gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Schnittstellen- und Prozessspezifikation für die Produkttypen „TSP-X.509 nonQES (HBA, SMC-B und eGK)“, „TSP-CVC (HBA und SMC-B)“ und „TSP-X.509 QES (HBA)“

Bundesdruckerei GmbH

Version:	1.03.0
Revision:	\main\rel_ors1\2
Stand:	27.06.2014
Status:	Freigegeben
Klassifizierung:	öffentlich
Referenzierung	[gemSpec_SST_Proz_TSP]

Dokumentinformationen

Änderungen zur Vorversion

Änderung nach der Güteprüfung

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.01.0	07.03.2014	Inhalt	Inhaltsverzeichnis erstellt	BDr
0.10.0	10.03.2014	alle	Review	Pashah
0.11.0	17.03.2014	Deckblatt	Anpassung Titel	Klett
0.12.0	19.03.2014	alle	Fortführung Inhalt	Byszio
0.15.0	02.04.2014	alle	Einarbeitung FB Gematik	Byszio
0.16.0	04.04.2014	alle	Fortführung Inhalt (AP_TSM)	Byszio
0.17.0	07.04.2014	alle	Ergänzung Grafiken, Tabellen, Verschiebung Verifikationskarte in gemspec_KP	Byszio
0.18.0	07.04.2014	all	Einarbeitung Review-Kommentare	Byszio
0.19.0	10.04.2014	alle	Einarbeitung Review-Kommentare gematik	Byszio
0.20.0	14.04.2014	alle	Review QS	Kubis
0.21.0	14.04.2014	alle	Einarbeitung Review QS	Byszio
1.00.0	15.04.2014	alle	Endredaktion und Freigabe	Klett
1.00.1	15.05.2014	alle	Einarbeitung Kommentare Gematik	Byszio
1.00.2	16.05.2014	alle	Endredaktion	Klett
1.01.0	16.05.2014	alle	Review Qualität und Freigabe	Kubis Pashah
1.01.1	04.06.2014	alle	Einarbeitung Kommentare Gematik	Byszio
1.02.0	11.06.2014	alle	Review Qualität und Freigabe	Kubis Pashah

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.02.1	26.06.2014	Kapitel 2.2, 4.1.2.3, 4.1.6.3, 4.2.1.2, 4.2.5.2, 4.3.1.2, 4.3.5.2, 4.4.5.2,	Einarbeitung Kommentare Gematik	Byszio
1.02.2	27.06.2014	alle	Endredaktion	Klett
1.03.0	27.06.2014	alle	Review Qualität und Freigabe	Kubis Pashah

Inhaltsverzeichnis

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation beschreibt die Anforderungen zu Schnittstellen und Prozessen an die verschiedenen PKI-Komponenten, die den Zugang für Kartenherausgeber, Zertifikatsnutzer und Kartenproduzenten ermöglichen.

1.2 Zielgruppe

Das Dokument richtet sich an **Kartenpersonalisierer, Teilnehmer der Lose G2 Los 1 und 2, ORS1 Los 1 und 2** sowie informativ an Kartenherausgeber.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen für die Schnittstellen und Prozesse der folgenden Produkte:

- TSP-X.509 nonQES (HBA, SMC-B, HSM-B und eGK)
- TSP-X.509 pseudo QES (HBA)
- TSP-X.509 QES (HBA)
- TSP-CVC (HBA, HSM-B und SMC-B)

1.4 Abgrenzungen

Dieses Dokument beschreibt die Schnittstellen des Gesamtsystems für die Beantragung und Sperrung von Zertifikaten sowie die Schnittstellen der entsprechenden Statusauskünfte. Da sich alle aufgeführten Schnittstellen für das Beantragen und Sperren von Zertifikaten nur an die Losnehmer der Lose ORS1 Los 1 und 2 sowie G2 Los 1 und 2 für Tests richten, wird im Dokument auf eine Unterteilung nach Betriebsumgebungen verzichtet.

Die sonstigen Schnittstellen für Kartenprodukte, u. a. zur TSP-Schnittstelle, sind in der Spezifikation Kartenpersonalisierung [gemSpec_KP] beschrieben.

1.5 Methodik

1.5.1 Beschreibung von Anforderungen

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

Offene Punkte sind in Anhang A6 aufgeführt und im Text „gelb" markiert.

1.5.2 Schnittstellenbeschreibungen

Die Nomenklatur für Schnittstellen ist in diesem Dokument wie folgt:

Schnittstelle <Bezeichner[I|P]_Bezeichnung_Adressat>

Der Bezeichner ist I [interface] für technische Schnittstellen und P [process] für organisatorische Schnittstellen.

Die Bezeichnung stellt einen sprechenden Namen für die Schnittstelle an.

Der Adressat beschreibt als Abkürzung wer Empfänger bzw. Nutzer der Schnittstelle ist.

Die Schnittstellenbezeichnung wird komplett in Großbuchstaben beschrieben.

2 Systemüberblick

Das nachfolgend beschriebene System stellt Schnittstellen für die Prüfung der Gültigkeit von ausgestellten Zertifikaten aus den Infrastrukturen der X.509 CA nonQES, CA pseudoQES und der CA QES sowohl in der Telematik-Infrastruktur (TI) wie auch im Internet zur Verfügung.

Die aufgeführten CA-Systeme (certification authority) werden in der sicheren Umgebung der D-TRUST betrieben. Der Zugang für berechtigte Nutzer aus diesem Dokument ist nur über die nachfolgend beschriebenen Schnittstellen möglich.

So können Antragsteller aus G2 Los 1 und 2 über die beschriebenen Schnittstellen eGK, HBA und SMC-B Testzertifikate beantragen und sperren. Antragsteller aus ORS1 Los 1 und 2 können für die Erprobungsphase Zertifikate für HSM-B beantragen und sperren.

Der Zugang für die Beantragung von Zertifikaten und Sperrungen („Antragsverwaltung TSP") aus ORS1 Los 1 und 2 wird mittels des BDr-Serviceportals realisiert.

Die folgenden vier Darstellungen geben eine Übersicht der zur Verfügung stehenden Schnittstellen aus der Perspektive des Nutzers. Zusätzlich gibt Abbildung 5 eine Gesamtansicht des Systems inklusive der von den angrenzenden Systemen bereitgestellten Schnittstellen wieder.

Abbildung 1 zeigt eine Übersicht der Schnittstellen, die Nutzer aus G2 Los 1 und 2 sowie ORS1 Los 1 und 2 nach ihrer Registrierung beim TSP nutzen können. Die genaue Beschreibung der Schnittstellen ist im Kapitel 4 enthalten.

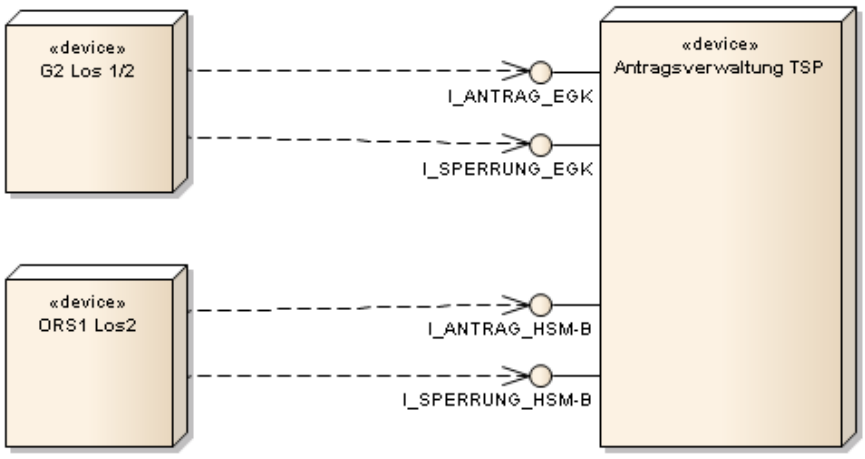

Abbildung 1: Schnittstellen aus Sicht G2 Los 1 und 2, ORS1 Los 1 und 2

Die Schnittstellen aus Sicht der Nutzer in der TI und dem Internet sind für die nonQES CA in Abbildung 2, für die pseudoQES CA in Abbildung 3 und die QES CA in Abbildung 4 dargestellt.

