Einführung der Gesundheitskarte

Schnittstellen- und Prozessspezifikation TSP X509 und **CVC**

HPC-TSP T-Systems

Version:	1.1.0
Revision:	\main\rel_ors1\2
Stand:	06.06.2014
Status	Freigegeben
Klassifizierung:	öffentlich
Referenzierung	[HPC002]

Dokumentinformationen

Änderungen zur Vorversion

Letzte Korrektur nach Freigabe

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.0.1	23.11.2013		Erste Gliederung	SK
0.0.2	06.12.2013		Übernahme XML-Schema, grobe Beschreibung Registrierung	SK
0.0.3	17.12.2013		Detaillierung nach Rückmeldung der gematik und Abstimmung mit den G2 Losen 1 und 2	SK
0.0.4	18.12.2013		QS	DD
0.0.5	19.12.2013		Einarbeitung der Anmerkungen aus der ersten QS, Vorlage zur zweiten QS bei G2-Losen 1 und 2, sowie interne QS	SK
0.0.6	20.12.2013		Einarbeitung der Anmerkungen aus der internen QS und G2-Los1 Version zur Güteprüfung bei der gematik	SK
0.0.7	24.01.2014		Einarbeitung der Rückmeldungen zur Güteprüfung, Vorlage zur internen QS	SK
0.1.0	27.01.2014		interne QS	DD, AW
0. 9.0	27.01.2014		Einarbeitung der Anmerkungen aus der internen QS. Version zur Güteprüfung bei der gematik	SK
0.9.1	17.02.2014		Einarbeitung der Rückmeldungen zur Güteprüfung	SK
1.0.0	07.03.2014		Letzte Korrektur nach Freigabe	SK
1.0.1	06.06.2014		Update auf Basistypen aus TKDÜS 1.6	OB
1.1.0	06.06.2014		QS	TV

Inhaltsverzeichnis

1 Einführung

1.1 Zielsetzung

Die vorliegende Spezifikation beschreibt die Schnittstellen und Formate sowie die Prozesse zur Beantragung von Zertifikaten für Testkarten und HSM-B (Test und Produktiv).

1.2 Zielgruppe

Das Dokument richtet sich an die G2-Lose 1 und 2, welche diese Schnittstelle zur Beantragung von Testzertifikaten bei Los 3 nutzen, sowie die ORS1-Lose 1 und 2, welche über diese Schnittstelle Zertifikate für die HSM-B bei Los 3 beantragen. Für diese Lose ist das Dokument normativ.

Informativ richtet sich das Dokument auch an die G2-Lose 4 und 5, welche analog zu G2-Los 3 den o.g. Losen Zertifikate zur Verfügung stellen können. Es wird im Sinne der Vereinheitlichung der Schnittstellen und der Reduzierung des Gesamtaufwandes für die betroffenen Lose empfohlen, die gleichen Schnittstellen zu nutzen bzw. anzubieten.

1.3 Geltungsbereich

Das Dokument gilt im Bereich der Erprobung in ORS1.

1.4 Abgrenzung des Dokuments

Dieses Dokument beschreibt den Austausch der Daten und das Datenformat der übermittelten Daten sowie die Prozesse bei G2-Los 3. Es werden keine Vorgaben zu den Prozessen zur Erstellung der Datensätze durch den Sender oder der Prüfung der Daten durch die Empfänger gemacht, diese Prüfungen liegen in der Verantwortung des jeweiligen Loses.

2 Überblick: Schnittstellen und Prozesse

2.1 Datenaustausch per Offline-Schnittstelle

Die Schnittstelle zur Beantragung und Übergabe von Zertifikaten zwischen den Losen „G2 Los 1/2" und „ORS1-Los 1/2" als Antragsteller und Empfänger der Zertifikate und „G2 Los 3" wird als XML-basierte Datei-Schnittstelle abgebildet, d.h.

- die Requests/Zertifikatsanträge werden als XML-Datei an G2-Los 3 übergeben und
- die Responses/Zertifikate werden als XML-Datei von G2-Los 3 zurück geliefert.

Die Übergabe der Dateien erfolgt dabei signiert und ggf. verschlüsselt zwischen registrierten Antragstellern und G2-Los 3 (nachfolgend allgemein „TSP" genannt), d.h. der Austausch der Daten erfolgt Offline.

Die nachfolgende Grafik gibt einen Überblick über den Gesamtprozess, die Details sind in den darauf folgenden Kapiteln beschrieben.

