Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Spezifikation

TSL-Dienst

Version:	1.7.0
Revision:	\main\rel_online\rel_ors1\27
Stand:	17.07.2015
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	[gemSpec_TSL]

Dokumentinformationen

Änderungen zur Vorversion

Einarbeitung bzgl. Errata

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.5.0	07.08.12		zur Abstimmung freigegeben	PL P77
1.0.0	12.11.12		Einarbeitung Kommentierung Gesellschafter	P77
1.1.0	12.11.12		Einarbeitung Kommentare aus der übergreifenden Konsistenzprüfung	
1.1.9	22.04.13		Überarbeitung anhand interner Änderungsliste (Fehlerkorrekturen, Inkonsistenzen)	P77
1.2.0	06.06.13		Einarbeitung Kommentare aus Kommentierung Gesamtpaket	P77
1.3.0	15.08.13		Einarbeitung lt. Änderungsliste vom 08.08.13	P77
1.4.0	21.02.14		Losübergreifende Synchronisation	P77
1.5.0	17.06.14		Die Anforderung TIP1-A_4051 besitzt zwei End-Tags und wurde gemäß P-11 Änderungsliste angepasst.	P77
1.6.0	26.08.14		Einarbeitung gemäß P12-Änderungsliste	
			Einarbeitung Errata 1.4.3	
1.7.0	17.07.15		freigegeben	gematik

Inhaltsverzeichnis

Dokumentinformationen 2

Inhaltsverzeichnis 3

1 Einordnung des Dokumentes 7

1.1 Zielsetzung 7

1.2 Zielgruppe 7

1.3 Geltungsbereich 7

1.4 Abgrenzung des Dokuments 7

1.5 Methodik 8

2 Systemüberblick 9

2.1 Zweck der TSL 9

2.2 TSL als zentraler Vertrauensraum der TI 9

3 Systemkontext 11

3.1 Akteure und Rollen 11

3.2 Übersicht Zertifikatshierarchie 12

4 Zerlegung des Produkttyps 13

5 Übergreifende Festlegungen 15

5.1 Allgemeine Maßnahmen 15

5.1.1 Zeitpunkt und Häufigkeit von Veröffentlichungen 15

5.2 Betriebliche Maßnahmen 15

5.3 Grundlagen für die Sicherheit der TSL-Erstellung 15

5.3.1 Organisatorische Vorgaben 15

5.3.2 Betriebliche Vorgaben 16

5.4 Allgemeine Sicherheitsmaßnahmen 17

5.4.1 Bauliche Sicherheitsmaßnahmen 18

5.4.2 Verfahrensvorschriften 18

5.4.2.1 Rollenkonzept *18*

5.4.2.2 Involvierte Mitarbeiter pro Arbeitsschritt *20*

5.4.2.3 Rollenausschlüsse *20*

5.4.3 Personalkontrolle 21

5.4.3.1 Anforderungen an freie Mitarbeiter *21*

5.4.3.2 Einsicht in Dokumente für Mitarbeiter *21*

5.4.4 Überwachungsmaßnahmen 21

5.4.4.1 Arten von aufgezeichneten Ereignissen ... 21
5.4.4.2 Schutz der Aufzeichnungen ... 22
5.4.5 Archivierung von Aufzeichnungen ... 23
5.4.5.1 Arten von archivierten Aufzeichnungen ... 23
5.4.6 Schlüsselwechsel beim Anbieter des TSL-Dienstes ... 23
5.4.7 Kompromittierung und Geschäftsweiterführung ... 23
5.4.7.1 Allgemein ... 23
5.4.7.2 Ungeplante Schlüssel-Migration TSL-Signer-CA-Zertifikat ... 23
5.4.8 Schließung des Anbieter des TSL-Dienstes ... 24

5.5 Technische Sicherheitsmaßnahmen ... 24
5.5.1 Erzeugung und Installation von Schlüsselpaaren ... 24
5.5.1.1 Erzeugung von Schlüsselpaaren und Zertifikaten ... 24
5.5.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module 26
5.5.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module 27
5.5.2.2 Hinterlegung privater Schlüssel ... 27
5.5.2.3 Vernichtung privater Schlüssel ... 28
5.5.3 Andere Aspekte des Managements von Schlüsselpaaren ... 28
5.5.3.1 Archivierung öffentlicher Schlüssel ... 28
5.5.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren ... 28
5.5.4 Aktivierungsdaten ... 28
5.5.4.1 Aktivierungsdaten ... 28
5.5.5 Sicherheitsmaßnahmen in den Rechneranlagen ... 29
5.5.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen ... 29

5.6 Format der Zertifikate ... 29

6 Funktionsmerkmale ... 30

6.1 TSL_Eintragsverwaltung ... 31
6.1.1 Schnittstelle I_TSL-Management ... 31
6.1.1.1 Schnittstellendefinition ... 32
6.1.1.2 Umsetzung ... 32
6.1.2 Schnittstelle P_TSL-Management ... 33
6.1.2.1 Schnittstellendefinition ... 33
6.1.2.2 Umsetzung Erstellungs- und Aktualisierungsprozesse ... 34
6.1.2.2.1 Aktualisierung ... 34
6.1.2.2.2 Prüfung des TSL-Eintragsantrages ... 35
6.1.2.2.3 TSL-Signatur ... 35
6.1.2.2.4 Prüfung ... 35
6.1.2.2.5 Freigabe ... 36
6.1.2.2.6 Veröffentlichung ... 36
6.1.2.2.7 Service Level ... 36
6.1.3 Schnittstelle P_Trust_Approval ... 37
6.1.3.1 Schnittstellendefinition ... 37
6.1.3.2 Umsetzung ... 37
6.1.4 Testunterstützung ... 38

6.2 TSL_PKI-Verwaltung 38
6.2.1 Schnittstelle P_TSL-PKI-Zertifikats-Management 38
6.2.1.1 Schnittstellendefinition 38
6.2.1.2 Umsetzung 38
6.2.2 Schnittstelle P_Trust-Anchor-Change 39
6.2.2.1 Schnittstellendefinition 39
6.2.2.2 Umsetzung 40
6.2.3 Testunterstützung 40

6.3 TSL_Download 41
6.3.1 Schnittstelle I_TSL_Download 41
6.3.1.1 Schnittstellendefinition 41
6.3.1.2 Umsetzung 41
6.3.2 Schnittstelle I_Cert_Download 43
6.3.2.1 Schnittstellendefinition 43
6.3.2.2 Umsetzung 43
6.3.3 Testunterstützung 44

6.4 TSL_OCSP_Responder 44
6.4.1 Schnittstelle I_OCSP_Status_Information 45
6.4.2 Schnittstelle P_Cert_Revocation 45
6.4.2.1 Schnittstellendefinition 45
6.4.2.2 Umsetzung 45
6.4.3 Testunterstützung 45

7 Informationsmodell: Technische Spezifikation TSL 47

7.1 Aufbau der TSL 47

7.2 Inhalte des Elements „SchemeInformation“ 49
7.2.1 Allgemeine TSL-Angaben 50
7.2.2 Version und Nummerierung 51
7.2.3 Aktualität der TSL 51
7.2.4 Postalische Adresse 52
7.2.5 Policy-Angaben 52
7.2.6 Informationshistorien-Angaben 53
7.2.7 Lokalisierungs-Angaben 53

7.3 Angaben zum Trust Service Provider 53
7.3.1 Angaben zum Betreiber 54
7.3.2 Angaben zum TSP-Dienst 55
7.3.2.1 Verwendung des Elements ServiceInformationExtensions 58

7.4 TI-Vertrauensankerwechsel 60

7.5 DNSSEC Trust Anchor für den Namensraum TI 60

7.6 CVC-Root-Update 61

7.7 Testunterstützung 63

Anhang A - Verzeichnisse 66

A1 – Abkürzungen 66

A2 – Glossar 66

A3 – Abbildungsverzeichnis.....67

A4 – Tabellenverzeichnis.....67

A5 - Referenzierte Dokumente.....68

A5.1 – Dokumente der gematik.....68

A5.2 – Weitere Dokumente.....68

Anhang B – Leseanleitung für XML-Schema-Fragmente.....70

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen an den Produkttyp TSL-Dienst und stellt darüber hinaus Anforderungen hinsichtlich Sicherheit und Betrieb des TSL-Dienstes. Es werden übergreifende Festlegungen sowie Anforderungen an die technischen und organisatorischen Schnittstellen zum Betrieb des TSL-Dienstes beschrieben.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter einer TSL, Trust Service Provider sowie Hersteller und Anbieter von Produkttypen, die Zertifikate nutzen.

1.3 Geltungsbereich

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

Schutzrechts-/Patentrechtshinweis

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

1.4 Abgrenzung des Dokuments

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

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps TSL-Dienst verzeichnet.

Nicht Bestandteil des vorliegenden Dokumentes sind die Festlegungen zu folgenden Themenbereichen:

- CVC-Zertifikate und die Zulassung der TSPs, die CVC-Zertifikate ausgeben, werden in den CVC-spezifischen Dokumenten beschrieben.
- Die Anforderungen an TSPs, die X.509-Zertifikate ausgeben, werden in [gemSpec_X.509_TSP] beschrieben.
- Die zugehörigen Policy-Aspekte, bzw. die Vorgaben für die Vereinheitlichung der Public-Key-Infrastrukturen, werden in [gemRL_TSL_SP_CP] angesprochen.
- Detaillierte Vorgaben zur Validierung und Verarbeitung von Zertifikaten und der hier beschriebenen Trust-service Status List (TSL) der vertrauenswürdigen Herausgeber werden in [gemSpec_PKI#8] gemacht. Dort wird auch der Wechsel des TI-Vertrauensankers auf der Client-Seite beschrieben.
- Die normativen Vorgaben bzgl. verwendbarer kryptographischer Algorithmen trifft das Dokument [gemSpec_Krypt].
- Deshalb wird als Basis zur Referenzierung der kryptographischen Algorithmen auf [gemSpec_Krypt#2.1] für X.509-Zertifikate und [gemSpec_Krypt#3.1] für XML-Signaturen, verwiesen.

1.5 Methodik

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

Sie werden im Dokument wie folgt dargestellt:

⌦ **TIP1-A_nnnn <Titel der Afo>**

Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

2 Systemüberblick

2.1 Zweck der TSL

Jedes Zertifikat und somit jeder öffentliche Schlüssel innerhalb der PKI der Telematikinfrastruktur ist durch eine Zertifizierungsstelle bzw. Certification Authority (CA) signiert. Das Vertrauen in eine CA bzw. den sie betreibenden Trust Service Provider (TSP) kann nur bestehen, wenn alle CAs einheitlichen Sicherheitsvorgaben genügen, deren Einhaltung durch eine unabhängige Instanz (die Zulassungs- und Registrierungsstelle der gematik) bestätigt wird.

Um den Vertrauensraum für X.509-Zertifikate in der Telematikinfrastruktur technisch abzubilden, wird die TSL verwendet. Die TSL-Datei ist eine signierte Whitelist der zugelassenen Zertifikatsherausgeber. Das heißt, die TSL-Datei enthält sämtliche nonQES- und QES-X.509-CA-Zertifikate, die in der TI verwendet werden. Des Weiteren enthält sie die nötigen Informationen für die Statusprüfung der von den CAs ausgestellten End-Entity-Zertifikate innerhalb der TI. Dies geschieht in Form der Adressen und Zertifikate der zuständigen OCSP-Responder bzw. der Adresse des CRL-Verteilungspunktes für den Sonderfall der Zertifikate des VPN-Zugangsdienstes.

Die TSL dient auch der Verteilung weiterer kryptographischer Infrastruktur-Elemente. Diese sind:

- Die aktuell gültigen Root-CA-Zertifikate und deren zugehörigen Cross-Zertifikate der BNetzA
- Die aktuell gültigen CVC-Root-CA-Zertifikate und deren zugehörigen Cross-CV-Zertifikate.

(Bei diesen beiden Typen von Root-CAs muss die Aktualisierung durch Ausstellen von Cross-Zertifikaten zwischen zeitlich auf einander folgenden CA-Instanzen erfolgen.)

Auch für die Verteilung des aktuellen TI DNSSEC Root Keys wird die TSL für den Transport genutzt. (S. Kap. 7.5)

Für die Auswertung der Zertifikate sind die normativen Festlegungen bzgl. der Prüfung des TI-Vertrauensraumes (kommt das Zertifikat aus einer vertrauenswürdigen Quelle?) und des Zertifikatsstatus (ist das Zertifikat gültig oder gesperrt?) in [gemSpec_PKI#8] zu finden.

2.2 TSL als zentraler Vertrauensraum der TI

Alle Komponenten in der Telematikinfrastruktur, die Zertifikate prüfen, müssen dabei die TSL in die Validierung mit einbeziehen. Aus diesem Grund ist der TSL-Dienst als zentraler Dienst in die Telematikinfrastruktur implementiert. Jede Komponente muss in der Lage sein, die notwendigen Daten regelmäßig herunterzuladen und zu validieren.

In den folgenden Abschnitten und Kapiteln wird der TSL-Dienst spezifiziert.

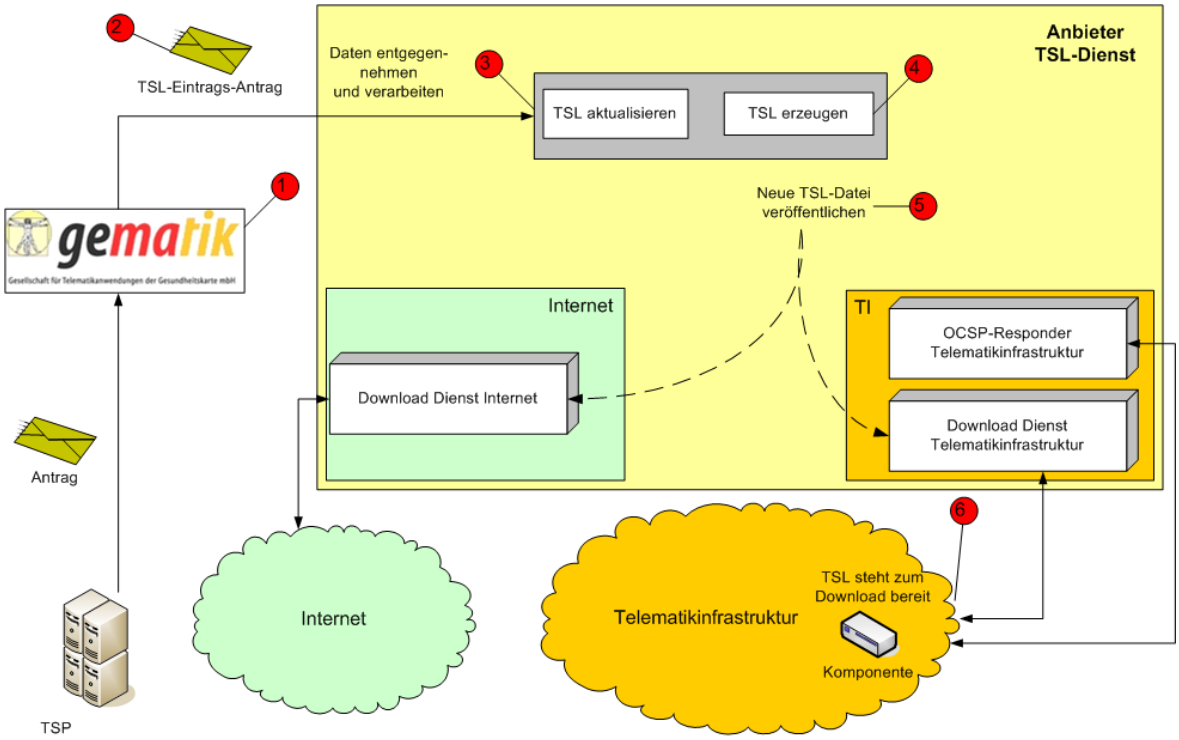


Abbildung 1: Ablauf des Eintrags in TSL

Die Kernfunktionen des TSL-Dienstes sind im Kapitel 4 „Zerlegung des Produkttyps“ beschrieben.

In der Abbildung 1 ist der Kernprozess zur Registrierung (Eintrag in die TSL) eines TSP und seiner Dienste eingezeichnet. In der Produktivumgebung ist ein solcher Eintrag die technische Abbildung des Abschlusses eines erfolgreich verlaufenen Zulassungs-verfahrens. Kurz dargestellt sehen diese Prozesse folgendermaßen aus:

Der Ablauf beginnt mit dem Antrag eines TSP an die gematik (Schritt 1). Die gematik erstellt einen TSL-Eintragsantrag (Schritt 2). Der Anbieter des TSL-Dienstes nimmt diese Daten entgegen und verarbeitet sie (Schritt 3). Im nächsten Schritt erzeugt der Anbieter des TSL-Dienstes eine aktualisierte TSL-Datei mit einem neuen Eintrag. Anschließend wird sie zum Download zur Verfügung gestellt (Schritt 5). Die Komponenten der TI können die aktualisierte TSL-Datei herunterladen und validieren (Schritt 6).

3 Systemkontext

3.1 Akteure und Rollen

Die Akteure und Rollen sind im Konzept PKI der TI-Plattform beschrieben [gem-KPT_PKI_TIP#2.7]. Im Betrieb des TSL-Dienstes gehören hierzu:

- Der Anbieter des TSL-Dienstes
- Die gematik stellt (nach erfolgter Zulassung) eines Trust Service Provider (TSP) und seiner Dienste für X.509-Zertifikate den Antrag für deren Eintrag in die (produktive) TSL-Datei.
  Die gematik beantragt auch die Aufnahme von Infrastruktur-Elementen (DNSSEC-Vertrauensanker, BNetz-A- und dazugehörige Cross-Zertifikate, CVC-Root-CA-Zertifikate und dazugehörige Cross-CV-Zertifikate).
- Die TSP-X.509 beantragen die Zulassung (und damit die Aufnahme ihrer Dienste für X.509-Zertifikate in den TI-Vertrauensraum) bei der gematik.
- Die Zertifikatsnutzer bzw. die zertifikatsprüfenden Komponenten laden die TSL-Datei herunter und nutzen die darin enthaltenen Informationen im Rahmen der Validierung von X.509-Zertifikaten.

 © gematik – öffentlich

3.2 Übersicht Zertifikatshierarchie

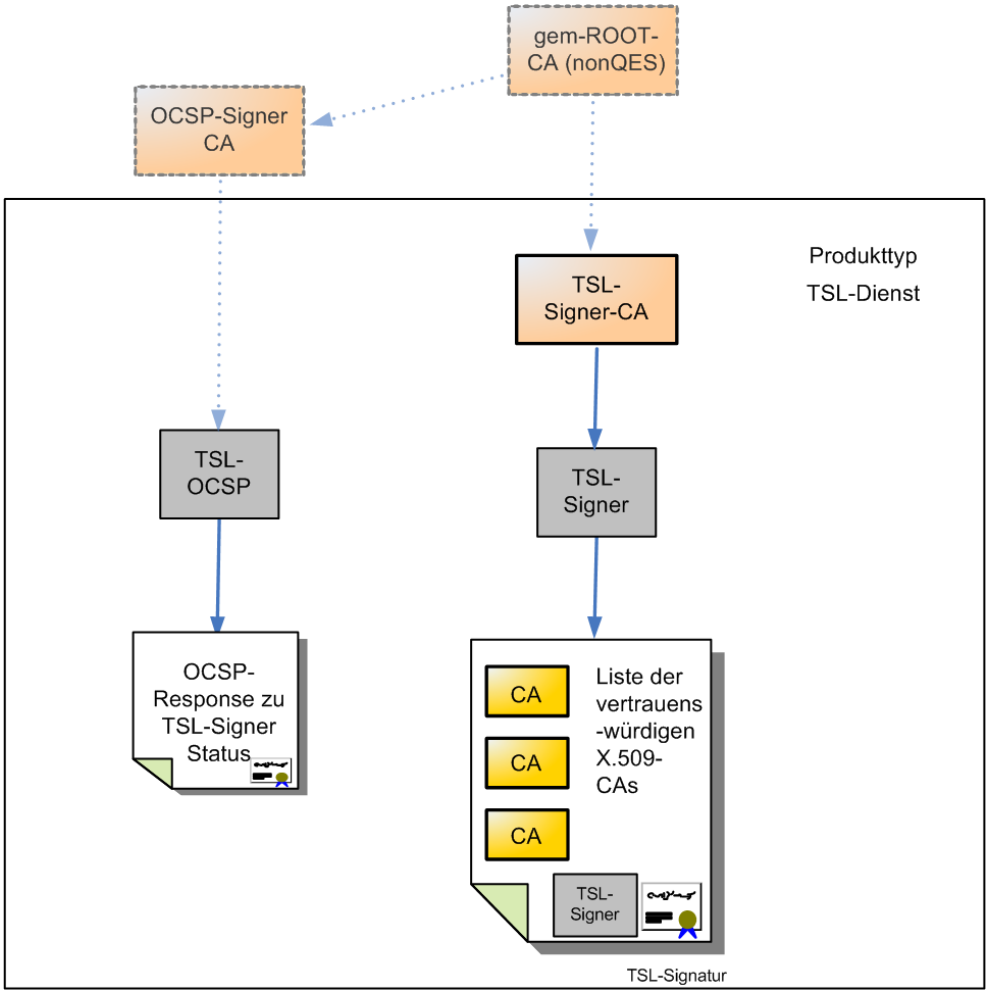


Abbildung 2: Zertifikate und Signaturen

Der Anbieter des TSL-Dienstes verwaltet das Schlüsselpaar der **TSL-Signer-CA**. Dieses ist von der gematik-Root-CA (nonQES) zertifiziert.

