Einführung der Gesundheitskarte

Schnittstellen- und Prozessspezifikation gematik Root-CA

Version:	1.2.2
Stand:	08.06.2017
Status:	Freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[ARV_706.3_Spec_SST_gematik-Root-CA]

Dokumentinformationen

Änderungen zur Vorversion

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.0.1	29.01.2014		Initiale Erstellung	ARV
0.0.2	19.02.2014		Umstrukturierung, Überarbeitung	ARV
0.0.3	05.03.2014		QS	ARV
1.0.0	05.03.2014		Freigabe durch Release Board	ARV, gematik
1.0.1	17.03.2014		Einarbeitung Kommentare der gematik	ARV
1.1.0	17.03.2014		Freigabe Release-Mngt.	gematik
1.1.1	09.01.2015	4.5.1	Spezifizierung Sub-CA-Zertifikate	ARV
1.1.2	29.01.2015	4.4	Spezifizierung der Sperrung von Sub-Ca-Zertifikaten	ARV
1.2.0	30.01.2015		Freigabe Release-Mngt.	gematik
1.2.1	19.05.2017		Anpassungen CR093	ARV
1.2.2	08.06.2017		Begebung Mangel der gematik-Rückmeldung	ARV

Inhaltsverzeichnis

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die notwendigen Schnittstellen- und Prozesse, damit TSP-X.509 nonQES und der Anbieter des TSL-Dienstes unter Verwendung der gematik Root-CA Sub-CA-Zertifikate beantragen und sperren können.

1.2 Zielgruppe

Das Dokument richtet sich an die gematik sowie an den Hersteller und Betreiber der gematik Root-CA.

1.3 Geltungsbereich

Dieses Dokument spezifiziert die Schnittstellen und Prozesse der gematik Root-CA.

1.4 Abgrenzungen

Die Verwaltung und Übermittlung von Zulassungsinformationen der berechtigten Zertifikatsantragsteller erfolgt durch die gematik über das Zulassungsmanagement der Komponenten-PKI (siehe [ARV_706.3_Spec_SST_Komponenten-PKI]).

Die konkrete Ausgestaltung der Prozesse UC-Root-CA-002 X.509-Sub-CA-Zertifikat beantragen (wie z. B. die Zutrittskontrolle zum Rechenzentrum, Zutritt zur gematik Root-CA bzw. zu den verschiedenen Zonen, Durchführung verschiedener Aktionen im Vier-Augen-Prinzip (beispielsweise die Freischaltung des HSMs der gematik Root-CA per OCS zur Erzeugung des X.509-Sub-CA-Zertifkats) etc. sowie UC-Root-CA-003 X.509-Sub-CA-Zertifikat sperren erfolgt im Rahmen der Erstellung des Betriebskonzept der PKI-Dienste.

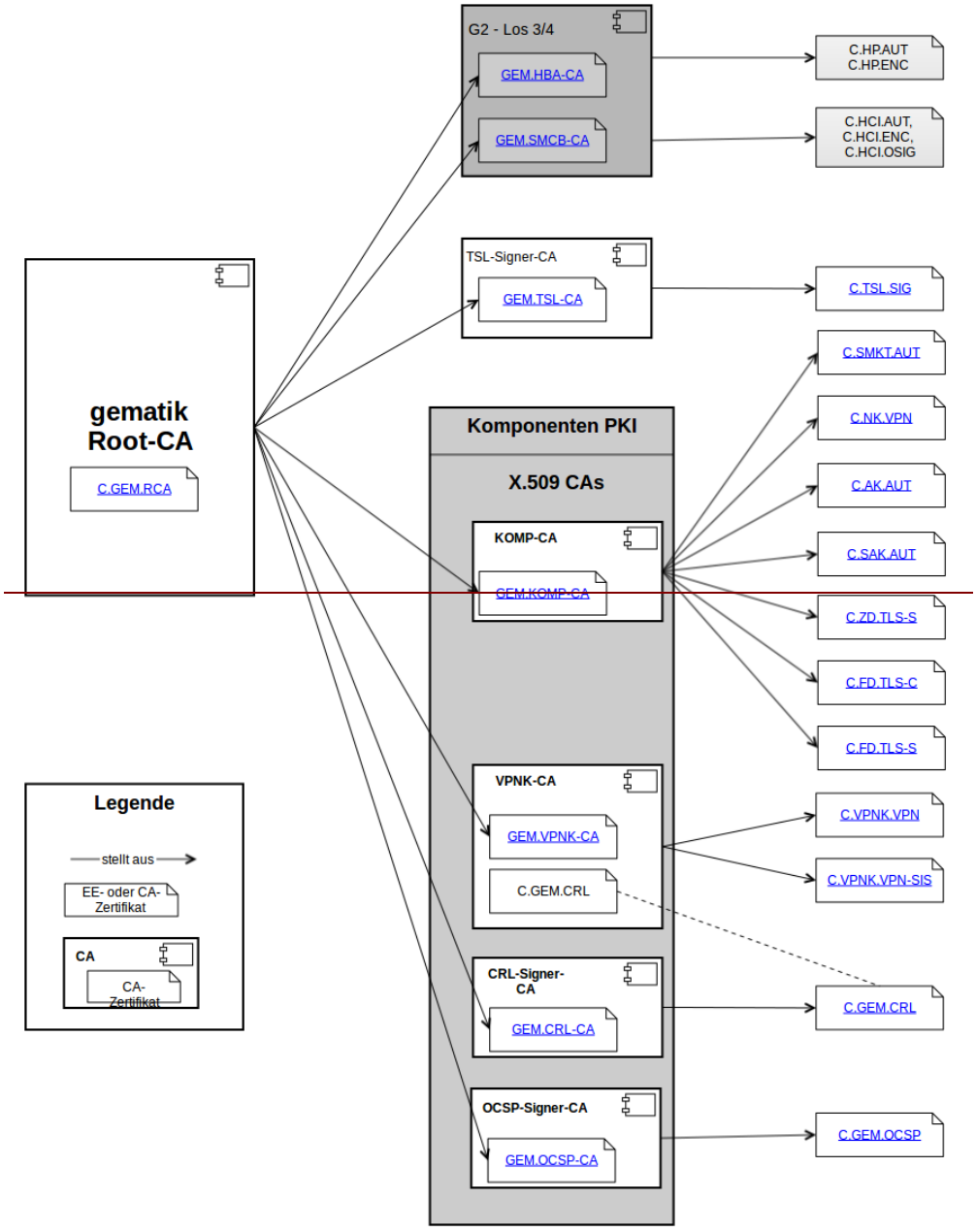
Die Sperrung von X.509-Sub-CA-Zertifikaten durch die gematik erfolgt mit Hilfe der TSL-Applikation des TSL-Dienstes (siehe [ARV_706.3_Spec_SST_TSL-Dienst]).

