 nonQES MUSS für alle Versichertenzertifikate die zu „oid_versicherter“
959 zugeordnete Beschreibung in das Feld professionItem sowie die zugehörige OID in das
960 Feld professionOID gemäß [gemSpec_OID#Tab_PKI_402] für das Attribut Admission des
961 X.509-Zertifikates zu den Zertifikatsdaten hinzufügen.
962 [=]

963 **TIP1-A_3577 - Optionale Eingangsdaten**

964 Der TSP-X.509 nonQES MUSS die in den Zertifikatsprofilen [gemSpec_PKI#5] als
965 optional gekennzeichneten Daten an den Erstellungsdienst des TSP-X.509 nonQES
966 übermitteln, wenn diese vom berechtigten Zertifikatsantragssteller für Personen- und
967 Organisationszertifikate im Rahmen des Antragsverfahrens übermittelt werden.
968 [=]

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

970 Der Registrierungsdienst des TSP-X.509 nonQES MUSS für die Erstellung der X.509-
971 Personen- und Organisationszertifikate mindestens alle notwendigen Zertifikatsdaten an
972 den Erstellungsdienst weiterleiten.
973 [=]

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

975 Der Registrierungsdienst des TSP-X.509 nonQES MUSS pro Zertifikatsantrag mindestens
976 das erstellte X.509-Personen- und Organisationszertifikat als Ausgabedatum sowie

weitere Daten, die einen eindeutigen Bezug zur Bestellung ermöglichen, bereitstellen.

[<=]

TIP1-A_5090 - Rückmeldung Zertifikatsinformationen (nonQES) an

Bestätigende Stelle

TSP-X.509 nonQES MUSS der Bestätigenden Stelle des Berufsgruppenattributes 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 Zertifikatsantragsteller 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 negativen 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 Zertifikatsantragsteller ausliefern.
7. Der Registrierungsdienst des TSP-X.509 nonQES MUSS der Bestätigenden Stelle des Berufsgruppenattributes das Zertifikat und zertifikatsrelevante Informationen zurückliefern.

[<=]

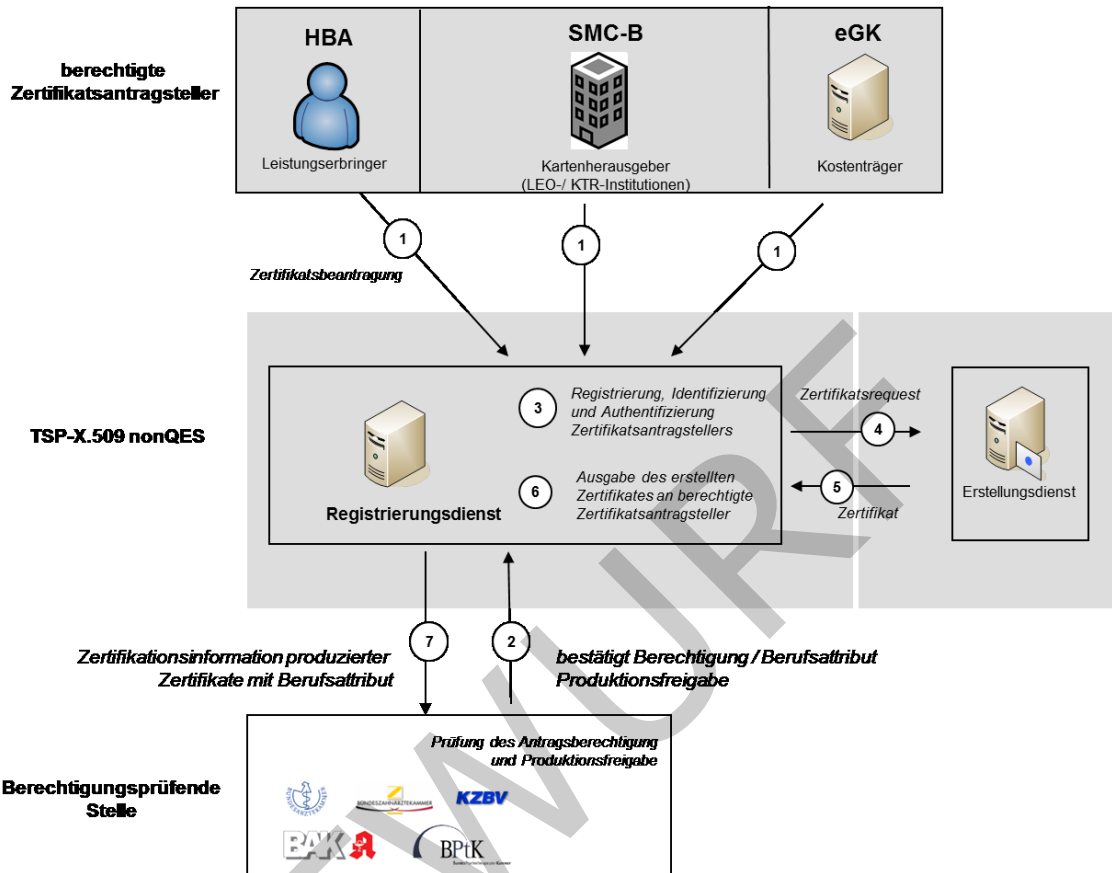


Abbildung 11: Abb_PKI_512 Prozessablauf Registrierungsdienst nonQES-Personen- und Organisationszertifikate

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

Der TSP-X.509 QES MUSS seine Antrags- und Ausgabeprozesse sowie Registrierungs-, Erstellungs- und Statusprüfdienst OCSP-Responder für QES-Zertifikate gemäß den Vorgaben aus [eIDAS] durchführen.

[<=]

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 weitergeleitet 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 angegebenen 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_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-Zertifikaten beauftragt wird.

[<=]

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

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

- das erzeugte QES-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

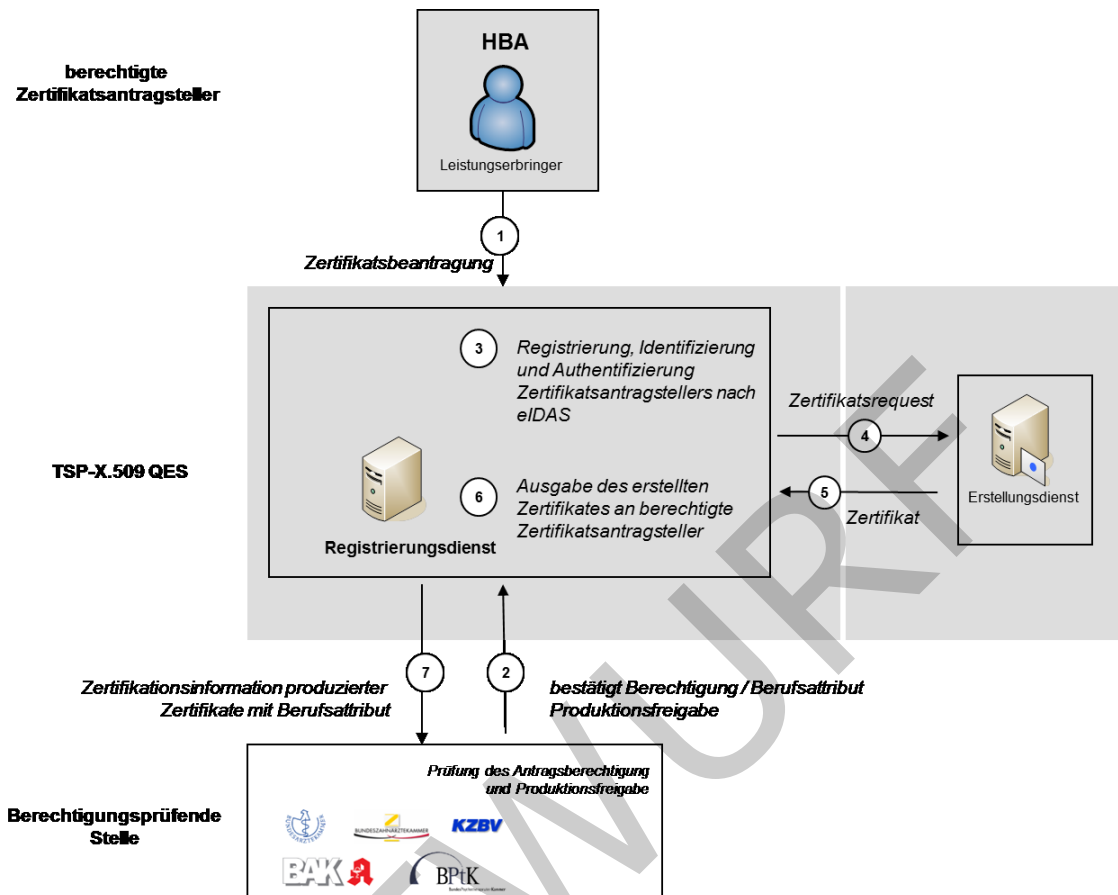
Der TSP-X.509 QES MUSS in seinem Registrierungsdienst für QES-Zertifikate die folgenden Schritte durchführen:

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 [eIDAS] 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 Zertifikatsantragsteller 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.

1116



1117

1118

1119

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 sicherstellen, dass der SubjectDN eines X.509-Personen- und Organisationszertifikates den Zertifikatsinhaber TI-weit eindeutig bezeichnet. Dies erfolgt durch die geeignete Wahl der Attributsinhalte und gilt unabhängig davon, ob die Attribute optional oder obligatorisch sind.

[<=]

1138 Für die Erzeugung des X.509-Personen- und Organisationszertifikats sind die
1139 Festlegungen gemäß [gemSpec_PKI] hinsichtlich der Zertifikatsprofile sowie der
1140 Kodierung von Identitäten zu berücksichtigen.