Die TSL-Signer-CA stellt das Zertifikat des **TSL-Signers** aus. Der TSL-Signer signiert die Liste der vertrauenswürdigen X.509-Dienste, die **Trustservice Status List (TSL)**.

Das Zertifikat des **TSL-OCSP-Responders** ist von der OCSP-Signer-CA ausgestellt. Der TSL-OCSP-Responder signiert die Statusauskünfte zum TSL-Signer-Zertifikat in Form von OCSP-Responses.

4 Zerlegung des Produkttyps

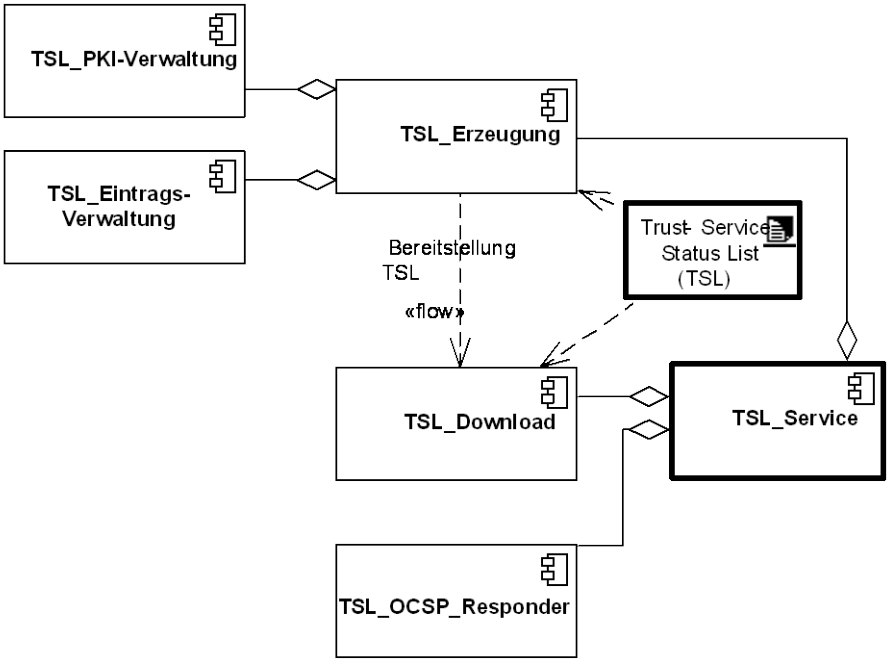


Abbildung 3: Komponenten des TSL-Dienstes

Der TSL-Dienst aggregiert die folgenden funktions-spezifischen Komponenten:

TSL_Download, zur Bereitstellung der Liste zum Download für alle Systeme, die die TSL im Rahmen der Zertifikatsprüfung validieren müssen.

TSL_OCSP_Responder, um die Gültigkeit des TSL-Signer-Zertifikats prüfbar zu halten.

TSL_Erzeugung, die TSL wird periodisch in (von der gematik) festgelegten Intervallen oder bei Bedarf auch ad hoc erzeugt. Anstehende Aktualisierungs-Requests müssen dabei in die TSL integriert werden. Die Erzeugung beinhaltet auch die Signatur der TSL. Die Komponente TSL_Erzeugung besteht aus den zwei im Folgenden dargelegten Teil-Komponenten:

- TSL_Eintragsverwaltung
- TSL_PKI-Verwaltung

TSL_Eintragsverwaltung, jeder TSP muss gemäß [gemSpec_X.509_TSP] von der gematik zugelassen werden, bevor er in der TSL der Produktivumgebung registriert wird. Auch die Eintragung seiner Dienste (CA, OCSP, CRL) muss beantragt und zugelassen werden.

Des Weiteren muss die gematik auch in der Lage sein, TSPs und ihre Dienste in der TSL zeitnah zu sperren.

Gemäß der Funktionalität TSL_Eintragsverwaltung stellt der Anbieter des TSL-Dienstes die notwendigen Tools zur Verfügung und unterstützt dadurch den Beantragungsprozess. Diese Tools beinhalten die Bereitstellung eines Management-Clients für die gematik, um TSL-Eintragsanträge an den Anbieter des TSL-Dienstes zu schicken. Diese dienen dazu Einträge in die TSL hinzuzufügen, zu verwalten.

TSL_PKI-Verwaltung, diese Teil-Komponente erlaubt die Verwaltung von PKI-spezifischen Anforderungen wie bspw. Schlüssel- und Zertifikats-Management. Dies beinhaltet daneben auch die Möglichkeit eines TI-Vertrauensankerwechsels.

Die Funktionsmerkmale dieser Komponenten werden in Kapitel 6 detailliert beschrieben und spezifiziert.

5 Übergreifende Festlegungen

Der Anbieter des TSL-Dienstes muss den kontinuierlichen und sicheren Betrieb der Komponenten des TSL-Dienstes gewährleisten. Die Anforderungen daran entsprechen teilweise denjenigen an den Betrieb einer CA in der TI für die Ausgabe von nicht-qualifizierten Zertifikaten (siehe [gemRL_TSL_SP_CP]).

5.1 Allgemeine Maßnahmen

Die Veröffentlichung von Informationen steht im Verantwortungsbereich des Anbieters des TSL-Dienstes.

5.1.1 Zeitpunkt und Häufigkeit von Veröffentlichungen

⌦ TIP1-A_3949 Veröffentlichungspflicht und kritische Informationen

Der Anbieter des TSL-Dienstes MUSS geschäftskritische Informationen, wie z. B. eine Betriebseinstellung, unverzüglich gegenüber der gematik bekannt geben.⌫

⌦ TIP1-A_3950 Mitteilungspflicht bei Änderungen

Der Anbieter des TSL-Dienstes MUSS unverzüglich Änderungen an der Architektur und den organisatorischen Abläufen gegenüber der gematik bekannt geben, sofern die Sicherheit verringert oder das Außenverhalten verändert wird.⌫

5.2 Betriebliche Maßnahmen

⌦ TIP1-A_3951 Vorlage der technischen Dokumentation und des Betriebskonzepts bei der gematik

Der Anbieter des TSL-Dienstes MUSS nach Aufforderung der gematik technisch relevante Dokumentationen, das Sicherheitskonzept und das Betriebskonzept zur Prüfung durch die gematik vorlegen.⌫

5.3 Grundlagen für die Sicherheit der TSL-Erstellung

5.3.1 Organisatorische Vorgaben

⌦ TIP1-A_3953 Anzeige von Änderung an der Gesellschafterstruktur des Betreibers

Der Anbieter des TSL-Dienstes MUSS jede Änderung an seiner Gesellschafterstruktur unverzüglich der gematik anzeigen. ⌫

⌦ TIP1-A_3954 Obligatorische Vorgaben für das Rollenkonzept

Der Anbieter des TSL-Dienstes MUSS sein Rollenkonzept umsetzen, und die operative Umsetzung der Vorgaben im Rahmen seines betreiberspezifischen Sicherheitskonzepts darlegen. ⌫

⌦ **TIP1-A_3955 Revisionssicherheit der Protokollierung**

Der Anbieter des TSL-Dienstes MUSS seine Arbeit durch eine revisionssichere Protokollierung gemäß den gesetzlichen und vertraglichen Regelungen nachweisen. ⌫

⌦ **TIP1-A_3956 Bereitstellung der Protokollierungsdaten**

Der Anbieter des TSL-Dienstes MUSS auf Antrag der gematik Einblick in die revisionssichere Protokollierung gewähren. ⌫

5.3.2 Betriebliche Vorgaben

In Kapitel 5.5 wird ein Backup-HSM gefordert und es werden die technischen Anforderungen daran spezifiziert.

Anforderungen an Standards und Sicherheitsmaßnahmen für kryptographische Module sind im Abschnitt 5.5.2.1 enthalten.

⌦ **TIP1-A_5782 Schlüsselbackup bei der gematik**

Der Anbieter des TSL-Dienstes MUSS der gematik das Schlüsselmaterial, welches für das Ausstellen von TSL-Signer-Zertifikaten notwendig ist, gemäß dem zwischen BSI und gematik abgestimmten Verfahren übergeben. ⌫

⌦ **TIP1-A_3957 Standort für Backup-HSM**

Der Anbieter des TSL-Dienstes MUSS das Backup-HSM an einem sicheren Ort außerhalb des primären Standorts aufbewahren. ⌫

⌦ **TIP1-A_3958 Verwendung des HSM gemäß Vier-Augen-Prinzip**

Der Anbieter des TSL-Dienstes MUSS in seinem betreiberspezifischen Sicherheitskonzept beschreiben, wie sichergestellt wird, dass ein Zugriff auf das Backup-HSM und sein Freischalten im Rahmen des Einbringens in das eigentliche Produktivsystem nur unter Wahrung des Vier-Augen-Prinzips möglich ist. ⌫

⌦ **TIP1-A_3959 Backup-Konzept**

Der Anbieter des TSL-Dienstes MUSS für die im Rahmen des Betriebs benötigte Hardware, Software und den Datenbestand ein Backup-Konzept erstellen und umsetzen. ⌫

⌦ **TIP1-A_3960 Besetzung von Rollen und Informationspflichten**

Der Anbieter des TSL-Dienstes MUSS eine Rollenzuordnung erstellen und umsetzen, so dass zu jeder der relevanten Rollen mindestens ein verantwortlicher Mitarbeiter sowie ein Stellvertreter benannt werden und die Rollenzuordnung initial und fortlaufend bei Änderungen der gematik mitgeteilt wird. ⌫

(Siehe Kapitel 5.4.2.1 und 5.4.2.2)

⌦ **TIP1-A_3961 Durchgängige Verfügbarkeit spezifischer Rollen**

Der Anbieter des TSL-Dienstes MUSS eine Rollenzuordnung derart umsetzen, dass zu jedem Zeitpunkt der festgelegten Betriebszeit für jede der relevanten Rollen mindestens ein für diese Rolle verantwortlicher Mitarbeiter bzw. sein Stellvertreter kurzfristig (höchstens eine Stunde Wartezeit) erreichbar sind. ⌫

(Siehe Kapitel 5.4.2.1 und 5.4.2.2)

⌦ **TIP1-A_3962 Rollenzuordnung unter Wahrung der Vier-Augen-Prinzips**

Der Anbieter des TSL-Dienstes MUSS bei der Zuordnung von Rollen zu Personen (für Aktivitäten mit gefordertem Vier-Augen-Prinzip) gewährleisten, dass eine einzelne Person nicht zwei Rollen ausübt und somit Zugriffe auf das HSM unter Umgehung des Vier-Augen-Prinzips für diese einzelne Person ermöglicht werden.⌫

(Siehe Kapitel 5.4.2.2)

⌦ **TIP1-A_3963 Nutzung des HSM im kontrollierten Bereich**

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass das zu realisierende System einschließlich der HSM in einem kontrollierten Bereich der Betriebsstätte untergebracht ist und dass der Zugang zu diesem Bereich nur für berechtigte Personen möglich ist.⌫

Die Definition der Sicherheitsbereiche erfolgt gemäß [gemSpec_SiBetrUmg].

⌦ **TIP1-A_3964 Zugang zu Systemen für die TSL-Erzeugung**

Der Anbieter des TSL-Dienstes MUSS im Rahmen der Zugangskontrolle gewährleisten, dass den Mitarbeitern der gematik bzw. durch die gematik beauftragten Personen nach Ankündigung (ggf. in Begleitung eines Mitarbeiters des Betreibers des TSL-Dienstes) Zugang zu den für die TSL-Erzeugung im Kontext der TI-relevanten Systemen gewährt wird und genaue Regelungen (Vorlaufzeit für die Ankündigung, Mitteilung der berechtigten Personen) festlegen. ⌫

⌦ **TIP1-A_3965 Niederlassungsregelung für Betriebsstätten**

Der Anbieter des TSL-Dienstes MUSS seine Systeme in Betriebsstätten betreiben, die in einem Land der Europäischen Union liegen. ⌫

5.4 Allgemeine Sicherheitsmaßnahmen

⌦ **TIP1-A_3967 Vorgaben für die informationstechnische Trennung sicherheitskritischer Bestandteile der Systemumgebung**

Der Anbieter des TSL-Dienstes MUSS sicherheitskritische Bestandteile der Systemumgebung informationstechnisch trennen. Falls eine Online-Verbindung zu den sicherheitskritischen Bestandteilen der Systemumgebung besteht, muss durch technische Maßnahmen sichergestellt werden, dass schreibende Zugriffe auf sicherheitskritische Systembestandteile unterbunden werden. ⌫

⌦ **TIP1-A_3968 Manipulationsschutz veröffentlichter Daten**

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass die Internetseite zur Bereitstellung der öffentlichen Schlüssel sowie der File- bzw. Web-Server für den

Download der Dateien vor Manipulationen entsprechend dem BSI-Grundschutz-Baustein B 5.4 "Webserver" geschützt wird.⌫

⌦ **TIP1-A_3969 Vorgaben zur Betriebsumgebung für sicherheitskritische Bestandteile des Systems**

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass sicherheitskritische Bestandteile des Systems in einem kontrollierten Bereich betrieben werden.⌫

⌦ **TIP1-A_3970 Gewährleistung des Zugangs zur Betriebsstätte**

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass Vertreter der gematik auf Antrag uneingeschränkten Zugang zu den Teilen der Betriebsstätte haben, die für den Betrieb im Kontext der TI relevant sind.⌫

⌦ **TIP1-A_5382 Zugang zu HSM-Systemen im Vier-Augen-Prinzip**

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass alle Zugriffe auf das HSM und die direkt zur Administration des HSM verwendeten IT-Systeme im Vier-Augen-Prinzip erfolgen.⌫

Die Anforderungen an die Erstellung des betreiberspezifischen Sicherheitskonzepts und eines betreiberspezifischen Betriebskonzepts werden in [gemSpec_SiBetrUmg#B] beschrieben. Diese Spezifikation enthält keine darüber hinausgehenden Anforderungen.

5.4.1 Bauliche Sicherheitsmaßnahmen

Die Anforderungen an bauliche Sicherheitsmaßnahmen sind in [gemSpec_SiBetrUmg] enthalten. Diese Spezifikation enthält keine darüber hinausgehenden Anforderungen.

5.4.2 Verfahrensvorschriften

Der Betrieb des TSL-Dienstes erfolgt anhand von dokumentierten Verfahrensvorschriften im Rahmen des Sicherheitskonzepts.

5.4.2.1 Rollenkonzept

Um einen ordnungsgemäßen und revisionssicheren Betrieb des TSL-Dienstes zu gewährleisten, ist u. a. eine entsprechende Aufgabenverteilung und Funktionstrennung vorzunehmen.

⌦ **TIP1-A_3971 Organisatorische Trennung von anderen Rollen in TI**

Der Anbieter des TSL-Dienstes MUSS eine klare organisatorische Trennung zwischen seinen verschiedenen Aufgaben und Rollen mit Interessenskonfliktpotential in der TI gemäß Beurteilung des Sicherheitsbeauftragten umsetzen und dokumentieren. ⌫

⌦ **TIP1-A_3972 Rollenunterscheidung im organisatorischen Konzept**

Der Anbieter des TSL-Dienstes MUSS in seinem Organisationskonzept die relevanten Rollen unter Beachtung von Tab_PKI_702 unterscheiden.⌫

Tabelle 1: Tab_PKI_702 Beschreibung der Rollen beim Anbieter des TSL-Dienstes

Rolle	Funktion	Kürzel
TSL-Eintrags-Dienst	Schnittstelle zur gematik für Annahme von TSL-Eintragsanträgen seitens der gematik	
TSL-Eintrags-Service	Schnittstelle zur gematik für Annahme von TSL-Eintragsanträgen seitens der gematik, Prüfung der notwendigen Unterlagen	TES
TSL-Eintrags-Registrator	Prüfung des TSL-Eintragsantrags hinsichtlich Vollständigkeit und Korrektheit Archivierung von Dokumenten, falls erforderlich Freigabe von TSL-Eintragsanträgen	TER
Registrierungsdienst	Schnittstelle zur gematik für Annahme von Anträgen für Generierung von Schlüsselpaaren (und Zertifikaten oder Zertifikatsanträgen), Prüfung der notwendigen Unterlagen und Annahme von Sperranträgen	
Zertifikatsservice	Entgegennahme von Schlüsselgenerierungs-Anträgen und Sperranträgen Identifizierung, Authentifizierung und Prüfung der Autorisierung der Mitarbeiter der gematik Verifikation der Dokumente	ZS
Zertifikats-Registrator	Prüfung des Zertifikatsantrags hinsichtlich Vollständigkeit und Korrektheit Archivierung von Dokumenten, falls erforderlich Freigabe von Anträgen für Schlüsselgenierung und Sperrantrag	RG
Zertifizierung	Ausstellen von Zertifikat, Erzeugung und Verwahrung der TSP-Schlüssel	
TSL-SP-Mitarbeiter	verantwortlich für die Anwendung und Lagerung von elektronischen Datenträgern, auf denen die privaten Schlüssel gespeichert sind	CAO1
PIN-Geber	Kenntnis eines Geheimnisses (z. B. Passwort) zur Anwendung der privaten Schlüssel	CAO2
Systembetreuung	Administration der IT-Systeme und des täglichen Betriebs (Backups usw.)	
System- und Netzwerk-Administrator	Installation, Konfiguration, Administration und Wartung der IT- und Kommunikationssysteme. vollständige Kontrolle über die eingesetzte Hard- und Software, jedoch kein Zugriff auf und keine Kenntnis von kryptographischen Schlüsseln und deren Passwörtern für Zertifizierungsprozess, Zertifikats- und Sperrmanagement sowie ausschließliche Kenntnis der Boot- und Administrator-Passwörter der Systeme	SA
Systemoperator	Betreuung der Anwendungen (Datensicherung und -wiederherstellung, Web-Server, Zertifikats- und Sperrmanagement)	SO

Rolle	Funktion	Kürzel
Überwachung des Betriebs	keine Funktion im operativen Betrieb, zuständig für die Durchsetzung der im Sicherheitskonzept festgelegten Grundsätze	
Revision	Durchführung der betriebsinternen und externen Audits, Überwachung und Einhaltung der Datenschutzbestimmungen	R
Sicherheitsbeauftragter	Definition und Einhaltung der Sicherheitsbestimmungen Überprüfung der Mitarbeiter Vergabe von Berechtigungen Ansprechpartner für sicherheitsrelevante Fragen	ISO

Ein Mitarbeiter kann auch in mehr als einer Rolle auftreten. Dabei ist jedoch zu beachten, dass es Rollenunverträglichkeiten (Abschnitt 5.4.2.3) gibt. Ebenso ist es möglich, dass Funktionen einer Rolle auf mehrere Mitarbeiter mit dieser Rolle verteilt werden.