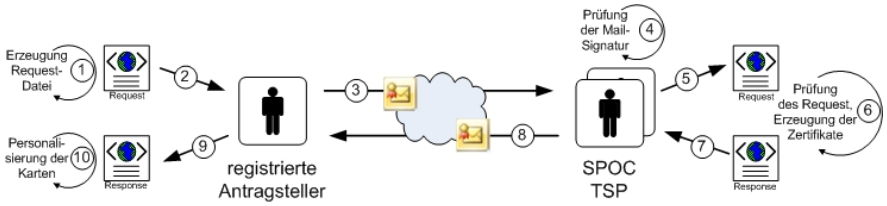

Abbildung 1: Übersicht Ausgabeprozess

Hinweise:

- Es sind verschiedene Varianten von Request- und Response-Dateien definiert. Die Varianten unterscheiden sich insbesondere dadurch, ob Antragsteller oder TSP die Schlüssel generieren und in welcher Form die Schlüssel (Plaintext oder PKCS#10-Request) übergeben werden. Die Varianten werden in Kap. 5.1 näher beschrieben.
- Die konkreten Adressen und Ansprechpartner der Endpunkte werden im Rahmen der Registrierung (siehe Kap. 3) bilateral zwischen Antragstellern und TSP abgestimmt. Die Kontakte des SPOC des TSP zur ersten Kontaktaufnahme und Abstimmung der Prozesse sind in Kap. 3.1 aufgeführt.

2.2 Rollen

In dem oben beschriebenen Beantragungs- und Ausgabeprozess werden folgende Rollen berücksichtigt:

- Personalisierer: Mitarbeiter der G2-Lose 1 und 2 sowie ORS1-Lose 1 und 2, welche aus den Personalisierungsdaten die Antragsdaten für die Zertifikate extrahieren und daraus die Request-Dateien erstellen und aus den Response-Dateien die Zertifikate extrahieren und diese in die Karten schreiben (personalisieren).

- Antragsteller: Mitarbeiter der G2-Lose 1 und 2 sowie ORS1-Lose 1 und 2, welche als berechtigte Antragsteller registriert sind und die Requestdateien per signierter E-Mail dem TSP übergeben und die Responsedateien des TSP entgegennehmen.
- SPOC des TSP: Der SPOC des TSP ist für G2 Los 3 im providerspezifischen Betriebskonzept als einzige Schnittstelle des TSP für Anwender und andere Service-Provider der TI definiert und wird auch zur Beantragung der Zertifikate über die hier beschriebenen Prozesse ausschließlich genutzt.

2.3 Voraussetzungen für die Beantragung von Zertifikaten

Die Beantragung von Zertifikaten setzt voraus, dass die Antragsteller initial registriert wurden und berechtigt sind, Zertifikate zu beantragen.

Die Registrierung der Antragsteller wird in Kap. 3 beschrieben. Die Berechtigung wird an das im Rahmen der Registrierung vereinbarte X.509-Zertifikat des Antragstellers geknüpft, mit dem die E-Mail signiert wird. Zur Prüfung der Anträge siehe Kap. 4.2.

Die in den Beantragungs- und Ausgabeprozessen definierten Rollen sind in Kap. 2.2 beschrieben.

Den Antragstellern werden die E-Mail Adresse(n) und die E-Mail Zertifikate der zuständigen Instanz beim TSP (Single Point of Contact, SPOC) bei der Registrierung mitgeteilt, siehe Kap.3.

2.4 Übersicht: Beantragungs- und Ausgabeprozess

Der Beantragungs- und Ausgabeprozess läuft gemäß Abbildung 1 grundsätzlich wie folgt ab:

1. Der Personalisierer erzeugt die Request-Datei als XML-Datei gemäß dem in Kap. 5.2.2 definierten Schema.

   Hinweis: Dieser Prozess ist nicht im Scope dieses Dokuments und unterliegt den internen Vorgaben des Personalisierers, er wird daher nicht näher betrachtet.

2. Der Personalisierer übergibt diese Datei an einen zuständigen, beim TSP registrierten Mitarbeiter, der gegenüber dem TSP als Antragsteller auftritt.

   Hinweis: Dieser Prozess ist nicht im Scope dieses Dokuments und unterliegt den internen Vorgaben des Personalisierers, er wird daher nicht näher betrachtet.

3. Der Antragsteller packt die XML-Request-Datei als Anlage an eine E-Mail und sendet diese signiert und ggf. verschlüsselt an den SPOC des TSP (siehe Kap. 4.1).

4. Ein Mitarbeiter des TSP (SPOC) prüft die Berechtigung des Antragstellers anhand der Mailsignatur (siehe Kap. 4.2) und extrahiert die Request-Datei.

5. Anschließend stellt der Mitarbeiter des TSP die Request-Datei zur Verarbeitung im CA-System des TSP ein.

   Hinweis: Dieser Prozess ist nicht im Scope dieses Dokuments und unterliegt den internen Vorgaben des TSP, er wird daher nicht näher betrachtet.

6. Im CA-System werden die Zertifikate erzeugt, und in einer Response-Datei gemäß Kap. 5.2.3 zur Verfügung gestellt.

   Hinweise:

   - Testzertifikate können sofort, d.h. ohne weitere Freigabe durch eine Leistungserbringer-Organisation ausgestellt werden. Bei der Erzeugung von Produktiv-Zertifikaten für die HSM-B ist vor Ausstellung der Zertifikate eine Freigabe durch die entsprechende Leistungserbringer-Organisation erforderlich.
   - Diese Prozesse sind nicht im Scope dieses Dokuments und unterliegen den Vorgaben des TSP, sie werden daher nicht näher betrachtet.