1141 **TIP1-A_3886 - OCSP-Adresse im X.509-Zertifikate**

1142 Die TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN im Feld AIA der ausgegebenen
1143 X.509-Zertifikate den URL des zugeordneten OCSP-Responders eintragen.
1144 [\leq]

1145 **TIP1-A_3592 - Erstellung von X.509-Personen- und Organisationszertifikaten**

1146 TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN mit Hilfe der X.509-CA zur Erzeugung
1147 von X.509-Personen- und Organisationszertifikaten das X.509-Zertifikat erstellen und das
1148 erstellte X.509-Zertifikat an den Registrierungsdienst TSP-X.509 QES bzw. TSP-X.509
1149 nonQES zurückliefern.
1150 [\leq]

1151 **TIP1-A_3583 - Erstellung QES-Zertifikat nach eIDAS**

1152 Der TSP-X.509 QES MUSS die Erstellung von QES-X.509-Zertifikaten gemäß den
1153 Vorgaben von [eIDAS] durchführen.
1154 [\leq]

1155 **TIP1-A_3887 - Verarbeitung von Anträgen bei einem nicht-sicherheitskritischen
1156 Incidents von X.509-Personen- und Organisationszertifikaten**

1157 TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN sicherstellen, dass ab dem Zeitpunkt
1158 der Feststellung eines nicht-sicherheitskritischen Incidents, bis zur Klärung des
1159 Sachverhaltes über das weitere Vorgehen im Rahmen des Incident Managements, keine
1160 Zertifikatsanträge für Personen- und Organisationszertifikate der betroffenen CA von dem
1161 Registrierungsdienst des TSP-X.509 QES und TSP-X.509 nonQES entgegennehmen oder
1162 bereits entgegengenommene verarbeiten werden.
1163 [\leq]

1164 **TIP1-A_3888 - Zertifikatsstatusinformationen der Personen- und
1165 Organisationszertifikate**

1166 TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN die Statusinformation für die erstellten
1167 Personen- und Organisationszertifikat dem OCSP-Responder in der TI und im Internet zur
1168 Verfügung stellen.
1169 [\leq]

1170 Für die QES-Zertifikatsprüfung in der TI benötigen zertifikatsprüfende Komponenten die
1171 jeweiligen OCSP-Responder-Adressen in der TI. Diese werden der TSL entnommen (vgl.
1172 gemSpec_TSL#TIP1-A_7219 und gemSpec_PKI#TUC_PKI_030) und müssen durch die
1173 TSP-X.509 QES zur Verfügung gestellt werden.

1174 **A_18040 - Verpflichtung Meldung Übersetzung QES Internet-OCSP- in TI-OCSP-
1175 Adressen für TSL**

1176 Der TSP-X.509 QES MUSS alle in den End-Entity-Zertifikaten im AuthorityInfoAccess-Feld
1177 (AIA) eingetragenen OCSP-Responder-Adressen im Internet (vgl.
1178 gemSpec_PKI#Tab_PKI_270) sowie die zugehörigen Adressen der zuständigen OCSP-
1179 Responder in der TI der gematik mitteilen, damit diese Informationen für QES-
1180 Zertifikatsprüfungen gem. gemSpec_PKI#TUC_PKI_030 in die TSL aufgenommen werden
1181 können.[\leq]

1182

1183 **TIP1-A_3594 - Bereitstellungszeitpunkt der Zertifikatsstatusinformation für
1184 Personen- und Organisationszertifikate**

1185 TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN die Zertifikatsstatusinformation für die
1186 erstellten Personen- und Organisationszertifikate dem OCSP-Responder in der TI und im
1187 Internet gemäß den in Tabelle Tab_PKI_509 definierten Bereitstellungszeitpunkten zur

1188 Verfügung stellen.
1189 [\leq]

1190

1191 **Tabelle 4: Tab_PKI_509 Bereitstellungszeitpunkt der Zertifikatsstatusinformation durch**
1192 **den Erstellungsdiens**

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 C.CH.AUT_ALT	Unmittelbar nach Erstellung des X.509-Zertifikates

1193

1194 **TIP1-A_3595 - Anforderungen von LEO- und KTR-Institutionen**

1195 TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN weitere Anforderungen und
1196 Konkretisierungen an den Erstellungsdiens für Personen- und Organisationszertifikate
1197 durch die jeweiligen LEO- und KTR-Organisationen in ihren Prozessen berücksichtigen.
1198 [\leq]

1199 6.1.3.2 Umsetzung

1200 **TIP1-A_3596 - Umsetzung Erstellungsdiens TSP-X.509 QES und TSP-X.509**
1201 **nonQES für Personen- und Organisationszertifikate**

1202 TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN in Ihrem Erstellungsdiens für
1203 Personen- und Organisationszertifikate die folgenden Schritte durchführen:

- 1204 1. TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN nach erfolgreicher Identifizierung
1205 des Antragstellers die erforderlichen Angaben zur Zertifikatserstellung an den
1206 Erstellungsdiens des TSP-X.509-CA weiterleiten.
- 1207 2. TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN auf Grund der übermittelten
1208 Angaben die Personen- und Organisationszertifikate erzeugen und diese mit dem
1209 privaten Schlüssel der ausstellenden X.509-CA signieren.
- 1210 3. TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN die erzeugten Personen- und
1211 Organisationszertifikate an den Registrierungsdiens TSP-X.509 QES bzw. TSP-
1212 X.509 nonQES zurückliefern.
- 1213 4. TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN dem OCSP-Responder die
1214 Zertifikatsstatusinformationen nach den in Tabelle Tab_PKI_509 definiertem
1215 Zeitpunkten zur Verfügung stellen.

1216 [\leq]

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.

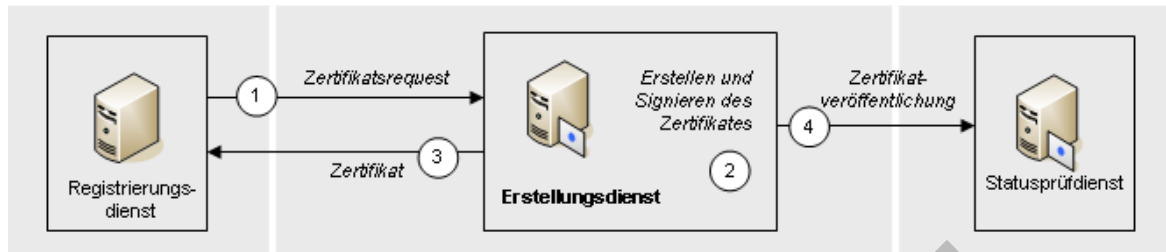


Abbildung 13: Abb_PKI_514 Prozessablauf Erstellungsdienstes des TSP-X.509-CA

6.1.4 Schnittstelle I_Cert_Provisioning

Der TSP-X.509 nonQES eGK stellt die Schnittstelle I_Cert_Provisioning für die AUT_ALT-Zertifikate zur Verfügung.

Für die Zertifikate C.CH.AUT_ALT der alternativen Versichertenidentitäten gelten bzgl. der Ausstellung die gleichen Vorgaben wie für die analogen Zertifikate auf der eGK (s. Kap. 6.1). Die abweichenden Regelungen sind in den nachfolgenden Unterabschnitten angegeben.

A_17615 - Automatisierter Ablauf der Operationen an der Schnittstelle I_Cert_Provisioning

Ein TSP-X.509 nonQES eGK MUSS einen vollständig automatisierten Ablauf der Operationen an der Schnittstelle I_Cert_Provisioning ermöglichen. [\leq]

~~A_17659 - Eintrag der Schnittstelle I_Cert_Provisioning in das Interoperabilitätsverzeichnis vesta~~

~~Ein TSP-X.509 nonQES eGK MUSS die Spezifikation seiner Implementierung der Schnittstelle I_Cert_Provisioning in das Interoperabilitätsverzeichnis vesta der gematik aufnehmen lassen. [\leq]~~

Die Regeln zur Aufnahme in das Interoperabilitätsverzeichnis vesta sind in der Geschäfts- und Verfahrensordnung [GVO_IOPVZ] beschrieben.

6.1.4.1 AUT_ALT

A_17617 - Berechtigungserteilung an der Schnittstelle I_Cert_Provisioning

Der TSP-X.509 nonQES eGK MUSS für die Schnittstelle I_Cert_Provisioning der C.CH.AUT_ALT-Zertifikate sicherstellen, dass nur dann eine Berechtigung erteilt wird, wenn

- der Nutzer ein durch die gematik zugelassener Signaturdienst ist (der Hinweis zu TIP1-A_3603 gilt hier sinngemäß) und
- vom zuständigen eGK Kartenherausgeber als Berechtigter benannt wurde.

[\leq]

A_17618 - Bereitstellung der Operation I_Cert_Provisioning:provide_Certificate für C.CH.AUT_ALT

Ein TSP-X.509 nonQES eGK MUSS die Operation I_Cert_Provisioning:provide_Certificate zur Verfügung stellen, über die ein berechtigter Signatordienst C.CH.AUT_ALT-Zertifikate integritätsgeschützt und vertraulich abrufen kann.[<=]

A_17619 - Umsetzung der Operation I_Cert_Provisioning:provide_Certificate für C.CH.AUT_ALT

Ein TSP-X.509 nonQES eGK MUSS sicherstellen, dass die Operation I_Cert_Provisioning:provide_Certificate nur mit Erfolg durchgeführt und das Zertifikat zurückgegeben wird, wenn

- der Kartenherausgeber beim TSP-X.509 nonQES eGK eine Registrierung des Versicherten auf Basis von bestehenden Datensätzen vorgenommen hat, die bei der Erstellung des Zertifikats verwendet werden (vgl. gemSpec_PKI#GS-A_4966 und gemRL_TSL_SP_CP#GS-A_4187),
- ein Zertifikatsrequest gem. PKCS#10 (RFC2986) mit den restlichen erforderlichen Daten übergeben wurde,
- alle lt. gemSpec_PKI#Tab_PKI_232 obligatorischen Zertifikatsdaten vorliegen,
- der Aufrufer als ein berechtigter Nutzer der Schnittstelle authentifiziert werden konnte.

[<=]

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

Die gematik hat die Verantwortung für die Ausgabe von Komponentenzertifikaten 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.