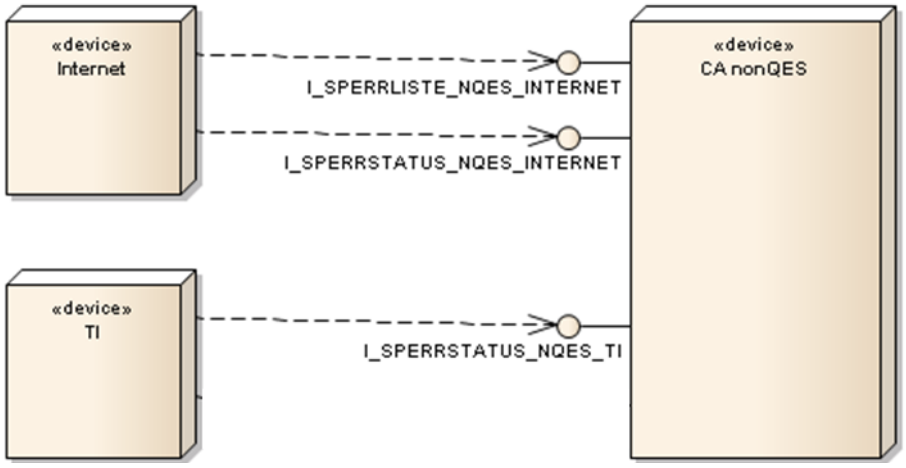

Abbildung 2: Schnittstellen nonQES aus Sicht TI- und Internetnutzer

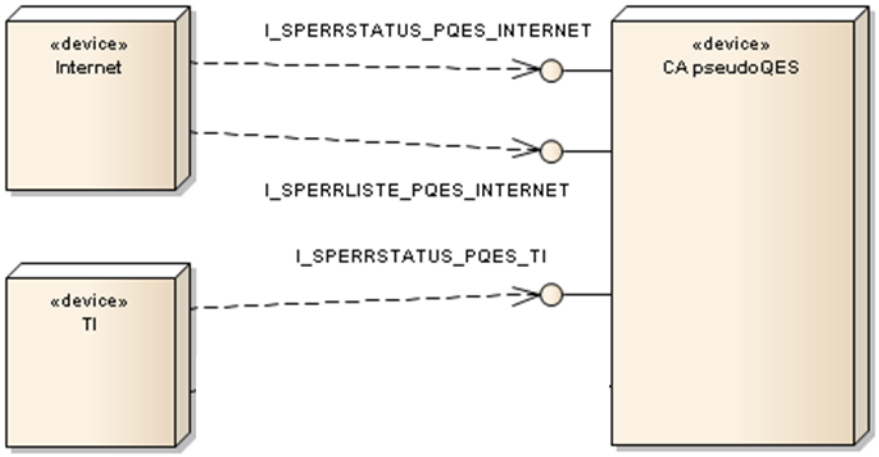

Abbildung 3: Schnittstellen pseudoQES aus Sicht TI- und Internetnutzer

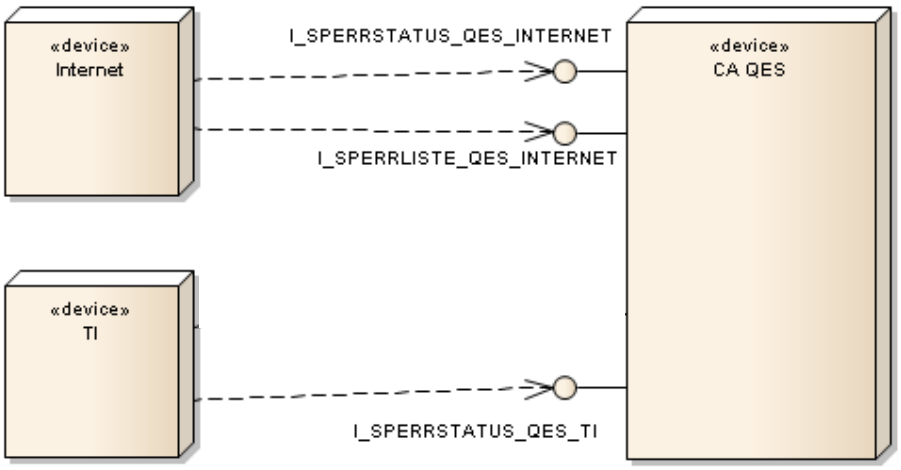

Abbildung 4: Schnittstellen QES aus Sicht TI- und Internetnutzer

In diesen Darstellungen sind die Schnittstellen des TSP mit den zugehörenden Namen der Schnittstellen abgebildet. Der einfacheren Lesbarkeit wegen, sind immer die Namen der technischen Schnittstellen (I_XX_XX) aufgeführt, auch wenn im Kapitel 4 zusätzlich die Prozessschnittstellen (P_XX_XX) beschrieben werden.

Zum vollständigen Überblick zeigt Abbildung 5 alle Schnittstellen des beschriebenen Systems. Es sind hier zur Information auch die von Dritten bereitgestellten Schnittstellen (grau hinterlegt) aufgeführt, die vom TSP zur Beantragung und Sperrung von Zertifikaten selbst verwendet werden. Mit Grün umrahmte Schnittstellen sind in der gemspec_KP beschrieben.