Die Umsetzung des mit dem BSI abgestimmten Backupverfahrens gemäß [gemLB_ORS1_Los_3#Anhang F] für die Sicherung des Schlüsselmaterials der gematik Root-CA wird in einem gesonderten Dokument beschrieben.

Die konkreten Prüfregeln für die Berechtigung zur Antragsstellung werden in der CP (bzw. CPS) der gematik Root-CA definiert.

2 Systemüberblick

Nachfolgende Abbildung stellt die PKI-Gesamtübersicht des ORS 1 Vorhabens mit Einordnung der gematik Root-CA, den aus der Root-CA abgeleiteten X.509-Sub-CA-Zertifikaten sowie die entsprechenden Endnutzerzertifikate dar.


G2 - Los 3/4
GEM.HBA-CA
GEM.SMCB-CA
C.HP.AUT
C.HP.ENC
C.HCI.AUT,
C.HCI.ENC,
C.HCI.OSIG
TSL-Signer-CA
GEM.TSL-CA
C.TSL.SIG
gematik
Root-CA
C.GEM.RCA
Komponenten PKI
X.509 CAs
KOMP-CA
GEM.KOMP-CA
C.SMKT.AUT
C.NK.VPN
C.AK.AUT
C.SAK.AUT
C.ZD.TLS-S
C.FD.TLS-C
C.FD.TLS-S
VPNK-CA
GEM.VPNK-CA
C.GEM.CRL
C.VPNK.VPN
C.VPNK.VPN-SIS
CRL-Signer-CA
GEM.CRL-CA
C.GEM.CRL
OCSP-Signer-CA
GEM.OCSP-CA
C.GEM.OCSP
Legende
stellt aus
EE- oder CA-Zertifikat
CA
CA-Zertifikat