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

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

1293

1294

1295

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

1296

1297

1298

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

Zertifikatstyp	Berechtigte Zertifikatsantragsteller	Berechtigungsprüfende Stelle	Zertifikatsnehmer
C.NK.VPN	Hersteller	gematik	Konnektor
C.NK.VPN	Diensteanbieter, gematik	gematik	Service Monitoring
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-C	Diensteanbieter, gematik	gematik	Service Monitoring
C.FD.TLS-S	Diensteanbieter	gematik	Fachanwendungsspezifischer Dienst

C.FD.SIG	Diensteanbieter	gematik	Fachanwendungsspezifischer Dienst
C.FD.AUT	Diensteanbieter	gematik	Fachanwendungsspezifischer Dienst
C.FD.ENC	Diensteanbieter	gematik	Fachanwendungsspezifischer Dienst
C.CM.TLS-CS	Diensteanbieter	gematik	Fachanwendungsspezifischer Dienst
C.SGD-HSM.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
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 Gesellschafterorganisations- Geschäftsstelle/Betriebsstätte Kostenträrgeschäftsstelle
C.HCI.ENC	Kartenherausgeber	gematik Kartenherausgeber	med. Institution Gesellschafterorganisations- Geschäftsstelle/Betriebsstätte Kostenträrgeschäftsstelle
C.HCI.OSIG	Kartenherausgeber	gematik Kartenherausgeber	med. Institution Gesellschafterorganisations- Geschäftsstelle/Betriebsstätte Kostenträrgeschäftsstelle

*) geplant

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

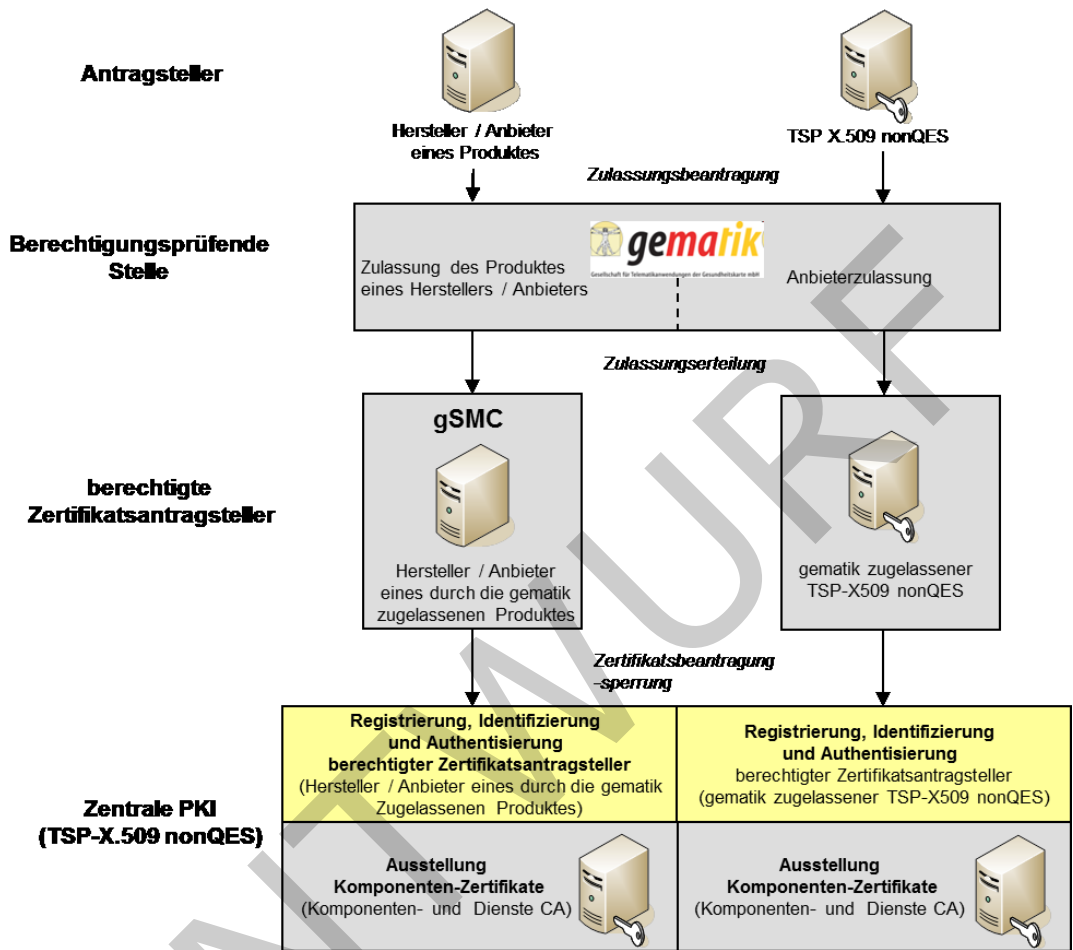


Abbildung 14: Abb_PKI_515 Zuständigkeiten der Rollen bei der Beantragung von Komponenten- und Signerzertifikaten

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

1309

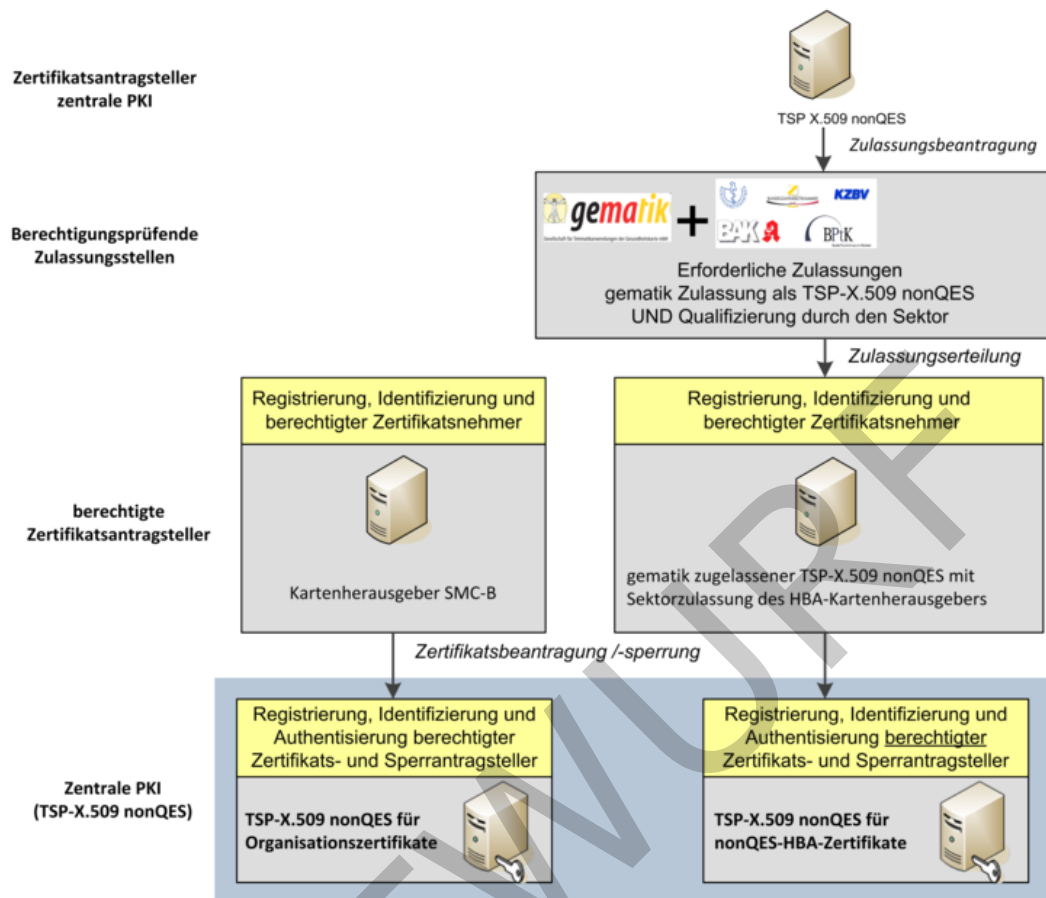


Abbildung 15: Abb_PKI_520 Zuständigkeiten der Rollen bei nonQES-HBA- und Organisationszertifikatsantragstellung

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? [\leq]

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 (Qualifizierung) zur Ausgabe einer HBA bzw. SMC-B durch den jeweiligen Kartenherausgeber. [\leq]

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. [\leq]

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. [\leq]

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. [\leq]

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 Prüfregelein für die Berechtigung zur Antragsstellung von Komponenten- und Signerzertifikaten in seiner CP (bzw. CPS) definieren. [\leq]

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 Signerzertifikate zu beziehen und b) eine Freigabe der gematik zum Abruf produktiver Zertifikate für diesen Antragsteller vorliegt. [\leq]

1379 Hinweis: Die Möglichkeit zum Abruf produktiver Zertifikate kann auch vor formaler
1380 Erteilung der Zulassung des Produkts durch die gematik erfolgen. Der Bedarf hierzu ist
1381 durch den Hersteller unter Nennung von Gründen anzuzeigen und wird unter folgenden
1382 Rahmenbedingungen erteilt:

- 1383 • erfolgreiche Prüfung der Sicherheitseignung gemäß [gemRL_PruefSichEig]
1384 durch den Personalisierer der Gerätekarte abgeschlossen,
- 1385 • der Bestätigung des sicheren Transports zum Kartenherausgeber,
- 1386 • eine ausreichende funktionale Qualität des Produktes wurde durch die gematik
1387 geprüft und
- 1388 • ggf. Bestätigung der erfolgreichen fachlichen und technischen Prüfung seitens
1389 BSI.