7. Der Mitarbeiter des TSP lädt die Response-Datei aus dem CA-System und packt diese als Anlage in eine Antwortmail auf die ursprüngliche E-Mail mit der korrespondierenden Request-Datei.

   Hinweis: Dieser Prozess ist nicht im Scope dieses Dokuments und unterliegt den internen Vorgaben des TSP, er wird daher nicht näher betrachtet.

8. Der Mitarbeiter des TSP sendet die E-Mail signiert und verschlüsselt an den Sender der ursprünglichen E-Mail (siehe Kap. 4.3).

9. Der Empfänger der Response-Mail prüft den Absender der Antwortmail anhand der Signatur der E-Mail, extrahiert die Response-Datei aus der E-Mail und übergibt diese dem Personalisierer.

   Hinweis: Dieser Prozess ist nicht im Scope dieses Dokuments und unterliegt den internen Vorgaben des Personalisierers, er wird daher nicht näher betrachtet.

10. Der Personalisierer extrahiert die Zertifikate (und ggf. die Schlüssel) aus der Response-Datei, prüft diese ggf. und schreibt sie im Rahmen der Personalisierung in die korrespondierenden Karten.

    Hinweis: Dieser Prozess ist nicht im Scope dieses Dokuments und unterliegt den internen Vorgaben des Personalisierers, er wird daher nicht näher betrachtet.

Hinweise zur Nutzung der E-Mail-Schnittstelle und zur Verschlüsselung:

- Bei Beantragung von Testzertifikaten kann die Verschlüsselung entfallen, für die Beantragung von Produktiv-Zertifikaten ist sie obligatorisch.
- Sollte ein Personalisierer aufgrund der Systemvoraussetzungen keine signierten oder verschlüsselten E-Mails austauschen können, so können alternativ andere Kommunikationsschnittstellen bilateral zwischen dem Personalisierer und dem TSP vereinbart werden, dabei gelten jedoch folgende Grundsätze:
  - Die Sicherheit der Übermittlung muss das gleichen Niveau haben, d.h. die Daten müssen signiert und ggf. verschlüsselt übergeben werden können.
  - Das Format der übergebenen Request- und Response-Dateien bleibt davon unberührt.

3 Registrierung der Antragsteller

Wie in Kap. 2.1 beschrieben, erfolgt der Austausch der Request- und Response-Dateien per signierter und ggf. verschlüsselter E-Mail. Da die E-Mail-Zertifikate nur von berechtigten Antragstellern beantragt werden dürfen, müssen diese einmalig identifiziert und registriert werden. Dazu sind folgende Schritte erforderlich:

1. Benennung der Antragsteller:

   Die zur Beantragung von Zertifikaten berechtigten Antragsteller werden im Rahmen der Los-übergreifenden Projektkommunikation zwischen den Projekten ORS1 und G2 benannt.

2. Bereitstellung der Registrierungsunterlagen für den Antragsteller:

   Über den SPOC des TSP (siehe Kap. 3.1) werden den benannten Antragstellern eine Prozessbeschreibung sowie die benötigten Registrierungsunterlagen (PDF-Formulare zur Angabe von Identifizierungs- und Registrierungsdaten sowie der Vereinbarung der zu verwendenden X.509-Zertifikate, siehe dazu auch Kap.3.2) bereitgestellt.

3. Übergabe der Registrierungsunterlagen an den TSP:

   Diese Formulare müssen durch die benannten Antragsteller ausgefüllt, ausgedruckt und unterschrieben werden. Bei der Übergabe der Formulare müssen die Mitarbeiter persönlich identifiziert werden, dazu gibt es folgende Varianten:

   1. Persönliche Übergabe des Formulars: Die Identifizierung des Antragstellers erfolgt durch Vorlage eines gültigen amtlichen Ausweisdokuments bei der persönlichen Übergabe des Formulars an den TSP.

   2. PostIdent: Der Mitarbeiter sendet das Formular per PostIdent zum TSP.

      Hinweis: Das benötigte Formular für das Postident-Verfahren ist in dem bereitgestellten PDF (siehe Schritt 2) enthalten

4. Prüfung der Unterlagen und Registrierung der Antragsteller:

   Die Formulare werden durch den TSP geprüft. Nach erfolgreicher Prüfung werden die benannten Mitarbeiter als berechtigte Antragsteller beim TSP registriert und darüber informiert. Mit der Information übergibt der TSP dem Antragsteller auch die Verschlüsselungszertifikate des TSP für die Mailkommunikation.

3.1 Kontakte des SPOC des TSP

Der SPOC des TSP T-Systems ist für alle Betriebsumgebungen wie folgt erreichbar:

- Telefon: 0271/708-1699
- E-Mail: trustcenter.notary@t-systems.com

3.2 S/MIME-Zertifikate der Antragsteller

Wie in Kap. 2.3 und 4.2 beschrieben, benötigen die Antragsteller ein X.509-Zertifikat eines vertrauenswürdigen Anbieters zur Signatur und ggf. Verschlüsselung der E-Mail-Kommunikation.