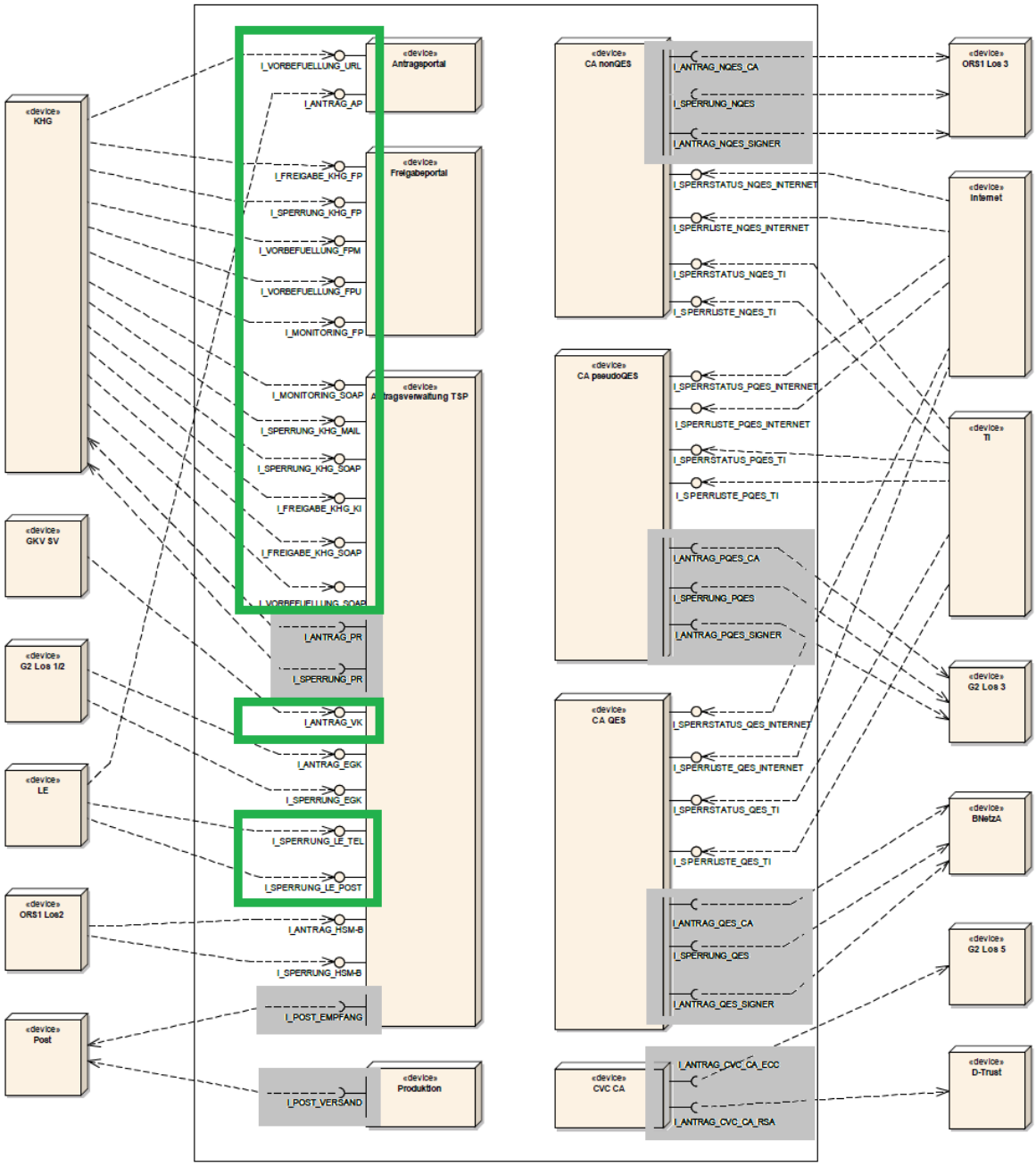

Abbildung 5: Schnittstellenübersicht im Systemkontext

2.1 Akteure und Rollen

Die Definition der Rollen entspricht [gemSpec_TSP_X.509], Kapitel 6.1. und [gemSpec_CVC_TSP] Kapitel 3.1.

Tabelle 1: Rollen

Rolle	Beschreibung
Antragsberechtigter	Im Sinne dieser Spezifikation in den Rollen „Berechtigter Testzertifikate" bzw. „BerechtigteHSM-B".
Berechtigter Testzertifikate	Beim TSP im Rahmen der Los-übergreifenden Kooperation registrierter Nutzer aus G2 Los 1 und 2, der für die Beantragung und Sperrung von Testzertifikaten verantwortlich ist.
Berechtigter HSM-B	Beim TSP im Rahmen der Los-übergreifenden Kooperation registrierter Nutzer aus ORS1 Los 1 und 2, der für die Beantragung und Sperrung von HSM-B Zertifikaten verantwortlich ist.
Berechtigter Zertifikatsantragsteller	Im Sinne dieser Spezifikation in den Rollen „Berechtigter Testzertifikate" bzw. „Berechtigter HSM-B".
DKG	Deutsche Krankenhausgesellschaft: Die Deutsche Krankenhausgesellschaft ist der Zusammenschluss von Spitzen- und Landesverbänden der Krankenhausträger.
gematik	Die gematik übt als Auftraggeber eine Kontrollfunktion während der Erprobungsphase der Einführung von HBA und SMC-B aus.
GKV-Spitzenverband	Der GKV Spitzenverband beantragt durch den Bevollmächtigten die Verifikationskarten für die gesetzlichen Krankenversicherungen beim TSP. Der GKV-Spitzenverband ist Herausgeber der Verifikationskarte.
Identitätsprüfer	Person oder Institution, die die Identität einer Person verifizieren und bestätigen kann. Es kann die Post (im Fall des Verfahrens PostIdent), die zuständige Kammer (im Fall des Verfahrens KammerIdent) oder ein berechtigter Mitarbeiter des TSP sein.
Kartenherausgeber	Kartenherausgeber vergeben/bestätigen die berufsspezifischen bzw. institutionsspezifischen Attribute für eine Berufsgruppe. Sie geben HBA oder SMC-B/HSM-B heraus und sind für die ausgegebenen Karten sperrberechtigt.

Rolle	Beschreibung
Kostenträger	Die Kostenträger im Gesundheitswesen sind die gesetzlichen Krankenversicherungen (GKV).
Leistungserbringerorganisation (LEO)	Wird in dieser Spezifikation dem Kartenherausgeber gleichgesetzt.
Praxisregister	Das Praxisregister ist ein System zur Verwaltung von SMC-B-Anträgen und Karten der Ärzte und Psychotherapeuten. Das Praxisregister stellt dem TSP fertige Aufträge zur Produktion und Sperrung von SMC-Bs zur Verfügung.
Sektor	Ein Sektor umfasst einen abgrenzbaren Bereich der Leistungserbringer, für den eine Spitzenorganisation zuständig ist.
Spitzenorganisation eines Sektors	Eine Spitzenorganisation legt für die ihr zugehörigen Kartenherausgeber die sektorspezifische Ausgestaltung der TSP-Schnittstelle fest. Sie können eine Kontrollfunktion für ihren jeweiligen Sektor während der Erprobungsphase der Einführung von HBA und SMC-B ausüben.
TSP	Der Trust Service Provider (TSP) verantwortet den Betrieb der PKI (RA, CA, OCSP) und stellt die Schnittstellen für die Kartenpersonalisierung bereit. Der TSP ist zudem verantwortlich für die Personalisierung und Ausgabe der Karten. Im Rahmen dieses Dokuments wird nicht zwischen den Rollen TSP, ZDA und Personalisierer unterschieden. Der TSP stellt für die Antragsteller und Kartenherausgeber einen „Single Point of Contact" (SPOC) bereit, über den per E-Mail, Telefon, Fax oder Postweg mit dem TSP kommuniziert werden kann. Im Sinne dieser Spezifikation ist der TSP die Bundesdruckerei GmbH.
Sperrberechtigter	Mitarbeiter eines Kartenherausgebers, der die Berechtigung hat administrative Sperrungen für HBA bzw. SMC-B zu veranlassen. Im Sinne dieser Spezifikation in den Rollen „Berechtigter Testzertifikate" bzw. „Berechtigter HSM-B".

2.2 Nachbarsysteme

Die Nachbarsysteme des TSP-X.509 und TSP-CVC bestehen aus der gematik, als Betreiber der CVC- und X.509-Root-CA, den Kartenherausgebern, ORS1 Los 1 und 2, G2 Los 1 und 2 sowie den Standesorganisationen der Leistungserbringer (KHG Kartenherausgeber).