1390 **TIP1-A_4465 - Überprüfung bei Registrierung der Antragsteller für nonQES-**
1391 **HBA- und Organisationszertifikate**

1392 Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS bei der Registrierung von
1393 Antragsberechtigten für nonQES-HBA- und Organisationszertifikate prüfen, ob a) der
1394 Antragsteller berechtigt ist, nonQES-HBA- bzw. Organisationszertifikate zu beziehen, b)
1395 eine Zulassung durch die gematik erfolgt ist und c) eine Qualifizierung durch den Sektor
1396 vorliegt.
1397 [\leq]

1398 **TIP1-A_3605 - Registrierungsdienst für Komponenten- und Signer-, nonQES-**
1399 **HBA- und Organisationszertifikate**

1400 Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS einen Registrierungsdienst für
1401 Komponenten- und Signer-, nonQES-HBA- und Organisationszertifikate zur Verfügung
1402 stellen, der aus dem Zertifikatsantragsdienst und der Zertifikatsausgabe besteht.
1403 [\leq]

1404 **TIP1-A_3606 - Automatisierter Registrierungsdienst für**
1405 **Komponentenzertifikate**

1406 Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS
1407 eine vollständig automatisierte Authentisierung, Berechtigungsprüfung, Anlieferung und
1408 Bearbeitung der Requests sowie Ausgabe der erstellten Komponenten, Signer-, nonQES-
1409 HBA- und Organisationszertifikate ermöglichen.
1410 [\leq]

1411 **TIP1-A_3607 - Request-Inhalte**

1412 Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS
1413 prüfen, ob in dem eingereichten Zertifikatsantrag alle obligatorisch geforderten Inhalte
1414 für die Erstellung eines Komponenten-, Signer-, nonQES-HBA oder
1415 Organisationszertifikats enthalten sind.
1416 [\leq]

1417 **TIP1-A_3608 - Überprüfung Zertifikatsantrag für Komponentenzertifikate**

1418 Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS bei
1419 Eingang eines Zertifikatsantrags folgende Überprüfungen durchführen: a) Ist der
1420 Hersteller oder Anbieter von der gematik berechtigt Zertifikatsanträge für
1421 Komponentenzertifikate zu stellen? b) Ist der Hersteller oder Anbieter durch den TSP-
1422 X.509 nonQES registriert? c) Ist das Produkt für den der Zertifikatsantrag des
1423 zugelassenen Herstellers oder Anbieters bei dem TSP-X.509 nonQES eingereicht wurde,
1424 von der gematik zugelassen? d) Ist die angegebene Seriennummer so gewählt, dass der
1425 SubjectDN des zu erstellenden Komponentenzertifikats eindeutig ist? e) Sind alle Inhalte
1426 für die Erstellung eines Komponentenzertifikats enthalten?
1427 [\leq]

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.
[<=]

1477 Auswirkungen auf die Gültigkeit bereits ausgestellter X.509-Zertifikate hat der Vorgang
1478 nicht.

1479 **TIP1-A_3616 - Weiterleitung der Daten an den Registrierungsdienst des TSP-**
1480 **X.509**

1481 Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) MUSS
1482 nach erfolgreicher Authentifizierung und Prüfung des Zertifikatsantrags die Daten zur
1483 Zertifikatserstellung von Komponenten-, Signer-, nonQES-HBA- und
1484 Organisationszertifikate an den Erstellungsdienst weiterleiten.

1485 [\leq]

1486 **TIP1-A_3890 - Umgang mit nicht-sicherheitskritischen Incidents für**
1487 **Komponentenzertifikate**

1488 Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS sicherstellen, dass ab dem
1489 Zeitpunkt der Feststellung eines nicht-sicherheitskritischen Incidents, bis zur Klärung des
1490 Sachverhaltes über das weitere Vorgehen im Rahmen des Incident Managements, keine
1491 Zertifikatsanträge für Komponenten-, Signer-, nonQES-HBA- oder
1492 Organisationszertifikate der betroffenen CA entgegengenommen oder an den
1493 Erstellungsdienst des TSP-X.509 nonQES weitergeleitet werden.

1494 [\leq]

1495 **6.2.1.2 Umsetzung**

1496 Voraussetzung für den Bezug von X.509-Zertifikaten über die zentrale PKI der TI ist die
1497 erfolgreiche Zulassung/Qualifizierung des Herstellers (Komponentenzertifikate) oder TSP-
1498 X.509 nonQES (Signerzertifikate, HBA- und SMC-B Zertifikate) durch

- 1499 • den zuständigen Sektor (LEO, KTR) und die gematik für nonQES X.509-
1500 Zertifikate für HBA und SMC-B
- 1501 • die gematik für nonQES X.509-Zertifikate für Signer- und
1502 Komponentenzertifikate.

1503 Nachfolgend werden kurz Zulassungsablauf sowie spezifische Anforderungen an den
1504 Anbieter der zentralen PKI aufgezeigt. Eine grafische Übersicht dieser Zusammenhänge
1505 erfolgt in der Abb_PKI_516.

1506 Zuständigkeiten und Ablauf für die Zulassung:

- 1507 1. TSP-X.509 nonQES und Hersteller von Komponenten beantragen eine Zulassung
1508 bei der gematik in ihrer Eigenschaft als Herausgeber von Zertifikaten.
- 1509 2. TSP-X.509 nonQES beantragen eine Qualifizierung bei der zuständigen LEO / KTR,
1510 sofern sie nonQES-Zertifikate für HBA oder SMC-B anbieten wollen.

1511 **TIP1-A_3618 - Umsetzung Registrierungsdienst für Komponenten-, Signer-,**
1512 **nonQES-HBA- und Organisationszertifikate**

1513 Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS sicherstellen, dass zur
1514 Bearbeitung einer Registrierung und eines Antrags auf die Ausstellung eines
1515 Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikat die folgenden Schritte
1516 durchgeführt werden:

- 1517 1. Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS der gematik eine
1518 Schnittstelle zur Verfügung stellen, über die die gematik dem beauftragtem TSP-
1519 X.509 nonQES Berechtigungsinformationen authentisch, integritätsgeschützt und
1520 vertraulich übermitteln kann.
- 1521 2. Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die von der gematik
1522 übermittelten Berechtigungsinformationen auf Authentizität und Integrität prüfen
1523 und in dem eigenen Registrierungssystem übernehmen.

- 1524 3. Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES)
 1525 MUSS nach erfolgreicher Prüfung aus (2) die Antragsberechtigten zur
 1526 Zertifikatsantragstellung für zugelassene Produkte autorisieren und ihnen
 1527 geeignete Authentifizierungsmittel vertraulich zustellen, mit deren Hilfe sie sich an
 1528 der Schnittstelle I_Cert_Provisioning authentifizieren können.
- 1529 4. Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES)
 1530 MUSS über einen vertraulichkeitsgeschützten Kanal der bereitgestellten
 1531 Schnittstelle den Antragsteller sicher authentifizieren und den Request des
 1532 Zertifikatsantragstellers entgegennehmen.
- 1533 5. Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES)
 1534 MUSS im Rahmen der Prüfung des Zertifikatsantrags die eindeutige Identität und
 1535 die Berechtigung des Antragsberechtigten anhand der gematik-
 1536 Berechtigungsinformationen zum Erhalt des verlangten Zertifikatstyps sowie die
 1537 Korrektheit und Vollständigkeit des eingereichten Zertifikats-Requests prüfen
- 1538 6. Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES)
 1539 MUSS nach erfolgreicher Überprüfung den Zertifikatsantrag an den
 1540 Erstellungsdienst des TSP-X.509 nonQES weiterleiten.
- 1541 7. Der Erstellungsdienst des TSP-X.509 nonQES produziert das X.509-Zertifikat und
 1542 liefert dies an den Registrierungsdienst zurück.
- 1543 8. Der Registrierungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES)
 1544 MUSS das erzeugte X.509-Zertifikat an den Antragsberechtigten ausliefern.
- 1545 [**<=**]
- 1546 In der Abbildung Abb_PKI_516 ist der Prozessablauf des Registrierungsdienstes für
 1547 Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate und dessen
 1548 Schnittstellen im Überblick dargestellt.

1549

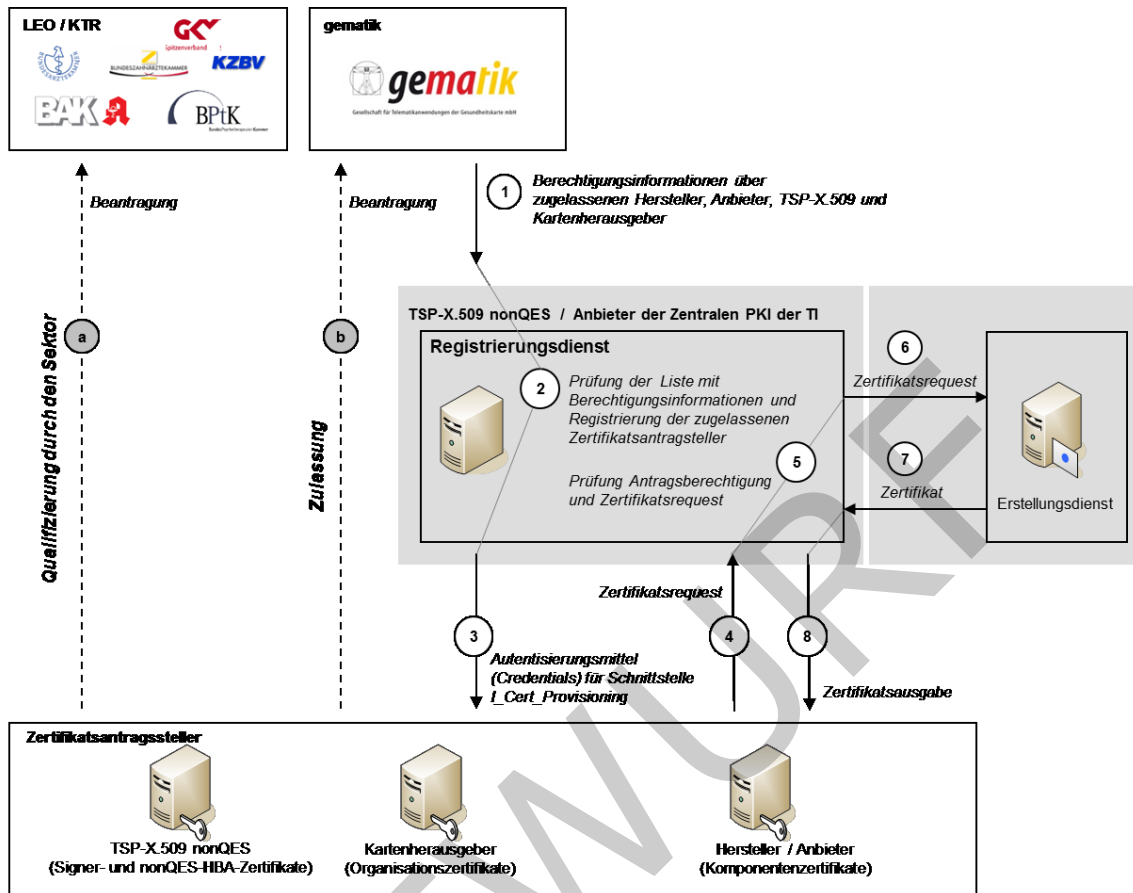


Abbildung 16: Abb_PKI_516 Prozessabläufe der zentralen PKI

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_Provisioning::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_Provisioning::provide_Certificate:SEND_REQUEST

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die logische Operation I_Cert_Provisioning::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_Provisioning::provide_Certificate:AUTHENTICATE_REQUESTOR