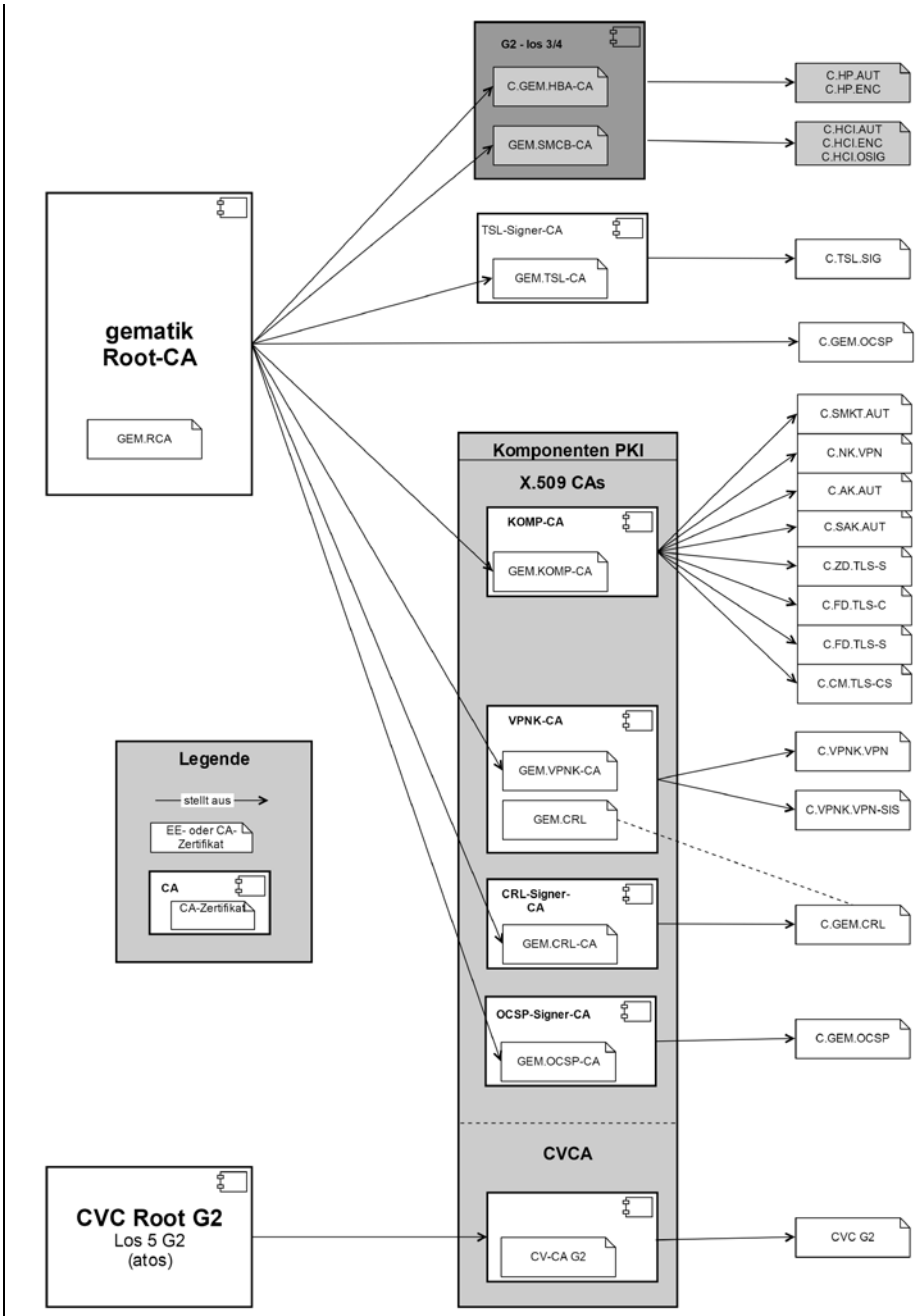


Abbildung 1: Zertifikatshierarchie der gematik Root-CA

Die gematik Root-CA wird offline und physikalisch getrennt von anderen Systemen und deren Signaturidentitäten aufgebaut und betrieben.

Die von der gematik Root-CA ausgestellten X.509-Sub-CA-Zertifikate müssen der Zertifikatsstruktur gemäß [gemSpec_PKI#Tab_PKI_212] entsprechen und die Namenskonvention der Tabelle 5 umsetzen.

Die gematik Root-CA stellt die Schnittstelle P_Sub_CA_Certification_X.509 zur Verfügung, über die zugelassene TSP-X.509 nonQES und der Anbieter des TSL-Dienstes

X.509-Sub-CA-Zertifikatsanträge und -Sperranträge stellen können. X.509-Sub-CA-Zertifikate können nur von TSP-X.509 nonQES und dem Anbieter des TSL-Dienstes beantragt werden, die aktuell bei der gematik zugelassen sind. Zugelassene TSP-X.509 nonQES und der Anbieter des TSL-Dienstes werden auch als berechtigte Zertifikatsantragsteller bezeichnet (siehe [gemSpec_TSP_X.509#Tab_PKI_519]). Berechtigte Sperrantragsteller sind die zertifikatsnehmenden TSP-X.509 nonQES und der Anbieter des TSL-Dienstes ([gemSpec_TSP_X.509#Tab_PKI_520]).

Zur Registrierung und Verwaltung Antragsberechtigter und derer berechtigter Zertifikatsantragsteller bzw. Sperrantragsteller wird der gematik die Applikation „Zulassungsmanagement“ (ZM) bereitgestellt. Das Zulassungsmanagement dient als Schnittstelle zwischen gematik und dem Betreiber der Komponenten-PKI sowie dem Betreiber der gematik Root-CA. Antragsberechtigte im Kontext der gematik Root-CA sind zugelassene TSP-X.509 nonQES und der Anbieter des TSL-Dienstes. Berechtigte Zertifikatsantragsteller sind legitimierte Personen des Antragsberechtigten, die X.509-Sub-CA-Zertifikate beantragen und sperren können. Die Antragsberechtigten und zugehörigen berechtigten Zertifikatsantragsteller werden durch die gematik im Zulassungsmanagement erfasst und an den Betreiber der gematik Root-CA übermittelt. Im Rahmen der Erfassung werden jedem Antragsberechtigten die CA-Einsatzbereiche (siehe Tabelle 5) zugewiesen, für die die berechtigten Zertifikatsantragsteller X.509-Sub-CA-Zertifikate beantragen dürfen.

Die Schnittstellen und Prozesse des Zulassungsmanagements sind im Detail in der Schnittstellen- und Prozessspezifikation der Komponenten-PKI [ARV_706.3_Spec_SST_-Komponenten-PKI] beschrieben.

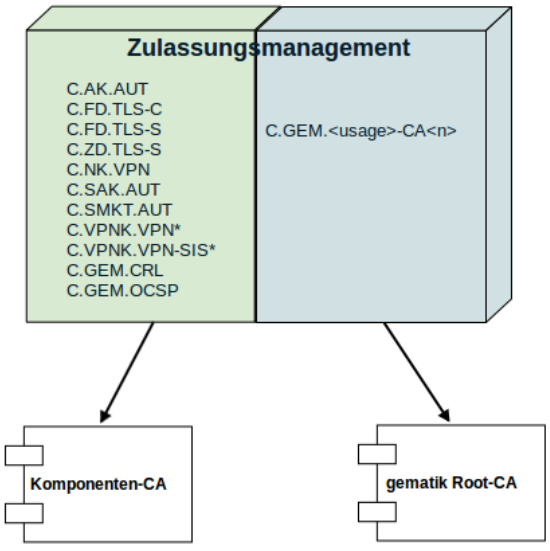


Abbildung 2: Zuständigkeiten (Zertifikatstypen bzw. CA-Einsatzbereiche) der Komponenten-PKI und gematik Root-CA

Nach Zulassung durch die gematik (und Übermittlung der erforderlichen Informationen über das Zulassungsmanagement) erfasst der berechtigte Zertifikatsantragsteller unter Verwendung der Anwendung "Sub-CA-Antragsdatenerfassung" die Zertifikatsantragsdaten und überträgt diese an den Betreiber der gematik Root-CA. Die Bereitstellung der

Anwendung erfolgt über die zentrale Komponente "Trust Management System" (TMS). Zur Authentisierung an der Anwendung kommen RSA-Token zum Einsatz, die den berechtigten Zertifikatsantragsteller im Rahmen des Zulassungsmanagements zur Verfügung gestellt werden.

Die Zertifikatausstellung des X.509-Sub-CA-Zertifikats findet anschließend Vorort beim Betreiber der gematik Root-CA statt.

Die gematik wird über die beim Betreiber von den zertifikatsnehmenden TSP-X.509 nonQES eingehenden Sperranträge für X.509-Sub-CA-Zertifikate informiert.