Die erforderlichen Zertifikate können vom TSP bereit gestellt werden, sofern die Antragsteller noch nicht über entsprechende Zertifikate verfügen, siehe dazu Kap. 3.2.1.

Sollten die Antragsteller aber bereits Zertifikate eines vertrauenswürdigen Anbieters besitzen, die für die Absicherung der E-Mail-Kommunikation genutzt werden können (z.B. im Rahmen einer Corporate PKI) so können diese Zertifikate verwendet werden, siehe dazu Kap. 3.2.2.

Unabhängig davon, ob die Zertifikate vom TSP ausgestellt werden oder bereits vorhanden sind, gelten die gleiche Vorgaben zur Vereinbarung der zu verwendenden Zertifikate für die Absicherung der E-Mail-Kommunikation:

- Der Antragsteller definiert im Registrierungsformular das Zertifikat, das verwendet werden soll und macht dazu folgende Angaben:
  - Aussteller des Zertifikats,
  - Seriennummer des Zertifikats,
  - Fingerprint des Zertifikats (Hashwert).
- Ergänzend zu den Angaben zum Zertifikat im Formular sendet der Antragsteller das Zertifikat (inkl. der Aussteller-Zertifikate als ZIP-File) per E-Mail unter Bezugnahme auf die Registrierung an den SPOC des TSP.
- Der TSP prüft nach Eingang des Zertifikats und des korrespondierenden Formulars die Angaben und das Zertifikat und bindet es zum Kontakt des Antragstellers im E-Mail-System ein, so dass es ggf. zur Verschlüsselung und Prüfung der Signatur (über die mitgelieferte Zertifikatskette) genutzt werden kann.

3.2.1 Bezug von X.509-Zertifikaten des TSP

Sollten die Antragsteller noch nicht über nutzbare X.509-Zertifikate zur Absicherung der E-Mail-Kommunikation verfügen, so können sie diese über eine Dienstleistung des TSP beziehen. Die Beantragungsprozesse werden bilateral zwischen dem TSP und dem Antragsteller abgestimmt, der Antragsteller wendet sich dazu bei Bedarf an den SPOC des TSP.

3.2.2 Nutzung bereits vorhandener X.509-Zertifikate des Antragstellers

Sollten die Antragsteller bereits über nutzbare X.509-Zertifikate zur Absicherung der E-Mail-Kommunikation verfügen, so können sie diese verwenden, sofern der Aussteller der Zertifikate vom TSP als vertrauenswürdig eingestuft wird (liegt im Ermessensspielraum des TSP).

4 Übergabeschnittstelle

4.1 Übergabe der Anträge und Antragsdaten

Nach erfolgreicher Registrierung (siehe Kap. 3) können Zertifikate durch die registrierten Antragsteller beantragt werden. Die Antragsteller senden dazu die Request-Dateien als Anhänge von E-Mails an den SPOC des TSP. Das Format der E-Mails wird in den folgenden Kapiteln beschrieben.

4.1.1 Empfänger

Aufgrund des verschlüsselten Austauschs der E-Mails können die E-Mails ggf. nicht an ein Funktionspostfach sondern nur an persönliche E-Mail-Accounts der Mitarbeiter des SPOC des TSP gesendet werden. Die zu verwendenden E-Mail-Adressen und damit verknüpfte Zertifikate zur E-Mailverschlüsselung werden im Rahmen der Registrierung der Antragsteller (siehe Kap. 3) bilateral zwischen den Antragstellern und dem TSP vereinbart.

4.1.2 Betreffzeile

Zur Zuordnung (im Sinne einer späteren Nachvollziehbarkeit) der Request-Dateien zu den Request-Mails und der entsprechenden Betriebsumgebung müssen die Betreffzeilen der E-Mails den Namen der korrespondierenden Request-Datei beinhalten und durch den Zusatz „REQUEST“ sowie „TEST“ oder „PROD“ vor dem Dateinamen wie folgt gekennzeichnet werden:

- Requests für Testzertifikate:

  Betreff: TEST REQUEST *<Dateiname gemäß Kap. 5.2.2.1>*

- Requests für Produktivzertifikate:

  Betreff: PROD REQUEST *<Dateiname gemäß Kap. 5.2.2.1>*

4.1.3 Signatur

Die Signatur der E-Mails erfolgt gemäß S/MIME-Standard mit dem bei der Registrierung vereinbarten X.509-Zertifikat des Antragstellers.

4.1.4 Verschlüsselung

Die E-Mails werden mit den vom TSP bereit gestellten Verschlüsselungs-Zertifikaten (siehe Kap. 3 und 4.1.1) gemäß S/MIME-Standard verschlüsselt

Hinweis: Bei Beantragung von Testzertifikaten kann die Verschlüsselung der E-Mails entfallen, für die Beantragung von Produktiv-Zertifikaten ist sie obligatorisch.