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

1573 Zertifikatsantragsstellung und des angeforderten Zertifikatstyps überprüft.
1574 [**<=**]

1575 **TIP1-A_4431 - Cert_Provisioning::provide_Certificate: GET_CERTIFICATE**

1576 Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die logische Operation
1577 I_Cert_Provisioning::GET_CERTIFICATE so implementieren, dass sie durch den Befehl
1578 GET-CERTIFICATE angestoßen wird und zum zuvor übermittelten Zertifikats-Request das
1579 erstellte X.509-Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikat
1580 zurück erhält.
1581 [**<=**]

1582 **6.2.1.3 Nutzung**

1583 **TIP1-A_3619 - Voraussetzungen zur Umsetzung Registrierungsdienst TSP-**
1584 **X.509 nonQES für Komponenten-, Signer, nonQES-HBA- und**
1585 **Organisationszertifikate**

1586 Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS alle Voraussetzungen
1587 schaffen, dass die durchzuführenden Schritte von der Berechtigungsprüfung bis zur
1588 Rückgabe des erzeugten X.509-Zertifikats an den Antragsteller vollautomatisiert ablaufen
1589 können.
1590 [**<=**]

1591 Die Nutzung erfolgt, wenn die Schritte (1) bis (4) aus [TIP1-A_3618] erfolgreich
1592 abgeschlossen wurden.

1593 **TIP1-A_3620 - Technische Umsetzung Registrierungsdienst TSP-X.509 nonQES**
1594 **für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikat**

1595 Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die technische Umsetzung der
1596 Schnittstelle zur Beantragung und Auslieferung der Komponenten-, Signer-, nonQES-
1597 HBA- oder Organisationszertifikate so realisieren, dass eine beidseitige Authentisierung
1598 (Zertifikatsantragsteller und TSP-X.509 nonQES) realisiert wird sowie die Daten
1599 verschlüsselt übertragen werden.
1600 [**<=**]

1601 Die Durchführung kann auf unterschiedliche Weisen realisiert werden, wie z. B.

- 1602 • Beantragung über Web-GUI mit sicherer beidseitiger Authentisierung,
- 1603 • Automatisierte Beantragung über SOAP nach sicherer beidseitiger
- 1604 Authentisierung

1605 **TIP1-A_5097 - Zertifikatsbeantragung über SOAP-Schnittstelle**

1606 Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS für die Beantragung und
1607 Ausgabe von Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate eine
1608 SOAP-Schnittstelle zur Verfügung stellen.
1609 [**<=**]

1610 **TIP1-A_5098 - Zertifikatsbeantragung über Web-Portal**

1611 Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS für die Beantragung und
1612 Ausgabe von Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate ein
1613 Web-Portal zur Verfügung stellen.
1614 [**<=**]

1615 **TIP1-A_3621 - Zertifikatsmanagementprotokolle des Registrierungsdienstes für**
1616 **Komponenten-, Signer, nonQES-HBA- und Organisationszertifikate**

1617 Der Anbieter der zentralen PKI (TSP-X.509 nonQES) für die Ausstellung von
1618 Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikate MUSS mindestens
1619 das Zertifikatsmanagementprotokoll CMP [RFC4210] unterstützen.
1620 [**<=**]

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-Komponenten-, 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-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 von dem zugehörigen Registrierungsdienst des TSP-X.509 nonQES entgegengenommen oder bereits entgegengenommene verarbeitet 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.

[<=]

1668 **Tabelle 7: Tab_PKI_512 Bereitstellungszeitpunkte der Zertifikatsstatusinformation durch**
 1669 **den Erstellungsdiens**

Zertifikatstyp	Bereitstellungszeitpunkt der Zertifikatsstatusinformation
C.NK.VPN	unmittelbar nach Erstellung
C.SAK.AUT	unmittelbar nach Erstellung
C.AK.AUT	unmittelbar nach Erstellung
C.SMKT.AUT	Nie (Veröffentlichung nicht erforderlich)
C.FD.TLS-C	unmittelbar nach Erstellung
C.FD.TLS-S	unmittelbar nach Erstellung
C.FD.SIG	unmittelbar nach Erstellung
C.FD.AUT	unmittelbar nach Erstellung
C.FD.ENC	unmittelbar nach Erstellung
C.CM.TLS-CS	unmittelbar nach Erstellung
C.SGD-HSM.AUT	Nie (Veröffentlichung nicht erforderlich)
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

*) geplant

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

6.2.2.2 Umsetzung

TIP1-A_3629 - Umsetzung Erstellungsdiens für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikaten

Der Erstellungsdiens 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 Zertifikatsstatusinformation des erstellten Zertifikates bereitstellen.

[<=]

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

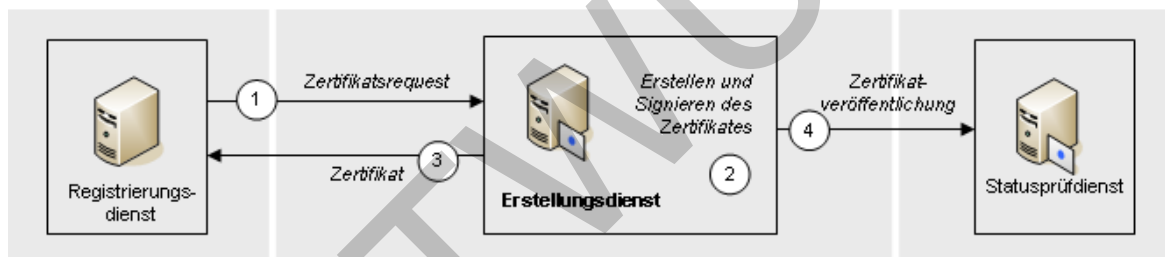


Abbildung 17: Abb_PKI_517 Prozessablauf Erstellungsdienst des Anbieters der zentralen PKI (TSP-X.509 nonQES) für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate

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 Berufs-attributes in einem geregelten Verfahren gemäß Ausgabepolicy
C.HCI.AUT C.HCI.ENC C.HCI.OSIG	Zertifikatsnehmende med. Institution, Gesellschafterorganisations- oder Kostenträgergeschäftsstelle	zu jeder Zeit ohne Angabe von Gründen
	Herausgebende Organisation (LEO bei SMC-B für medizinische Institutionen, Vertretende Gesellschafterorganisation bei SMC-B für Gesellschafterorganisationen, Vertretende Kostenträger-Organisation für SMC-B für Kostenträger)	festgestellter Wegfall der Voraussetzungen für den Betrieb einer SMC-B gemäß deren Ausgabepolicy
C.CH.AUT C.CH.ENC C.CH.AUTN C.CH.ENCV C.CH.AUT_ALT	Kostenträger	zu jeder Zeit ohne Angabe von Gründen

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

1726 **Tabelle 9: Tab_PKI_515 Berechtigte Sperrantragsteller für QES-Zertifikat für**
 1727 **Leistungserbringer**

Zertifikatstyp	Berechtigte Sperrantragsteller	zulässiger Sperrgrund
C.HP.QES	Leistungserbringer selbst	zu jeder Zeit ohne Angabe von Gründen
	Berufsattributvergebene LEO	bei Entzug oder Wegfall des Berufsattributes in einem geregelten Verfahren gemäß Ausgabepolicy
	Alle gemäß [eIDAS] berechtigten Sperrantragsteller	Sperrgrund gemäß [eIDAS]

1728 Gemäß Tab_PKI_516 gelten folgenden Berechtigungen für die Sperrantragstellung von
 1729 Komponenten- und Signerzertifikaten sowie die jeweils zulässigen Sperrgründe:
 1730

1731 **Tabelle 10: Tab_PKI_516 Berechtigte Sperrantragsteller für Komponenten- und**
 1732 **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.FD.SIG C.FD.AUT C.FD.ENC C.CM.TLS-CS C.SGD-HSM.AUT	Zertifikatsnehmender Hersteller und Anbieter,	zu jeder Zeit ohne Angabe von Gründen
C.ZD.TLS-C *) C.ZD.TLS-S C.VPNK.VPN C.VPNK.VPN-SIS	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

1733 *) *geplant*

1734 Bei der organisatorischen Schnittstelle P_Cert_Revocation zur Sperrung von X.509-
1735 Zertifikaten wird zwischen

- 1736 • nonQES-X.509-Zertifikate und
 - 1737 • QES-X.509-Zertifikate
- 1738 unterschieden.

1739 6.3.1 Schnittstelle P_Cert_Revocation

1740 6.3.1.1 Schnittstellendefinition

1741 6.3.1.1.1 Prozess zur Sperrung nonQES-Personen- und Organisationszertifikate

1742 **TIP1-A_3631 - Prüfung der Berechtigung des Antragstellers für nonQES-** 1743 **Personen- und Organisationszertifikate**

1744 Der TSP-X.509 nonQES MUSS Sperranträge für Personen- und Organisationszertifikate
1745 des Antragsberechtigten entgegennehmen und prüfen, ob der Sperrantragsteller für
1746 Personen- und Organisationszertifikate gemäß Tab_PKI_514 sperrberechtigt ist
1747 [\leq]

1748 Für die Identifizierung und Autorisierung eines Sperrantragstellers gelten die
1749 Anforderungen gemäß [gemRL_TSL_SP_CP#4.2.3]

1750 **TIP1-A_3632 - Angaben des Sperrantrags für nonQES-Personen- und** 1751 **Organisationszertifikate**

1752 Der TSP-X.509 nonQES MUSS die Angaben des Sperrantrags prüfen, ob diese dem
1753 Anspruch auf zweifelsfreie Identifizierung des Sperrberechtigten für Personen- und
1754 Organisationszertifikate entsprechen.
1755 [\leq]

1756 **TIP1-A_3633 - Identifizierung des zu sperrenden nonQES-Personen- und** 1757 **Organisationszertifikates**

1758 Der TSP-X.509 nonQES MUSS nach erfolgreicher Identifizierung und Authentisierung des
1759 Sperrantragstellers das zu sperrende Personen- und Organisationszertifikat eindeutig
1760 identifizieren.
1761 [\leq]

1762 **TIP1-A_3634 - Eingangsdaten zur Identifizierung des nonQES-Personen- und** 1763 **Organisationszertifikates**

1764 Der TSP-X.509 nonQES SOLL zur Identifizierung des zu sperrenden Personen- und
1765 Organisationszertifikates mindestens die Eingangsdaten gemäß Tabelle Tab_PKI_517
1766 abfragen.
1767 [\leq]