Die Sperrung von X.509-Sub-CA-Zertifikaten erfolgt im Rahmen des TSL-Dienstes (siehe [ARV_706.3_Spec_SST_TSL-Dienst]) über die TSL-Applikation durch die gematik.

Der Zertifikatsstatus der X.509-Sub-CA-Zertifikate für HBA und SMC-B wird im OCSP-Responder der gematik Root-CA im Internet zur Verfügung gestellt.

Nachfolgende Tabelle gibt einen Überblick über die umzusetzenden Schnittstellen der gematik Root-CA.

Tabelle 1: Überblick über die zu realisierenden Schnittstellen der gematik Root-CA

Schnittstelle	Kurzbeschreibung
P_Sub_CA_Certification_X.509 Siehe Kapitel 4	Die Schnittstelle zur Ausstellung und Sperrung von X.509-Sub-CA-Zertifikaten.
I_OCSP_Status_Information Siehe Kapitel 5	Die technische Schnittstelle zur Bereitstellung der Zertifikatsstatusinformation der gematik Root-CA Zertifikat(e) sowie für alle von Ihr abgeleiteten X.509-Sub-CA-Zertifikate, welche HBA- und SMC-B-Zertifikate ausstellen.

Der Anbieter der gematik-Root-CA stellt sowohl eine produktive Root-CA in der PU als auch eine Test-Root-CA in der RU/TU zur Verfügung.

Die Umsetzung der Schnittstellen und Prozesse zur Beantragung und Sperrung von X.509 Sub-CA-Zertifikaten ist für die Betriebsumgebungen RU/TU und PU identisch.

3 Systemkontext

3.1 Nutzer und Rollen

3.1.1 Nutzer

Nutzer der Schnittstellen und Prozesse der gematik Root-CA sind die berechtigten Zertifikatsantragsteller sowie die berechtigten Sperrantragsteller.

3.1.1.1 Berechtigte Zertifikatsantragsteller

Berechtigte Zertifikatsantragsteller für X.509-Sub-CA-Zertifikate sind zugelassene TSP-X.509 nonQES und der Anbieter des TSL-Dienstes gemäß [gemSpec_TSP_-X.509#Tab_PKI_519].

Berechtigte Zertifikatsantragsteller stellen über die Schnittstelle P_Sub_CA_Certification_X.509 Zertifikatsanträge für X.509-Sub-CA-Zertifikate.

3.1.1.2 Berechtigte Sperrantragsteller

Berechtigte Sperrantragsteller für X.509-Sub-CA-Zertifikate sind die zertifikatsnehmenden TSP-X.509 nonQES gemäß [gemSpec_TSP_X.509#Tab_PKI_520].

3.1.1.3 gematik

Die gematik lässt TSP-X.509 nonQES und den Anbieter des TSL-Dienstes zu. Sie übermittelt im Rahmen der Zulassung die Antragsberechtigten und berechtigten Zertifikatsantragsteller bzw. Sperrantragsteller mit Hilfe des Zulassungsmanagements an den Betreiber der gematik Root-CA.

Die gematik sperrt X.509-Sub-CA-Zertifikate im Rahmen des TSL-Dienstes über die TSL-Applikation.

3.1.1.4 Betreiber der gematik Root-CA

Der Betreiber der gematik Root-CA führt alle erforderlichen Tätigkeiten im Zuge der X.509-Sub-CA-Zertifikatsbeantragung und -sperrung durch.

3.1.2 Rollen

Für die Umsetzung der im Folgenden beschriebenen Use Cases (siehe Kapitel 4) der gematik Root-CA sind verschiedene Rollen erforderlich. Nachfolgende Tabelle stellt die Rollen und Berechtigungen der gematik Root-CA im Überblick dar.

Die für die Umsetzung der Use Cases "UC-Root-CA-002 X.509-Sub-CA-Zertifikat " und "UC-Root-CA-003 X.509-Sub-CA-Zertifikat sperren" erforderlichen Rollen des Betreibers der gematik Root-CA werden im Rahmen des Betriebskonzepts konkretisiert.

Tabelle 2: Rollen der gematik Root-CA

Rolle	Kürzel	Rolleninhaber	Berechtigung
Berechtigter Zertifikatsantrag-steller	BZA	Zugelassener TSP-X.509 nonQES Anbieter TSL-Dienst	Berechtigung zum Erstellen der Antragsdaten und der Beantragung von X.509-Sub-CA-Zertifikaten (für die zugelassenen CA-Einsatz-bereiche).
Berechtigter Sperrantragsteller	BSA	Zertifikatsnehm-ender TSP-X.509 nonQES Anbieter TSL-Dienst	Berechtigung zum Sperren von X.509-Sub-CA-Zertifikaten.
Sperrantragsteller gematik	SAG	gematik	Berechtigung zum Sperren von X.509 Sub-CA-Zertifikaten.
Administrator Root-CA	ARC	Betreiber gematik Root-CA	Speicherung des im TMS vorliegenden Zertifikatsantrages auf Medium und Übergabe an ORC.
Operator Root-CA	ORC	Betreiber gematik Root-CA	Erstellung des X.509-Sub-CA-Zertifikats unter Verwendung der gematik Root-CA.
Sperrantragad-ministrator Root-CA	SRC	Betreiber gematik Root-CA	Nimmt Sperranträge entgegen und leitet diese an die gematik weiter.
Anmerkung:	BZA dürfen nur für die ihnen über das Zulassungsmanagement zugewiesenen CA-Einsatzbereiche X.509 Sub-CA-Zertifikate beantragen. BSA können nur die von ihrem Antragsberechtigten (Organisation) beantragte X.509 Sub-CA-Zertifikate sperren. Die gematik kann alle erstellten X.509 Sub-CA-Zertifikate sperren.		