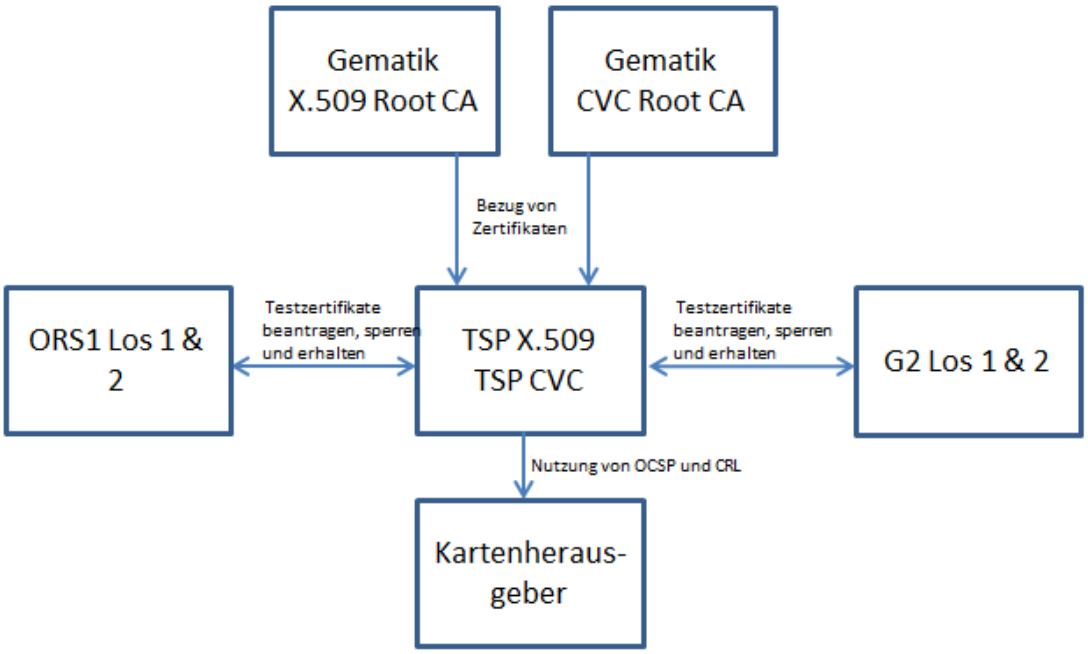

Abbildung 6: Angrenzende Systeme

3 Übergreifende Festlegungen

3.1 Nachweis der Erfüllung von SigG und SigV

Der Nachweis der Erfüllung aller Anforderungen im Rahmen des Deutschen Signaturgesetzes und nachfolgender Verordnung wird erbracht durch Vorlage der Bestätigung durch den beauftragten und BNetzA-akkreditierten Auditor sowie das zugehörige Zertifikat.

3.2 Nachweis der Mindestanforderungen an die Sicherheit zur Aufnahme in die TSL der gematik

Der Nachweis zur Erfüllung der Mindestanforderungen an die Sicherheit zur Aufnahme in die TSL erfolgt durch den von der gematik akkreditierten und geschulten Auditor sowie die Bereitstellung des Auditberichts, insofern dieser keine verhindernden Ergebnisse benennt.

3.3 Berechtigte Stellen zum Beantragen und Sperren von Zertifikaten

Auftragnehmer der Lose ORS1 Los 1 und 2 sowie G2 Los 1 und 2 sind nach ihrer Registrierung durch den TSP antragsberechtigt. Sie können nach dieser Registrierung Zertifikate beantragen und sperren. Hierfür MUSS die Bundesdruckerei als TSP im Rahmen der losübergreifenden Kommunikation kontaktiert werden. Die Freigabe der Registrierung erfolgt durch die gematik. Registrierungsverfahren und Kommunikation sind in Kapitel 4 detailliert beschrieben.

4 Funktionsmerkmale

Der TSP nutzt einerseits Schnittstellen anderer Systeme, wie beispielsweise der gematik-Root-CA oder BNetzA-Root-CA, auf der anderen Seite stellt der TSP auch Schnittstellen zu Verfügung. Hier KÖNNEN insbesondere Systeme der Lose ORS1 Los 1 und 2 und G2 Los 1 und 2 die angebotenen Schnittstellen zur Beantragung von Zertifikaten nutzen.

Darüber hinaus sind Schnittstellen für die Nachprüfung der Gültigkeit von Zertifikaten für die Nutzung aus der TI und aus dem Internet heraus beschrieben.

4.1 Funktionsmerkmal Antragsverwaltung TSP

4.1.1 Schnittstelle < I_ANTRAG_HSM-B >

4.1.1.1 Schnittstellendefinition

Diese Schnittstelle ist die technische Schnittstelle für die Kommunikation zur Erzeugung von X.509- und CVC-Zertifikaten für HSM-B/SMC-B durch den „Berechtigten HSM-B" aus ORS1 Los 1 und 2 mit anschließender Bereitstellung des Zertifikats durch den TSP G2 Los 4 (BDr).

4.1.1.2 Umsetzung

Diese Schnittstelle wird durch Request (Zertifikatsantrag) und Response (Zertifikat) mittels XML-Datei umgesetzt.

Die genaue Verwendung ist in < P_ANTRAG_HSM-B > beschrieben.

4.1.1.3 Nutzung

Es wird das Schema „CertficateRequestDataExample.xml" der Firma Giesecke & Devrient (vgl. Anhang B) verwendet, das bereits zwischen den verschiedenen Losen abgestimmt ist.

Die Benennung der Datei erfolgt nach folgendem Schema:

<Personalisierer>_<Datum>_<Auftragsnummer>_<TESToder PROD>_request.xml

4.1.2 Schnittstelle < P_ANTRAG_HSM-B >

4.1.2.1 Schnittstellendefinition

Die Prozessschnittstelle dient der Veranlassung der Erzeugung von X.509 und CV-Zertifikaten für HSM-B durch den „Berechtigten HSM-B" aus ORS1 Los1 und 2 mit anschließender Bereitstellung des Zertifikats durch G2 Los 4 (Bundesdruckerei).

4.1.2.2 Umsetzung

Diese Schnittstelle wird technisch durch Request (Zertifikatsantrag) und Response (Zertifikat) mittels XML-Datei umgesetzt (< I_ANTRAG_HSM-B >).

Für den Prozess MUSS die Übergabe der XML-Datei (Request) durch den „Berechtigten HSM-B" signiert erfolgen. Die Kommunikation MUSS zwischen dem registrierten „Berechtigten HSM-B" und dem TSP offline oder mittels des Serviceportals der Bundesdruckerei GmbH (BDr) https://support.bundesdruckerei.de/ erfolgen. Die Kommunikation SOLL über das Serviceportal abgewickelt werden.

Das Serviceportal steht in den Betriebszeiten zwischen 9:00-17:00 Uhr zur Verfügung.

4.1.2.3 Nutzung

Da die Zertifikate nur von „Berechtigten HSM-B" beantragt werden dürfen, MÜSSEN diese einmalig identifiziert und registriert werden.

Tabelle 2: Use Case 001 Registrierung im Serviceportal

Use Case:	UC 001
Name:	Registrierung im Serviceportal
Kurzbeschreibung	Dieser Use Case beschreibt, wie berechtigte Zertifikatsantragsteller das Serviceportal der BDr nutzen können, um Anträge zur Ausstellung und Sperrung von Zertifikaten zu stellen.
Auslösender Akteur	Berechtigter HSM-B
Vorbedingung	Die Kontaktdaten des "Berechtigten HSM-B" inklusive der E-Mail Adresse wurden im Rahmen der Projektübergreifenden Kommunikation der Gematik an den TSP übergeben.
Eingangsdaten	Kontaktdaten des Berechtigten HSM-B
Ergebnisse	Der „Berechtigte HSM-B" KANN Zertifikatsrequests auslösen und Zertifikate sperren
Anmerkungen	*keine*

Tabelle 3: Schritte zum Use Case 001 Registrierung im Serviceportal

Schritt	Akteur	Prozessschritt
1.	Gematik	Benennung der „Berechtigten HSM-B": Die zur Beantragung von Zertifikaten „Berechtigten HSM-B" werden im Rahmen der Los-übergreifenden Projektkommunikation zwischen den Projekten ORS1 Los 1 und 2 und G2 Los 4 benannt.