⌦ TIP1-A_3973 Mitteilungspflicht für Zuordnung der Rollen

Der Anbieter des TSL-Dienstes MUSS die Belegung der Rollen mit ihren benannten Mitarbeitern der gematik mitteilen.⌫

5.4.2.2 Involvierte Mitarbeiter pro Arbeitsschritt

⌦ TIP1-A_3974 Obligatorisches 4-Augen-Prinzip für sicherheitsrelevante Tätigkeiten

Der Anbieter des TSL-Dienstes MUSS die Rollenzuordnung der folgenden Tätigkeiten gemäß dem Vier-Augen-Prinzip umsetzen:
(a) Sämtliche HSM-Operationen für TSL-Signer-CA und TSL-Signer
(b) Schlüssellebenszyklus-Operationen für OCSP-Responder
(c) Schlüsselhinterlegung
(d) Ausstellen des TSL-Signer-Zertifikats
(e) Sperren des TSL-Signer-Zertifikats
(f) Technische Vergabe von Berechtigungen
(g) Registrierungsdienst
(h) TSL-Eintrags-Dienst⌫

5.4.2.3 Rollenausschlüsse

⌦ TIP1-A_3975 Ausschluss von Rollenzuordnungen

Der Anbieter des TSL-Dienstes MUSS bei der Aufteilung der Rollen auf Mitarbeiter unter Beachtung von Tab_PKI_702 und Tab_PKI_703 sicherstellen, dass einer Person keine miteinander unverträglichen Rollen zugewiesen werden. ⌫

Tabelle 2: Tab_PKI_703 Rollenausschlüsse

Rolle	Unverträglich mit
R - Revision	TER, TES, ZS, RG, CAO1, CAO2, SA, SO

Rolle	Unverträglich mit
ISO - Sicherheitsbeauftragter	TER, TES, ZS, RG, CAO1, CAO2, SA, SO
TES - TSL-Eintrags-Service	R, ISO, SA, SO
TER - TSL-Eintrags-Registrator	R, ISO, SA, SO
ZS - Zertifikatsservice	R, ISO, SA, SO
RG - Zertifikats-Registrator	R, ISO, SA, SO
SA - Systemadministrator	R, ISO, TER, TES, ZS, RG, CAO1
SO - Systemoperator	R, ISO, TER, TES, ZS, RG, CAO1
CAO1 TSL-SP-Mitarbeiter	R, ISO, CAO2, SA, SO
CAO2 PIN-Geber	R, ISO, CAO1

5.4.3 Personalkontrolle

5.4.3.1 Anforderungen an freie Mitarbeiter

⌦ TIP1-A_3976 Anforderungen an den Einsatz freier Mitarbeiter

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass freie Mitarbeiter die gleichen Sicherheitsanforderungen erfüllen, wie festangestellte Mitarbeiter.⌫

5.4.3.2 Einsicht in Dokumente für Mitarbeiter

⌦ TIP1-A_3977 Einsicht in Dokumente für Mitarbeiter

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass seine Mitarbeiter in
(a) das betreiberspezifische Betriebskonzept,
(b) das Rollenkonzept,
(c) das betreiberspezifische Sicherheitskonzept,
(d) die Prozessbeschreibungen und Formulare für den regulären Betrieb,
(e) die Verfahrensanweisungen für den Notfall,
(f) die Dokumentation der IT-Systeme,
(g) die Bedienungsanleitungen für die eingesetzte Software und
(h) die Datenschutzerklärung (falls vorhanden)
Einsicht erhalten.⌫

5.4.4 Überwachungsmaßnahmen

5.4.4.1 Arten von aufgezeichneten Ereignissen

⌦ TIP1-A_3978 Aufzeichnung von technischen Ereignissen

Der Anbieter des TSL-Dienstes MUSS die folgenden technischen Ereignisse protokollieren:
(a) Bootvorgänge der Hardware,
(b) Installation und Konfiguration von Software,
(c) Fehlgeschlagene Login-Versuche,
(d) Durchführung von Änderungen an Zugriffsrechten ⌫

TIP1-A_3979 Aufzeichnung von organisatorischen Ereignissen

Der Anbieter des TSL-Dienstes MUSS die folgenden organisatorischen Ereignisse protokollieren:
(a) Vergabe und Entzug von Berechtigungen,
(b) Änderungen des betreiberspezifischen Betriebshandbuches und der korrespondierenden Richtlinien,
(c) Änderungen an Rollendefinitionen,
(d) Änderungen an Prozessbeschreibungen,
(e) Wechsel von Verantwortlichkeiten,
(f) Ausscheiden von Mitarbeitern ⌫

TIP1-A_3980 Protokollierung wichtiger TSL-spezifischer Ereignisse

Der Anbieter des TSL-Dienstes MUSS mindestens die folgenden wichtigen TSL-spezifischen Ereignisse protokollieren:
(a) Das Generieren eines neuen Schlüsselpaares
(b) Die Aktivierung eines Schlüsselpaares
(c) Das Generieren, Signieren und Bereitstellen einer neuen TSL
(d) Das Generieren eines neuen TSP Eintrags, Signieren und Bereitstellen der TSL ⌫

TIP1-A_3981 Protokollierung wichtiger TSL-spezifischer Ereignisse: Angaben

Der Anbieter des TSL-Dienstes MUSS für die wichtigen TSL-spezifischen Ereignisse mindestens die folgenden Angaben protokollieren:
(a) Das Datum des Auftrags der gematik
(b) Angaben zur eindeutigen Identifizierung aller an den Schritten und Teilschritten der Ereignisse beteiligten Personen
(c) Das technische Ergebnis eines Ereignisses ⌫

TIP1-A_3982 Aufbewahrungsfrist für Protokolldaten

Der Anbieter des TSL-Dienstes MUSS Protokolldaten mindestens entsprechend den gesetzlichen und vertraglichen Regelungen aufbewahren. ⌫

5.4.4.2 Schutz der Aufzeichnungen

TIP1-A_3983 Schutz vor Zugriff, Löschung und Manipulation elektronischer Protokolldaten

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass Protokolldaten trotz privilegierter Berechtigungen der System- und Netzadministratoren gegen unberechtigten Zugriff, Löschung und Manipulation dauerhaft geschützt werden.⌫

Durch die regelmäßige Speicherung nach Kapitel 5.4.5 können solche Daten dauerhaft geschützt werden.

5.4.5 Archivierung von Aufzeichnungen

5.4.5.1 Arten von archivierten Aufzeichnungen

⌦ **TIP1-A_3984 Archivierung: Relevante Daten**

Der Anbieter des TSL-Dienstes MUSS eine sichere Archivierung aller relevanten Daten im Betriebsprozess realisieren. Dazu gehören:
(a) Alle Versionen der TSL,
(b) Alle Anträge, Aufträge und Registrierungsunterlagen von der gematik,
(c) Zertifikate des Anbieters des TSL-Dienstes und
(d) Protokolldaten. ⌫

5.4.6 Schlüsselwechsel beim Anbieter des TSL-Dienstes

⌦ **TIP1-A_3985 Dokumentationspflicht für Prozesse zum Schlüsselwechsel**

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass der Schlüsselwechsel anhand dokumentierter Prozesse erfolgt. ⌫

5.4.7 Kompromittierung und Geschäftsweiterführung

5.4.7.1 Allgemein

⌦ **TIP1-A_3986 Aktionen und Verantwortlichkeit im Rahmen der Notfallplanung**

Der Anbieter des TSL-Dienstes MUSS im Rahmen der Notfallplanung gewährleisten, dass
(a) für den Fall einer Kompromittierung oder eines Desasters Prozesse zur Aufrechterhaltung des Betriebs dokumentiert werden und
(b) die Bewertung der Sicherheitslage durch den Sicherheitsbeauftragten vollzogen wird.⌫

Die Anforderungen an Notfallpläne und die Aufrechterhaltung des Regelbetriebs nach dem Eintreten eines Notfalls bei dem Anbieter des TSL-Dienstes sind in [gemSpec_SiBetrUmg] enthalten.

Die Notfallplanung für den Fall einer Kompromittierung der TSL-Signer-CA kann sich darauf abstützen, dass die Authentizität der Download-Punkte immer noch gesichert ist (in der TI über DNSSEC, im Internet über TLS). Mittels TI-Vertrauensankerwechsel (siehe Kapitel 6.2.2) kann deshalb auch über die kompromittierte CA eine neue, umkompromittierte TSL-Signer-CA in Kraft gesetzt werden, und der Weiterbetrieb der TI kann (zumindest provisorisch bis zum Ergreifen weiterer Maßnahmen) aufrecht erhalten werden.

5.4.7.2 Ungeplante Schlüssel-Migration TSL-Signer-CA-Zertifikat

Bei einer ungeplanten Übernahme des TSL-Dienstes muss der neue Anbieter das Schlüsselpaar oder die Schlüsselpaare und dazugehörige TSL-Signer-CA-Zertifikate des bisherigen Anbieters des TSL-Dienstes in sein System importieren können und dadurch den laufenden Betrieb übernehmen. In der Regel erhält der neue Anbieter dazu das HSM des bisherigen Anbieters des TSL-Dienstes.

Das HSM muss in das System des neuen Anbieters eingebunden werden können, das heißt, das Schlüsselmaterial und die Zertifikate werden extrahiert und in das HSM des neuen Anbieters importiert (siehe dazu auch Kapitel 5.5.1 und 5.5.2 insbesondere 5.5.2.1).

TIP1-A_3987 Herausgabe des Schlüsselmaterials

Der Anbieter des TSL-Dienstes MUSS bei der ungeplanten Einstellung seines Betriebes das für den Betrieb erforderliche Schlüsselmaterial in Form des HSMs herausgeben. Dabei MUSS er die Autorisierung der berechtigten Mitarbeiter der gematik prüfen. Der Prozess dieser Prüfung MUSS in seinem betreiberspezifischen Sicherheitskonzept dokumentiert sein. Der Anbieter des TSL-Dienstes MUSS bei einer Herausgabe des Schlüsselmaterials die darin beschriebenen Schritte durchführen. ⌫

TIP1-A_3988 Bewilligung der Herausgabe der Schlüsselmaterials

Der Anbieter des TSL-Dienstes DARF NICHT ohne schriftlichen Antrag der gematik eine Herausgabe des Schlüsselmaterials der TSL-Signer-CA durchführen. ⌫

5.4.8 Schließung des Anbieter des TSL-Dienstes

TIP1-A_3989 Anzeigepflicht bei Beendigung der Dienstleistungen

Der Anbieter des TSL-Dienstes MUSS die Beendigung seiner Dienstleistungen im Kontext der TI als Prozess dokumentieren und die Beendigung seiner Dienstleistungen der gematik unverzüglich anzeigen. ⌫

TIP1-A_3990 Fortbestand von Archiven und die Abrufmöglichkeit aller TSL-Dateien und Zertifikate

Der Anbieter des TSL-Dienstes MUSS den Fortbestand der Archive und die Abrufmöglichkeit aller ausgestellten TSL-Dateien sowie aller verwendeten Zertifikate für den zugesicherten Aufbewahrungszeitraum sicherstellen.⌫

TIP1-A_3991 Fristen bei Einstellung des Betriebs

Der Anbieter des TSL-Dienstes MUSS die mit der gematik vereinbarte Ankündigungsfrist bei der Einstellung des Betriebs einhalten. ⌫

TIP1-A_3992 Erforderliche Form bei Einstellung des Betriebs

Der Anbieter des TSL-Dienstes MUSS die Einstellung des Betriebs schriftlich gegenüber der gematik ankündigen.⌫

5.5 Technische Sicherheitsmaßnahmen

5.5.1 Erzeugung und Installation von Schlüsselpaaren

5.5.1.1 Erzeugung von Schlüsselpaaren und Zertifikaten

TIP1-A_3993 TSL-Signer-CA offline

Der Anbieter des TSL-Dienstes MUSS die TSL-Signer-CA vollständig offline initialisieren und betreiben. ⌫

⌦ **TIP1-A_3994 Schlüsselverwaltung: zwingend unterschiedliche Schlüssel für unterschiedliche Entitäten**

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass TSL-Signer-CA, TSL-Signer und OCSP-Responder nicht dasselbe Schlüsselpaar verwenden.⌫

⌦ **TIP1-A_3995 Beachtung des betreiberspezifischen Sicherheitskonzepts bei der Erzeugung von Schlüsselpaaren**

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass die technischen Sicherheitsmaßnahmen zur Erzeugung und Installation von Schlüsselpaaren die Rahmenbedingungen des eigenen, betreiberspezifischen Sicherheitskonzeptes erfüllen und sich am aktuellen Stand der Technik orientieren.⌫

⌦ **TIP1-A_3996 Sicherheitsniveau bei der Generierung von Signaturschlüsseln**

Der Anbieter des TSL-Dienstes MUSS Signaturschlüssel in einem von einer akkreditierten Evaluierungsstelle geprüften HSM oder alternativ in einer Chipkarte mit vergleichbarer geforderter Zertifizierungstiefe erzeugen.⌫

Die für HSM geforderte Zertifizierungstiefe wird im Abschnitt 5.5.2.1 definiert.

⌦ **TIP1-A_3997 Verwendung eines Backup-HSM zum Im-/Export von privaten Schlüsseln**

Der Anbieter des TSL-Dienstes MUSS ein Backup-HSM zum sicheren Export bzw. Import von privaten Schlüsseln verwenden, wobei zu beachten ist:
(a) Primäres HSM und Backup-HSM MÜSSEN die gleichen Sicherheitsanforderungen erfüllen,
(b) zwischen primärem HSM und Backup-HSM MUSS ein kryptographisch gesicherter Transportkanal hergestellt werden, um den privaten Schlüssel aus dem einen HSM sicher zu exportieren und in das andere HSM zu importieren. ⌫

⌦ **TIP1-A_3998 Unterstützung des sicheren Löschen von Schlüsseln durch HSM**

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass alle eingesetzten HSM eine Funktion unterstützen, mit der ein vorhandenes Schlüsselpaar innerhalb des HSM sicher gelöscht werden kann, wobei der sichere Löschvorgang durch ein Überschreiben mit einem vorgegebenen Wert oder durch das interne dauerhafte Sperren aller Zugriffe auf den Schlüssel realisiert werden kann.⌫

TIP1-A_3999 Generieren und Löschen von Schlüsselpaaren gemäß Vier-Augen-Prinzip

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass das Generieren eines neuen Schlüsselpaares und das Löschen eines Schlüsselpaares nur nach erfolgreicher, gemeinsamer Authentisierung zweier hierfür autorisierter Nutzer (Vier-Augen-Prinzip) durch das Verifizieren einer PIN oder ein gleichwertiges Verfahren ausführbar sind.

TIP1-A_4000 Berechnungen mit dem privaten Schlüssel gemäß Vier-Augen-Prinzip

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass alle kryptographischen Berechnungen mit dem privaten Schlüssel für das Erstellen eines Zertifikats innerhalb des HSM erfolgen, wobei das HSM diese Berechnungen nur nach erfolgreicher, gemeinsamer Authentisierung zweier hierfür autorisierter Nutzer (Vier-Augen-Prinzip) durch das Verifizieren einer PIN oder ein gleichartiges Verfahren durchführen darf.

TIP1-A_4001 Protokollierung der HSM-Nutzung

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass die Nutzung des HSM revisionssicher protokolliert wird, insbesondere welche Rolle/Person zu welchem Zeitpunkt für welche Funktion das HSM genutzt hat und für welche Profile das HSM konfiguriert ist. Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass auch die Nutzung und die Übergabe zur Verwahrung des Backup-HSM revisionssicher protokolliert werden.

TIP1-A_4002 Berücksichtigung des aktuellen Erkenntnisstands bei der Generierung von Schlüsseln

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass bei der Generierung von Schlüsseln jeweils der aktuelle Stand der Technik berücksichtigt wird.

TIP1-A_4003 Anlass für den Wechsel von Schlüsselpaaren

Der Anbieter des TSL-Dienstes MUSS die verwendeten Schlüsselpaare der TSL-Signer-CA, des TSL-Signers und des OCSP-Responders auswechseln, wenn
(a) organisatorische Regelungen der gematik dies erfordern,
(b) die maximale Verwendungsdauer für ein Schlüsselpaar erreicht wurde und
(c) wenn ein aktuell verwendetes Schlüsselpaar kompromittiert wurde.

Vorgaben zu den relevanten organisatorischen Regelungen für die Verwendung von Schlüsselpaaren finden sich in [gemSpec_SiBetrUmg#B1.11], Vorgaben zur maximalen Verwendungsdauer von Schlüsseln in [gemSpec_Krypt#2].

5.5.2 Sicherung des privaten Schlüssels und Anforderungen an kryptographische Module

TIP1-A_4005 Sicherung des privaten Schlüssels

Der Anbieter des TSL-Dienstes MUSS die Sicherung des privaten Schlüssels nach dem aktuellen Stand der Technik gewährleisten und die Anforderungen an kryptographische Module im Rahmen ihres betreiberspezifischen Sicherheitskonzeptes definieren.

TIP1-A_4006 Verwendung von privaten Schlüsseln

Der Anbieter des TSL-Dienstes MUSS gewährleisten, dass
(a) alle kryptographischen Berechnungen mit einem privaten Schlüssel intern in einem Hardware-Sicherheitsmodul (HSM) durchgeführt werden und
(b) private Schlüssel des Anbieters des TSL-Dienstes nicht im Klartext aus dem HSM exportiert werden. ⌫

TIP1-A_4007 Vorgaben an HSM-Funktionalität

Der Anbieter des TSL-Dienstes MUSS Hardware-Sicherheitsmodule (HSM) einsetzen, die mindestens Funktionen
(a) zur Generierung eines neuen Schlüsselpaares,
(b) zur Aktivierung eines Schlüsselpaares,
(c) zum kryptographisch abgesicherten Import und Export eines privaten Schlüssels,

(d) zum sicheren (physikalischen) Löschen eines Schlüsselpaares,
(e) zur m-von-n-Aktivierung und
(f) zum Erstellen eines Zertifikats mit interaktiv einzugebenden Zertifikatsdaten beinhalten.⌫

TIP1-A_4008 Speicherung und Auswahl von Schlüsselpaaren im HSM

Der Anbieter des TSL-Dienstes MUSS ein Hardware-Sicherheitsmodul (HSM) einsetzen, das mehrere Schlüsselpaare speichern kann und über eine Funktion zur Aktivierung eines einzelnen, spezifischen Schlüsselpaares verfügt, dass nach erfolgter Auswahl zur Erzeugung von Zertifikaten verwendet wird.⌫

5.5.2.1 Standards und Sicherheitsmaßnahmen für kryptographische Module

TIP1-A_4010 Vorgaben an die Prüftiefe der Evaluierung eines HSM

Der Anbieter des TSL-Dienstes MUSS für alle eingesetzten Hardware-Sicherheitsmodule (HSM) sicherstellen, dass diese nach einer der folgenden Kombinationen aus Evaluierungsschema und Prüftiefe (sowie einem fachlich geeignetem Schutzprofil) oder einem äquivalenten Zertifizierungsstandard evaluiert wurden:
(a) FIPS 140-2 Level 3,
(b) CC EAL4+ mit Prüfung gegen hohes Angriffspotenzial oder
(c) ITSEC E3 der Stärke „hoch“. ⌫

TIP1-A_4011 PKCS#11

Der Anbieter des TSL-Dienstes MUSS die PKCS#11-Kommandos für verschlüsselten Export des Schlüsselmaterials der TSL-Signer-CA unterstützen. ⌫

5.5.2.2 Hinterlegung privater Schlüssel

TIP1-A_4012 Hinterlegung des privaten Schlüssels

Der Anbieter des TSL-Dienstes DARF NICHT den privaten Schlüssel eines Schlüsselpaars ungeschützt bei Dritten hinterlegen.⌫

5.5.2.3 Vernichtung privater Schlüssel

Verantwortlich für die Vernichtung sind die dafür bestimmten Rollen „ISO“ und „CAO1“ (siehe Tab_PKI_702).

Die Anforderungen an die Vernichtung privater Schlüssel bei dem Anbieter des TSL-Dienstes werden als Teil der Anforderungen an die Schlüsselverwaltung in [gemSpec_Sich_DS#3.8] beschrieben. Diese Spezifikation enthält keine darüber hinaus gehenden Anforderungen.

5.5.3 Andere Aspekte des Managements von Schlüsselpaaren

5.5.3.1 Archivierung öffentlicher Schlüssel

Die Anforderungen an Archivierung öffentlicher Schlüssel bei dem Anbieter des TSL-Dienstes werden als Teil der Anforderungen an die Schlüsselverwaltung in [gemSpec_Sich_DS#3.7] beschrieben. Diese Spezifikation enthält keine darüber hinausgehenden Anforderungen.

5.5.3.2 Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren

Die maximale Gültigkeitsdauer von Zertifikaten ist in [gemRL_TSL_SP_CP#7.3.2] definiert. auf 5 (Endbenutzer-) bzw. 8 Jahre (CA-Zertifikate). Diese Vorgaben sind auch für die TSL-Zertifikate umzusetzen.

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

Der Anbieter des TSL-Dienstes SOLL die Gültigkeitsdauer des TSL-Signer-CA-Zertifikats auf 8 Jahre ansetzen. ⌫

⌦ **TIP1-A_4016 Maximale Gültigkeitsdauer des TSL-Signer-Zertifikats**

Der Anbieter des TSL-Dienstes SOLL die Gültigkeitsdauer des TSL-Signer-Zertifikats auf 5 Jahre ansetzen. ⌫

5.5.4 Aktivierungsdaten

5.5.4.1 Aktivierungsdaten

⌦ **TIP1-A_4017 Sichere Übermittlung von Aktivierungsdaten**

Der Anbieter des TSL-Dienstes MUSS Prozesse für die sichere Übermittlung von Aktivierungsdaten definieren und von seinem Sicherheitsbeauftragten bestätigen lassen. ⌫

5.5.5 Sicherheitsmaßnahmen in den Rechneranlagen

5.5.5.1 Spezifische technische Sicherheitsanforderungen in den Rechneranlagen

⌦ **TIP1-A_4018 Konformität zum betreiberspezifischen Sicherheitskonzept**

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass alle Systemkomponenten der PKI bzw. der TSL-Signatur konform zu den Sicherheitsanforderungen seines betreiberspezifischen Sicherheitskonzepts betrieben werden.⌫

⌦ **TIP1-A_4019 Härtung von Betriebssystemen**

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass alle sicherheitsrelevanten, technischen Abläufe auf Basis gehärteter Betriebssysteme nach IT-Grundschutz-Katalog ([BSI#B3]) ausgeführt werden.⌫

5.6 Format der Zertifikate

Die Festlegung der Zertifikatsprofile erfolgt in [gemSpec_PKI#5.13].