4.2 Bearbeitung der Anträge

Nach dem Eingang der Request-Mail überprüft ein Mitarbeiter des TSP den Absender und die Signatur der E-Mail. Wenn die E-Mail von einem berechtigten Antragsteller gesendet wurde und die Signaturprüfung erfolgreich ist, extrahiert der Mitarbeiter die Request-Datei aus der E-Mail und stellt Sie in das CA-System zur Erzeugung der Zertifikate.

Vor der Verarbeitung durch die CA erfolgt eine Plausibilitätsprüfung der Request-Datei. Sollte diese nicht den Vorgaben entsprechen, so wird eine Fehlermeldung mit entsprechenden Hinweisen angezeigt, welche der Mitarbeiter des TSP dem Antragsteller in einer Antwortmail als Rückmeldung zur Information zusendet, siehe dazu Kap. 4.2.1.

Sollte die Plausibilitätsprüfung erfolgreich sein, so wird der Auftrag zur Freigabe weitergegeben. Bei der Freigabe wird zwischen Test- und Produktivdaten wie folgt unterschieden:

- Anträge für Testzertifikate können direkt nach Prüfung der Plausibilität durch den Mitarbeiter des TSP freigegeben werden.
- Anträge für Produktivzertifikate (nur für HSM-B relevant) müssen erst durch die zuständige Leistungserbringer-Organisation freigegeben werden. Diese erhalten vom TSP eine E-Mail-Notification, dass ein neuer Antrag zur Freigabe vorliegt. Die Freigabe erfolgt analog zur Freigabe von HBA und SMC-B über das Freigabeportal der TSP-Schnittstelle, d.h. dieser Prozess liegt nicht im Fokus dieses Dokuments, es wird daher an dieser Stelle nicht näher auf den Freigabeprozess eingegangen.

Nach Freigabe der Anträge werden die Zertifikate erzeugt und in Form einer Response-Datei gemäß Kap. 5.2.3 dem Mitarbeiter des TSP zur Verfügung gestellt. Die Übergabe ist in Kap. 4.3 beschrieben.

4.2.1 Rückmeldung über fehlerhafte Request-Datei

Wenn die übermittelte Request-Datei fehlerhaft sein sollte, so informiert der Mitarbeiter des TSP den Antragsteller in einer Antwortmail darüber und gibt dabei soweit möglich die Fehlerbeschreibung mit an.

Zur Zuordnung (im Sinne einer späteren Nachvollziehbarkeit) der Antwortmail zur ursprünglichen Request-Mail wird in der Betreffzeile der E-Mail neben dem Dateinamen der Request-Datei der Hinweis auf einen Fehler wie folgt dargestellt:

Betreff: RÜCKMELDUNG: FEHLER <*Dateiname gemäß Kap. 5.2.2.1*>

4.3 Übergabe der Zertifikate

Nach einer erfolgreichen Produktion lädt ein Mitarbeiter des TSP die Response-Datei aus dem CA-System und packt sie als Anhang in eine signierte und ggf. verschlüsselte Antwortmail an den Antragsteller. Das Format der E-Mails wird in den folgenden Kapiteln beschrieben.

4.3.1 Empfänger

Als Empfänger der Antwortmail wird standardmäßig der ursprüngliche Antragsteller, d.h. der Sender der Request-Mail verwendet, sofern vom Antragsteller kein anderer berechtigter Empfänger (z.B. ein Funktionspostfach des Personalisierers) benannt wurde.

4.3.2 Betreffzeile

Zur Zuordnung (im Sinne einer späteren Nachvollziehbarkeit) der Response-Dateien zu den Request-Mails und der entsprechenden Betriebsumgebung müssen die Betreffzeilen der E-Mails den Namen der korrespondierenden Request-Datei beinhalten und durch den Zusatz „RESPONSE“ sowie „TEST“ oder „PROD“vor dem Dateinamen wie folgt gekennzeichnet werden:

- Response für Testzertifikate:

  Betreff: TEST RESPONSE <*Dateiname gemäß Kap. 5.2.3.1*>

- Response für Produktivzertifikate:

  Betreff: PROD RESPONSE <*Dateiname gemäß Kap. 5.2.3.1*>

4.3.3 Signatur

Die Signatur der Mails erfolgt gemäß S/MIME-Standard mit dem X.509-Zertifikat des TSP-Mitarbeiters.

4.3.4 Verschlüsselung

Die E-Mails werden mit dem im Rahmen der Registrierung mit dem Antragsteller vereinbarten Verschlüsselungs-Zertifikaten (siehe Kap. 3.2 und 4.1.1) gemäß S/MIME-Standard verschlüsselt.

Hinweis: Bei Versand von Testzertifikaten kann die Verschlüsselung der E-Mails entfallen, für den Versand von Produktiv-Zertifikaten ist sie obligatorisch.