Schritt	Akteur	Prozessschritt
2.	Bundesdruckerei	Bereitstellung Zugang zum Serviceportal: Für die „Berechtigten HSM-B" von ORS1 Los 1 und 2 wird ein personalisierter Zugang zum Serviceportal der BDr eingerichtet. Dieser Zugang zum Serviceportal ist mittels Nutzername und Passwort geschützt. Der Nutzername und das erste Passwort für das Portal werden dem „Berechtigten HSM-B" per E-Mail zugesendet. Um das Portal verwenden zu können, MUSS der „Berechtigte HSM-B" sofort das Passwort ändern. Anschließend MUSS die Passwort-Änderung vom „Berechtigten HSM-B" per E-Mail bestätigt werden.
3.	Applikation	Registrierungsunterlagen für den „Berechtigten HSM-B" zur Nutzung des Serviceportals: Über das Serviceportal der BDr wird den benannten „Berechtigten HSM-B" eine Prozessbeschreibung und die für die Beantragung und Sperrung von Zertifikaten der PU benötigten Registrierungsunterlagen (PDF-Formulare) zur Angabe von Identifizierungs- und Registrierungsdaten sowie der Vereinbarung der zu verwendenden X.509-Zertifikate bereitgestellt.
4.	Berechtigter HSM-B	NUR für die Beantragung und Sperrung von Zertifikaten für die PU: Übergabe der Registrierungsunterlagen an den TSP: Diese Formulare MÜSSEN durch die benannten „Berechtigten HSM-B" ausgefüllt, ausgedruckt und unterschrieben werden. Bei der Übergabe der Formulare MÜSSEN die Mitarbeiter des "Berechtigten HSM-B" persönlich identifiziert werden.
5.	Bundesdruckerei	Prüfung der Unterlagen und Registrierung der „Berechtigten HSM-B": Die Formulare beziehungsweise die Bestätigung der Passwortänderung werden durch den TSP geprüft. Nach erfolgreicher Prüfung werden die benannten Mitarbeiter als „Berechtigter HSM-B" beim TSP registriert und darüber informiert.

Tabelle 4: Use Case 002 Nutzung des Serviceportals für Zertifikats-Erstellung

Use Case:	UC 002
Name:	Nutzung des Serviceportals für Zertifikats-Erstellung
Kurzbeschreibung	Dieser Use Case beschreibt, in welcher Form berechtigte Zertifikatsantragsteller das Serviceportal der BDr nutzen können, um Anträge zur Ausstellung von Zertifikaten zu stellen.
Auslösender Akteur	Berechtigter HSM-B
Vorbedingung	UC 001
Eingangsdaten	Signierte XML-Datei des Berechtigten HSM-B
Ergebnisse	Zertifikate
Anmerkungen	*keine*

Tabelle 5: Schritte zum Use Case 002 Nutzung des Serviceportals für Zertifikats-Erstellung

Schritt	Akteur	Prozessschritt
1.	Berechtigter HSM-B	Senden der Zertifikatsanträge: Über den Zugang zum Serviceportal kann der „Berechtigten HSM-B" seine Zertifikatsanträge in Form einer signierten XML-Datei einstellen.
2.	Bundesdruckerei	Verarbeitung der Zertifikatsanträge: Die Signatur der XML-Datei wird von einem Mitarbeiter des TSP geprüft. Bei erfolgreicher Prüfung wird die XML-Datei von einem Mitarbeiter des TSP verarbeitet und im Serviceportal als Response für den „Berechtigten HSM-B" bereitgestellt.
3.	Berechtigter HSM-B	Abholen der Zertifikatsresponse: Der „Berechtigte HSM-B" KANN die erstellten Zertifikate in Form einer XML-Datei über seinen personalisierten Zugang zum Serviceportal herunter laden.

Ergänzende oder abweichende Festlegungen KÖNNEN jeweils bilateral getroffen werden.

4.1.3 Schnittstelle < I_SPERRUNG_HSM-B >

4.1.3.1 Schnittstellendefinition

Die technische Schnittstelle für die Kommunikation zur Veranlassung der Sperrung eines X.509-Zertifikates für HSM-B wird lediglich durch Schnittstelle „Serviceportal" https://support.bundesdruckerei.de/ und Sperrhotline unter 030 / 25 93 91 600 repräsentiert.

Die zugehörenden Methoden werden in der „Schnittstelle < P_SPERRUNG_HSM-B >" beschrieben.

4.1.3.2 Umsetzung

entfällt

4.1.3.3 Nutzung

entfällt

4.1.4 Schnittstelle < P_SPERRUNG_HSM-B >

4.1.4.1 Schnittstellendefinition

Die Prozessschnittstelle für die Veranlassung der Sperrung eines X.509-Zertifikates für HSM-B wird durch eine schriftliche Sperrung mittels Ticket im BDr-Serviceportal sowie die telefonische Sperrmöglichkeit über die BDr-Sperrhotline repräsentiert.

4.1.4.2 Umsetzung

Nutzer eines HSM-B als „Berechtigte HSM-B" wurden mit der Registrierung für die Zertifikatsbeantragung eindeutig identifiziert. Somit sind die für eine schriftliche Sperrung notwendigen Unterschriftsproben beim TSP vorhanden.

„Berechtigte HSM-B" KÖNNEN ebenfalls mit Hilfe ihres bei der Registrierung übergebenen Sperrkennworts telefonisch sperren.

4.1.4.3 Nutzung

Die Kontaktdaten für eine Sperrung werden mit den „Berechtigten HSM-B" bei der Registrierung mitgeteilt. Zusätzlich befinden sich diese Daten auf der Webseite der BDr.

Das Sperrkennwort für die telefonische Sperrung MUSS spätestens bei Antragstellung für ein Zertifikat festgelegt sein. Sperrberechtigte „Berechtigte HSM-B" nutzen ihr Sperrkennwort aus dem Prozess der Registrierung.

An der Sperrhotline MUSS das Sperrkennwort angegeben werden. Die Sperrung des zugehörenden Zertifikats wird dann entsprechend der Gematik Certificate Policy umgesetzt.

Der Ablauf für die schriftliche Sperrung ist für Sperrberechtigte „Berechtigte HSM-B" wie folgt: Auf der Website der BDr ist das Sperrformular als PDF-Datei hinterlegt. Dieses ist entsprechend der beiliegenden Vorgaben auszufüllen und unterschrieben an die BDr-Kontaktadresse zu senden.

Nur im Falle von TU/RU kann der „Berechtigte HSM-B" über den geschützten Zugang zum Serviceportal der BDr ein Ticket eröffnen und eine formlose Liste mit den zu sperrenden Zertifikaten an den TSP senden. Mindestens MUSS die Zertifikatsseriennummer des zu sperrenden Zertifikats angegeben werden.

Das Serviceportal steht in den Betriebszeiten zwischen 9:00-17:00 Uhr zur Verfügung.

4.1.5 Schnittstelle < I_ANTRAG_EGK >

4.1.5.1 Schnittstellendefinition

Diese Schnittstelle ist die technische Schnittstelle für die Kommunikation zur Erzeugung von X.509-Zertifikaten für eGK, SMC-B und HBA durch die „Berechtigten HSM-B" aus G2 Los 1 und 2 mit anschließender Bereitstellung der Zertifikate durch G2 Los 4.

4.1.5.2 Umsetzung

Diese Schnittstelle wird durch Request (Zertifikatsantrag) und Response (Zertifikat) mittels XML-Datei umgesetzt.

Die Übergabe der XML-Datei zwischen dem registrierten „Berechtigter Testzertifikate" und

dem TSP erfolgt über das Serviceportal der BDr.