6 Funktionsmerkmale

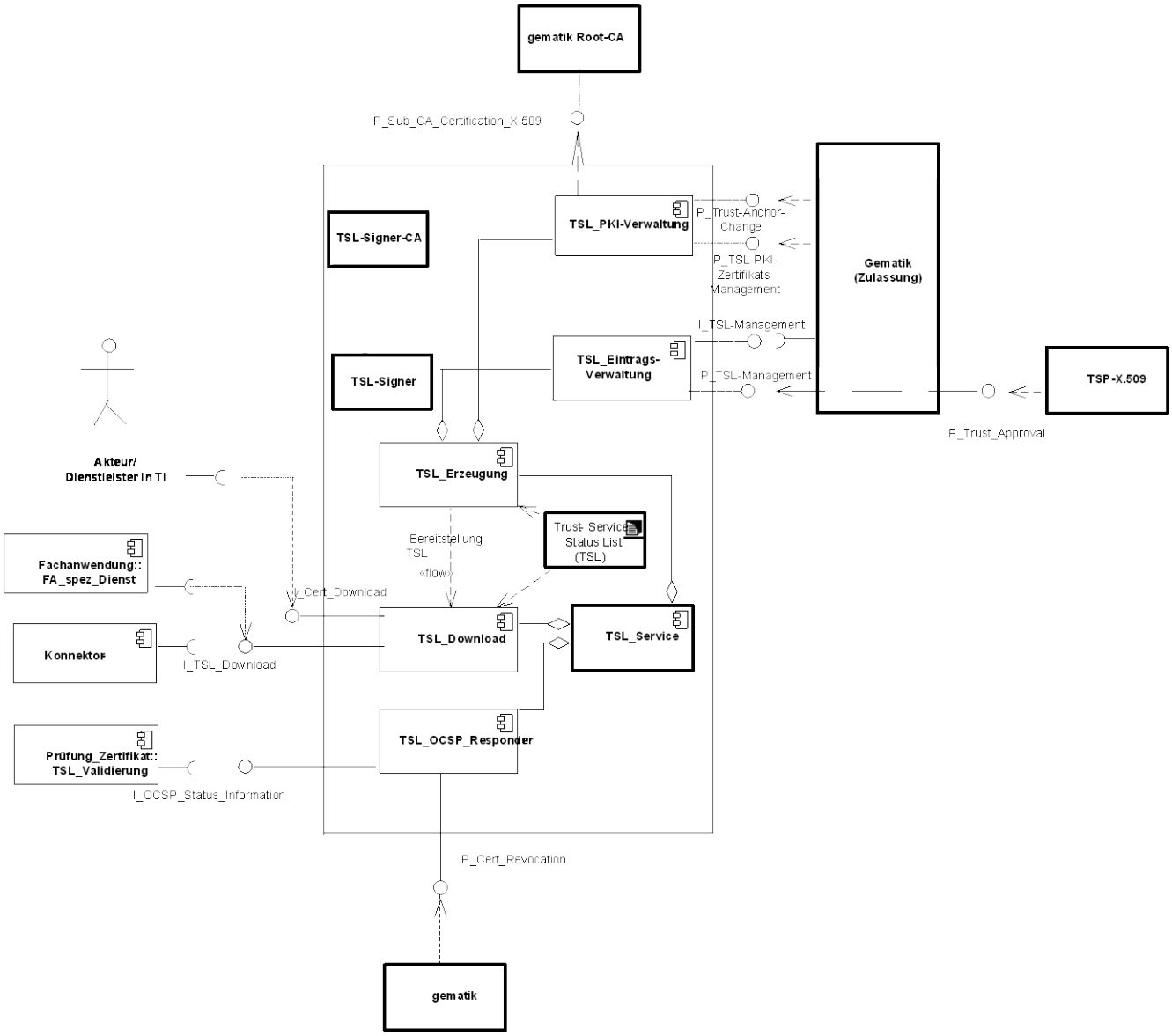


Abbildung 4: Funktionsmerkmale und ihre Schnittstellen (Schematische Darstellung)

Hinweis: Die gematik Root-CA und deren Schnittstelle P_Sub_CA_Certification_X.509 sind in der obigen Darstellung nur aus Gründen der besseren Verständlichkeit enthalten. Deren Beschreibung erfolgt andernorts.

Tabelle 3: Schnittstellen des TSL-Dienstes

Funktions-merkmal	Schnittstelle	Kurzbeschreibung
TSL_ Eintragsverwaltung	I_TSL-Management	Technische Schnittstelle zur Verwaltung der TSL-Einträge durch gematik (XML-basiert)
	P_TSL-Management	Organisatorische Schnittstelle zur Verwaltung der TSL-Einträge durch gematik
	P_Trust_Approval	Organisatorische Schnittstelle für einen TSP, um in den Vertrauensraum der TI zu gelangen
TSL_ PKI-Verwaltung	P_TSL-PKI-Zertifikats-Management	Organisatorische Schnittstelle für Schlüssel- und Zertifikatserneuerung
	P_Trust-Anchor-Change	Organisatorische Schnittstelle für den TI-Vertrauensankerwechsel
TSL_ Download	I_TSL_Download	Technische Schnittstelle für das Herunterladen der TSL
	I_Cert_Download	Technische Schnittstelle für das Herunterladen des TSL-Signer-CA-Zertifikats
TSL_ OCSP_ Responder	I_OCSP_Sta-tus_Information	Technische Schnittstelle für die Statusabfrage an den OCSP-Responder
	P_Cert_Revocation	Organisatorische Schnittstelle für Sperrung (Änderung des Status der OCSP-Response)

6.1 TSL_Eintragsverwaltung

Für die Registrierung eines TSP und seiner benötigten Dienste in der TSL der Produktivumgebung muss der TSP ein Zulassungsverfahren durchlaufen. Die Prozesse dieses Verfahrens obliegen der Zulassungs- und Registrierungsstelle der gematik. Sie veranlasst die Eintragung in die TSL nach erfolgreicher Prüfung. Des Weiteren kann die gematik z. B. auch den Widerruf eines TSPs veranlassen, also dessen Ausschluss aus der TSL.

6.1.1 Schnittstelle I_TSL-Management

Die Schnittstelle I_TSL-Management unterstützt die Abläufe der organisatorischen Schnittstelle P_TSL-Management und soll eine in technischer Hinsicht reibungslose Verwaltung der TSL-Einträge sicherstellen:

Die Prozesse der TSL-Eintragsverwaltung bedingen, dass eine klar definierte Kommunikation zwischen der gematik und dem Anbieter des TSL-Dienstes stattfindet. Diese besteht aus TSL-Eintragsanträgen, welche seitens der gematik an den Anbieter des TSL-Dienstes geschickt werden und den Antworten dazu.

Dazu wird ein Tool benötigt, welches der gematik erlaubt, die TSL-Eintragsanträge (Aufnahme, Änderung oder Löschen eines TSP oder TSP-Dienstes) zu erstellen.

6.1.1.1 Schnittstellendefinition

⌦ **TIP1-A_4027 Bereitstellung Schnittstelle I_TSL-Management**

Der TSL-Dienst MUSS eine technische Schnittstelle I_TSL-Management bereitstellen, welche die TSL-Eintragsanträge (Aufnahme, Änderung oder Löschen eines TSP oder TSP-Dienstes) der gematik entgegennimmt. ⌫

⌦ **TIP1-A_4435 I_TSL-Management, Zeitstempel**

Der TSL-Dienst MUSS die Schnittstelle I_TSL-Management so implementieren, dass diese bei Erhalt eines TSL-Eintragsantrages einen prüffähigen Zeitstempel erstellt. ⌫

⌦ **TIP1-A_4028 I_TSL-Management, Bestätigung**

Der TSL-Dienst MUSS nach erfolgreicher Entgegennahme und nach Verarbeitung eines TSL-Eintragsantrages eine Bestätigung an die gematik senden. ⌫

⌦ **TIP1-A_4030 Bereitstellung I_TSL-Management:Client**

Der Anbieter des TSL-Dienstes MUSS der gematik einen Client für die Schnittstelle I_TSL-Management („I_TSL-Management:Client“) zur Verfügung stellen. ⌫

⌦ **TIP1-A_4031 I_TSL-Management:Client, TSL-Eintragsanträge**

Der I_TSL-Management:Client MUSS sämtliche TSL-Eintragsanträge der gematik an den Anbieter des TSL-Dienstes erzeugen können:
(a) Hinzufügen eines neuen TSP und eines dazugehörigen TSP-Dienstes
(b) Hinzufügen eines zusätzlichen TSP-Dienstes zu einem bestehenden TSP
(c) Ändern eines TSP
(d) Ändern eines TSP-Dienstes
(e) Löschen eines TSP
(f) Löschen eines TSP-Dienstes
(g) Widerruf (auf Status „revoked“ setzen) eines TSP-Dienstes ⌫

⌦ **TIP1-A_4032 I_TSL-Management:Client, XML-Format**

Der I_TSL-Management:Client MUSS die Möglichkeit bieten, die TSL-Eintragsanträge direkt im XML-Format gemäß [ETSI_TS_102_231_V3.1.2#AnhangB] zu erstellen und zu bearbeiten.⌫

⌦ **TIP1-A_4034 I_TSL-Management:Client, Qualifizierte Signatur**

Der I_TSL-Management:Client SOLL die Funktion anbieten, die TSL-Eintragsanträge qualifiziert elektronisch zu signieren. ⌫

6.1.1.2 Umsetzung

⌦ **TIP1-A_4035 TSL-Signer-CA-Zertifikat als TSL-Eintrag**

Der TSL-Dienst MUSS die aktuelle TSL-Signer-CA als TSP-Dienst in der TSL eintragen. ⌫

Hinweis:Daraus folgt auch, dass für das TSL-Signer-CA-Zertifikat die Adresse und das Zertifikat des zuständigen OCSP-Responders angegeben werden.

Auf die entsprechende Syntax bzw. erlaubten Werte wird in Kapitel 7.3.2 eingegangen.

Der OCSP-Responder wird in Kapitel 6.4 beschrieben.

⌦ **TIP1-A_4036 Syntaktische und semantische Prüfung der TSL**

Der TSL-Dienst MUSS nach Erstellung der Signatur die Korrektheit der TSL sicherstellen:
Der TSL-Dienst MUSS eine Prüfung auf Vollständigkeit (Schemaprüfung) durchführen.
Der TSL-Dienst MUSS eine Prüfung auf korrekte Umsetzung der Vorgaben der gematik für inhaltliche Werte durchführen.
Der TSL-Dienst MUSS eine Signaturprüfung durchführen. ⌫

Hinweis: Die Korrektheit der inhaltlichen Werte ist, sofern nicht schon durch das XML-Schema gemäß [ETSI_TS_102_231_V3.1.2] abgedeckt, durch das Kapitel 7 „Informationsmodell: Technische Spezifikation TSL“ vorgegeben.

6.1.2 Schnittstelle P_TSL-Management

6.1.2.1 Schnittstellendefinition

Die Schnittstelle definiert die Prozesse der TSL-Eintragsverwaltung.

Für die Produktionsumgebung gilt: Der Prozess der Zulassung (bereits erfolgt) und somit auch der TSL-Eintragung ist in zwei separate Sub-Prozesse unterteilt. Zuerst muss eine Zulassung des TSP erfolgen. Danach meldet der TSP seine zuzulassenden Dienste an. Ein Eintrag in der TSL erfolgt nachdem ein Dienst zugelassen wurde.

Folgende Abbildung verdeutlicht das Zusammenspiel zwischen den beiden Akteuren gematik und Anbieter des TSL-Dienstes:

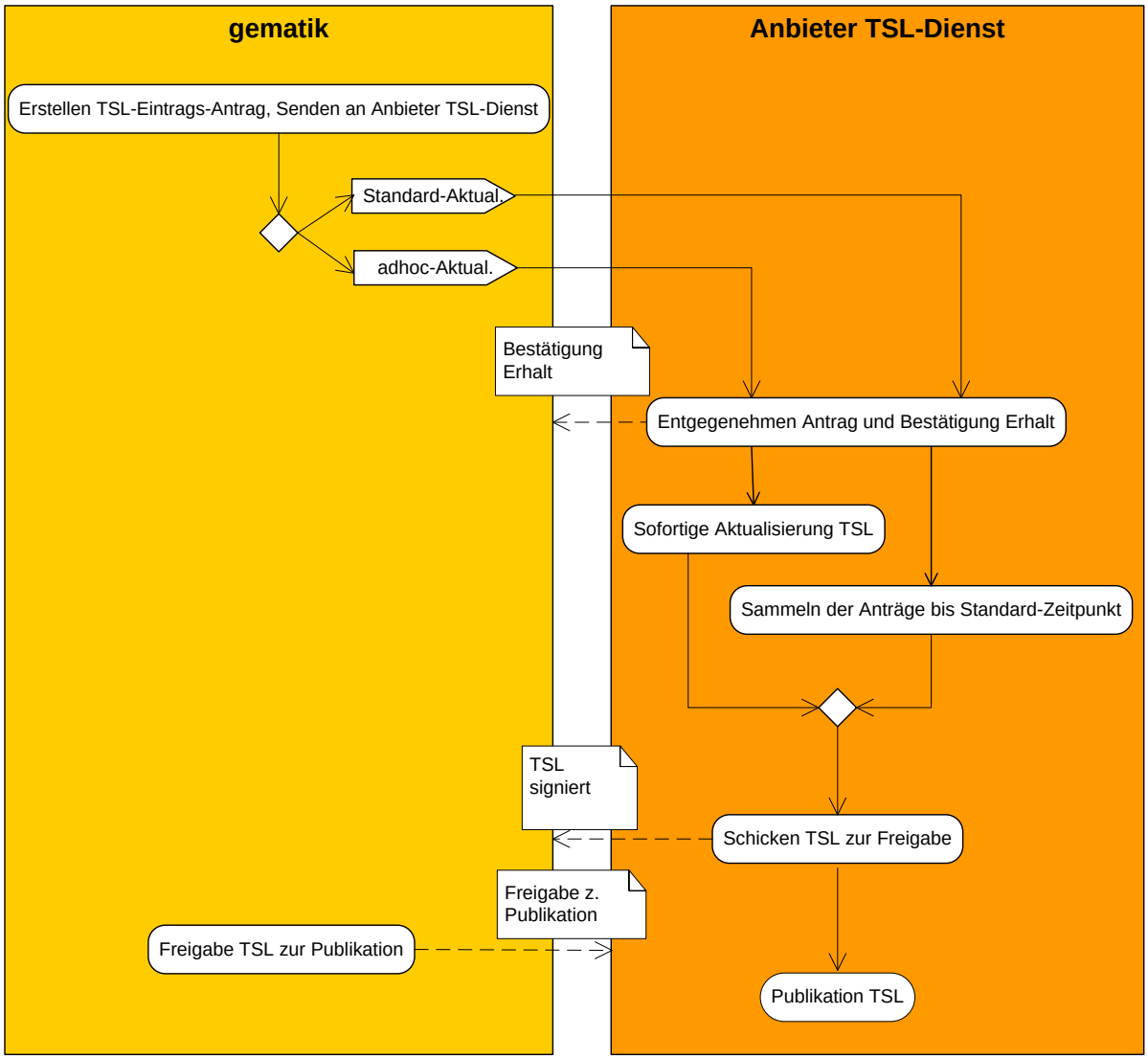


Abbildung 5: Prozess zur Aktualisierung der TSL (schematische Darstellung)

6.1.2.2 Umsetzung Erstellungs- und Aktualisierungsprozesse

Bezüglich der organisatorischen Prozesse der TSL-Eintragsverwaltung sind die folgenden Anforderungen hinsichtlich Aktualisierung und Änderung zu berücksichtigen.

6.1.2.2.1 Aktualisierung

⌦ **TIP1-A_4037 Aktualisierungen: Standard und adhoc**

Bei der Aktualisierung der TSL-Datei MUSS der Anbieter des TSL-Dienstes zwei verschiedene Prozesse unterstützen:
(a) Standardaktualisierung
(b) adhoc-Aktualisierung auf Aufforderung der gematik ⌫

⌦ **TIP1-A_4038 Standardaktualisierung: periodisch**

Die Standardaktualisierung der TSL-Datei MUSS zu konfigurierbaren periodischen Zeitpunkten stattfinden. ⌫

Das Aktualisierungsintervall wird in [gemSpec_PKI] festgelegt.

⌦ **TIP1-A_4039 Standardaktualisierung: Berücksichtigung TSL-Eintragsanträge**

Der Anbieter des TSL-Dienstes MUSS bei einer Standardaktualisierung alle TSL-Eintragsanträge der gematik berücksichtigen, die bis zum festgelegten Stichtag eingegangen und noch nicht umgesetzt sind.

Falls keine TSL-Eintragsanträge eingetroffen sind, MUSS der Anbieter des TSL-Dienstes den Aktualisierungsprozess basierend auf den bestehenden Einträgen fortsetzen. ⌫

Dadurch stellt der Anbieter des TSL-Dienstes sicher, dass das Ablaufdatum der aktuellsten TSL-Datei in der Zukunft liegt. (Vgl. Erläuterungen zum Element NextUpdate in Kapitel 7.2.3)

Neben der Standardaktualisierung zu festgelegten Zeitpunkten werden auch außerplanmäßige adhoc-Aktualisierungen für dringende Änderungen unterstützt (z. B. Entfernen einer CA aus dem TI-Vertrauensraum nach vorgefallenem Security Incident).

Für alle TSL-Eintragsanträge gelten die folgenden Anforderungen:

6.1.2.2.2 Prüfung des TSL-Eintragsantrages

⌦ **TIP1-A_4042 Prüfung von TSL-Eintragsanträgen**

Der Anbieter des TSL-Dienstes SOLL die mit einem TSL-Eintragsantrag erhaltenen Daten auf Vollständigkeit und Plausibilität (Syntax, Schemavalidierung, erlaubte Werte, Zertifikate etc.) prüfen. Alle korrekten Einträge werden danach in die TSL integriert. ⌫

⌦ **TIP1-A_4043 Prüfung von Änderungsanträgen**

Der Anbieter des TSL-Dienstes MUSS bei Folgeanträgen durch den Vergleich der Betreiberdaten des Ursprungsantrages mit dem Änderungsantrag sicherstellen, dass keine Unstimmigkeiten mit den hinterlegten Informationen vorhanden sind. ⌫

6.1.2.2.3 TSL-Signatur

Jede zu veröffentlichende TSL wird vom Anbieter des TSL-Dienstes signiert. Die Anforderungen an diese Signatur sind in TIP1-A_4083 im Kapitel 7.1 „Aufbau der TSL“ spezifiziert.

6.1.2.2.4 Prüfung

⌦ **TIP1-A_4044 Prüfung auf ungültige Einträge**

Der Anbieter des TSL-Dienstes MUSS auch sicherstellen, dass in der aktuellen Version keine zum Zeitpunkt der TSL-Erstellung abgelaufene nonQES-Einträge ent-

halten sind. Der Anbieter des TSL-Dienstes MUSS abgelaufene Einträge und andere Normabweichungen der gematik melden. ⌫

⌦ **TIP1-A_4851 Beibehalten von abgelaufenen QES-CA-Zertifikaten in der TSL**

Der TSL-Dienst MUSS QES-CA-Zertifikate, deren Gültigkeitszeitraum überschritten ist, noch 30 Jahre in der TSL belassen, nachdem das letzte von dieser CA ausgestellte QES-EE-Zertifikat zeitlich abgelaufen ist. ⌫

6.1.2.2.5 Freigabe

Die gematik gibt final die zu veröffentlichende TSL frei.

⌦ **TIP1-A_4045 Übermittlung zur Freigabe**

Der Anbieter des TSL-Dienstes MUSS die zu veröffentlichende TSL der gematik zur finalen Freigabe übermitteln. ⌫

⌦ **TIP1-A_4046 Freigabe vor Veröffentlichung**

Der Anbieter des TSL-Dienstes DARF NICHT die TSL ohne Freigabe der gematik veröffentlichen. ⌫

6.1.2.2.6 Veröffentlichung

Der Anbieter des TSL-Dienstes veröffentlicht die TSL-Datei.

Hinweis: Die Schnittstelle I_TSL_Download wird in Kapitel 6.3.1 beschrieben.

6.1.2.2.7 Service Level

⌦ **TIP1-A_4026 Service Level**

Der Anbieter des TSL-Dienstes MUSS die Produkttyp-spezifischen Service Level für seine Prozesse gemäß Tab_PKI_701 umsetzen. ⌫

Tabelle 4: Tab_PKI_701 Service Level für Prozesse des Anbieters des TSL-Dienstes

ID	Service Level Cluster	Service-paramter	Beschreibung	Leistungs übergabe punkt	Mess-methode	Wert
TSL_1	Service Level Service-erbringung	Standard-TSL-Eintragsantrag	Es handelt sich um die Frist zur Berücksichtigung von TSL-Eintragsanträgen für Änderungen in der TSL vor dem periodischen Aktualisierungs-zeitpunkt der TSL-Datei. Die TSL-Eintragsanträge, die vor dieser Frist eingegangen sind, müssen berücksichtigt werden.	Meldungs-eingang Anbieter TSL	Durch die Schnittstelle I_TSL-Management erzeugter Zeitstempel	3 WT
TSL_2	Service Level Service-erbringung	adhoc-TSL-Eintragsantrag: Löschen	Maximale Zeitspanne zwischen: Der Anbieter des TSL-Dienstes nimmt den TSL-Eintragsantrag für das adhoc-Löschen von Einträgen in der TSL-Datei entgegen. Der Anbieter des TSL-Dienstes legt die signierte TSL-Datei der gematik zur finalen Freigabe zur adhoc-Publikation vor.	1. Meldungs-eingang Anbieter TSL 2. Rück-	1. Durch die Schnittstelle I_TSL-Management erzeugter Zeitstempel	4 h

ID	Service Level Cluster	Service-paramter	Beschreibung	Leistungs übergabe punkt	Mess-methode	Wert
TSL_3	Service Level Service-erbringung	adhoc-TSL-Eintragsantrag: Hinzufügen und Ändern	Maximale Zeitspanne zwischen: Der Anbieter des TSL-Dienstes nimmt den TSL-Eintragsantrag für Hinzufügungen und Änderungen von Einträgen in der TSL-Datei entgegen. Der Anbieter des TSL-Dienstes legt die signierte TSL-Datei der gematik zur finalen Freigabe vor.	meldung an gematik	2. Zeitstempel Eingang E-Mail oder äquivalent	1 WT
TSL_4	Service Level Service-erbringung	Veröffentli-chung der TSL-Datei nach adhoc-Löschen	Maximale Zeitspanne zwischen: Die gematik gibt die neu erstellte TSL-Datei nach erfolgtem adhoc-Löschen frei. Die neu erstellte TSL-Datei kann unter den Adressen der Download-Punkte heruntergeladen werden.	1. Meldungs-eingang Anbieter TSL 2. I_TSL_Download	1. Zeitstempel E-Mail oder äquivalent 2. Durch http-Client generierter Zeitstempel	2h
TSL_5	Service Level Service-erbringung	Normale Veröffentli-chung der TSL-Datei	Maximale Zeitspanne zwischen: Die gematik gibt die neu erstellte TSL-Datei frei, nachdem diese periodisch aktualisiert wurde oder adhoc Einträge hinzugefügt oder geändert wurden. Die neu erstellte TSL-Datei kann unter den Adressen der Download-Punkte heruntergeladen werden.			1 WT

Hinweis: Weitere Anforderungen im Hinblick auf produkttyp-übergreifendes Service Level Management werden in [gemRL_Betr_TI] gestellt. Performance-Anforderungen sind in [gemSpec_Perf] geregelt.