4 P_Sub_CA_Cert_Certification_X.509

4.1 Übersicht

Die Ausführungen in den nachfolgenden Kapiteln beschreiben die Use Cases zur Umsetzung der Schnittstelle P_Sub_CA_Cert_Certification_X.509. Die Erfassung der X.509-Sub-CA-Antragsdaten erfolgt über die Anwendung Sub-CA-Antragsdatenerfassung Tabelle 3 gibt einen Überblick über die in den nachfolgenden Kapiteln beschriebenen Use Cases.

Tabelle 3: Use Cases zur Umsetzung der Schnittstelle P_Sub_CA_Cert_Certification_X.509

Use Case	Beschreibung
UC-Root-CA-001	Antragsdaten für X.509-Sub-CA-Zertifikat erfassen
UC-Root-CA-002	X.509-Sub-CA-Zertifikat beziehen
UC-Root-CA-003	X.509-Sub-CA-Zertifikat sperren

4.2 UC-Root-CA-001 Antragsdaten für X.509-Sub-CA-Zertifikat erfassen

Use Case: Name:	UC-Root-CA-001 Antragsdaten für X.509-Sub-CA-Zertifikat erfassen
Kurzbeschreibung	Dieser Use Case beschreibt, wie berechtigte Zertifikats-antragsteller Antragsdaten für ein X.509-Sub-CA-Zertifikat erfassen und an den Betreiber der gematik Root-CA übermitteln.
Auslösender Akteur	BZA
Vorbedingungen	Ein Antragsberechtigter (Organisation) und zugehöriger berech-tigter Zertifikatsantragsteller (legitimierte Kontaktperson) wurden im Zulassungsmanagement angelegt. Der Zulassungsstatus des berechtigten Zertifikatsantragstellers sowie der zugehörigen Organisation ist aktiviert. Dem berechtigten Zertifikatsantragsteller wurde mindestens ein CA-Einsatzbereich zugewiesen. Der berechtigte Zertifikatsantragsteller besitzt ein Active-Directory-Benutzerkonto mit dem Status "aktiv".

Use Case: Name:	UC-Root-CA-001 Antragsdaten für X.509-Sub-CA-Zertifikat erfassen
	Dem Berechtigten Zertifikatsantragsteller wurde ein RSA-Token zur Verfügung gestellt. Der Akteur ist in der Applikation angemeldet und autorisiert.
Eingangsdaten	Antragsdaten für ein X.509-Sub-CA-Zertifikat gemäß Tabelle 4.
Ergebnisse	Die Antragsdaten wurden an den Betreiber der gematik Root-CA übermittelt. Der Betreiber der gematik Root-CA und die gematik wurden über die eingegangenen Antragsdaten per E-Mail benachrichtigt.
Anmerkungen	

Nr.	Akteur	Prozessschritt
1.	BZA	Der Akteur löst in der Applikation die Funktion "Antragsdaten für X.509-Sub-CA-Zertifikat erfassen" aus.
2.	Applikation	Die Applikation stellt eine Eingabemaske mit allen Eingabefeldern für den Zertifikatsantrag zur Verfügung.
3.	Applikation	Der Akteur gibt die erforderlichen Daten ein und speichert diese.
4.	Applikation	Die Applikation prüft die Eingaben auf Vollständigkeit und Plausibilität. Fehlerfälle: • Unvollständige oder fehlende Daten: Die Applikation kehrt zur Eingabemaske zurück und zeigt die festgestellten Plausibilitätsverletzungen, z. B. durch eine farbliche Kennzeichnung, an. Der Akteur kann diese korrigieren. • Signatur-Prüfung des PKCS#10-Requests schlägt fehl: Die Applikation kehrt zur Eingabemaske zurück und zeigt die festgestellten Plausibilitätsverletzungen, z. B. durch eine farbliche Kennzeichnung, an. Der Akteur kann diese korrigieren. • Der ausgewählte CA-Einsatzbereich (siehe Tabelle 5) entspricht nicht einem dem berechtigten Zertifikatsantragsteller über das Zulassungsmanagement zugewiesenen CA-Einsatzbereich: Die Applikation kehrt zur Eingabemaske zurück und zeigt die festgestellten Plausibilitätsverletzungen, z. B. durch eine farbliche Kenn-

Nr.	Akteur	Prozessschritt
		zeichnung, an. Der Akteur kann diese korrigieren.
5.	Applikation	Die Applikation fordert den Akteur zur Bestätigung der Erfassung auf.
6.	BZA	Der Akteur bestätigt die Erfassung.
7.	TMS	Das TMS speichert die erfassten Daten in der TMS-Datenbank. Der Vorgang wird protokolliert.
8.	Applikation	Die Applikation meldet die erfolgreiche Erfassung und Speicherung der Antragsdaten und kehrt zur aufrufenden Funktion zurück.
9.	Applikation	Die Applikation stellt dem Akteur ein Merkblatt zur weiteren Vorgehensweise und ein Antragsformular zum Download bereit. Darüber hinaus werden dem Akteur das Merkblatt und das Antragsformular im PDF-Format per E-Mail zugestellt.
10.	BZA	Der Akteur druckt das Antragsformular aus, unterschreibt es und sendet es postalisch an den Betreiber der gematik Root-CA.
11.	TMS	Das TMS benachrichtigt den Betreiber der gematik Root-CA und die gematik über die eingegangenen Antragsdaten per E-Mail.