5 Beschreibung der XML-Struktur

Die Request- und Response-Dateien sind als XML-Dateien gemäß einem zwischen den betroffenen ORS1- und G2-Losen abgestimmten Schema aufgebaut.

Die Ausgangsstruktur für dieses Schema bildet der von der gematik bei den „G1-Karten“ verwendete Personalisierungsdatensatz (xmlschema\cm\pers\gematik_TK_Auftrag.xsd) in Version 1.6. Dieser wurde auf die für die Zertifikatsproduktion erforderlichen Angaben reduziert und angepasst, so dass sich daraus zwei neue Schemata ergeben:

- CertificateRequest.xsd und
- CertificateResponse.xsd.

Für diese beiden Schema-Dateien wurde der Namespace „http://hpc.telesec-gud.de/testcert-hsmb/v1.0“ definiert. Es werden darin Typen der TKDÜS aus dem Namespace „http://ws.gematik.de/cm/pers/testkarten/v1.6“ verwendet. Über Änderungen an gematik_TK_Keys.xsd oder gematik_TK_Typen.xsd sind die Nutzer der hier beschriebenen Schnittstelle durch die gematik zu informieren. Von Änderungen an gematik_TK_Auftrag.xsd ist die Schnittstelle hingegen nicht betroffen.

Die beiden Schema-Dateien werden den beteiligten Personalisierern im Rahmen der übergreifenden Projektkommunikation zwischen den verschiedenen Losen von ORS1 und G2 zur Verfügung gestellt und dienen somit als eindeutige Referenz für die Implementierung.

5.1 Varianten der Request- und Response-Dateien

Zur Beantragung und Ausstellung der Zertifikate werden drei Varianten angeboten:

- Variante A: Schlüsselerzeugung beim Antragsteller, siehe Kap. 5.1.1..
  - Variante A1: Übergabe der Schlüssel als Plaintext (nur für Testzertifikate für eGK, HBA und SMC-B)
  - Variante A2: Übergabe der Schlüssel innerhalb von PKCS#10-Requests (für Test- und Produktivzertifikate HSM-B)
- Variante B: Schlüsselerzeugung beim TSP, siehe Kap. 5.1.2. (nur für Testzertifikate für eGK, HBA und SMC-B).

Diese Varianten sind erforderlich, da zum einen in der Testkartenspezifikation [gemSpec_TK] die Übergabe der Schlüssel mit den Zertifikaten definiert ist (Variante B), zum anderen aber bei Produktivzertifikaten die Private Keys nicht über die in diesem Dokument beschriebene Schnittstelle übertragen werden dürfen, sondern bei dem Personalisierer bzw. durch die Karten selbst erzeugt werden müssen (Variante A).

Die sich daraus ergebenden Optionen für die XML-Struktur sind in den Kap. 5.2.2.2 und 5.2.3.2 beschrieben.

5.1.1 Variante A: Schlüsselerzeugung beim Antragsteller

In dieser Variante werden die Schlüssel beim Personalisierer/Antragsteller erzeugt, so dass die Public Keys zusammen mit den Antragsdaten mit der Request-Datei übergeben werden. Der TSP erzeugt die Zertifikate auf Basis der mitgelieferten Schlüssel und übergibt in der Response-Datei nur die Zertifikate.

5.1.2 Variante B: Schlüsselerzeugung beim TSP

In dieser Variante werden die Schlüssel für die Zertifikate beim TSP erzeugt, so dass mit dem Request nur die Antragsdaten, aber keine Public Keys übergeben werden. Der TSP erzeugt dann die Schlüssel und Zertifikate in einem Schritt und liefert in der Response-Datei neben den Zertifikaten auch die Private Keys mit.

5.2 Format der Dateien

5.2.1 Grundsätzliche Anforderungen

Für die Request-Dateien (und somit indirekt auch für die Response-Dateien) gelten folgende grundsätzlichen Anforderungen:

- Je Request-Datei kann nur eine Variante der Schlüsselerzeugung (siehe Kap. 5.1) genutzt werden.
- Je Request-Datei können nur Zertifikate für einen Kartentyp beantragt werden.
- Je Karte werden alle Zertifikate in einem Request beantragt.

Beide Parameter werden im Header der Datei unter „Order“ festgelegt.

5.2.2 Format der Request-Dateien

Die Request-Dateien bestehen aus folgenden Elementen:

- Header: Definition der Request-Datei, einmalig je Antrag, bestehend aus den Elementen *CertificateRequest* und *Order* sowie der Variante der Schlüsselgenerierung *publicKeysIncluded und pkcs10Included*, siehe dazu Kap. 5.2.2.2.
- *CardData*: Daten für jede Karte, für die Zertifikate in dem Request beantragt werden. *CardData* besteht jeweils aus der *ICCSN* als eindeutiges Zuordnungskriterium der beantragten Zertifikate zur Karte, der laufenden Nummer *LfdNo* zur eindeutigen Zuordnung der Karte innerhalb der Request-Datei und den Zertifikatsrequests als *CVRequest* oder *X.509Request* zu dieser Karte.