6.1.3 Schnittstelle P_Trust_Approval

6.1.3.1 Schnittstellendefinition

P_Trust_Approval stellt die Schnittstelle dar, die alle Prozesse beinhaltet, die ein TSP-X.509 nutzt, um seine Dienste in der TSL-Datei einzutragen. Diese Prozesse sind in den Gesamtablauf der Zulassungs- und Registrierungsprozesse eingebettet, bei welchem der TSP-X.509 immer zwingend mit der gematik kommuniziert. So muss der TSP-X.509 etwa für den Eintrag in die TSL-Datei der Produktivumgebung erst die Zulassung von der Zulassungs- und Registrierungsstelle der gematik erhalten.

Aus diesem Grund übernimmt die gematik im Sinne der Komplexitätsreduktion sämtliche Kommunikation mit den TSP-X.509. Aus Sicht des Anbieters des TSL-Dienstes kanalisiert sie die TSL-Eintragsanträge und reicht sie an ihn weiter. Für den Anbieter des TSL-Dienstes sind deshalb die Prozesse, die er der gematik zur Verfügung stellen muss, relevant. Diese werden im Kapitel 6.1.2 „Schnittstelle P_TSL-Management“ besprochen.

6.1.3.2 Umsetzung

Die Umsetzung der Schnittstelle P_Trust_Approval wird von der gematik übernommen (siehe oben) und wird deshalb gematik-intern geregelt.

⌦ TIP1-A_4048 Eintrag in der TSL nach erfolgter Zulassung

Die gematik MUSS den Eintrag eines TSP-Dienstes in der TSL-Datei veranlassen, wenn dieser sämtliche Voraussetzungen dafür erfüllt. ⌫

6.1.4 Testunterstützung

Neben der PKI für die Produktivumgebung (PU) wird eine davon separierte PKI für Test- und Referenzzwecke betrieben. (Siehe dazu [gemSpec_PKI#3.2.2]).

Pro PKI-Umgebung muss also eine eigene TSL-Datei herausgegeben werden.

⌦ **TIP1-A_4438 TSL-Datei für Testzwecke**

Der TSL-Dienst MUSS eine spezifische TSL-Datei erstellen, die den TI-Vertrauensraum für Testzwecke abbildet. ⌫

Die Felder, in denen sich diese TSL-Datei von derjenigen für die Produktivumgebung unterscheidet, sind in Kapitel 7.6 beschrieben.

⌦ **TIP1-A_4439 Schnittstelle I_TSL-Management für Test**

Der TSL-Dienst MUSS eine getrennte Instanz der Schnittstelle I_TSL-Management für Testzwecke implementieren. ⌫

6.2 TSL_PKI-Verwaltung

Der Anbieter des TSL-Dienstes muss für den TSL-Dienst sämtliche Prozesse und Schnittstellen implementieren, welche das Management von PKI-spezifischen Anforderungen, also bspw. die Abwicklung von Prozessen bei der Schlüssel- und Zertifikatsverwaltung der TSL-Signer-CA, des TSL-Signers und des OCSP-Responders erlauben.

Das Funktionsmerkmal TSL_PKI-Verwaltung beinhaltet grundsätzlich auch den TI-Vertrauensankerwechsel. Da dieser erst zu einem späteren Zeitpunkt durchgeführt wird, wird dieser nur konzeptionell beschrieben, also nicht detailliert ausspezifiziert.

6.2.1 Schnittstelle P_TSL-PKI-Zertifikats-Management

6.2.1.1 Schnittstellendefinition

Die Schnittstelle P_TSL-PKI-Zertifikats-Management setzt organisatorisch die Prozesse um, welche für die Generierung von Schlüsselpaaren und Zertifikaten notwendig ist.

6.2.1.2 Umsetzung

⌦ **TIP1-A_4049 Prozess für Schlüsselpaargenerierung und Zertifizierung**

Der Anbieter des TSL-Dienstes MUSS den Prozess der Schlüsselpaargenerierung und Zertifizierung anstoßen. Der Anbieter des TSL-Dienstes MUSS dies zu einer mit der gematik vereinbarten Frist vor dem Ablauf eines bestehenden Zertifikates tun. ⌫

⌦ **TIP1-A_4440 Konzept Prozess für Schlüsselpaargenerierung und Zertifizierung**

Der Anbieter des TSL-Dienstes MUSS ein Konzept für den Prozess der Schlüsselpaargenerierung und Zertifizierung erstellen. ⌫

TIP1-A_4050 Zertifikatswechsel

Der Anbieter des TSL-Dienstes MUSS zu einem mit der gematik vereinbarten Zeitpunkt den Prozess des Zertifikatswechsels (Erneuerung TSL-Signer-, TSL-Signer-CA- und OCSP-Signer-Zertifikat) anstoßen. ⌫

TIP1-A_4441 Konzept Zertifikatswechsel

Der Anbieter des TSL-Dienstes MUSS ein Konzept für den Prozess des Zertifikatswechsels (Erneuerung TSL-Signer-, TSL-Signer-CA- und OCSP-Signer-Zertifikat) erstellen. ⌫

TIP1-A_4442 Auftrag für Schlüsselerzeugung TSL-Signer

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass ein neues Schlüsselpaar und das darauf basierende Zertifikat für den TSL-Signer nur im Auftrag der gematik erzeugt werden. ⌫

TIP1-A_4051 Auftrag für Schlüsselerzeugung TSL-Signer-CA und OCSP-Responder

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass ein neues Schlüsselpaar und der darauf basierende Zertifikats-Request für TSL-Signer-CA und OCSP-Responder nur aufgrund eines geprüften (Authentizität, Autorisierung) Auftrages der gematik erzeugt werden. ⌫

TIP1-A_4052 Auftrag für Schlüsselerzeugung, 2 Mitarbeiter

Der Anbieter des TSL-Dienstes MUSS überprüfen, dass der Auftrag für eine Schlüsselerzeugung der TSL-Signer-CA, des TSL-Signers und des OCSP-Responders durch zwei verantwortliche Mitarbeiter der gematik unterschrieben ist. Er MUSS dabei die Authentizität und Autorisierung dieser Mitarbeiter auf geeignete verlässliche Weise überprüfen. ⌫

TIP1-A_4053 Auftrag für Erzeugung, Inhalt

Der Anbieter des TSL-Dienstes MUSS prüfen, ob der Auftrag der gematik mindestens die folgenden Daten enthält:
(a) Datum des Auftrags
(b) Name des verantwortlichen Mitarbeiters 1 der gematik
(c) Name des verantwortlichen Mitarbeiters 2 der gematik
(d) Indikator, ob es sich um einen „normalen“ oder einen „notfallmäßigen“ Wechsel bzw. um eine initiale Schlüsselgenerierung handelt
(e) Vorgabe für die Länge und für den Algorithmus des neuen Schlüsselpaares ⌫

6.2.2 Schnittstelle P_Trust-Anchor-Change

6.2.2.1 Schnittstellendefinition

Die Schnittstelle P_Trust-Anchor-Change dient der organisatorischen Abwicklung des TI-Vertrauensankerwechsels auf Seite des Anbieters des TSL-Dienstes, also des Updates des Schlüsselpaares und Zertifikates der TSL-Signer-CA. Dieser wird folgendermaßen umgesetzt:

Das neue TSL-Signer-CA-Zertifikat wird nach dessen Generierung vom Anbieter des TSL-Dienstes mit dem Aktivierungszeitpunkt markiert und rechtzeitig in die TSL integriert. Dabei wird die Integrität des neuen Schlüssels und des dazugehörigen Zertifikates durch den gültigen alten TI-Vertrauensanker gesichert.

6.2.2.2 Umsetzung

⌦ **TIP1-A_4054 TI-Vertrauensankerwechsel, Prozess**

Der Anbieter des TSL-Dienstes MUSS den TI-Vertrauensankerwechsel (neues TSL-Signer-CA-Zertifikat und spezifischer Eintrag in die TSL) umsetzen können. ⌫

⌦ **TIP1-A_4852 TI-Vertrauensankerwechsel, Konzept**

Der Anbieter des TSL-Dienstes MUSS über ein Konzept verfügen, wie er die folgenden Prozesse rechtzeitig initiiert und korrekt umsetzt:
(a) Schlüssel- und Zertifikatserneuerung für die TSL-Signer-CA
(b) Eintragung des neuen TSL-Signer-CA unter TSP-Diensten, markiert als neuer TI-Vertrauensanker
Der Anbieter des TSL-Dienstes MUSS in diesem Konzept die Fristen der jeweiligen Prozessschritte festlegen. ⌫

Nach dem Initiieren des Prozesses seitens des Anbieters des TSL-Dienstes erfolgt die Schlüssel- und Zertifikatserneuerung gemäß Kapitel 6.2.1 „Schnittstelle P_TSL-PKI-Zertifikats-Management“. (Ein Antrag der gematik wird benötigt.)

Die technischen Anforderungen an einen TSP-Dienst-Eintrag werden in Kapitel 7.3.2 „Angaben zum TSP-Dienst“ gestellt.

Die Abweichungen, um eine solchen Dienst als neuen TI-Vertrauensanker zu markieren, werden in [gemSpec_PKI], insbesondere [gemSpec_PKI#8.1.2.2] beschrieben.

6.2.3 Testunterstützung

Neben der PKI für die Produktivumgebung (PU) wird eine davon separierte PKI für Test- und Referenzzwecke betrieben. (Siehe dazu [gemSpec_PKI#3.2.2]). Pro PKI-Umgebung müssen also individuelle Schlüsselpaare und Zertifikate erzeugt werden.

⌦ **TIP1-A_4443 TSL-Zertifikate für Testzwecke**

Der Anbieter des TSL-Dienstes MUSS pro PKI-Umgebung separate Schlüsselpaare und Zertifikate für die TSL-Signer-CA, den TSL-Signer und seine OCSP-Responder erzeugen. ⌫

⌦ **TIP1-A_4444 Namen für TSL-Zertifikate für Testzwecke**

Der Anbieter des TSL-Dienstes MUSS die Namen (CN: und O:) sämtlicher seiner Zertifikate für Testzwecke entsprechend den korrespondierenden Zertifikatsprofilen der Produktivumgebung verwenden und diese um den String „TEST-ONLY“ im CN-Feld sowie „NOT-VALID“ im O-Feld ergänzen.⌫

⌦ **TIP1-A_4445 Profile TSL-Zertifikate für Testzwecke**

Der Anbieter des TSL-Dienstes SOLL die Feldattribute (außer CN: und O:) für sämtliche seiner Zertifikate für Testzwecke gemäß den korrespondierenden Profilen der Produktivumgebung setzen. ⌫

⌦ **TIP1-A_4446 Trennung von Komponenten PU und Test-PKI**

Der Anbieter des TSL-Dienstes DARF NICHT ein HSM oder eine andere Komponente aus der Produktivumgebung für die Test-PKI benutzen. Der Anbieter des TSL-Dienstes DARF NICHT ein HSM oder eine andere Komponente aus der Test-PKI für die Produktivumgebung benutzen. ⌫

6.3 TSL_Download

Das Funktionsmerkmal TSL_Download stellt das Herunterladen der aktuellsten TSL-Datei sicher (Schnittstelle I_TSL_Download). Dies geschieht in der TI über HTTP, für den (manuellen) Download über das Internet wird der Downloadpunkt über HTTPS erreicht. Über das Internet können auch das TSL-Signer-CA- und das TSL-Signer-Zertifikat, sowie Angaben dazu heruntergeladen werden (Schnittstelle I_Cert_Download).

6.3.1 Schnittstelle I_TSL_Download

6.3.1.1 Schnittstellendefinition

Die Schnittstelle I_TSL_Download wird durch [gemKPT_Arch_TIP] vorgegeben: Nach erfolgreicher Veröffentlichung der TSL muss diese allen Komponenten zur Verfügung stehen.

Die Schnittstelle I_TSL_Download stellt also die TSL den TSL-validierenden Systemen zum Download bereit.

6.3.1.2 Umsetzung

⌦ **TIP1-A_4055 Web-Server**

Der TSL-Dienst MUSS die Schnittstelle I_TSL_Download über einen eigenen, selbstbetriebenen Web-Server zur Verfügung stellen. ⌫

Siehe auch Kapitel 5.4, TIP1-A_3968 bezüglich der Sicherheit des Web-Servers.

⌦ **TIP1-A_4056 I_TSL_Download: HTTP für TI**

Der TSL-Dienst MUSS die Schnittstelle I_TSL_Download gemäß HTTP Version 1.1 [RFC2616] implementieren. Die Schnittstelle MUSS ohne Verwendung des TLS-Protokolls (HTTPS) erreichbar sein. ⌫

⌦ **TIP1-A_4057 I_TSL_Download: HTTPS für Internet**

Der TSL-Dienst MUSS die Schnittstelle I_TSL_Download im Internet gemäß HTTP Version 1.1 [RFC2616] über TLS (HTTPS) implementieren. Dabei MUSS das TLS-Protokoll gemäß [gemSpec_Krypt#GS-A_4385] und [gemSpec_Krypt#GS-A_4386] mit einseitiger Authentifizierung (Server-Authentisierung) implementiert sein. ⌫

⌦ **TIP1-A_4058 X.509-Zertifikat für HTTPS-Verbindung**

Der TSL-Dienst MUSS für die HTTPS-Verbindung ein X.509-Zertifikat verwenden, welches in keinem marktüblichen Webbrowser (z.B. Firefox, Internet Explorer, Chrome und Safari) zu einer Warn- oder Fehlermeldung führt. ⌫

⌦ **TIP1-A_4059 EV-SSL-Zertifikat für HTTPS-Schnittstelle**

Der TSL-Dienst SOLL für die HTTPS-Schnittstelle ein Extended-Validation-SSL-Zertifikat gemäß [EVSSL] verwenden. ⌫

⌦ **TIP1-A_4060 I_TSL_Download: URIs**

Der TSL-Dienst MUSS diese URIs, unter denen die Schnittstelle I_TSL_Download erreichbar ist, gemäß den Vorgaben für den Namensraum der gematik gestalten. ⌫

Der HTTP-URI für die TI wird in das entsprechende Element der TSL integriert (siehe 7.2.6).

Die Schnittstelle I_TSL_Download enthält genau eine logische Operation download_TSL, welche als Output die TSL in der in Kapitel 7 beschriebenen Form liefert.

⌦ **TIP1-A_4062 I_TSL_Download::download_TSL: GET-Befehl**

Der TSL-Dienst MUSS die logische Operation I_TSL_Download::download_TSL so implementieren, dass sie durch den HTTP-GET-Befehl angestoßen werden. ⌫

⌦ **TIP1-A_4063 I_TSL_Download::download_TSL: Header**

Der TSL-Dienst MUSS die logische Operation I_TSL_Download::download_TSL so implementieren, dass die Server-Antwort die notwendigen HTTP-Header-Datenfelder gemäß [RFC2616] enthält. ⌫

⌦ **TIP1-A_4064 I_TSL_Download::download_TSL: Content-Type**

Der TSL-Dienst SOLL die logische Operation I_TSL_Download::download_TSL so implementieren, dass das Datenfeld „Content-Type“ im HTTP-Header der Server-Antwort als Wert den MIME-Type „application/vnd.etsi.tsl+xml“ enthält.⌫

Hinweis: Dieser MIME-Type entspricht der IANA-Registrierung (siehe http://www.iana.org/assignments/media-types/application/vnd.etsi.tsl+xml) für TSL-Dateien im XML-Format. Der von [ETSI_TS_102_231_V3.1.2] bis Version 3.1.2 vorgeschriebene MIME-Type „application/vnd.etsi.tsl.xml“ ist nicht korrekt. Dies wird für die folgenden Versionen korrigiert werden.

⌦ **TIP1-A_5119 TSL-Dienst: HTTP-Komprimierung unterstützen**

Der TSL-Dienst MUSS die Komprimierung der Daten mittels HTTP-Komprimierung gemäß HTTP1.1 mit dem Algorithmus gzip unterstützen. ⌫

⌦ **TIP1-A_5120 Clients des TSL-Dienstes: HTTP-Komprimierung unterstützen**

Die Produkttypen der TI, die die TSL-Datei herunterladen, SOLLEN die Komprimierung der Daten mittels HTTP-Komprimierung gemäß HTTP1.1 mit dem Algorithmus gzip unterstützen. ⌫

⌦ **TIP1-A_4065 I_TSL_Download::download_TSL: Body**

Der TSL-Dienst MUSS die logische Operation I_TSL_Download::download_TSL so implementieren, dass die Server-Antwort im HTTP-Body die TSL als XML-Datei enthält. ⌫

Hinweis: Auf das genaue Format der TSL-XML-Datei wird in Kapitel 7 eingegangen.

6.3.2 Schnittstelle I_Cert_Download

6.3.2.1 Schnittstellendefinition

Die Schnittstelle I_Cert_Download stellt das TSL-Signer-CA-Zertifikat den Herstellern von Produkttypen, die Zertifikate prüfen, unter einer statischen URL zum sicheren Download zur Verfügung (vgl. [gemSpec_PKI#GS-A_4640]). Auch wird das TSL-Signer-Zertifikat selbst als einzelne Datei bereitgestellt.

6.3.2.2 Umsetzung

⌦ **TIP1-A_4066 Web-Server I_Cert_Download**

Der TSL-Dienst MUSS die Schnittstelle I_Cert_Download via eigenen, selbstbetriebenen Web-Server zur Verfügung stellen. ⌫

Siehe auch Kapitel 5.4, TIP1-A_3968 bezüglich der Sicherheit des Web-Servers.

⌦ **TIP1-A_4067 I_Cert_Download: HTTPS**

Der TSL-Dienst MUSS die Schnittstelle I_Cert_Download im Internet gemäß HTTP Version 1.1 [RFC2616] über TLS (HTTPS) implementieren. Dabei MUSS das TLS-Protokoll gemäß [gemSpec_Krypt#GS-A_4385] und [gemSpec_Krypt#GS-A_4386] mit einseitiger Authentifizierung (Server-Authentisierung) implementiert sein. ⌫

⌦ **TIP1-A_4068 X.509-Zertifikat für HTTPS-Verbindung I_Cert_Download**

Der TSL-Dienst MUSS für die HTTPS-Verbindung ein X.509-Zertifikat verwenden, welches in keinem marktüblichen Webbrowser (z.B. Firefox, Internet Explorer, Chrome und Safari) zu einer Warn- oder Fehlermeldung führt. ⌫

⌦ **TIP1-A_4069 EV-SSL-Zertifikat für HTTPS-Schnittstelle I_Cert_Download**

Der TSL-Dienst SOLL für die HTTPS-Verbindung ein Extended-Validation-SSL-Zertifikat gemäß [EVSSL] verwenden. ⌫

⌦ **TIP1-A_4070 feste URIs I_Cert_Download**

Der TSL-Dienst MUSS sicherstellen, dass die Schnittstelle I_Cert_Download über statische, vollständige URIs erreichbar ist. ⌫

Die Schnittstelle I_Cert_Download enthält genau eine logische Operation download_Cert, welche als Output das jeweilige Zertifikat liefert.

⌦ **TIP1-A_4071 I_Cert_Download::download_Cert**

Der TSL-Dienst MUSS für die Schnittstelle I_Cert_Download die logische Operation download_Cert implementieren. ⌫

⌦ **TIP1-A_4072 I_Cert_Download::download_Cert: GET-Befehl**

Der TSL-Dienst MUSS die logische Operation I_TSL_Download::download_Cert so implementieren, dass sie durch den HTTP-GET-Befehl angestoßen wird. ⌫

⌦ **TIP1-A_4073 I_Cert_Download::download_Cert: Body**

Der TSL-Dienst MUSS die logische Operation I_TSL_Download::download_Cert so implementieren, dass die Server-Antwort im HTTP-Body das entsprechende DER-codierte Zertifikat enthält. ⌫

⌦ **TIP1-A_4074 TSL-Signer-CA-, TSL-Signer-, Komponenten-CA-Zertifikat: Angaben**

Der TSL-Dienst MUSS für das TSL-Signer-CA-Zertifikat und das TSL-Signer-Zertifikat sowie auch für das Komponenten-CA-Zertifikate die folgenden Angaben im Web veröffentlichen:
(a) Das X.509-Zertifikat an sich
(b) Den Fingerprint des Zertifikates gemäß [gemSpec_Krypt#GS-A_4393]
(c) Das Datum, des Beginns der Gültigkeit des zugehörigen Schlüsselpaares für den Einsatz als TSL-Signer-CA (TI-Vertrauensanker), als TSL-Signer oder als Komponenten-CA⌫

⌦ **TIP1-A_4075 Fingerprint TSL-Signer-CA-Zertifikat per Post**

Der Anbieter des TSL-Dienstes MUSS auf Anfrage von Herstellern von Produkttypen und anderen berechtigten Teilnehmern in der TI den Fingerprint des TSL-Signer-CA-Zertifikats schriftlich per Post verschicken. ⌫

6.3.3 Testunterstützung

Neben der PKI für die Produktivumgebung (PU) wird eine davon separierte PKI für Test- und Referenzzwecke betrieben. (Siehe dazu [gemSpec_PKI#3.2.2]). Die Schnittstellen I_TSL_Download und I_Cert_Download müssen deshalb für alle PKI-Umgebungen zur Verfügung gestellt werden.