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 PrüfregeIn für die berechnigte 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 PrüfregeIn für die berechnigte 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 von Zertifikaten der eGK und der alternativen Versichertenidentitäten 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 Zertifikatsstatus 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

1806 Sperrung zurückgeben.
1807 [\leq]

1808 6.3.1.1.2 Prozess zur Sperrung QES-Zertifikate

1809 **TIP1-A_3641 - Sperrdienst gemäß den Vorgaben von eIDAS**

1810 Ein TSP-X.509 QES MUSS den Sperrdienst für QES-Zertifikate betreiben und Sperrungen
1811 gemäß den Vorgaben aus [eIDAS] durchführen.
1812 [\leq]

1813 **TIP1-A_4243 - Prüfung der Berechtigung des Antragstellers für QES-Zertifikate**

1814 Der TSP-X.509 QES MUSS Sperrantrag für QES-Zertifikate des Antragsberechtigten
1815 entgegennehmen und prüfen, ob der Sperrantragsteller gemäß Tab_PKI_515
1816 sperrberechtigt ist.
1817 [\leq]

1818 **6.3.1.2 Umsetzung**

1819 **TIP1-A_3642 - Umsetzung der Schnittstelle des Sperrdienstes für Personen-**
1820 **und Organisationszertifikate**

1821 TSP X.509 QES und TSP-X.509 nonQES MÜSSEN zur Umsetzung der Schnittstelle bzw.
1822 zur Durchführung des Sperrdienstes für Personen- und Organisationszertifikate die
1823 folgenden Schritte durchführen:

- 1824 1. TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN eine Schnittstelle bereitstellen
1825 über die ein Sperrberechtigter einen Sperrantrag für Personen- und
1826 Organisationszertifikate stellen kann.
- 1827 2. TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN den Sperrantragsteller von
1828 Personen- und Organisationszertifikate eindeutig identifizieren.
- 1829 3. TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN nach positiver Prüfung des
1830 Sperrantrags und eindeutiger Identifizierung des zu sperrenden Personen- und
1831 Organisationszertifikates dieses auf Grund der übermittelten Angaben sperren und
1832 die aktuellen Statusinformationen der Personen- und Organisationszertifikate dem
1833 OCSP-Responder in der TI und im Internet unmittelbar bereitstellen.
- 1834 4. TSP-X.509 QES und TSP-X.509 nonQES MÜSSEN dem Sperrantragsteller von
1835 Personen- und Organisationszertifikaten eine Rückinformation zur erfolgreichen
1836 Sperrung mitteilen.

1837 [\leq]

1838 In der Abbildung Abb_PKI_518 sind der Prozessablauf des Sperrdienstes und dessen
1839 Schnittstellen im Überblick dargestellt.

1840

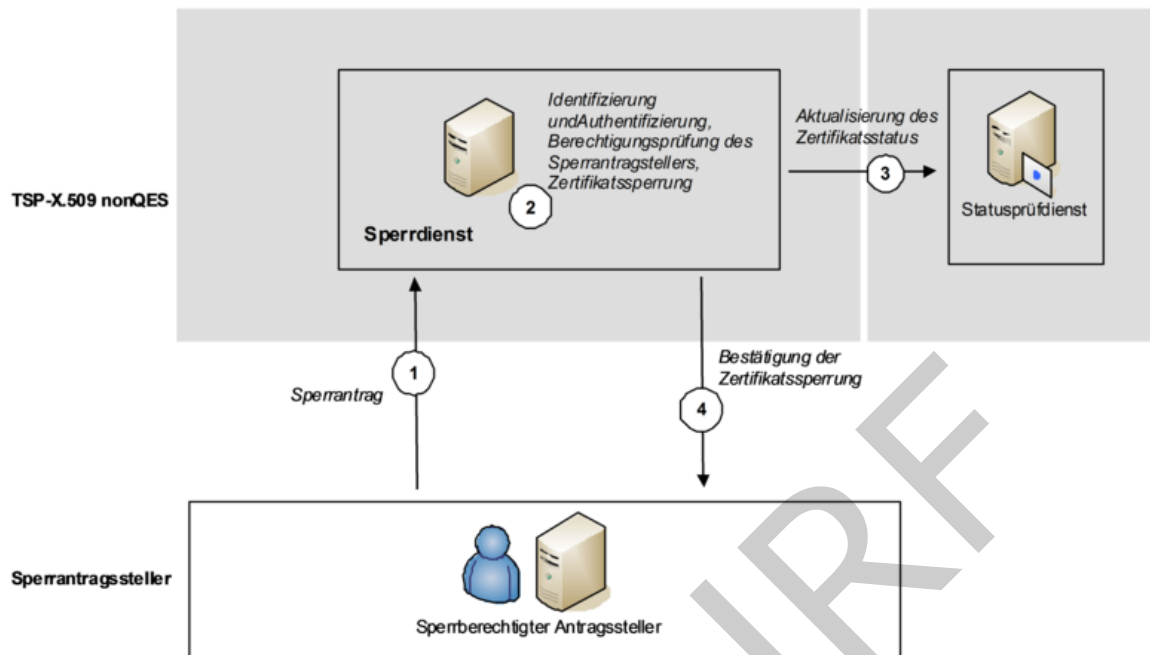


Abbildung 18: Abb_PKI_518 Prozessablauf Sperrdienst Personen- und Organisationszertifikate

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

1904 Zur Sperrung von nonQES-HBA- und Organisationszertifikaten gelten die Eingangsdaten
1905 aus Tab_PKI_517.

1906 **TIP1-A_3652 - Regelungen zum Sperrprozess**

1907 Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS die genauen Regelungen für
1908 den Sperrprozess für Komponenten, Signer-, nonQES-HBA- oder Organisationszertifikate
1909 sowie Prüfregele für die berechnigte Sperrantragsstellung in seiner Certificate Policy und
1910 in seinem Certification Practice Statement definieren.

1911 [\leq]

1912 **TIP1-A_3653 - Keine Bearbeitung von Sperranträgen bei nicht berechtigter** 1913 **Beantragung**

1914 Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS sicherstellen, dass keine
1915 Sperranträge bearbeitet werden, die von einem nicht registrierten oder nicht
1916 zugelassenen Hersteller und Anbieter, TSP-X.509 nonQES oder Kartenherausgeber zu
1917 einem nicht zugelassenen Produkt gestellt wurden.

1918 [\leq]

1919 **TIP1-A_3646 - Automatisierte Anlieferung und Bearbeitung von Sperranträgen** 1920 **für Komponenten- und Signerzertifikate**

1921 Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS eine vollständig
1922 automatisierte Anlieferung und Bearbeitung der Sperranträge von Komponenten, Signer-,
1923 nonQES-HBA- oder Organisationszertifikate ermöglichen.

1924 [\leq]

1925 **TIP1-A_4244 - Unmittelbare Ausführung der Sperrung für Komponenten,** 1926 **Signer-, nonQES-HBA- oder Organisationszertifikate**

1927 Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS nach eindeutiger
1928 Identifizierung des berechtigten Sperrantragstellers und des Komponenten-, Signer-,
1929 nonQES-HBA- oder Organisationszertifikates die Sperrung ausführen.

1930 [\leq]

1931 **TIP1-A_4246 - Erzeugung einer CRL für Zertifikate von VPN-Zugangsdiensten**

1932 Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS zur Bereitstellung der
1933 Sperrinformationen für VPN-Zugangsdienstzertifikate, neben der Bereitstellung über
1934 OCSP (vgl. gemSpec_PKI#GS-A_5074), eine CRL erzeugen.

1935 [\leq]

1936 **A_14621 - Gültigkeitsdauer OCSP-Antworten VPNK-CA**

1937 Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS zur Bereitstellung der
1938 Sperrinformationen für VPN-Zugangsdienstzertifikate die Gültigkeitsdauer der über OCSP
1939 bereit gestellten OCSP-Responses auf 7 Tage festlegen (Differenz aus thisUpdate und
1940 nextUpdate in den OCSP-Responses). [\leq]

A_14622 - Caching OCSP-Antworten VPNK-CA

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) KANN zur Bereitstellung der Sperrinformationen für VPN-Zugangsdienstzertifikate die Antworten für alle von der VPNK-CA bestätigten (ausgegebenen) Zertifikate vorproduzieren (alle vier Stunden bzw. auch direkt nach Sperrung) und auf Anfrage nur die vorproduzierten OCSP-Antworten liefern (Caching).

[<=]

Hinweis: Die Anzahl der durch eine VPNK-CA bestätigten Zertifikate ist im Vergleich zur restlichen Komponenten-PKI sehr niedrig. Auch ist die Gültigkeitsdauer einer OCSP-Response für ausgegebene Zertifikate einer VPNK-CA relativ lang (vgl. A_14621).

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 berechtigten 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

- 1989 Zertifikatsstatusinformation an den OCSP-Responder in der TI und im Internet
1990 übermitteln.
- 1991 5. Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS dem Sperrantragsteller
1992 in geeigneter Art eine Rückinformation zur erfolgreichen Sperrung des
1993 Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikates mitteilen.
- 1994
1995 [\leq]