Das Serviceportal steht in den Betriebszeiten zwischen 9:00-17:00 Uhr zur Verfügung.

4.1.5.3 Nutzung

Da nur Zertifikate für die RU/TU ausgestellt werden, erfolgt die Berechtigungsprüfung des „Berechtigten Testzertifikate" über den geschützten Zugang zum Serviceportal der Bundesdruckerei.

Es wird das Schema „CertficateRequestDataExample.xml" der Firma Giesecke & Devrient verwendet, das bereits zwischen den verschiedenen Losen abgestimmt ist.

Die Benennung der Datei erfolgt nach folgendem Schema:

<Personalisierer>_<Datum>_<Auftragsnummer>_<TEST oder PROD>_request.xml

4.1.6 Schnittstelle < P_ANTRAG_EGK >

4.1.6.1 Schnittstellendefinition

Die Prozessschnittstelle dient der Veranlassung der Erzeugung von X.509 und CV Zertifikaten für eGK durch den „Berechtigten Testzertifikate" aus G2 Los1 und 2 mit anschließender Bereitstellung des Zertifikats durch G2 Los 4 (Bundesdruckerei).

4.1.6.2 Umsetzung

Diese Schnittstelle wird technisch durch Request (Zertifikatsantrag) und Response (Zertifikat) mittels bekannter XML-Datei umgesetzt (< I_ANTRAG_EGK >).

Für den Prozess MUSS die Übergabe der XML-Datei (Request) durch den „Berechtigten Testzertifikate" signiert erfolgen. Die Kommunikation MUSS zwischen dem registrierten „Be-

rechtigten Testzertifikate“ und dem TSP offline oder mittels des Serviceportals der Bundesdruckerei GmbH (BDr) https://support.bundesdruckerei.de/ erfolgen. Die Kommunikation SOLL über das Serviceportal abgewickelt werden Das Serviceportal steht in den Betriebszeiten zwischen 9:00-17:00 Uhr zur Verfügung.

4.1.6.3 Nutzung

Da die Zertifikate nur von den „Berechtigten Testzertifikate“ beantragt werden dürfen, MÜSSEN diese einmalig identifiziert und registriert werden.

Tabelle 6: Use Case 003 Registrierung im Serviceportal „Berechtigter Testzertifikate“

Use Case:	UC 003
Name:	Registrierung im Serviceportal „Berechtigter Testzertifikate“
Kurzbeschreibung	Dieser Use Case beschreibt, wie berechtigte Zertifikatsantragsteller das Serviceportal der BDr nutzen können, um Anträge zur Ausstellung und Sperrung von Zertifikaten zu stellen.
Auslösender Akteur	„Berechtigter Testzertifikate“
Vorbedingung	Die Kontaktdaten des "Berechtigten Testzertifikate" inklusive der E-Mail-Adresse wurden im Rahmen der projektübergreifenden Kommunikation der gematik an den TSP übergeben
Eingangsdaten	Kontaktdaten des “Berechtigten Testzertifikate“
Ergebnisse	Der “Berechtigte Testzertifikate“ kann Zertifikatsrequests auslösen und Zertifikate sperren
Anmerkungen	*keine*

Tabelle 7: Schritte zum Use Case 003 Registrierung im Serviceportal „Berechtigter Testzertifikate“

Schritt	Akteur	Prozessschritt
1.	Gematik	Benennung der „Berechtigten Testzertifikate“: Die zur Beantragung von Zertifikaten „Berechtigte Testzertifikate“ werden im Rahmen der Los-übergreifenden Projektkommunikation zwischen den Projekten ORS1 Los 1 und 2 und G2 Los 4 benannt.
2.	Bundesdruckerei	Bereitstellung Zugang zum Serviceportal: Für die „Berechtigten Testzertifikate“ von G2 Los 1 und 2 wird ein personalisierter Zugang zum Serviceportal der BDr eingerichtet. Der Zugang zum Serviceportal ist mittels Nutzername und Passwort geschützt. Der Nutzername und das erste Passwort für das Portal wird dem „Beauftragen Testzertifikate“ per E-Mail zugesendet. Um das Portal verwenden zu können, MUSS der Kunde sofort das Passwort än-

Schritt	Akteur	Prozessschritt
		dern. Anschließend MUSS die Passwort-Änderung vom „Beauftragen Testzertifikate" per E-Mail bestätigt werden.
3.	Applikation	Registrierungsunterlagen für den „Berechtigten Testzertifikate" zur Nutzung des Serviceportals: Über das Serviceportal der BDr wird den benannten „BeauftragtenTestzertifikate" eine Prozessbeschreibung und die für die Beantragung und Sperrung von Zertifikaten der PU benötigten Registrierungsunterlagen (PDF-Formulare) zur Angabe von Identifizierungs- und Registrierungsdaten sowie der Vereinbarung der zu verwendenden X.509-Zertifikate bereitgestellt.
4.	Berechtigter Testzertifikate	NUR für die Beantragung und Sperrung von Zertifikaten für die PU: Übergabe der Registrierungsunterlagen an den TSP: Diese Formulare MÜSSEN durch die benannten „Berechtigten Testzertifikate" ausgefüllt, ausgedruckt und unterschrieben werden. Bei der Übergabe der Formulare MÜSSEN die Mitarbeiter des "Berechtigten Testzertifikate "persönlich identifiziert werden.
5.	Bundesdruckerei	Prüfung der Unterlagen und Registrierung der „Berechtigten Testzertifikate": Die Formulare beziehungsweise die Bestätigung der Passwortänderung werden durch den TSP geprüft. Nach erfolgreicher Prüfung werden die benannten Mitarbeiter als „Berechtigte Testzertifikate" beim TSP registriert und darüber informiert.

Tabelle 8: Use Case 004 Nutzung des Serviceportals für Zertifikats-Erstellung

Use Case:	UC 004
Name:	Nutzung des Serviceportals für Zertifikats-Erstellung
Kurzbeschreibung	Dieser Use Case beschreibt, in welcher Form berechtigte Zertifikatsantragsteller das Serviceportal der BDr nutzen können, um Anträge zur Ausstellung von Zertifikaten zu stellen.
Auslösender Akteur	Berechtigter Testzertifikate
Vorbedingung	UC 003
Eingangsdaten	Signierte XML-Datei des Berechtigten Testzertifikate
Ergebnisse	Zertifikate

Use Case:	UC 004
Name:	Nutzung des Serviceportals für Zertifikats-Erstellung
Anmerkungen	*keine*

Tabelle 9: Schritte zum Use Case 004 Nutzung des Serviceportals für Zertifikats-Erstellung

Schritt	Akteur	Prozessschritt
1.	Berechtigter Test-zertifikate	Senden der Zertifikatsanträge: Über den Zugang zum Serviceportal kann der „Berechtigten Testzertifikate" seine Zertifikatsanträge in Form einer signierten XML-Datei einstellen.
2.	Bundesdruckerei	Verarbeitung der Zertifikatsanträge: Die Signatur der XML-Datei wird von einem Mitarbeiter des TSP geprüft. Bei erfolgreicher Prüfung wird die XML-Datei von einem Mitarbeiter des TSP verarbeitet und im Serviceportal als Response für den „Berechtigten Testzertifikate" bereitgestellt.
3.	Berechtigter Test-zertifikate	Abholen der Zertifikatsresponse: Der „Berechtigte Testzertifikate" KANN die erstellten Zertifikate in Form einer XML-Datei über seinen personalisierten Zugang zum Serviceportal herunter laden.

Ergänzende oder Abweichende Festlegungen KÖNNEN jeweils bilateral getroffen werden.