⌦ **TIP1-A_4447 Publikation von Test-TSL und -Zertifikaten**

Der TSL-Dienst MUSS die TSL-Datei für Testzwecke, sowie seine Zertifikate für Testzwecke und die dazugehörigen Angaben zum Download bereitstellen und publizieren. Der TSL-Dienst MUSS diese Daten als Testdaten kennzeichnen. ⌫

⌦ **TIP1-A_4448 I_TSL_Download: Eigene Instanz für Test-TSL in TI**

Der TSL-Dienst SOLL eine eigene Dienstinstanz für die Schnittstelle I_TSL_Download für den Download der TSL für Testzwecke in der TI betreiben. ⌫

6.4 TSL_OCSP_Responder

Das TSL-Signer-Zertifikat muss von den Komponenten der Telematikinfrastruktur Status-geprüft werden können. Dafür wird ein dedizierter OCSP-Responder betrieben.

⌦ **TIP1-A_4076 Erreichbarkeit OCSP-Responder**

Der TSL-Dienst MUSS sicherstellen, dass der Validierungsdienst in Form eines OCSP-Responders über das Netzwerk der Telematikinfrastruktur erreichbar ist. ⌫

6.4.1 Schnittstelle I_OCSP_Status_Information

Die technischen Parameter und Anforderungen der Schnittstelle *I_OCSP_Status_Information des* Funktionsmerkmals „TSL_OCSP_Responder“ sind in [gemSpec_PKI#9.1] vollständig beschrieben. Es gelten die Anforderungen, welche dort an den TSL-Dienst gestellt werden.

6.4.2 Schnittstelle P_Cert_Revocation

6.4.2.1 Schnittstellendefinition

Die organisatorische Schnittstelle P_Cert_Revocation stellt sicher, dass das TSL-Signer-Zertifikat gesperrt werden kann.

6.4.2.2 Umsetzung

⌦ **TIP1-A_4077 Organisatorische Trennung für OCSP**

Der Anbieter des TSL-Dienstes MUSS eine klare organisatorische Trennung zwischen dem Betrieb und den Verantwortlichkeiten der Prozesse zum Sperren und des OCSP-Responders einerseits und sonstigen Betrieb und Rollen in der TI andererseits umsetzen und dokumentieren. ⌫

⌦ **TIP1-A_4078 Sperrantrag**

Der Anbieter des TSL-Dienstes DARF NICHT Sperranträge von anderen Stellen als von vorgängig bezeichneten Mitarbeitern der gematik entgegennehmen und bearbeiten.⌫

⌦ **TIP1-A_4079 Verfahren für Sperrung TSL-Signer-Zertifikat**

Der Anbieter des TSL-Dienstes MUSS ein Verfahren für die unverzügliche Sperrung des TSL-Signer-Zertifikats bereitstellen und dokumentieren. Der Anbieter des TSL-Dienstes MUSS in der Dokumentation aufzeigen, dass dieses Verfahren auf höchstem Niveau sicher und stabil ist. ⌫

6.4.3 Testunterstützung

Neben der PKI für die Produktivumgebung (PU) wird eine davon separierte PKI für Test- und Referenzzwecke betrieben. (Siehe dazu [gemSpec_PKI#3.2.2]). Der Validierungsdienst in Form eines OCSP-Responders muss für jede PKI-Umgebung bereitgestellt werden.

- Die OCSP-Responder für das TSL-Signer-Zertifikat müssen in allen Umgebungen (PU, RU/TU und Internet) als separate Instanzen realisiert werden.
- Alle im Internet bereitzustellenden OCSP-Responder müssen als von der TI separierte Instanzen realisiert werden. Separiert bedeutet: auf separater Hardware und, sofern zur Synchronisation eine gemeinsame Datenbasis genutzt wird, gemäß [gemSpec_Net#GS-A_4062] über ein Sicherheitsgateway zu synchronisieren
- Alle weiteren von einem Anbieter in einer Umgebung angebotenen OCSP-Responder können unter Beachtung der Regeln 1) und 2) sowohl

zusammengefasst über einen einzelnen OCSP-Responder als auch über verschiedene virtualisierte OCSP-Responder realisiert werden. Werden die OCSP-Responder zusammengefasst, so ist dies in gleicher Weise in PU und RU/TU zu realisieren.

⌦ **TIP1-A_4449 OCSP-Responder für Test-TSL-Signerzertifikat**

Der TSL-Dienst MUSS einen individuellen OCSP-Responder zur Validierung des TSL-Signer-Zertifikats zu Testzwecken betreiben. ⌫

7 Informationsmodell: Technische Spezifikation TSL

7.1 Aufbau der TSL

Der strukturelle Aufbau sowie die einzelnen TSL-Elemente und ihre Inhalte sind in [ETSI_TS_102_231_V3.1.2] beschrieben.

⌦ **TIP1-A_4081 ETSI_TS_102_231**

Der TSL-Dienst MUSS die TSL gemäß den Vorgaben nach [ETSI_TS_102_231_V3.1.2] erzeugen und befüllen. ⌫

⌦ **TIP1-A_4082 ETSI_TS_102_231 Annex B und XML-Schema**

Der TSL-Dienst MUSS die TSL als XML-Datei gemäß [ETSI_TS_102_231_V3.1.2#B] und somit auch konform zu dem durch [ETSI_TS_102_231_V3.1.2#B] definierten XML-Schema [ts_102231v030102_xsd.xsd] erzeugen.⌫

Für die TI, insbesondere für das Funktionieren der PKI-spezifischen Technischen Use Cases (TUCs), müssen die allgemeinen Vorgaben aus [ts_102231v030102_xsd.xsd] (das Schema gemäß ETSI) weiter eingeschränkt werden.

⌦ **TIP1-A_5121 XML-Schema spezifisch für TI**

Der TSL-Dienst MUSS die TSL als XML-Datei gemäß Tab_PKI_710 bis Tab_PKI_716 erstellen.⌫

In den nachfolgenden Abschnitten werden Vorgaben zur Verwendung und zum Inhalt relevanter Felder gemacht, die vom TSL-Dienst einzuhalten sind.

Die Abbildung 6 zeigt die Grundstruktur der TSL. Die Schemainformationen geben Auskunft u. a. über den Herausgeber der TSL. Die "TrustServiceProviderList“ beinhaltet die Angaben der registrierten TSPs.

⌦ **TIP1-A_4083 XML-Signatur**

Der TSL-Dienst MUSS die Integrität der Inhalte der TSL durch eine Signatur der XML-Datei gemäß [ETSI_TS_102_231_V3.1.2#B.6] gewährleisten.
Der TSL-Dienst MUSS die Signatur der TSL entsprechend der Vorgaben aus [gemSpec_Krypt#GS-A_4371] wählen. ⌫

Das Signaturfeld ist also obligatorisch.

Tabelle 5: Tab_PKI_710 TSL-Datei – Element TrustStatusList

Bezeichnung	TrustServiceStatusList
Beschreibung	Siehe [ETSI_TS_102_231_V3.1.2#B.5]
Optional	Nein

Wertebereich	Das Attribut „Id“ muss zwingend vorhanden sein. Das Element „TrustServiceProviderList" muss zwingend vorhanden sein. Das Element „ds:Signature“ muss zwingend vorhanden sein.

⌦ TIP1-A_4084 X.509-Zertifikate, Element X509Certificate

Der TSL-Dienst MUSS sämtliche in der TSL referenzierten X.509-Zertifikate (z.B. CA-, OCSP-, CRL- oder TSL-Signer) direkt als Element X509Certificate in der TSL eintragen. ⌫

Tabelle 6: Tab_PKI_711 TSL-Datei – Element DigitalId

Bezeichnung	DigitalId
Beschreibung	Siehe [ETSI_TS_102_231_V3.1.2#B.5]
Optional	Nein
Wertebereich	X509Certificate oder Other gemäß [ETSI_TS_102_231_V3.1.2#B.5]

Tabelle 7: Tab_PKI_712 TSL-Datei – Element KeyInfo

Bezeichnung	ds:KeyInfo
Beschreibung	Siehe [ETSI_TS_102_231_V3.1.2#B.5]
Optional	Nein
Wertebereich	X509Certificate gemäß [ETSI_TS_102_231_V3.1.2#B.5]

⌦ TIP1-A_4085 ETSI_TS_102_231 Annex B: nur erforderliche Elemente

Der TSL-Dienst SOLL neben den gemäß [ETSI_TS_102_231_V3.1.2#B] zwingend erforderlichen Elementen nur Elemente in die TSL einfügen, die durch Anforderungen explizit verlangt werden. ⌫

Eine Hilfe für das Verständnis der grafischen Darstellungen der Elemente ist in „Anhang B – Leseanleitung für XML-Schema-Fragmente beschrieben.

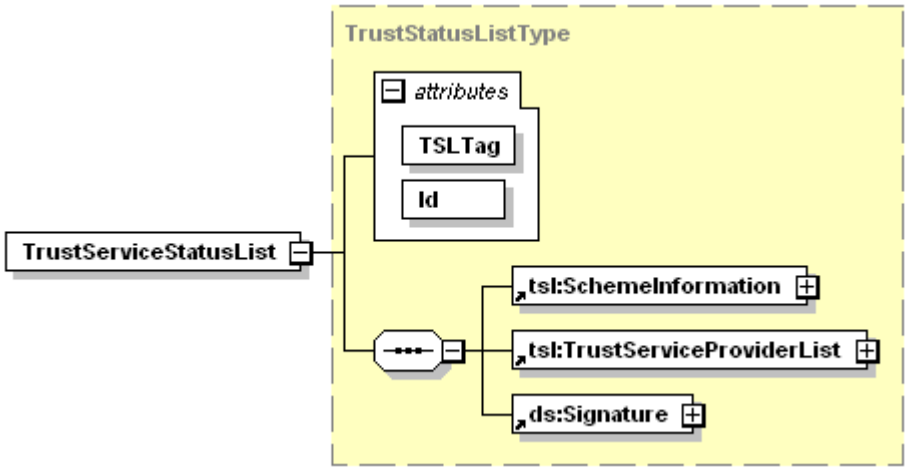


Abbildung 6: Grundstruktur der TSL-Elemente

⌦ **TIP1-A_4086 TSL ID**

TSL-Dienst MUSS das Attribut "Id" im Header der TSL-Datei befüllen und dabei das Erstellungsdatum in den Wert des Attributes einfließen lassen. (Id="ID*versionSequenzErstellungsdatumUhrzeit*"). Das Attribut "Id" besteht aus mehreren Datentypen in denen das ErstellungsdatumUhrzeit im Attribut "Id" folgendes, von [gemSpec_TSL#TIP1-A_4087] abweichendes, Format aufweisen muss: "YYYYMMDDhhmmssZ". ⌫

Übergreifend für die folgenden Ausführungen gilt:

⌦ **TIP1-A_4087 TSL Datumsformat**

Der TSL-Dienst MUSS Datumsformate nach [ETSI_TS_102_231_V3.1.2] als xsd:dateTime gestalten. Das Format MUSS wie folgt aufgebaut sein: *<YYYY-MM-DDThh:mm:ssZ>* **-** Beispiel: *2012-04-12T23:59:59Z*⌫

7.2 Inhalte des Elements „SchemeInformation“

Abbildung 7 stellt die Grundstruktur der TSL als Schemadiagramm dar. Das Element SchemeInformation gibt u. a. Auskunft über den Herausgeber der TSL.

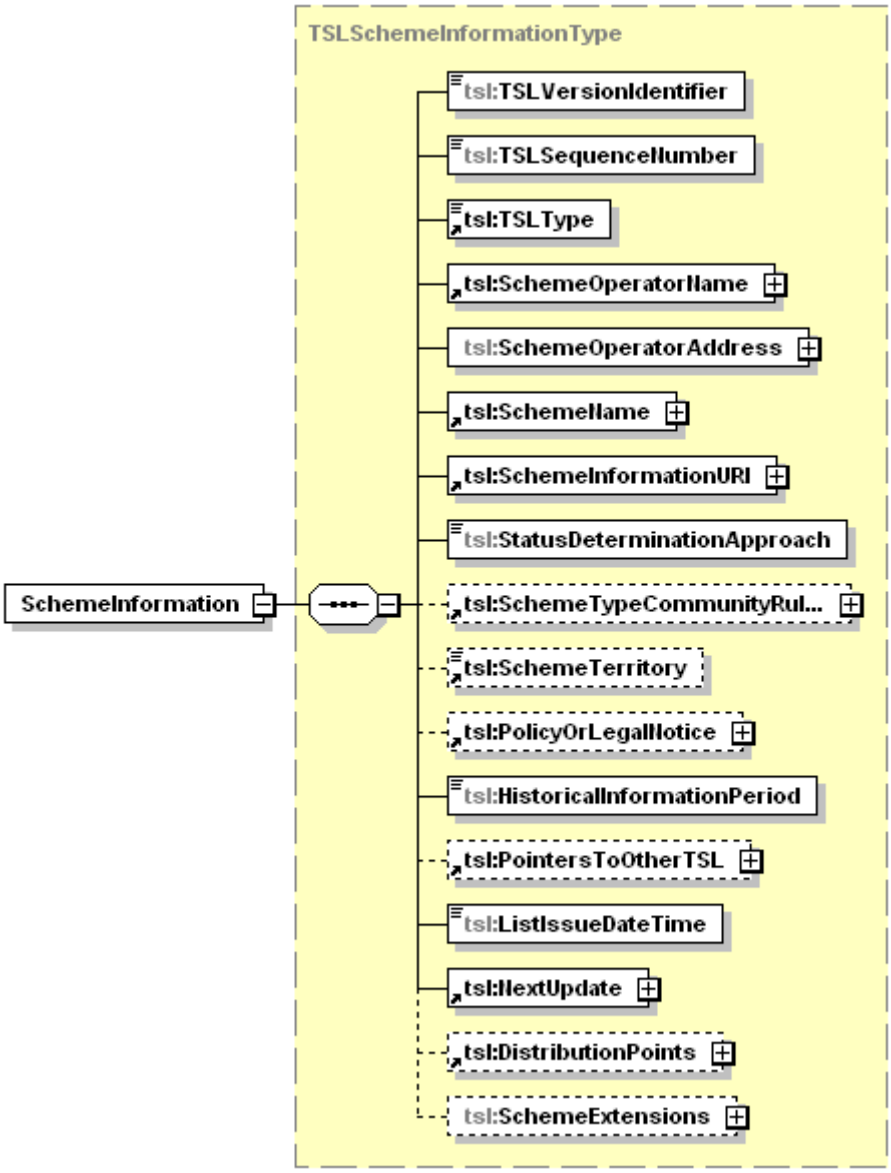


Abbildung 7: Element „SchemeInformation“

In den folgenden Abschnitten werden die normativen Werte für die Felder im Element SchemeInformation festgelegt.

7.2.1 Allgemeine TSL-Angaben

TIP1-A_4088 TSLType

Der TSL-Dienst MUSS das Element „TSLType“ wie folgt befüllen:
`<TSLType>http://uri.etsi.org/TrstSvc/TSLtype/generic</TSLType>`

TIP1-A_4089 TSL SchemeOperatorName

Der TSL-Dienst MUSS das Element SchemeOperatorName wie folgt befüllen:

```
<SchemeOperatorName>
 <Name xml:lang="DE">gematik Scheme</Name>
</SchemeOperatorName>
```

⌦ **TIP1-A_4090 TSL SchemeName**

Der TSL-Dienst MUSS das Element „SchemeName“ wie folgt befüllen:

```
<SchemeName>
 <Name xml:lang="DE">gematik TSL Scheme</Name>
</SchemeName> ⌫
```

⌦ **TIP1-A_4091 TSL SchemeInformationURI**

Der TSL-Dienst MUSS das Element „SchemeInformationURI“ wie folgt befüllen:

```
<SchemeInformationURI>
 <URI xml:lang="DE">http://www.gematik.de</URI>
</SchemeInformationURI> ⌫
```

⌦ **TIP1-A_4092 TSL StatusDeterminationApproach**

Der TSL-Dienst MUSS das Element „StatusDeterminationApproach“ wie folgt befüllen:

```
<StatusDeterminationApproach>
http://uri.etsi.org/TrstSvc/TSLType/StatusDetn/passive
</StatusDeterminationApproach>⌫
```

7.2.2 Version und Nummerierung

Die Version der TSL-Spezifikation wird entsprechend [ETSI_TS_102_231_V3.1.2] auf den Wert 3 gesetzt.

```
<TSLVersionIdentifier>3</TSLVersionIdentifier>
```

Die Nummerierung der TSL erfolgt über das Element TSLSequenceNumber. Bei jeder Erstellung wird der Inhalt um 1 inkrementiert. Der Anfangswert beträgt "1".

```
<TSLSequenceNumber> {Wert := "Bei jeder Erstellung wird diese Nummer inkrementiert"} </TSLSequenceNumber>
```

7.2.3 Aktualität der TSL

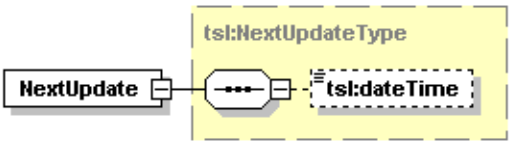


Abbildung 8: Element „NextUpdate“

Das Element NextUpdate ist gemäß [ETSI_TS_102_231_V3.1.2] in der TSL enthalten:

```
<NextUpdate>

      <dateTime> <Datum := "Erstellungsdatum + konfigurierbarer Wert (z.B. 30 Tage)"> </dateTime>

</NextUpdate>
```

7.2.4 Postalische Adresse

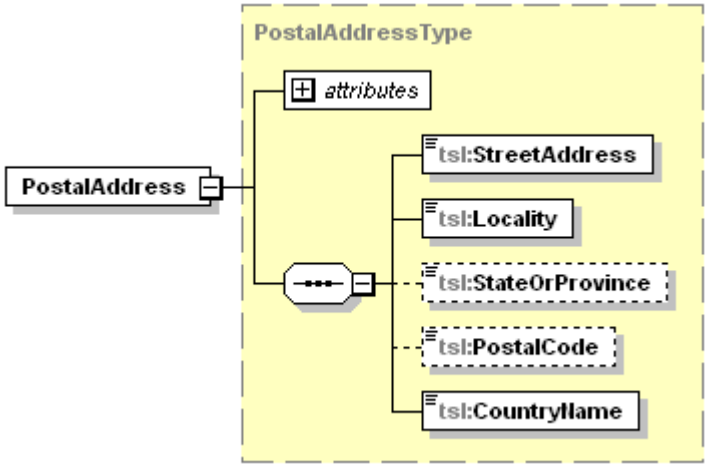


Abbildung 9: Element „PostalAddress“

TIP1-A_4093 TSL Postalische Adresse

Der TSL-Dienst MUSS das Element „PostalAddress“, welches die postalische Adresse des „SchemeOperator“ enthält, wie folgt befüllen:

```
<PostalAddress xml:lang="DE">
 <StreetAddress>Friedrichstrasse 136</StreetAddress>
 <Locality>Berlin</Locality>
 <StateOrProvince>Berlin</StateOrProvince>
 <PostalCode>10117</PostalCode>
       <CountryName>DE</CountryName>
</PostalAddress>
```

7.2.5 Policy-Angaben

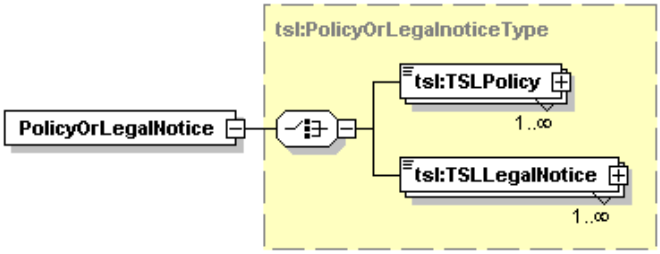


Abbildung 10: Element für „Policy-Angaben“

TIP1-A_4094 TSL Policy-Angaben

Der TSL-Dienst MUSS das Element „PolicyOrLegalNotice“ wie folgt befüllen:

```
<PolicyOrLegalNotice>
 <TSLLegalNotice xml:lang="DE">Certificate Policy der gematik, OID
{oid_policy_gem_or_cp}</TSLLegalNotice>
</PolicyOrLegalNotice>
```

Der Anbieter des TSL-Dienstes MUSS den OID (oid_policy_gem_or_cp) der Policy [gemRL_TSL_SP_CP] dem Dokument [gemSpec_OID#Tab_PKI_404] entnehmen.