- *CVRequest*: Request-Daten für ein CV-Zertifikat, bestehend aus folgenden Elementen:
  - *FlagList*: Liste der zu setzenden Flags.
  - *ValidNotBefore* und *ValidNotAfter*: Gültigkeitszeitraum des Zertifikats.
  - *Profilnummer*: Profil des Zertifikats.
  - *CVCertName*: angefordertes Zertifikat (Typ und Schlüssellänge).
  - *PublicKey*: öffentlicher Schlüssel.
  - *PKCS10*: PKCS#10-Request

- X.509Request: Request-Daten für ein X.509-Zertifikat, bestehend aus folgenden Elementen:
  - *ValidNotBefore* und *ValidNotAfter*: Gültigkeitszeitraum des Zertifikats.
  - *SubjectDN*: Daten des Zertifikatsinhabers, abhängig vom Karten- und Zertifikatstyp werden hier verschiedene Attribute beschrieben.
  - *X.509CertName*: angefordertes Zertifikat (Typ und Schlüssellänge).
  - *Extensions*: Werte für die variablen Zertifikatserweiterungen.
  - *PublicKey*: öffentlicher Schlüssel.
  - *PKCS10*: PKCS#10-Request

Die exakte Definition ist der Schemadatei CertificateRequest.xsd zu entnehmen.

5.2.2.1 Dateinamen der Request-Dateien

Der Dateiname der Request-Datei muss den Namen des Antrag stellenden Personalisierers, das Datum und die Auftragsnummer sowie den Dateityp „request“ und die Betriebsumgebung in folgendem Format enthalten:

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

Beispiel: T-Systems_2013-12-19_123_TEST_request

5.2.2.2 Optionen für die Schlüsselerzeugung

Wie in Kap. 5.1 beschrieben werden drei Varianten der Schlüsselerzeugung und-Übergabe unterschieden. Die Variante wird im Header in den Tags *publicKeysIncluded und pkcs10Included* definiert:

- *publicKeysIncluded* = *true* bedeutet, dass die Schlüssel durch den Personalisierer/ Antragsteller erstellt wurden und dementsprechend in den Tags *PublicKey* oder *PKCS10* enthalten sind (Variante A). In diesem Fall wird die Übergabe der öffentlichen Schlüssel zusätzlich durch das Tag *pkcs10Included* definiert:
  - *pkcs10Included* = *true* bedeutet, dass die Schlüssel innerhalb von PKCS#10-Requests übergeben werden (Variante A2),
  - *pkcs10Included* = *false* bedeutet, dass die Schlüssel als Plaintext übergeben werden (Variante A1).
- *publicKeysIncluded* = *false* bedeutet, dass die Schlüssel durch den TSP erzeugt werden sollen, dementsprechend bleiben die Tags *PublicKey* leer (Variante B).

5.2.2.3 Inhalte der PKCS#10-Requests

Wenn die Requests im PKCS#10-Format übergeben werden, so müssen diese neben den öffentlichen Schlüsseln die Werte der Attribute beinhalten, die individuell je Zertifikat gesetzt werden:

- Bei X.509-Zertifikaten sind das der *Subject-DN* und (falls gesetzt) der *SubjectAltName*. Diese werden im PKCS#10-Request mit den standardisierten Attributen gemäß [RFC2986] übergeben.
- Bei CV-Zertifikaten ist das der CHR. Dieser wird als *subject* im Request-Feld *certificationRequestInfo* übergeben. In Anlehnung an [SRQ_1201] wird für das Attribut die folgende OID verwendet: 1.3.6.1.4.1.4788.4.2.1.

  Hinweis: Die o.g. OID bezeichnet lt. [SRQ_1201] eigentlich den CA-Namen als einen Bestandteil des CHR in einem PKCS#10-Request für ein CVC-CA-Zertifikat, wird aber hier analog verwendet.

Alle anderen Werte werden entweder durch die Zertifikatstemplates definiert (festgelegete Attribute bzw. Extensions je Zertifikatstyp) oder werden als Werte in der XML-Struktur (s.o., z.B. Gültigkeitsdatum, Zertifikatstyp etc.) übergeben, so dass diese nicht Bestandteil des PKCS#10-Requests sein müssen und auch nicht sein sollen.

Hinweis: Werden im PKCS#10-Request noch weitere als die o.g. Attribute angegeben, so werden diese bei der Zertifikatserzeugung durch den TSP ignoriert.

5.2.3 Format der Response-Dateien

Das Format der Response-Dateien ist analog zu den Request-Dateien aufgebaut, es wird daher an dieser Stelle nur auf Unterschiede, d.h. andere/ zusätzliche Tags eingegangen, die exakte Definition ist der Schema-Datei CertificateResponse.xsd zu entnehmen.

Im Header gibt es das zusätzliche Tag *privateKeysIncluded*, in dem die Variante der Schlüsselgenerierung definiert wird, siehe dazu Kap. 5.2.3.2.