4.3 UC-Root-CA-002 X.509-Sub-CA-Zertifikat beziehen

Use Case: Name:	UC-Root-CA-002 X.509-Sub-CA-Zertifikat beziehen
Kurzbeschreibung	Dieser Use Case beschreibt, wie berechtigte Zertifikatsantragsteller ein X.509-Sub-CA-Zertifikat beim Betreiber der gematik Root-CA beantragen können.
Auslösender Akteur	Betreiber der gematik Root-CA
Vorbedingungen	Der Betreiber der gematik Root-CA hat den berechtigten Zertifikatsantragsteller nach Erhalt der Antragsdaten kontaktiert und einen Termin vereinbart. Der berechtigte Zertifikatsantragsteller ist beim Betreiber anwesend. Der berechtigte Zertifikatsantragsteller wurde von einem Mitarbeiter des Betreibers der gematik Root-CA erfolgreich identifiziert. Dabei fand ein Abgleich mit den Daten des von der

Use Case: Name:	UC-Root-CA-002 X.509-Sub-CA-Zertifikat beziehen
	gematik über das Zulassungsmanagement übermittelten berechtigten Zertifikatsantragstellers statt. Der berechtigte Zertifikatsantragsteller hat einen USB-Stick mit dem PKCS#10-Request an den Betreiber der gematik-Root-CA übergeben. Es sind alle Mitarbeiter mit den entsprechenden Rollen des Betreibers der gematik Root-CA anwesend, die für die Erstellung eines Sub-CA-Zertifikats erforderlich sind.
Eingangsdaten	PKCS#10-Request auf USB-Stick und ausgedrucktes und unterschriebenes Antragsformular des berechtigten Zertifikatsantragstellers. Ausweisdokumente des berechtigten Zertifikatsantragstellers.
Ergebnisse	Es wurde ein signierter Zertifikats-Request für die Ausstellung eines Sub-CA-Zertifikats durch die gematik Root CA erstellt und an den berechtigten Zertifikatsantragsteller übergeben. Sofern es sich um ein X.509-Sub-CA-Zertifikat für HBA oder SMC-B handelt, wurde das Zertifikat im OCSP-Responder der gematik Root-CA veröffentlicht.
Anmerkungen	Die konkrete Ausgestaltung des Prozesses (wie z. B. die Zutrittskontrolle zum Rechenzentrum der gematik Root-CA bzw. zu den verschiedenen Zonen, Durchführung verschiedener Aktionen im Vier-Augen-Prinzip (beispielsweise die Freischaltung des HSMs der gematik Root-CA per OCS zur Erzeugung des X.509-Sub-CA-Zertifkats)) etc. erfolgt im Rahmen der Erstellung des Betriebskonzepts der PKI-Dienste. Das X.509-gematik-Root-CA-Zertifikat sowie der zugehörige Zertifikatsfingerprint werden im Internet veröffentlicht.

Nr.	Akteur	Prozessschritt
1.	ARC	Der Akteur nimmt den USB-Stick mit dem PKCS#10-Request und das Antragsformular des berechtigten Zertifikatsantragstellers entgegen und prüft diese. Fehlerfall: • Das Antragsformular ist unvollständig oder fehlerhaft: Der Vorgang wird abgebrochen.
2.	ARC	Der Akteur übergibt den USB-Stick und das Antragsformular an

Nr.	Akteur	Prozessschritt
		den Akteur mit der Rolle ORC.
3.	ORC	Der Akteur meldet sich an der gematik Root-CA an.
4.	ORC	Der Akteur lädt PKCS#10-Request vom USB-Stick und importiert diesen in den RA-Client der gematik Root-CA.
5.	ORC	Der Akteur sendet den PKCS#10-Request unter Verwendung des RA-Clients an die gematik Root-CA.
6.	gematik Root-CA	Die gematik Root-CA nimmt den Zertifikatsantrag entgegen und erzeugt das X.509-Sub-CA-Zertifikat. Fehlerfälle: • Unvollständige oder fehlende Daten: Der Vorgang wird abgebrochen. • Signatur-Prüfung des PKCS#10-Requests schlägt fehl: Der Vorgang wird abgebrochen. • Der im PKCS#10-Request angegebene CA-Einsatzbereich (siehe Tabelle 5) entspricht nicht einem dem berechtigten Zertifikatsantragsteller über das Zulassungsmanagement zugewiesenen CA-Einsatzbereich: Der Vorgang wird abgebrochen.
7.	gematik Root-CA	Die gematik Root-CA sendet das erstellte X.509-Sub-CA-Zertifikat an den RA-Client.
8.	ORC	Der Akteur speichert das erstellte X.509-Sub-CA-Zertifikat auf einem Medium.
9.	ORC	Der Akteur importiert das erstellte X.509-Sub-CA-Zertifikat in das TMS.
10.	TMS	Fallunterscheidung: • Es handelt sich um ein SMC-B- oder HBA-Sub-CA-Zertifikat: Das TMS veröffentlicht das erstellte X.509-Sub-CA-Zertifikat im OCSP-Responder der gematik Root-CA.
11.	TMS	Das TMS veröffentlicht das erstellte X.509-Sub-CA-Zertifikat sowie den zugehörigen Zertifikatsfingerprint im Internet.
12.	ORC	Der Akteur übergibt das Medium mit dem X.509-Sub-CA-Zertifikat an den berechtigten Zertifikatsantragsteller.

4.4 UC-Root-CA-003 X.509-Sub-CA-Zertifikat sperren

Berechtigte Sperrantragsteller können nur die für Ihre Organisation ausgestellten X.509-Sub-CA-Zertifikate sperren. Hierfür beauftragt der Berechtigte Sperrantragsteller bei der gematik die Sperrung eines Sub-CA-Zertifikats. Die gematik veranlasst die Sperrung des Zertifikats beim Betreiber der gematik Root CA über einen Betreiberauftrag durch das Trust Management System (TMS) und führt die notwendigen Anpassungen in der TSL-Datei mit Hilfe der TSL-Applikation des TSL-Dienstes (siehe [ARV_706.3_Spec_SST_TSL-Dienst]). Der Betreiber der gematik Root-CA nimmt diese Betreiberauftrag der gematik entgegen und bearbeitet die enthaltene Aufforderung zur Sperrung eines Sub-CA-Zertifikats in der gematik Root CA.