7.2.6 Informationshistorien-Angaben

⌦ **TIP1-A_4095 TSL HistoricalInformationPeriod**

Der TSL-Dienst SOLL das Element HistoricalInformationPeriod mit dem Wert „0“ als Inhalt befüllen. ⌫

7.2.7 Lokalisierungs-Angaben

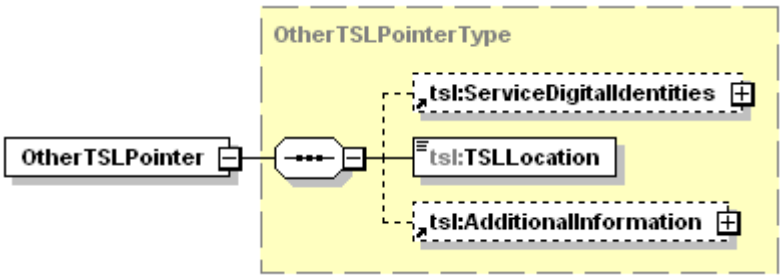


Abbildung 11: Element für „Lokalisierungspunkte der TSL“

⌦ **TIP1-A_4096 TSL Lokalisierungspunkte**

Der TSL-Dienst MUSS im Element "PointersToOtherTSL“ die Zugriffsadressen für die TSL-Datei integrieren. Er MUSS dieses Element wie folgt befüllen:

```
<PointersToOtherTSL>
 <OtherTSLPointer>
       <TSLLocation>{URL für TSL-Datei Primary Location}</TSLLocation>
       <AdditionalInformation>
             <TextualInformation xml:lang="DE">{oid_tsl_p_loc}</TextualInformation>
       </AdditionalInformation>
 </OtherTSLPointer>
 <OtherTSLPointer>
       <TSLLocation>{URL für TSL-Datei Backup Location}</TSLLocation>
       <AdditionalInformation>
             <TextualInformation xml:lang="DE">{oid_tsl_b_loc}</TextualInformation>
       </AdditionalInformation>
 </OtherTSLPointer>
</PointersToOtherTSL>
```

Der TSL-Dienst MUSS sowohl eine primäre als auch eine backup-Downloadadresse vorsehen.
Der TSL-Dienst MUSS den OID der TSLLocation (oid_tsl_p_loc, oid_tsl_b_loc) dem Dokument [gemSpec_OID#Tab_PKI_407] entnehmen. ⌫

7.3 Angaben zum Trust Service Provider

Zu einem TSP werden Informationen bezüglich seines Betriebs und seiner Dienste in den Elementen TSPInformation und TSPServices der TSL erfasst.

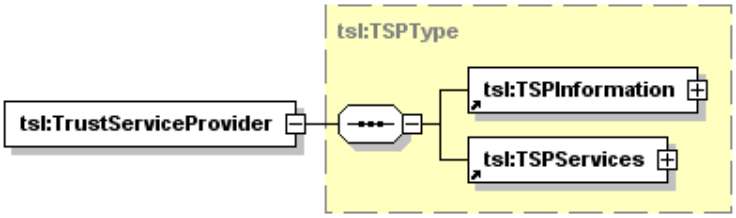


Abbildung 12: Angaben zum TSP

7.3.1 Angaben zum Betreiber

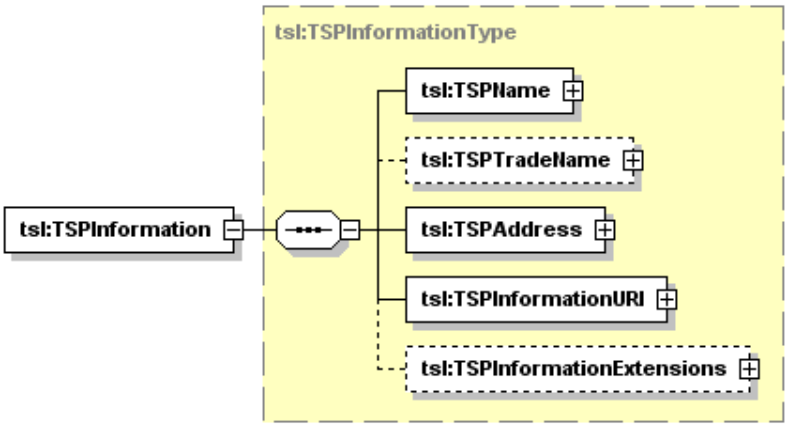


Abbildung 13: Betreiber Informationen

Mittels des Elements TSPName wird der Name der verantwortlichen juristischen Person des TSPs, deren TSP-Dienste über das Schema anerkannt werden, abgebildet ([ETSI_TS_102_231_V3.1.2#B.3.1]). Dabei muss es sich gemäß [ETSI_TS_102_231_V3.1.2#5.4.1] um den Namen handeln, unter dem alle formalen rechtlichen Registrierungen erfolgen und an den jegliche formale Kommunikation, unabhängig ob physisch oder elektronisch, gerichtet wird.

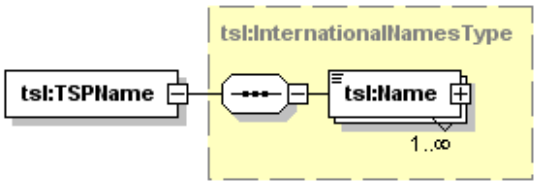


Abbildung 14: Angaben zur juristischen Person des TSP

Der alternative (Marken-)Name, unter dem die für die TSP verantwortliche juristische Person am Markt auftritt, wird durch das Element TSPTradeName abgebildet.

⌦ **TIP1-A_4097 TSL TSPTradeName**

Der TSL-Dienst MUSS das Element TSPTradeName für jeden TSP-Eintrag einsetzen und befüllen.⌫

⌦ **TIP1-A_4098 TSL TSPTradeName identisch mit TSPName**

Der Wert im Element TSPTradeName KANN identisch mit dem Wert des Elementes TSPName sein. ⌫

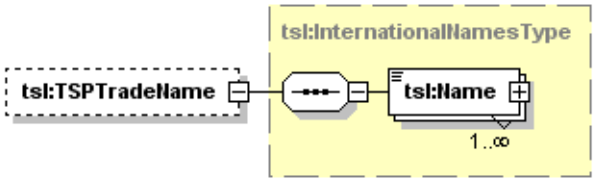


Abbildung 15: Angaben zum alternativen (Marken-)Namen des TSP

Der/die URI(s), unter der die Teilnehmer TSP-spezifische Informationen zu allgemeinen Geschäftsbedingungen, Haftung und ähnlichem erhalten können, werden in das Element TSPInformationURI abgelegt.

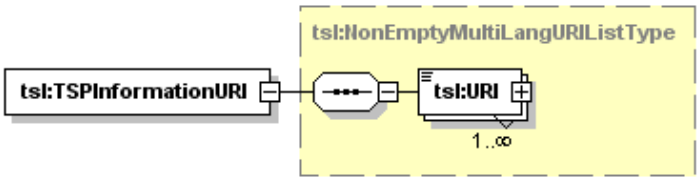


Abbildung 16: Angaben zur URI des TSPs

Die postalische sowie die elektronische Adresse des TSPs werden durch das Element TSPAddress dargestellt.

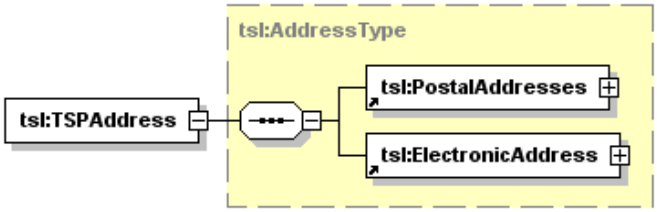


Abbildung 17: Angaben zur postalischen und elektronischen Adresse

7.3.2 Angaben zum TSP-Dienst

Pro Dienst des TSPs enthält das Element TSPServices ein Unterelement TSPService.

Das Element ServiceHistory wird in der Telematikinfrastruktur nicht verwendet und wird deshalb nicht befüllt.

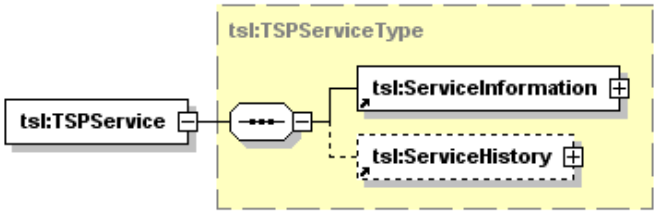


Abbildung 18: Angaben zu den TSP-Diensten

Pro Dienst wird das Element ServiceInformation verwendet. Die Abbildung 19 stellt die Struktur des Elementes dar.

Abbildung 19: Struktur der TSP-Service-Informationen

Das Element ServiceTypeIdentifier spezifiziert den Anwendungszweck des TSP-Dienstes.

⌦ **TIP1-A_4099 TSL ServiceTypeIdentifier**

Der TSL-Dienst MUSS pro TSP-Dienst einen der folgenden URIs als Wert in das Element ServiceTypeIdentifier einfügen (vgl. [ETSI_TS_102_231_V3.1.2#D.2):
(a) http://uri.etsi.org/TrstSvc/Svctype/CA/PKC (TSP, der X.509-Zertifikate ausstellt)
(b) http://uri.etsi.org/TrstSvc/Svctype/CA/QC (TSP, der qualifizierte Zertifikate ausstellt)
(c) http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP (TSP, der einen OSCP-Dienst betreibt)
(d) http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL (TSP, der einen CRL-Dienst betreibt)
(e) http://uri.telematik/TrstSvc/Svctype/DNSSEC (Trust Anchor für DNSSEC in der TI, bzw. dessen Hash)
(f) http://uri.telematik/TrstSvc/Svctype/CA/CVC (CVC-Root-CA-Zertifikat: Cross-CV-Zertifikat oder selbstsigniertes CVC-Root-CA-Zertifikat) ⌫

Das Element ServiceName spezifiziert den Namen, unter dem der TSP den mit „Service Type Identifier“ identifizierten Dienst anbietet. Dieses enthält gemäß [ETSI_TS_102_231_V3.1.2#B] 1 bis n Name-Elemente.

⌦ **TIP1-A_4100 TSL ServiceName: ein Name-Element**

Der TSL-Dienst SOLL genau ein Name-Element als Inhalt eines Elementes ServiceName eintragen. ⌫

⌦ **TIP1-A_4101 TSL ServiceName: eindeutig**

Der TSL-Dienst MUSS sicherstellen, dass der Inhalt des Name-Elementes, welches innerhalb des Elementes ServiceName verwendet wird, eindeutig ist. ⌫

⌦ **TIP1-A_4102 TSL ServiceName aus Subject-Feld**

Der TSL-Dienst SOLL innerhalb des Name-Elementes, welches innerhalb des Elementes ServiceName verwendet wird, den Inhalt des Subject-Feldes des Zertifikats für den TSP-Dienst eintragen.
Der TSL-Dienst SOLL aus dem Subject-Feld den vollständigen Distinguished Name übernehmen. ⌫

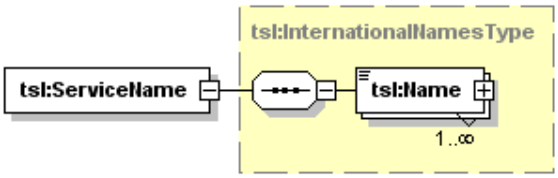


Abbildung 20: Name des TSP-Dienstes

Der Eintrag der digitalen Identität wird mit dem Element ServiceDigitalIdentity dargestellt.

⌦ **TIP1-A_4103 TSL DigitalId**

Der TSL-Dienst MUSS ein Element DigitalId in das Element ServiceDigitalIdentity einfügen. ⌫

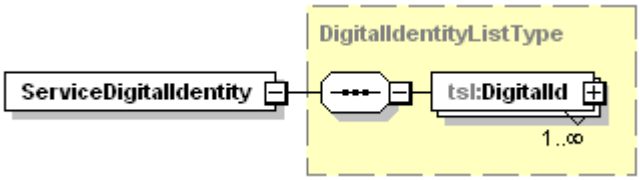


Abbildung 21: Eintrag der digitalen Identität

⌦ **TIP1-A_4104 TSL DigitalId: X.509-Zertifikat / Other-Element**

Der TSL-Dienst MUSS für jeden TSP-Dienst ein Element X509Certificate oder ein Element Other (für DNSSEC-Trustanchor, CVC-Root-CA-Zertifikate oder Cross-CV-Zertifikate) in das Element DigitalId einfügen.
Der TSL-Dienst MUSS das ihm gelieferte X.509-Zertifikat des TSP-Dienstes in das Element X509Certificate eintragen. ⌫

Der Status des TSP-Dienstes wird im Element ServiceStatus abgebildet. Der Dienstatus wird mit einem URI gemäß [ETSI_TS_102_231_V3.1.2#D.2] dargestellt.

⌦ **TIP1-A_4105 TSL ServiceStatus**

Der TSL-Dienst MUSS im Element ServiceStatus einen URI einfügen, welcher einem der in [gemSpec_PKI#Tab_PKI_271] aufgeführten Werte entspricht. ⌫

Im Element StatusStartingTime wird das Datum und die Uhrzeit spezifiziert zu dem der Status gesetzt wurde.

⌦ **TIP1-A_4106 TSL ServiceSupplyPoints**

Der TSL-Dienst MUSS in jedes Element ServiceInformation ein Element ServiceSupplyPoints mit mindestens einem Unterelement ServiceSupplyPoint einfügen, welches einen von der gematik bezeichneten URI enthält.
Der URI steht für die Adresse eines zuständigen OCSP-Responders oder CRL-Verteilungspunktes. Der URI kann in bestimmten Fällen (z. B. bei einem dedizierten CRL-Signer oder beim DNSSEC Trust Anchor) auch für einen Platzhalter stehen (z.B. http://ocsp00.gematik.invalid/not-used). ⌫

Der URI steht für die Adresse eines zuständigen OCSP-Responders oder CRL-Verteilungspunktes. Der URI kann in bestimmten Fällen (z. B. bei einem dedizierten CRL-Signer) auch für einen Platzhalter stehen.

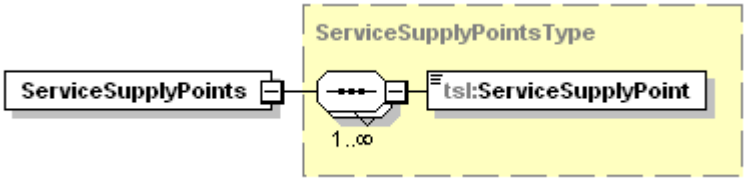


Abbildung 22: Struktur zur Ermittlung der Adresse des Validierungsdienstes

7.3.2.1 Verwendung des Elements ServiceInformationExtensions

Der TSL-Dienst verwendet das das Element ServiceInformationExtensions. Für dieses Element und seinen Inhalt gelten die folgenden Ausführungen:

Der Elementtyp ExtensionType beschreibt eine Erweiterung der TSL entsprechend den Erweiterungen in X.509-Zertifikaten. Nach [ETSI_TS_102_231_V3.1.2] muss ein Element Extension deshalb mit dem Attribut „Critical“ (mit Wert true oder false) ausgestattet werden.

Die Erweiterung spiegelt sich in dem Paar aus ExtensionOID und ExtensionValue bzw. ExtensionValues wieder. Eine Liste mit Paaren aus "OID" und "Value" wird von der gematik bereitgestellt. Die OIDs werden dem Dokument [gemSpec_OID] entnommen.

⌦ **TIP1-A_4107 TSL ServiceInformationExtensions**

Der TSL-Dienst MUSS für jeden TSP-Dienst-Eintrag das Element ServiceInformationExtensions eintragen. ⌫

⌦ **TIP1-A_4108 TSL ServiceInformationExtensions: Extension**

Der TSL-Dienst MUSS mindestens ein Element Extension in das Element ServiceInformationExtensions einfügen. Falls keine Angaben vorhanden sind, MUSS der TSL-Dienst das Element ServiceInformationExtensions mit dem Platzhalter-OID (oid_tsl_placeholder) gemäß [gemSpec_OID#Tab_PKI_407] erstellen. ⌫

⌦ **TIP1-A_4109 TSL Extension: Attribut „Critical“**

Der TSL-Dienst MUSS dem Attribut „Critical“ eines Elementes Extension den Wert „true“ oder „false“ gemäß den Vorgaben der gematik zuweisen. Der TSL-Dienst MUSS dieser Wert auf „false“ setzen, falls keine spezifischen Vorgaben gemacht werden. ⌫

⌦ TIP1-A_4110 TSL Extension: ExtensionOID & ExtensionValue

Der TSL-Dienst MUSS ein Element Extension gemäß Tab_PKI_713 befüllen.
Der TSL-Dienst MUSS die Inhalte dieser Unterelemente gemäß den Vorgaben der gematik setzen.
Der TSL-Dienst MUSS ein Element ExtensionOID gemäß Tab_PKI_714, ein Element ExtensionValue gemäß Tab_PKI_715 und Element ExtensionValues gemäß Tab_PKI_716 befüllen.
Der TSL-Dienst MUSS den Wert für ein ExtensionValue-Element auf die gematik-spezifische Referenz (startend mit „oid_“) gemäß [gemSpec_OID] setzen, falls der Wert für ein ExtensionValue-Element nicht spezifisch vorgegeben ist. ⌫

Tabelle 8: Tab_PKI_713 TSL-Datei – Element Extension

Bezeichnung	Extension
Beschreibung	Siehe [ETSI_TS_102_231_V3.1.2#B.5]
Optional	Nein
Wertebereich	Das Element muss mit einer Sequenz aus 1. einem Element ExtensionOID und 2. entweder einem Element ExtensionValue oder einem Element ExtensionValues befüllt werden.

Tabelle 9: Tab_PKI_714 TSL-Datei – Element ExtensionOID

Bezeichnung	ExtensionOID
Beschreibung	Das Element muss gemäß den Vorgaben der gematik mit einer OID in der Punkt-Notation gemäß [gemSpec_OID] befüllt werden.
Optional	Nein
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“ mit Pattern „[1-9\.]+“ .

Tabelle 10: Tab_PKI_715 TSL-Datei – Element ExtensionValue

Bezeichnung	ExtensionValue
Beschreibung	Dieses Element enthält den Wert für die OID, welcher im Schwesterelement ExtensionOID enthalten ist.
Optional	Ja
Wertebereich	Entspricht dem Wertebereich vom XML-Datentyp „string“.

Tabelle 11: Tab_PKI_716 TSL-Datei – Element ExtensionValues

Bezeichnung	ExtensionValues
Beschreibung	Alternative zum Element ExtensionValue
Optional	Ja
Wertebereich	Entspricht dem XML-Datentyp „complexType“.

7.4 TI-Vertrauensankerwechsel

Im Hinblick auf einen späteren Wirkbetrieb muss der TSL-Dienst die technischen Voraussetzungen beachten, die nötig sind, um einen TI-Vertrauensankerwechsel durchführen zu können.

Der TI-Vertrauensankerwechsel erfolgt mittels eines TSP-Diensteintrags mit spezifischen Eigenschaften (Update-Parametern). Die Anforderungen an den TSL-Dienst sind in [gemSpec_PKI#GS-A_4644] definiert.

7.5 DNSSEC Trust Anchor für den Namensraum TI

In der Telematikinfrastruktur (TI) wird DNSSEC (Domain Name System Security Extensions) für die Namensauflösung mit einem eigenen DNSSEC Trust Anchor in der Domäne „telematik“ implementiert. Die Einzelheiten dieser Implementierung sind in [gemSpec_Net] beschrieben und spezifiziert.

Neben der üblichen Vorgehensweise zur sicheren Einbringung des DNSSEC Trust Anchors der TI in eine Komponente (initiale Einbringung, Update gemäß DNSSEC-Protokoll) wird (für Komponenten, die lange offline waren,) die TSL-Datei als alternatives Transportmedium genutzt. Die Daten zur sicheren Übertragung des DNSSEC Trust Anchors der TI werden deshalb als speziell markierter TSP-Dienst in die Struktur der TSL-Datei eingebettet (mit dem Betreiber des Namensdienstes als TrustServiceProvider).

Die Angaben zum DNSSEC Trust Anchor der TI liefert die gematik als XML-Fragment dem Anbieter des TSL-Dienstes über die Schnittstellen des Funktionsmerkmals TSL_Eintragsverwaltung. Das Einbringen des DNSSEC Trust Anchors der TI erfolgt also analog demjenigen eines CA-Zertifikats.

Die Struktur des XML-Fragmentes richtet sich nach den Vorgaben von IANA. Ein Beispiel für eine solche Struktur (dort für die DNS-Root-Zone) wird unter http://data.iana.org/root-anchors/root-anchors.xml bereitgestellt.

⌦ **TIP1-A_5122 TSL DNSSEC Trust Anchor ServiceTypeIdentifier**

Der TSL-Dienst MUSS für den DNSSEC Trust Anchor der TI im Element ServiceTypeIdentifier den dafür in [TIP1-A_4099] spezifizierten URI einsetzen. ⌫

⌦ **TIP1-A_5123 TSL DNSSEC Trust Anchor Name**

Der TSL-Dienst MUSS für den DNSSEC Trust Anchor der TI im Element ServiceName ein Element Name einfügen, welches den Inhalt „*CN=DNSSEC-Trustanchor, DC=telematik*“ enthält. ⌫

⌦ **TIP1-A_5124 TSL DNSSEC Trust Anchor DigitalId**

Der TSL-Dienst MUSS für den DNSSEC Trust Anchor der TI im Element DigitalId (im Element ServiceDigitalIdentity) ein Element Other einfügen. Der TSL-Dienst MUSS in dieses Other-Element ein XML-Fragment gemäß [gemSpec_Net#GS-A_4815] eintragen. ⌫

⌦ **TIP1-A_5125 TSL DNSSEC Trust Anchor ServiceStatus**

Der TSL-Dienst MUSS für den DNSSEC Trust Anchor der TI im Element ServiveStatus den URI gemäß [gemSpec_PKI#Tab_PKI_271] für einen Dienst, der in Betrieb ist, einsetzen. ⌫

⌦ **TIP1-A_5126 TSL DNSSEC Trust Anchor StatusStartingTime**

Der TSL-Dienst SOLL für den DNSSEC Trust Anchor der TI im Element StatusStartingTime den Zeitpunkt, ab dem der DNSSEC Trust Anchor in Betrieb ist, einsetzen. ⌫

Hinweis: Es wird auch ein Element ServiceSupply-Point gesetzt und mit einem Platzhalter-URL befüllt. Siehe dazu [TIP1-A_4106] und die nachfolgenden Erklärungen.