4.1.7 Schnittstelle < I_SPERRUNG_EGK >

4.1.7.1 Schnittstellendefinition

Die technische Schnittstelle für die Nutzung durch G2 Los 1 und 2 zur Veranlassung der Sperrung eines X.509-Test-Zertifikates für eGKs, SMC-Bs und HBAs wird lediglich durch Schnittstelle „Serviceportal" https://support.bundesdruckerei.de/ repräsentiert. Die zugehörenden Methoden werden in der „Schnittstelle < P_SPERRUNG_EGK >" beschrieben.

4.1.7.2 Umsetzung

entfällt

4.1.7.3 Nutzung

entfällt

4.1.8 Schnittstelle < P_SPERRUNG_EGK >

4.1.8.1 Schnittstellendefinition

Die Prozessschnittstelle zur Veranlassung der Sperrung eines X.509-Test-Zertifikats für eGKs, SMC-Bs und HBAs wird durch eine schriftliche Sperrung mittels Ticket im BDr-Serviceportal repräsentiert.

4.1.8.2 Umsetzung

Nutzer der Lose G2 Los 1 und 2 als „Berechtigte Testzertifikate" wurden mit der Registrierung für die Zertifikatsbeantragung eindeutig identifiziert. Somit sind die für eine schriftliche Sperrung notwendigen Unterschriftsproben beim TSP vorhanden.

4.1.8.3 Nutzung

Die Kontaktdaten für eine Sperrung werden den „Berechtigten Testzertifikate" bei der Registrierung mitgeteilt. Zusätzlich befinden sich diese Daten auf der Webseite der BDr.

Im hier beschriebenen Falle von TU/RU kann der „Berechtigte Testzertifikate" über den geschützten Zugang zum Serviceportal der BDr ein Ticket eröffnen und eine formlose Liste mit den zu sperrenden Zertifikaten an den TSP senden. Mindestens MUSS die Zertifikatsseriennummer des zu sperrenden Zertifikats angegeben werden.

Das Serviceportal steht in den Betriebszeiten zwischen 9:00-17:00 Uhr zur Verfügung.

4.2 Funktionsmerkmal TSP X.509 nonQES in den Ausprägungen SMC-B, HSM-B, eGK und HBA

4.2.1 Schnittstelle < I_SPERRSTATUS_NQES_INTERNET >

4.2.1.1 Schnittstellendefinition

Diese Schnittstelle repräsentiert den OCSP-Dienst des TSP, d.h. der Status eines von der nonQES-CA ausgegebenen Zertifikats kann hier online geprüft werden.

4.2.1.2 Umsetzung

Der OCSP-Responder erfüllt die Common PKI 2.0 Part 9 Tabelle13 (#4) und kann somit zusätzlich positive Auskünfte liefern. Die Antwort ist mittels des zur OCSP-Signer-CA der zentralen PKI gehörenden separaten OCSP-Signers gesichert.

4.2.1.3 Nutzung

Der OCSP-Responder kann über ocsp.d-trust.net mittels des http-Protokolls abgefragt werden.

4.2.2 Schnittstelle < P_SPERRSTATUS_NQES_INTERNET >

Diese Schnittstelle wird nicht genutzt bzw. benötigt.

4.2.3 Schnittstelle < I_SPERRLISTE_NQES_INTERNET >

4.2.3.1 Schnittstellendefinition

Diese Schnittstelle beschreibt die Möglichkeit zum Download der Sperrliste beim TSP.

4.2.3.2 Umsetzung

Die Sperrliste wird in Form einer X.509 CRLv2-Datei jeweils „DER" und „PEM" codiert angeboten. Die CRL ist mittels des zur CRL-Signer-CA der zentralen PKI gehörenden separaten CRL-Signers gesichert.

4.2.3.3 Nutzung

Der Download kann über zwei Methoden realisiert werden:

1. Unter https://www.bundesdruckerei.de/ auf den Unterseiten „Roots und CRLs" werden die CRLs zum Download mittels Browser angeboten.
2. Via LDAP der Bundesdruckerei: ldap://directory.d-trust.net

   Folgende in verschiedenen Clients abgefragte Angaben gelten für den D-TRUST-Verzeichnisdienst:

   - Servername/Hostname: directory.d-trust.net
   - Anschluss/Port-Nr: 389
   - Suchbasis/Basis-DN: c=de
   - keine verschlüsselte Verbindung, keine Anmeldung erforderlich
   - Der CRL Name entspricht dem CA Namen

4.2.4 Schnittstelle < P_SPERRLISTE_NQES_INTERNET >>

Diese Schnittstelle wird nicht genutzt bzw. benötigt.

4.2.5 Schnittstelle < I_SPERRSTATUS_NQES_TI >>

4.2.5.1 Schnittstellendefinition

Diese Schnittstelle repräsentiert den OCSP-Dienst des TSP, d.h. der Status eines von der nonQES-CA ausgegebenen Zertifikats kann hier online geprüft werden.

4.2.5.2 Umsetzung

Der OCSP-Responder erfüllt die Common PKI 2.0 Part 9 Tabelle13 (#4) und kann somit zusätzlich positive Auskünfte liefern. Die Antwort ist mittels des zur OCSP-Signer-CA der zentralen PKI gehörenden separaten CRL-Signers gesichert.

4.2.5.3 Nutzung

Der OCSP-Responder kann über die aktuell noch nicht bekannte, später aber veröffentlichte Adresse für Statusabfragen mittels des http-Protokolls abgefragt werden.

4.2.6 Schnittstelle < P_SPERRSTATUS_NQES_TI >

Diese Schnittstelle wird nicht genutzt bzw. benötigt.

4.2.7 Schnittstelle < I_SPERRLISTE_NQES_TI >

Diese Schnittstelle wird nicht genutzt bzw. benötigt.

4.2.8 Schnittstelle < P_SPERRLISTE_NQES_TI >

Diese Schnittstelle wird nicht genutzt bzw. benötigt.

4.3 Funktionsmerkmal TSP X.509 pseudo QES in der Ausprägung HBA (RU/TU)

4.3.1 Schnittstelle < I_SPERRSTATUS_PQES_INTERNET >

4.3.1.1 Schnittstellendefinition

Diese Schnittstelle repräsentiert den OCSP-Dienst des TSP, d.h. der Status eines von der pseudoQES-CA ausgegebenen Zertifikats kann hier online geprüft werden.

4.3.1.2 Umsetzung

Der OCSP-Responder erfüllt die Common PKI 2.0 Part 9 Tabelle13 (#4) und kann somit zusätzlich positive Auskünfte liefern. Die Antwort ist mittels des zur OCSP-Signer-CA der zentralen PKI gehörenden separaten Signers gesichert.

4.3.1.3 Nutzung

Der OCSP-Responder kann über ocsp.d-trust.net mittels des http-Protokolls abgefragt werden.

4.3.2 Schnittstelle < P_SPERRSTATUS_PQES_INTERNET >

Diese Schnittstelle wird nicht genutzt bzw. benötigt.

4.3.3 Schnittstelle < I_SPERRLISTE_PQES_ INTERNET >

4.3.3.1 Schnittstellendefinition

Diese Schnittstelle beschreibt die Möglichkeit zum Download der Sperrliste beim TSP.

4.3.3.2 Umsetzung

Die Sperrliste wird in Form einer X.509 CRLv2-Datei jeweils „DER" und „PEM" codiert angeboten. Die CRL ist mittels des zur CRL-Signer-CA der zentralen PKI gehörenden separaten Signers gesichert.