Use Case: Name:	UC-Root-CA-003 X.509-Sub-CA-Zertifikat sperren
Kurzbeschreibung	Dieser Use Case beschreibt, wie berechtigte Sperrantragsteller X.509-Sub-CA-Zertifikate bei der gematik Root-CA sperren können.
Auslösender Akteur	Berechtigter Sperrantragsteller
Vorbedingungen	X.509-Sub-CA-Zertifikat der Organisation des berechtigten Sperrantragstellers liegt in gematik Root-CA sowie im TMS vor. Der berechtigte Sperrantragsteller hat einen Sperrantrag bei der gematik eingereicht.
Eingangsdaten	Sperrantrag des berechtigten Sperrantragstellers gemäß Tabelle 6.
Ergebnisse	Das Zertifikat wurde im OCSP-Responder der gematik Root CA gesperrt und die gematik sowie der Berechtigte Sperrantragsteller wurden benachrichtigt.
Anmerkungen	Berechtigte Sperrantragsteller können nur die von Ihrer Organisation ausgestellten X.509-Sub-CA-Zertifikate sperren. Die Beauftragung der Sperrung von X.509-Sub-CA-Zertifikaten beim Betreiber der gematik Root CA muss durch die gematik erfolgen. Neben dieser Beauftragung muss die gematik mit Hilfe der TSL-Applikation des TSL-Dienstes (siehe [ARV_706.3_Spec_SST_TSL-Dienst]) die TSP-Dienst-Informationen in der TSL-Datei entsprechend aktualisieren. Die konkrete Ausgestaltung des Prozesses erfolgt im Rahmen der Erstellung des Betriebskonzepts der PKI-Dienste.

Nr.	Akteur	Prozessschritt
1.	SAG	Die gematik nimmt den Sperrantrag entgegen.
2.	SAG	Die gematik beauftragt den Betreiber über einen Betreiberauftrag zur Sperrung des X.509-Sub-CA-Zertiifkats. Weiterhin setzt die gematik den zugehörigen TSP-Dienst über die TSL-Applikation über das TMS auf „revoked“.
3.	SRC	Der Betreiber nimmt den Betreiberauftrag zur Sperrung eines Sub-CA-Zertifikats entgegen und initiiert den internen Prozess zur Sperrung eines Sub-CA-Zertifikats
4.	ARC/ORC	Mithilfe des TMS wird der CMP-Sperrantrag zu dem zu sperrenden Sub-CA-Zertifikat erstellt.
5.	ORC	Import des CMP-Sperrantrags auf dem RCA-Client auf der gematik Root CA.
6.	SRC/SAG	Die gematik und der Betreiber dokumentiert den Vorgang.

4.5 Artefakte

4.5.1 Antragsdaten für ein X.509-Sub-CA-Zertifikat

Die nachfolgende Tabelle stellt Antragsdaten dar, die im Rahmen des Use Cases "UC-Root-CA001 Antragsdaten für X.509-Sub-CA-Zertifikat erfassen" erfasst werden. Die Zertifikatsantragsdaten in kursiver Schrift werden aus dem Zulassungsmanagement übernommen und können vom berechtigten Zertifikatsantragsteller nicht editiert werden.

Tabelle 4: Antragsdaten für ein X.509-Sub-CA-Zertifikat

Zertifikatsantragsdaten	Kurzbeschreibung
TSP-X.509-CA	*Name und Anschrift des über das Zulassungsmanagement übermittelten Antragsberechtigten (Organisation).*
CA-Name	CA-Name des Zertifikats gemäß [gemSpec_PKI#GS-A_4737]
Zertifikatstyp / CA-Einsatzbereich	Zertifikatstyp / CA-Einsatzbereich gemäß [gemSpec_PKI#GS-A_4735]. In Tabelle 5 sind die möglichen Werte für die Felder <TSP-Präfix> und <usage> für die CA-Einsatzbereiche aufgelistet. Der berechtigte Zertifikatsantragsteller kann nur die ihm über das Zulassungsmanagement zugewiesenen CA-Einsatzbereiche auswählen.

Kontaktperson	*Name, Vorname und Anschrift des über das Zulassungsmanagement übermittelten berechtigten Zertifikatsantragstellers. Dieser beantragt und bezieht das X.509-Sub-CA-Zertifikat beim Betreiber der gematik Root-CA (siehe Kapitel 4.3).*
Zertifikatsantrag	PKCS#10-Requests (Der PKCS#10-Request wird mit dem entsprechenden privaten Schlüssel signiert). Die Struktur des PKCS#10-Zertifikatsrequests kann dem Listing 1 entnommen werden.
Unterschrift	Unterschrift des über das Zulassungsmanagement übermittelten berechtigten Zertifikatsantragstellers.

4.5.2 PKCS#10-Request zur Beantragung eines X.509-Sub-CA-Zertifikats

Es werden folgenden Daten im PKCS#10-Request benötigt, um ein X.509-Sub-CA-Zertifikat auszustellen:

- SubjectPublicKeyInfo
- Subject

```
CertificationRequest ::= SEQUENCE {
   certificationRequestInfo    CertificationRequestInfo,
   signatureAlgorithm          AlgorithmIdentifier,
                        -- sha256WithRSAEncryption (1 2 840 113549 1 1 11) mit parameter NULL

   signature                   BIT STRING
}

CertificationRequestInfo ::= SEQUENCE {
   version             INTEGER { v1(0) },
   subject             Name,
   subjectPKInfo       SubjectPublicKeyInfo,
}

SubjectPublicKeyInfo ::= SEQUENCE{
   algorithm SEQUENCE {
      algorithm   OBJECT IDENTIFIER rsaEncryption (1 2 840 113549 1 1 1)
   }
   subjectPublicKey RSAPublicKey SEQUENCE {
      modulus        INTEGER,
```

```
    publicExponent  INTEGER
  }
}
```