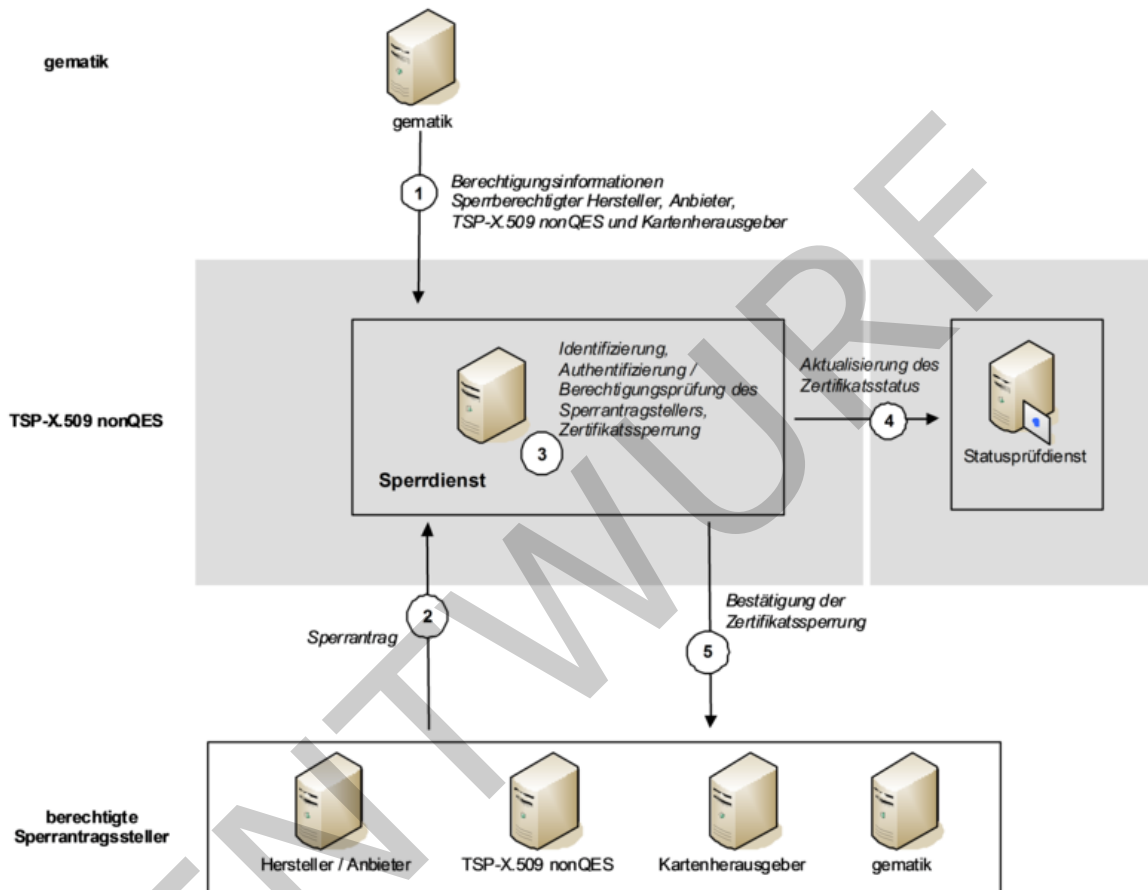


Abbildung 19: Abb_PKI_519 Prozessablauf Sperrdienst des TSP-X.509 nonQES

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
[\leq]

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.
[\leq]

**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 implementieren, dass sie durch den SEND_REVOCATE_DATA-Befehl angestoßen wird und den Zertifikatsantragsteller 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 die X.509-Sub-CA-Zertifikate 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 berechnigte Zertifikatsantragstellung von X.509-Sub-CA-Zertifikaten:

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

Zertifikatstyp	Berechnigte Zertifikatsantragsteller	Berechnigungsprüfende 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 berechnigte Sperrantragstellung von X.509-Sub-CA-Zertifikaten:

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

Zertifikatstyp	Berechnigte 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 berechnigte 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 berechnigt sind, b) wie die Registrierung zur eindeutigen Identifikation und Authentisierung der berechnigten Zertifikatsantragsteller durchzuführen ist und c) die vollständige Beschreibung der Regularien, wie die Zertifizierung von Sub-CA-Schlüsseln

2083 durch die gematik-Root-CA erfolgt.
2084 [=]

2085 Gemäß [gemRL_TSL_SP_CP#GS-A_4188] sind die konkreten Prüfregele für die
2086 Berechtigung zur Antragsstellung vom gematik-Root-CA in seinem CP (bzw. CPS) zu
2087 definieren.

2088 **TIP1-A_4250 - Betriebskonzept gematik-Root-CA**

2089 Der Anbieter der gematik-Root-CA MUSS ein Betriebskonzept auf Basis des
2090 Sicherheitskonzeptes erstellen, welches mindestens a) Root-Schlüsselerzeugung, b)
2091 Root-Zertifizierungszeremonie (self-signed) und c) die Ausstellungs- und Sperrprozesse
2092 der Sub-CA-Zertifikate beinhaltet.
2093 [=]

2094 **TIP1-A_4434 - Verfahren zur Zeitsynchronisierung gematik-Root-CA**

2095 Der Anbieter der gematik-Root-CA MUSS ein Verfahren zur Zeitsynchronisierung
2096 einsetzen, das eine maximale Abweichung von einer Sekunde gegenüber der gesetzlichen
2097 Zeit der PTB gewährleistet.
2098 [=]

2099 **TIP1-A_4251 - Auditierverfahren gematik-Root-CA**

2100 Der Anbieter der gematik-Root-CA MUSS die Sicherheit des Betriebes und der Root-
2101 Schlüsselerzeugung in einem Auditierverfahren durch die gematik nachweisen.
2102 [=]

2103 Das Audit der gematik-Root-CA kann auch durch einen von der gematik beauftragten
2104 Auditor erfolgen.

2105 **TIP1-A_3656 - abgestimmtes Antrags- und Sperrverfahren**

2106 Der Anbieter der gematik-Root-CA MUSS das Antrags- und Sperrverfahren mit der
2107 gematik abstimmen und bereitstellen.
2108 [=]

2109 **TIP1-A_3657 - Gesicherte Zertifikatserstellung der X.509-Sub-CA-Zertifikate**

2110 Der Anbieter der gematik-Root-CA MUSS sicherstellen, dass X.509-Sub-CA-Zertifikate
2111 nur generiert werden, wenn a) die Identifizierung und Authentifizierung des
2112 Zertifikatsantragstellers bzw. legitimierte Kontaktperson sowie b) der Zertifikatsantrag
2113 vollständig war und erfolgreich geprüft werden konnte, c) die gematik die Berechtigung
2114 der Antragsstellung bestätigt, d) alle für die Erstellung des beauftragten X.509-Zertifikats
2115 obligatorischen Antragsdaten übermittelt werden.
2116 [=]

2117 **TIP1-A_3658 - Antragsdaten X.509-Sub-CA-Zertifikat**

2118 Der Anbieter der gematik-Root-CA MUSS sicherstellen, dass mindestens die in
2119 Tab_PKI_521 enthaltenen Angaben bei dem Zertifikatsantrag vorliegen.
2120 [=]

2121

2122 **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

2123

2124 **TIP1-A_4015 - Maximale Gültigkeitsdauer des TSL-Signer-CA-Zertifikats**

2125 Die gematik Root-CA SOLL die Gültigkeitsdauer des TSL-Signer-CA-Zertifikats auf 8 Jahre ansetzen.

2126 [\leq]

2128 Bei der PKI für X.509-Sub-CA-Zertifikate wird zwischen einer gematik Produktiv-Root-CA und einer gematik Test-Root-CA unterschieden.

2130 Der Betreiber der gematik-Root-CA stellt sowohl eine produktive gematik-Root-CA als auch eine gematik Test-Root-CA zur Verfügung.

2132 **TIP1-A_3662 - Registrierung einer Test-TSP-X.509-CA**

2133 Der Anbieter der gematik-Root-CA MUSS ein mit der gematik abgestimmtes Antragsverfahren für Test-TSP-X.509-CA-Zertifikate abstimmen und bereitstellen.

2135 [\leq]

2136 Für die Registrierung einer Test-TSP-X.509-CA ist ein verkürztes Verfahren vorgesehen.

2137 **TIP1-A_3663 - Dokumentation von Sperrungen**

2138 Der Anbieter gematik-Root-CA MUSS sicherstellen, dass alle eingereichten Sperranträge von TSP-X.509 nonQES-CA-Zertifikate dokumentiert werden.

2140 [\leq]

2141 **TIP1-A_3664 - Sperrinformationen**

2142 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

2145 [\leq]

2146 Eingereichte Sperrungen werden gemäß den definierten Incidents behandelt:

- 2147 • sicherheitskritischer Incident gemäß [gemKPT_PKI_TIP#TIP1-A_2062]
- 2148 • nicht-sicherheitskritischer Incident gemäß [gemKPT_PKI_TIP#TIP1-A_2065].

2149 **6.4.1.2 Umsetzung**

2150 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

2199 **TIP1-A_5168 - Bereitstellung gematik Root-CA- und Sub-Ca-Zertifikate und**
2200 **Fingerprints im Internet**
2201 Der Anbieter der gematik Root-CA MUSS die erstellten X.509-gematik-Root-CA- und Sub-
2202 CA-Zertifikate sowie die zugehörigen Zertifikatsfingerprints im Internet publizieren.
2203 [\leq]

2204 **6.5 Statusprüfdienst**

2205 Die Schnittstelle des OCSP-Responder I_OCSP_Status_Information ist in
2206 [gemSpec_PKI#9] vollständig beschrieben.
2207 Die Algorithmen und Parameter für die Erstellung der Signaturen über die Antworten des
2208 OCSP werden in [gemSpec_Krypt] festgelegt.
2209

ENTWURF

2210

7 Anhang A – Verzeichnisse

2211 7.1 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
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
SM	Security Module
SMC-B	Sicherheitsmodul vom Typ B <Organisation>
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
VDA	Vertrauensdiensteanbieter
VPN	Virtual Private Network

7.2 Glossar

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

7.3 Abbildungsverzeichnis

Abbildung 1: Abb_PKI_502 Nachbarsysteme der gematik-Root-CA	14
Abbildung 2: Abb_PKI_503 Nachbarsysteme TSP-X.509-QES und TSP-X.509-nonQES...	15
Abbildung 3: Abb_PKI_504 Schnittstellen TSP-X.509-QES und TSP-X.509-nonQES.....	17
Abbildung 4: Abb_PKI_504 Schnittstellen Registrierungs- und Erstellungsdienst TSP-X.509-QES und TSP-X.509-nonQES	18
Abbildung 5: Abb_PKI_506 Organisatorische Anordnung der Schnittstelle Registrierungs- und Erstellungsdienst TSP-X.509-QES und TSP-X.509-nonQES	19
Abbildung 6: Abb_PKI_507 Schnittstellen Sperrdienst des TSP-X.509	20
Abbildung 7: Abb_PKI_508 Organisatorische Anordnung Sperrdienst	20
Abbildung 8: Abb_PKI_510 Schnittstellen Erstellung und Sperrung der gematik-Root-CA	21
Abbildung 9: Abb_PKI_509 Schnittstellen OCSP-Responder TSP-X.509-QES und TSP-X.509-nonQES	21
Abbildung 10: Abb_PKI_511 Zuständigkeiten der Rollen bei Zertifikatsantragstellung der Personen- und Organisationszertifikate.....	31