In den *CardData*-Tags sind anstelle der Requests die Zertifikate und, abhängig von der Variante der Schlüsselerzeugung, auch ggf. die vom TSP erzeugten Schlüssel enthalten, d.h. *CardData* besteht neben der *ICCSN* und der *LfdNo* aus folgenden Elementen:

- *CVCertName oder X.509CertName*: Zertifikatstyp.
- *CertValue*: Zertifikat.
- *PublicKey:* öffentlicher Schlüssel
- *PrivateKey:* privater Schlüssel

5.2.3.1 Dateinamen der Response-Dateien

Der Dateiname der Response-Datei entspricht dem Dateinamen der Request-Datei, mit dem Unterschied, dass der Dateityp am Ende des Namens durch „response“ ersetzt wird, d.h. in Anlehnung an das Beispiel aus Kap. 5.2.2.1 sieht der Dateiname z.B. wie folgt aus:

Beispiel: T-Systems_2013-12-19_123_TEST_response

5.2.3.2 Optionen für die Schlüsselerzeugung

Wie in Kap. 5.1 beschrieben werden drei Varianten der Schlüsselerzeugung unterschieden. Die Variante wird im Header im Tag *privateKeysIncluded* definiert:

- *privateKeysIncluded* = *false* bedeutet, dass die Schlüssel bereits vor Requesterstellung durch den Personalisierer/Antragsteller erstellt wurden, dementsprechend bleiben die Tags *PrivateKey* leer (Variante A1 oder A2),
- *privateKeysIncluded* = *true* bedeutet, dass die Schlüssel durch den TSP erzeugt wurden und in den Tags *PublicKey* und *PrivateKey* enthalten sind (Variante B).

Anhang A

A1 – Abkürzungen

Kürzel	Erläuterung
CA	Certification Authority
HBA	Heilberufeausweis
HSM-B	SMC-B in Form eines Hardware-Security Moduls
SMC-B	Security-Modul-Card Typ B
SPOC	Single Point of Contact
TSP	Trust Service Provider
XML	Extensible Markup Language

Tabelle 1 Abkürzungen

A2 - Glossar

keine

A3 – Abbildungsverzeichnis

A4 – Tabellenverzeichnis

A5 - Referenzierte Dokumente

A5.1 – Dokumente der gematik

[Quelle]	Herausgeber: Titel
[gemRL_TSL_SP_CP]	Gematik: Certificate Policy Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL, Version: 1.3.0
[gemSpec_TK]	Gematik: Spezifikation für Testkarten, Version 3.2.0
[gemKPT_Arch_TIP]	Gematik: Konzept Architektur der TIPlattform

[gemSpec_PKI]	Gematik: Übergreifende Spezifikation PKI
[gemSpec_TSP_X.509]	Gematik: Spezifikation Trust Service Provider X.509
[gemSpec_CVC_TSP]	Gematik: Spezifikation Trust Service Provider CVC
[gemProdT_X.509_TSP_nonQES_eGK_PTV1.0.0]	Gematik: Produkttypsteckbrief Trust Service Provider X.509nonQES – eGK
[gemProdT_X.509_TSP_nonQES_HBA_PTV1.0.0]	Gematik: Produkttypsteckbrief Trust Service Provider X.509nonQES – HBA
[gemProdT_X.509_TSP_nonQES_SMC-B_PTV1.0.0]	Gematik: Produkttypsteckbrief Trust Service Provider X.509nonQES – SMC-B
[gemProdT_CVC_TSP_PTV1.0.0]	Gematik: Produkttypsteckbrief Trust Service Provider CVC
[gemRL_SMC-B_ORS1]	Gematik: Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL, Sektorspezifische Präzisierung für SMC-B-Zertifikate in Erprobungsphase ORS1
[gemSpec_OID]	Gematik: Spezifikation Festlegung von OIDs
[SRQ_1201]	Gematik:SRQ_1201_gemPKI_Reg_V1_5_0_-Anpassung_normativer_Vorgaben.doc

A5.2 – Weitere Dokumente

[Quelle]	Herausgeber: Titel
[BAEK_HBA_Cert]	Bundesärztekammer: Zertifikatsprofile für X.509 Basiszertifikate
[BAEK_HBA_Attr]	Bundesärztekammer: Zertifikatsprofile für X.509 Attributzertifikate
[BZÄK_HBA_Cert]	Bundeszahnärztekammer: Zertifikatsprofil des elektronischen Zahnarztausweises
[PTK_HBA_Cert]	Bundespsychotherapeutenkammer: Zertifikatsprofile für X.509 Basiszertifikate
[PTK_HBA_Attr]	Bundespsychotherapeutenkammer: Zertifikatsprofile für X.509 Attributzertifikate
[RFC 2986]	Network Working Group: PKCS #10: Certification Request Syntax Specification
[RFC 1847]	Network Working Group: Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted
[XML Specification]	W3C Recommendation: Extensible Markup Language (XML) 1.0 (Fifth Edition)