Listing 1: Struktur des PKCS#10-Requests zur Beantragung eines X.509-Sub-CA-Zertifikats mit RSA

```
CertificationRequest ::= SEQUENCE {
   certificationRequestInfo    CertificationRequestInfo,
   signatureAlgorithm          AlgorithmIdentifier,
                       -- ecdsa-with-SHA256 (1 2 840 10045 4 3 2)

   signature                   BIT STRING
}

CertificationRequestInfo ::= SEQUENCE {
   version             INTEGER { v1(0) },
   subject             Name,
   subjectPKInfo       SubjectPublicKeyInfo,
}

SubjectPublicKeyInfo ::= SEQUENCE{
   algorithm SEQUENCE {
      algorithm   OBJECT IDENTIFIER ecPublicKey (1 2 840 10045 2 1) mit Parameter brainpoolP256r1 (1 3 36 3 3 2 8 1 1 7)
   }
   subjectPublicKey ecPublicKey BIT STRING
}
```

Listing 2: Struktur des PKCS#10-Requests zur Beantragung eines X.509-Sub-CA-Zertifikats mit ECDSA

"SubjectPublicKeyInfo" ist für alle CA-Einsatzbereiche gleich gestaltet. Der PKCS#10-Request wird mit dem zugehörigen privaten Schlüssel signiert. "Subject" variiert abhängig vom verwendeten CA-Einsatzbereich:

Zertifikattyp <TSP-Präfix>.<usage>-CA

- CN=<TSP-Präfix> || '.' || <usage> || '-CA' || <n>

Tabelle 5: CA-Einsatzbereiche der gematik Root-CA

Spezifischer CA-Einsatzbereich	<usage> im Feld commonName	<TSP-Präfix> im Feld common-Name

TSL-Dienst	TSL	GEM
VPN-Zugangsdienst	VPNK	GEM
Komponenten-PKI	KOMP	GEM
Heilberufsausweis	HBA	Über Zulassungsmanagement übermittelt
Berufsausweis	BA	Über Zulassungsmanagement übermittelt
Institutionskarten	SMCB	Über Zulassungsmanagement übermittelt
OCSP-Dienst	OCSP	Über Zulassungsmanagement übermittelt / GEM
CRL-Dienst	CRL	Über Zulassungsmanagement übermittelt / GEM

Die Sub-CA-Zertifikatsprofile können [gemSpec_PKI#5] entnommen werden.

TSP-X.509 nonQES können eigene OCSP-Signer-CA bzw. CRL-Signer-CA betreiben. Das OCSP-Signer-CA- und CRL-Signer-CA-Zertifikat muss aus der gematik Root-CA abgeleitet sein.

Der Anbieter des TSL-Dienstes beantragt das TSL-Signer-CA-Zertifikat bei der gematik Root-CA. Das TSL-Signer-CA-Zertifikat bildet den Vertrauensanker für die TI.

4.5.3 Sperrantragsdaten für ein X.509-Sub-CA-Zertifikat

Tabelle 6: Sperrantragsdaten für ein X.509-Sub-CA-Zertifikat

Zertifikatssperrantragsdaten	Kurzbeschreibung
Organisationsname des Sperrantragstellers	Name der zugehörigen Organisation, der das Zertifikat zugeordnet ist.
Seriennummer	Seriennummer des zu sperrenden X.509-Sub-CA-Zertifikats.
Name	Common-Name des zu sperrenden X.509-Sub-CA-Zertifikats.
Sperrgrund	Grund der Sperrung.

5 I_OCSP_Status_Information

Es wird ein OCSP-Responder gemäß [gemSpec_PKI#9] konzeptioniert und implementiert, der die Statusinformationen der X.509 Sub-CA-Zertifikate für HBA und SMC-B verfügbar macht. Der OCSP-Responder implementiert die Schnittstelle I_OCSP_Status_Information gemäß [Common-PKI] und wird im Internet bereitgestellt.

Anhang A – Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
CA	Certification Authority
CRL	Certificate Revocation List
HBA	Heilberufsausweis
HSM	Hardware Security Module
OCS	Operator Card Set
OCSP	Online Certificate Status Protocol
ORS 1	Online Rollout Stufe 1
PKI	Public Key Infrastructure
QES	Qualifizierte elektronische Signatur
SMC	Security Module Card
TI	Telematikinfrastruktur
TSL	Trust-service Status List
TSP	Trust Service Provider

A2 – Glossar

Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.

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

A3 – Abbildungsverzeichnis

A4 – Tabellenverzeichnis

A5 – Listings

A6 – Referenzierte Dokumente

A6.1 – Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[ARV_706.3_RL_gematik-Root-CA_CP]	Zertifizierungsrichtlinie der gematik Root-CA
[gemKPT_Arch_TIP]	gematik: Einführung der Gesundheitskarte – Konzept Architektur der TI-Plattform
[gemKPT_PKI_TIP]	gematik: Einführung der Gesundheitskarte – Konzept PKI der TI-Plattform

[gemRL_TSL_SP_CP]	gematik: Einführung der Gesundheitskarte – Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL
[gemSpec_OID]	gematik: Einführung der Gesundheitskarte – Spezifikation Festlegung von OIDs
[gemSpec_PKI]	gematik: Einführung der Gesundheitskarte – Spezifikation PKI
[gemSpec_TSL]	gematik: Einführung der Gesundheitskarte – Spezifikation TSL-Dienst
[gemSpec_TSP_X.509]	gematik: Einführung der Gesundheitskarte – Spezifikation Trust Service Provider X.509

A6.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
ARV_706.3_Spec_SST_TSL-Dienst	Schnittstellen- und Prozessspezifikation TSL-Dienst
ARV_706.3_Spec_SST_Komponenten-PKI	Schnittstellen- und Prozessspezifikation Komponenten-PKI