2231	Abbildung 11: Abb_PKI_512 Prozessablauf Registrierungsdienst nonQES-Personen- und	
2232	Organisationszertifikate.....	35
2233	Abbildung 12: Abb_PKI_513 Prozessablauf Registrierungsdienst QES-Zertifikate	38
2234	Abbildung 13: Abb_PKI_514 Prozessablauf Erstellungsdienstes des TSP-X.509-CA.....	41
2235	Abbildung 14: Abb_PKI_515 Zuständigkeiten der Rollen bei der Beantragung von	
2236	Komponenten- und Signerzertifikaten	45
2237	Abbildung 15: Abb_PKI_520 Zuständigkeiten der Rollen bei nonQES-HBA- und	
2238	Organisationszertifikatsantragstellung	46
2239	Abbildung 16: Abb_PKI_516 Prozessabläufe der zentralen PKI.....	52
2240	Abbildung 17: Abb_PKI_517 Prozessablauf Erstellungsdienst des Anbieters der zentralen	
2241	PKI (TSP-X.509 nonQES) für Komponenten-, Signer-, nonQES-HBA- und	
2242	Organisationszertifikate.....	56
2243	Abbildung 18: Abb_PKI_518 Prozessablauf Sperrdienst Personen- und	
2244	Organisationszertifikate.....	62
2245	Abbildung 19: Abb_PKI_519 Prozessablauf Sperrdienst des TSP-X.509 nonQES.....	66
2246	Abbildung 1: Abb_PKI_502 Nachbarsysteme der gematik-Root-CA	14
2247	Abbildung 2: Abb_PKI_503 Nachbarsysteme TSP-X.509 QES und TSP-X.509 nonQES...	15
2248	Abbildung 3: Abb_PKI_504 Schnittstellen TSP-X.509 QES und TSP-X.509 nonQES.....	17
2249	Abbildung 4: Abb_PKI_504 Schnittstellen Registrierungs- und Erstellungsdienst TSP-	
2250	X.509 QES und TSP-X.509 nonQES	18
2251	Abbildung 5: Abb_PKI_506 Organisatorische Anordnung der Schnittstelle Registrierungs-	
2252	und Erstellungsdienst TSP-X.509 QES und TSP-X.509 nonQES	19
2253	Abbildung 6: Abb_PKI_507 Schnittstellen Sperrdienst des TSP-X.509	20
2254	Abbildung 7: Abb_PKI_508 Organisatorische Anordnung Sperrdienst	20
2255	Abbildung 8: Abb_PKI_510 Schnittstellen Erstellung und Sperrung der gematik-Root-CA	
2256	21
2257	Abbildung 9: Abb_PKI_509 Schnittstellen OCSP-Responder TSP-X.509 QES und TSP-	
2258	X.509 nonQES	21
2259	Abbildung 10: Abb_PKI_511 Zuständigkeiten der Rollen bei Zertifikatsantragstellung der	
2260	Personen- und Organisationszertifikate.....	31
2261	Abbildung 11: Abb_PKI_512 Prozessablauf Registrierungsdienst nonQES-Personen- und	
2262	Organisationszertifikate.....	35
2263	Abbildung 12: Abb_PKI_513 Prozessablauf Registrierungsdienst QES-Zertifikate	38
2264	Abbildung 13: Abb_PKI_514 Prozessablauf Erstellungsdienstes des TSP-X.509-CA.....	41
2265	Abbildung 14: Abb_PKI_515 Zuständigkeiten der Rollen bei der Beantragung von	
2266	Komponenten- und Signerzertifikaten	45
2267	Abbildung 15: Abb_PKI_520 Zuständigkeiten der Rollen bei nonQES-HBA- und	
2268	Organisationszertifikatsantragstellung	46
2269	Abbildung 16: Abb_PKI_516 Prozessabläufe der zentralen PKI.....	52
2270	Abbildung 17: Abb_PKI_517 Prozessablauf Erstellungsdienst des Anbieters der zentralen	
2271	PKI (TSP-X.509 nonQES) für Komponenten-, Signer-, nonQES-HBA- und	
2272	Organisationszertifikate.....	56

2273	Abbildung 18: Abb_PKI_518 Prozessablauf Sperrdienst Personen- und	
2274	Organisationszertifikate.....	62
2275	Abbildung 19: Abb_PKI_519 Prozessablauf Sperrdienst des TSP-X.509 nonQES.....	66
2276		

2277 7.4 Tabellenverzeichnis

2278	Tabelle 1: Tab_PKI_501 Allgemeine Übersicht der Rollen und deren Aufgaben beim	
2279	Registrierungsdienst	29
2280	Tabelle 2: Tab_PKI_502 Berechtigte Zertifikatsantragsteller für non-QES	
2281	Leistungserbringer-, LEO bzw. KTR-Organisation und Versichertenzertifikate sowie	
2282	Prüfkartenzertifikate	29
2283	Tabelle 3: Tab_PKI_503 Berechtigte Zertifikatsantragsteller für QES	
2284	Leistungserbringerzertifikate	30
2285	Tabelle 4: Tab_PKI_509 Bereitstellungszeitpunkt der Zertifikatsstatusinformation durch	
2286	den Erstellungsdienst	40
2287	Tabelle 5: Tab_PKI_510 Zuständigkeiten Rollen beim Registrierungsdienst der zentralen	
2288	PKI für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate.....	42
2289	Tabelle 6: Tab_PKI_511 Berechtigte Zertifikatsantragsteller für Komponenten-, Signer-,	
2290	nonQES-HBA- und Organisationszertifikate	43
2291	Tabelle 7: Tab_PKI_512 Bereitstellungszeitpunkte der Zertifikatsstatusinformation durch	
2292	den Erstellungsdienst	55
2293	Tabelle 8: Tab_PKI_514 Berechtigte Sperrantragsteller für nonQES-Personen- und	
2294	Organisationszertifikate.....	57
2295	Tabelle 9: Tab_PKI_515 Berechtigte Sperrantragsteller für QES-Zertifikat für	
2296	Leistungserbringer.....	58
2297	Tabelle 10: Tab_PKI_516 Berechtigte Sperrantragsteller für Komponenten- und	
2298	Signerzertifikate.....	58
2299	Tabelle 11: Tab_PKI_517 Eingangsdaten zur Sperrung von nonQES-Personen- und	
2300	Organisationszertifikaten	60
2301	Tabelle 12: Tab_PKI_518 Eingangsdaten zur Sperrung von Komponenten- und	
2302	Signerzertifikaten	63
2303	Tabelle 13: Tab_PKI_519 Berechtigte Zertifikatsantragsteller für X.509-Sub-CA-	
2304	Zertifikate	68
2305	Tabelle 14: Tab_PKI_520 Berechtigte Sperrantragsteller für X.509-Sub-CA-Zertifikate ..	68
2306	Tabelle 15: Tab_PKI_521 Antragsdaten X.509-Sub-CA-Zertifikat.....	69
2307	Tabelle 1: Tab_PKI_501 Allgemeine Übersicht der Rollen und deren Aufgaben beim	
2308	Registrierungsdienst	29
2309	Tabelle 2: Tab_PKI_502 Berechtigte Zertifikatsantragsteller für non-QES	
2310	Leistungserbringer-, LEO bzw. KTR-Organisation und Versichertenzertifikate sowie	
2311	Prüfkartenzertifikate	29
2312	Tabelle 3: Tab_PKI_503 Berechtigte Zertifikatsantragsteller für QES	
2313	Leistungserbringerzertifikate	30

2314	Tabelle 4: Tab_PKI_509 Bereitstellungszeitpunkt der Zertifikatsstatusinformation durch	
2315	den Erstellungsdiens.....	40
2316	Tabelle 5: Tab_PKI_510 Zuständigkeiten Rollen beim Registrierungsdiens der zentralen	
2317	PKI für Komponenten-, Signer-, nonQES-HBA- und Organisationszertifikate.....	42
2318	Tabelle 6: Tab_PKI_511 Berechtigte Zertifikatsantragsteller für Komponenten-, Signer-,	
2319	nonQES-HBA- und Organisationszertifikate	43
2320	Tabelle 7: Tab_PKI_512 Bereitstellungszeitpunkte der Zertifikatsstatusinformation durch	
2321	den Erstellungsdiens.....	55
2322	Tabelle 8: Tab_PKI_514 Berechtigte Sperrantragsteller für nonQES-Personen- und	
2323	Organisationszertifikate.....	57
2324	Tabelle 9: Tab_PKI_515 Berechtigte Sperrantragsteller für QES-Zertifikat für	
2325	Leistungserbringer.....	58
2326	Tabelle 10: Tab_PKI_516 Berechtigte Sperrantragsteller für Komponenten- und	
2327	Signerzertifikate.....	58
2328	Tabelle 11: Tab_PKI_517 Eingangsdaten zur Sperrung von nonQES-Personen- und	
2329	Organisationszertifikaten	60
2330	Tabelle 12: Tab_PKI_518 Eingangsdaten zur Sperrung von Komponenten- und	
2331	Signerzertifikaten	63
2332	Tabelle 13: Tab_PKI_519 Berechtigte Zertifikatsantragsteller für X.509-Sub-CA-	
2333	Zertifikate	68
2334	Tabelle 14: Tab_PKI_520 Berechtigte Sperrantragsteller für X.509-Sub-CA-Zertifikate .	68
2335	Tabelle 15: Tab_PKI_521 Antragsdaten X.509-Sub-CA-Zertifikat.....	69
2336		

2337 7.5 Referenzierte Dokumente

2338 7.5.1 Dokumente der gematik

2339 Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument
 2340 referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der
 2341 vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und
 2342 Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert. Version und
 2343 Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht
 2344 aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummer ist in der
 2345 aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die
 2346 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_PruefSichEig]	gematik: Richtlinie zur Prüfung der Sicherheitseignung
[gemRL_TSL_SP_CP]	gematik: Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL
[gemSpec_Krypt]	gematik: Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur
[gemSpec_OID]	gematik: Spezifikation OID
[gemSpec_PKI]	gematik: Spezifikation PKI
[GVO_IOPVZ]	gematik: Geschäfts- und Verfahrensordnung für das Interoperabilitätsverzeichnis vesta: (Verzeichnis elektronischer Standards und Anwendungen im Gesundheitswesen)

2347 7.5.2 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
[eIDAS]	Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

2348