4.3.3.3 Nutzung

Der Download kann über zwei Methoden realisiert werden:

1. Unter https://www.bundesdruckerei.de/ auf den Unterseiten „Roots und CRLs" die CRLs mittels Browser herunter laden.
2. LDAP der Bundesdruckerei: ldap://directory.d-trust.net

   Folgende in verschiedenen Clients abgefragten Angaben gelten für den D-TRUST-Verzeichnisdienst:

   - Servername/Hostname: directory.d-trust.net
   - Anschluss/Port-Nr: 389
   - Suchbasis/Basis-DN: c=de
   - keine verschlüsselte Verbindung, keine Anmeldung erforderlich
   - Der CRL Name entspricht dem CA Namen

4.3.4 Schnittstelle < P_SPERRLISTE_PQES_ INTERNET >

Diese Schnittstelle wird nicht genutzt bzw. benötigt.

4.3.5 Schnittstelle < I_SPERRSTATUS_PQES_TI >

4.3.5.1 Schnittstellendefinition

Diese Schnittstelle repräsentiert den OCSP-Dienst des TSP, d.h. der Status eines von der pseudoQES-CA ausgegebenen Zertifikats kann hier online geprüft werden.

4.3.5.2 Umsetzung

Der OCSP-Responder erfüllt die Common PKI 2.0 Part 9 Tabelle13 (#4) und kann somit zusätzlich positive Auskünfte liefern. Die Antwort ist mittels des zur OCSP-Signer-CA der zentralen PKI gehörenden separaten OCSP-Signers gesichert.

4.3.5.3 Nutzung

Der OCSP-Responder kann über die aktuell noch nicht bekannte, später aber veröffentlichte Adresse für Statusabfragen mittels des http-Protokolls abgefragt werden.

4.3.6 Schnittstelle < P_SPERRSTATUS_PQES_TI >

Diese Schnittstelle wird nicht genutzt bzw. benötigt.

4.4 Funktionsmerkmal TSP X.509 QES in der Ausprägung HBA (PU)

4.4.1 Schnittstelle < I_SPERRSTATUS_QES_INTERNET >

4.4.1.1 Schnittstellendefinition

Diese Schnittstelle repräsentiert den OCSP-Dienst des TSP, d.h. der Status eines von der QES-CA ausgegebenen Zertifikats kann hier online geprüft werden.

4.4.1.2 Umsetzung

Der OCSP-Responder erfüllt die Common PKI 2.0 Part 9 Tabelle13 (#4)und kann somit zusätzlich positive Auskünfte (Positive Statement) liefern. Die Antwort ist mittels des zur OCSP-Signer-CA der zentralen PKI gehörenden separaten OCSP-Signers gesichert.

4.4.1.3 Nutzung

Der OCSP-Responder kann über ocsp.d-trust.net mittels des http-Protokolls abgefragt werden.

4.4.2 Schnittstelle < P_SPERRSTATUS_QES_INTERNET >

Diese Schnittstelle wird nicht genutzt bzw. benötigt.

4.4.3 Schnittstelle < I_SPERRLISTE_QES_ INTERNET >

4.4.3.1 Schnittstellendefinition

Diese Schnittstelle beschreibt die Möglichkeit zum Download der Sperrliste beim TSP.

4.4.3.2 Umsetzung

Die Sperrliste wird in Form einer X.509 CRLv2-Datei jeweils „DER" und „PEM" codiert angeboten. Die CRL ist mittels des zur CRL-Signer-CA der zentralen PKI gehörenden separaten CRL-Signers gesichert.

4.4.3.3 Nutzung

Der Download kann über zwei Methoden realisiert werden:

1. Unter https://www.bundesdruckerei.de/ auf den Unterseiten „Roots und CRLs" und die CRLs mittels Browser herunter laden.
2. LDAP der Bundesdruckerei: ldap://directory.d-trust.net

   Folgende in verschiedenen Clients abgefragten Angaben gelten für den D-TRUST-Verzeichnisdienst:

   - Servername/Hostname: directory.d-trust.net
   - Anschluss/Port-Nr: 389
   - Suchbasis/Basis-DN: c=de
   - keine verschlüsselte Verbindung, keine Anmeldung erforderlich
   - Der CRL Name entspricht dem CA Namen

4.4.4 Schnittstelle < P_SPERRLISTE_QES_ INTERNET >

Diese Schnittstelle wird nicht genutzt bzw. benötigt.

4.4.5 Schnittstelle < I_SPERRSTATUS_QES_TI >

4.4.5.1 Schnittstellendefinition

Diese Schnittstelle repräsentiert den OCSP-Dienst des TSP, d.h. der Status eines von der QES CA ausgegebenen Zertifikats kann hier online geprüft werden.

4.4.5.2 Umsetzung

Der OCSP-Responder erfüllt die Common PKI 2.0 Part 9 Tabelle13 (#4) und kann somit zusätzlich positive Auskünfte liefern. Die Antwort ist mittels des zur OCSP-Signer-CA der zentralen PKI gehörenden separaten OCSP-Signers gesichert.

4.4.5.3 Nutzung

Der OCSP-Responder kann über die aktuell noch nicht bekannte, später aber veröffentlichte Adresse für Statusabfragen mittels des http-Protokolls abgefragt werden.

4.4.6 Schnittstelle < P_SPERRSTATUS_QES_TI >

Diese Schnittstelle wird nicht genutzt bzw. benötigt.

5 Verteilungssicht

Eine gesonderte Darstellung der hardwareseitigen Verteilung und der Einbettung in die physikalische Umgebung wird nicht benötigt.

Anhang A

A1 – Abkürzungen

Kürzel	Erläuterung
BDr	Bundesdruckerei GmbH
CA	Certificate Authority
CRL	Certificate Revocation List (Zertifikatsperrliste)
DER	Distinguished Encoding Rules
KK	Krankenkasse
LDAP	Lightweight Directory Access Protocol
LEO	Leistungserbringerorganisation
OCSP	Online Certificate Status Protocol
PEM	Privacy-Enhanced Mail
QES	qualifizierte elektronische Signatur
TI	Telematikinfrastruktur

A2 – Glossar

Begriff	Erläuterung
Serviceportal der BDr	Dieses Portal enthält die verschiedenen personalisierten Serviceangebote im Internet und kann unter https://support.bundesdruckerei.de/ aufgerufen werden. Umsetzung während der Betrieszeiten 9:00-17:00
Sperrhotline der BDr	24*7 Betrieb: 030 / 25 93 91 600

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

A3 – Abbildungsverzeichnis

A4 – Tabellenverzeichnis

A5 - Referenzierte Dokumente

A5.1 – Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemSpec_KP]	Spezifikation Kartenpersonalisierung
[gemSpec_TSP_X.509]	Spezifikation Trust Service Provider X.509

[Quelle]	Herausgeber: Titel
[gemSpec_CVC_TSP]	Spezifikation Trust Service Provider CVC
[gemRL_TSL_SP_CP]	Certificate Policy; Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL
[gemGlossar]	Glossar der Telematikinfrastruktur

A5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[Common PKI V.2.0]	COMMON PKI SPECIFICATIONS FOR INTEROPERABLE APPLICATIONS FROM T7 & TELETRUST (2012)
[SigG]	Gesetz über Rahmenbedingungen für elektronische Signaturen (2001)
[SigV]	Verordnung zur elektronischen Signatur (2001)
[RFC 2119]	IETF: Key words for use in RFCs to Indicate Requirement Levels

A6 – Klärungsbedarf

Kap.	Offener Punkt	Zuständig
4.2.5.3, 4.3.5.3, 4.4.5.3	URL für Statusabfragen in der TI unklar	gematik

Anhang B

Schema „CertficateRequestDataExample.xml“ als ZIP-File

XSD Dateien
Schnittstellenspezifika