⌦ **TIP1-A_5128 TSL DNSSEC Trust Anchor Extension**

Der TSL-Dienst MUSS für den DNSSEC Trust Anchor der TI im Element ServiceInformationExtensions ein Element Extension eintragen, welches den Platzhalter-OID (oid_tsl_placeholder) gemäß [gemSpec_OID#Tab_PKI_407] enthält. ⌫

7.6 CVC-Root-Update

Der öffentliche Schlüssel der CVC-Root-CA ist der CV-Vertrauensanker einer Chipkarte der TI für die Card-To-Card-Authentisierung (C2C). Im Verlaufe der Zeit (i. d. R. alle zwei Jahre) werden neue CVC-Root-CA-Instanzen (Root-Versionen) aufgesetzt und als Vertrauensanker eingesetzt. Somit sind jeweils Chipkarten mit unterschiedlichen gültigen CVC-Root-CA-Schlüsseln im Feld. Um zwischen derartigen Karten eine erfolgreiche C2C-Authentisierung zu ermöglichen, stellen sich zeitlich aufeinander folgende CVC-Root-CA-Instanzen Cross-CV-Zertifikate aus (s. [gemSpec_CVC_Root#5.4.7]).

Die TSL wird genutzt, um diese Cross-CV-Zertifikate (und selbstsignierte CVC-Root-CA-Zertifikate) zu den die C2C-Authentisierung steuernden Komponenten (Konnektor, Mobiles Kartenterminal) zu transportieren. Diese Komponenten halten die Cross-CV-Zertifikate für eine C2C-Authentisierung vor.

In der TSL werden spezifische Einträge für diesen Zweck erstellt:

⌦ **TIP1-A_5963 TSL CV-Zertifikate der CVC-Root-CAs ServiceTypeIdentifier**

Der TSL-Dienst MUSS für das ein CVC-Root-CA-Zertifikat oder ein Cross-CV-Zertifikat im Element „ServiceTypeIdentifier“ den dafür in [TIP1-A_4099] spezifizierten URI einsetzen. ⌫

⌦ **TIP1-A_5964 TSL CV-Zertifikate der CVC-Root-CAs Name**

Der TSL-Dienst MUSS für ein CVC-Root-CA-Zertifikat oder für ein Cross-CV-Zertifikat im Element „ServiceName“ ein Element „Name“ einfügen, welches den Inhalt „*CHR={CHR}, CAR={CAR}*“ gemäß [gemSpec_PKI#6.7.2.2 und #6.7.2.4] enthält.
Der TSL-Dienst MUSS die Werte *{CHR}* und *{CAR}* gemäß dem CHR-Wert und dem CAR-Wert des CVC-Root-CA-Zertifikats oder des Cross-CV-Zertifikats als 11 Zeichen (5 Buchstaben und 6 Ziffern) lange Strings entsprechend

[gemSpec_PKI#Tab_PKI_266] eintragen.
Ist {CHR} gleich {CAR}, handelt es sich um ein CVC-Root-CA-Zertifikat. ⌫

Hinweis: Gemäß [gemSpec_PKI#Tab_PKI_266] beträgt die Länge eines CAR- (und somit auch eines CHR-Wertes in einem CA-Zertifikat) 8 Byte. Die letzten 3 Byte enthalten 6 „Binary Coded Decimals“ (BCD), also in Halbbytes codierte dezimale Ziffern. Diese Ziffern werden im Name-Element der TSL-Datei als normale Characters codiert.

⌦ **TIP1-A_5965 TSL CV-Zertifikate der CVC-Root-CAs DigitalId**

Der TSL-Dienst MUSS für ein CVC-Root-CA-Zertifikat oder für ein Cross-CV-Zertifikat im Element DigitalId (im Element ServiceDigitalIdentity) ein Element „*Other*“ einfügen. Der TSL-Dienst MUSS in dieses *Other*-Element ein *CVCertificate*-Element einfügen, welches das Base64-codierte CV-Zertifikat wie folgt aufnimmt.

```
<Other>
  <CVCertificate>
        Base64-codiertes CV-Zertifikat}
  </CVCertificate>
</Other>
```

⌫

⌦ **TIP1-A_5966 TSL CV-Zertifikate der CVC-Root-CAs ServiceStatus**

Der TSL-Dienst MUSS für ein CVC-Root-CA-Zertifikat oder für ein Cross-CV-Zertifikat im Element ServiceStatus den URI gemäß [gemSpec_PKI#Tab_PKI_271] für einen Dienst, der in Betrieb ist, einsetzen. ⌫

⌦ **TIP1-A_5967 TSL CV-Zertifikate der CVC-Root-CA Extension**

Der TSL-Dienst MUSS für ein CVC-Root-CA-Zertifikat oder für ein Cross-CV-Zertifikat im Element ServiceInformationExtensions ein Element Extension eintragen, welches die OID (oid_cv_*cert) bzw. OID (oid_cv*_rootcert für ein CVC-Root-Zertifikat) gemäß [gemSpec_OID# Tab_PKI_407] enthält. ⌫

Ein TSL-Eintrag für ein Cross-CV-Zertifikat sieht also dergestalt aus:

```
<TSPService>
      <ServiceInformation>
            <ServiceTypeIdentifier>
                  http://uri.telematik/TrstSvc/Svctype/CA/CVC          </
ServiceTypeIdentifier>
                  <ServiceName>
                        <Name xml:lang="DE">
                              CHR={CHR}, CAR={CAR}
                        </Name>
                  </ServiceName>
            <ServiceDigitalIdentity>
                  <DigitalId>
                        <Other>
                            <CVCertificate>
                             {Base64-codiertes CV-Zertifikat}
```

```
                    </CVCertificate>
                </Other>
            </DigitalId>
        </ServiceDigitalIdentity>
        <ServiceStatus>
        http://uri.etsi.org/TrstSvc/Svcstatus/inaccord
        </ServiceStatus>

        <StatusStartingTime>
        2014-02-27T01:00:00.000+01:00
        </StatusStartingTime>
        <ServiceSupplyPoints>
            <ServiceSupplyPoint>
                http://ocsp00.gematik.invalid/not-used
            </ServiceSupplyPoint>
        </ServiceSupplyPoints>
        <ServiceInformationExtensions>
            <Extension Critical="false">
                <ExtensionOID>
                        {oid_cv_cert}
                </ ExtensionOID>
                <ExtensionValue>
                    oid_cv_cert
                </ ExtensionValue>
            </Extension>
        </ServiceInformationExtensions>
    </ServiceInformation>
</TSPService>
```

7.7 Testunterstützung

Für Test- und Referenzumgebungen wird ein separater TI-Vertrauensraum bereitgestellt. Dieser wird in einer eigenen Test-TSL-Datei technisch abgebildet.

Die folgenden Ausführungen beschreiben die Anforderungen, welche an die Test-TSL-Datei abweichend von der Produktiv-TSL-Datei gestellt werden.

⌦ TIP1-A_4111 TSL Test SchemeOperatorName

Der TSL-Dienst MUSS in der TSL für die Test- und Referenzumgebungen das Element SchemeOperatorName wie folgt befüllen:
`<SchemeOperatorName>`

```
 <Name xml:lang="DE">TEST-ONLY gematik Scheme</Name>
</SchemeOperatorName> ⌫
```

⌦ TIP1-A_4112 TSL Test SchemeName

Der TSL-Dienst MUSS in der TSL für die Test- und Referenzumgebungen das Element SchemeName wie folgt befüllen:

```
<SchemeName>
 <Name xml:lang="DE">TEST-ONLY gematik TSL Scheme</Name>
</SchemeName>⌫
```

⌦ TIP1-A_4113 TSL Test Policy-Angaben

Der TSL-Dienst MUSS in der TSL für die Test- und Referenzumgebungen das Element „PolicyOrLegalNotice“ wie folgt befüllen:

```
<PolicyOrLegalNotice>
 <TSLLegalNotice xml:lang="DE">TEST-ONLY Abschnitt der Certificate
Policy der gematik, OID {oid_policy_gem_or_cp}</TSLLegalNotice>
</PolicyOrLegalNotice>
```

Der TSL-Dienst MUSS den OID (oid_policy_gem_or_cp) der Policy [gemRL_TSL_SP_CP] dem Dokument [gemSpec_OID# Tab_PKI_404] entnehmen. ⌫

⌦ TIP1-A_4114 TSL Test Lokalisierungspunkte

Der TSL-Dienst MUSS in der TSL-Datei für die Test- und Referenzumgebungen im Element "PointersToOtherTSL“ die Zugriffsadressen für die jeweilige TSL-Datei integrieren. Er MUSS dieses Element wie folgt befüllen:

```
<PointersToOtherTSL>
 <OtherTSLPointer>
       <TSLLocation>{URL       für       Test-TSL-Datei       Primary
Location}</TSLLocation>
       <AdditionalInformation>
       <TextualInformation
xml:lang="DE">{oid_tsl_p_loc}</TextualInformation>
       </AdditionalInformation>
 </OtherTSLPointer>
 <OtherTSLPointer>
       <TSLLocation>{URL       für       Test-TSL-Datei       Backup
Location}</TSLLocation>
       <AdditionalInformation>
             <TextualInformation
xml:lang="DE">{oid_tsl_b_loc}</TextualInformation>
       </AdditionalInformation>
 </OtherTSLPointer>
</PointersToOtherTSL>
```

Der TSL-Dienst MUSS sowohl eine primäre als auch eine backup-Downloadadresse vorsehen.

Der TSL-Dienst MUSS den OID der TSLLocation (oid_tsl_p_loc, oid_tsl_b_loc) dem Dokument [gemSpec_OID#3.6] entnehmen. ⌫

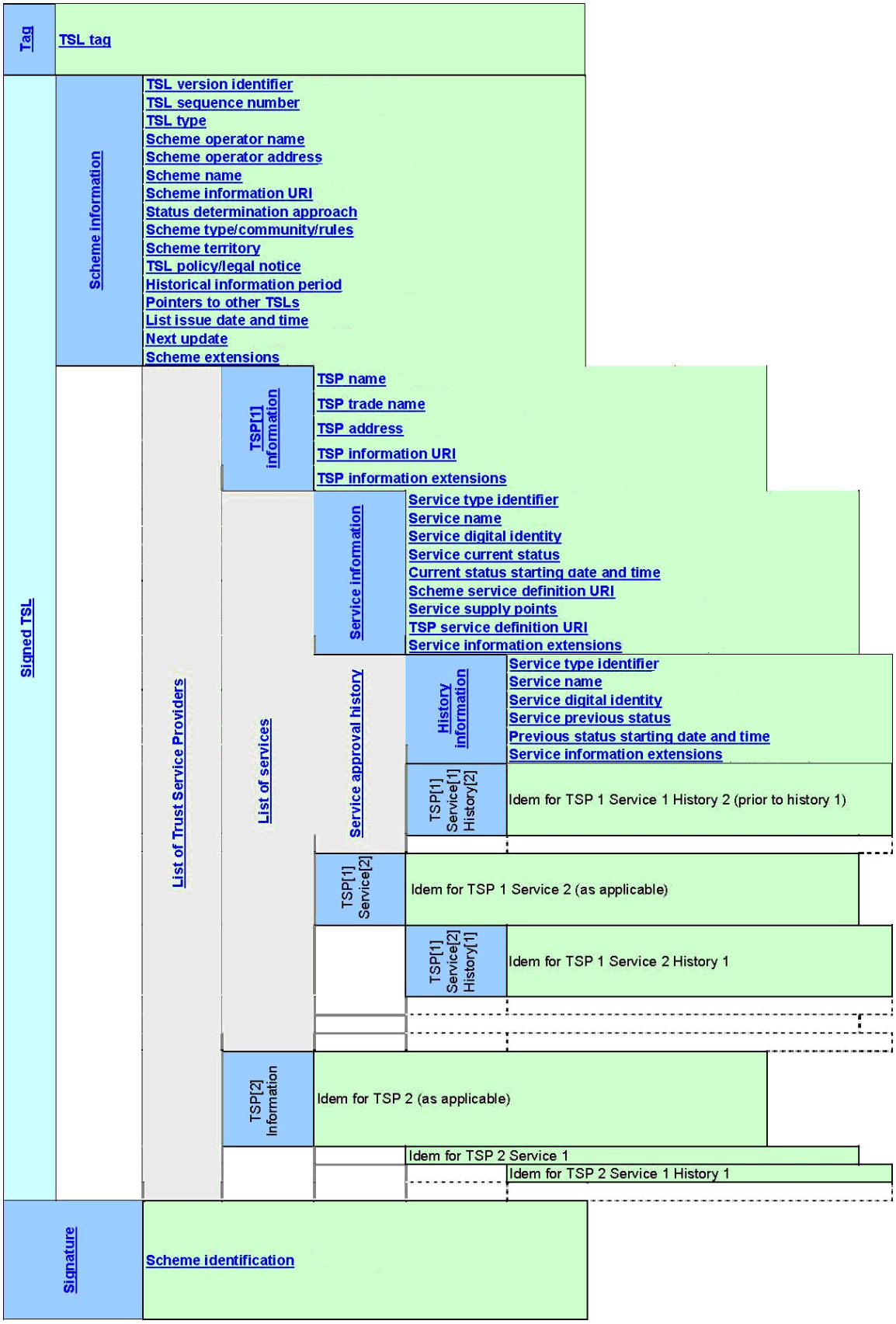


Abbildung 23: Struktur der TSL gemäß ETSI_TS_102_231

Anhang A - Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certification Authority
CP	Certificate Policy
CRL	Certificate Revocation Lists
DNSSEC	Domain Name System Security Extensions
ETSI	Europäisches Institut für Telekommunikationsnormen
HSM	Hardware Security Module
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IANA	Internet Assigned Numbers Authority
MPLS	Multi Protocol Label Switching
OCSP	Online Certificate Status Protokoll
PKI	Public Key Infrastructure
PU	Produktionsumgebung
SigG	Gesetz über Rahmenbedingungen für elektronische Signaturen
SMC-B	Secure Module Card Typ B
SM-K	Security-Modul-Konnektor
SM-KT	Security-Modul-Kartenterminal
SP	Service Provider
TI	Telematikinfrastruktur
TSL	Trust-service Status List
TSP	Trust Service Provider
VPN	Virtual Private Network
XML	Extensible Markup Language
ZDA	Zertifizierungsdiensteanbieter

A2 – Glossar

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

A3 – Abbildungsverzeichnis

Abbildung 1: Ablauf des Eintrags in TSL 10
Abbildung 2: Zertifikate und Signaturen 12
Abbildung 3: Komponenten des TSL-Dienstes 13
Abbildung 4: Funktionsmerkmale und ihre Schnittstellen (Schematische Darstellung) ...30
Abbildung 5: Prozess zur Aktualisierung der TSL (schematische Darstellung) 34
Abbildung 6: Grundstruktur der TSL-Elemente 49
Abbildung 7: Element „SchemeInformation“ 50
Abbildung 8: Element „NextUpdate“ 51
Abbildung 9: Element „PostalAddress“ 52
Abbildung 10: Element für „Policy-Angaben“ 52
Abbildung 11: Element für „Lokalisierungspunkte der TSL“ 53
Abbildung 12: Angaben zum TSP 54
Abbildung 13: Betreiber Informationen 54
Abbildung 14: Angaben zur juristischen Person des TSP 54
Abbildung 15: Angaben zum alternativen (Marken-)Namen des TSP 55
Abbildung 16: Angaben zur URI des TSPs 55
Abbildung 17: Angaben zur postalischen und elektronischen Adresse 55
Abbildung 18: Angaben zu den TSP-Diensten 55
Abbildung 19: Struktur der TSP-Service-Informationen 56
Abbildung 20: Name des TSP-Dienstes 57
Abbildung 21: Eintrag der digitalen Identität 57
Abbildung 22: Struktur zur Ermittlung der Adresse des Validierungsdienstes 58
Abbildung 23: Struktur der TSL gemäß ETSI_TS_102_231 65

A4 – Tabellenverzeichnis

Tabelle 1: Tab_PKI_702 Beschreibung der Rollen beim Anbieter des TSL-Dienstes 19
Tabelle 2: Tab_PKI_703 Rollenausschlüsse 20
Tabelle 3: Schnittstellen des TSL-Dienstes 31
Tabelle 4: Tab_PKI_701 Service Level für Prozesse des Anbieters des TSL-Dienstes 36
Tabelle 5: Tab_PKI_710 TSL-Datei – Element TrustStatusList 47
Tabelle 6: Tab_PKI_711 TSL-Datei – Element DigitalId 48
Tabelle 7: Tab_PKI_712 TSL-Datei – Element KeyInfo 48
Tabelle 8: Tab_PKI_713 TSL-Datei – Element Extension 59

Tabelle 9: Tab_PKI_714 TSL-Datei – Element ExtensionOID 59
Tabelle 10: Tab_PKI_715 TSL-Datei – Element ExtensionValue 59
Tabelle 11: Tab_PKI_716 TSL-Datei – Element ExtensionValues 59

A5 - Referenzierte Dokumente

A5.1 – Dokumente der gematik

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

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemKPT_Arch_TIP]	gematik: Konzept Architektur der TI-Plattform
[gemKPT_PKI_TIP]	gematik: Konzept PKI der TI-Plattform
[gemRL_Betr_TI]	gematik: Übergreifende Richtlinien zum Betrieb der TI
[gemRL_TSL_SP_CP]	gematik: Certificate Policy - Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL
[gemSpec_Net]	gematik: Spezifikation Netzwerk
[gemSpec_Perf]	gematik: Spezifikation Performance TI-Plattform
[gemSpec_PKI]	gematik: Spezifikation PKI
[gemSpec_Krypt]	gematik: Spezifikation kryptographischer Algorithmen in der TI
[gemSpec_OID]	gematik: Spezifikation Festlegung von OIDs
[gemSpec_Sich_DS]	gematik: Spezifikation Datenschutz- und Sicherheitsanforderungen
[gemSpec_SiBetrUmg]	gematik: Spezifikation der Sicherheitsanforderungen an die Betriebsumgebung für zentrale Produkte der TI
[gemSpec_X.509_TSP]	gematik: PKI für X.509-Zertifikate: Spezifikation Trust Service Provider X.509

A5.2 – Weitere Dokumente

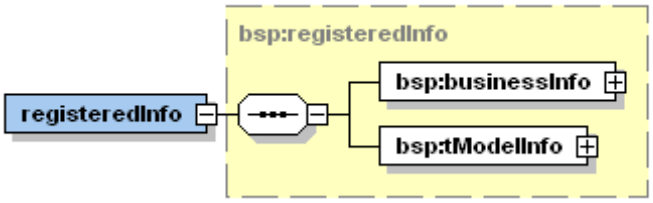
[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[BSI]	BSI (2005):

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	IT-Grundschutz-Kataloge (12. Ergänzungslieferung 2011) https://gsb.download.bva.bund.de/BSI/ITGSK12EL/IT-Grundschutz-Kataloge-12-EL.pdf
[ETSI_TS_102_231_V 3.1.2]	ETSI (Dezember 2009): ETSI Technical Specification TS 102 231 ('Provision of harmonized Trust Service Provider (TSP) status information') – Version 3.1.2
[EVSSL]	CA/Browser Forum: Guidelines For The Issuance And Management Of Extended Validation Certificates – Version 1.2, https://www.cabforum.org/Guidelines_v1_2.pdf
[PKCS#10]	RSA Laboratories (26.05.2000): PKCS #10 v1.7: Certification Request Syntax Standard ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-10/pkcs-10v1_7.pdf
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://tools.ietf.org/html/rfc2119
[RFC2616]	RFC 2616 (Juni 1999): Hypertext Transfer Protocol -- HTTP/1.1, http://tools.ietf.org/html/rfc2616
[ts_102231v030102_xsd.xsd]	ETSI: XML-Schemadatei zu ETSI Technical Specification TS 102 231 ('Provision of harmonized Trust Service Provider (TSP) status information') – Version 3.1.2

Anhang B – Leseanleitung für XML-Schema-Fragmente

Die XML Schema Language ist durch das W3-Konsortium standardisiert und ausführlich dokumentiert. Die Bedeutung der in diesem Dokument verwendeten grafischen Darstellungen wird im Folgenden kurz beschrieben.

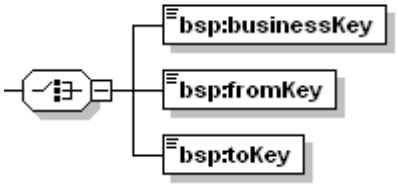
Struktur - Sequenz



Das Achteck mit der horizontalen gepunkteten Linie stellt eine Sequenz (‚sequence') dar. In diesem Beispiel bedeutet es, dass das Element *registeredInfo* aus den Elementen *BusinessInfo* und *tModelInfo* besteht. Alle drei Elemente gehören zum Namensraum *BSP*.

Das + Symbol am Ende der *businessInfo* und *tModelInfo* box bedeutet, dass das Diagramm hier verkürzt wurde und dass beide Elemente sich jeweils wieder aus weiteren, nicht angezeigten Elementen oder Attributen zusammensetzen.

Struktur - Auswahl



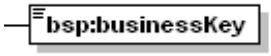
Das Auswahl (‚choice') Symbol bedeutet, dass genau eines der aufgelisteten Elemente auftreten MUSS. In diesem Fall eines der Elemente *businessKey*, *fromKey* und *toKey*.

Keines der hier angegebenen Elemente wurde verkürzt dargestellt (dies ist dadurch ersichtlich, dass *kein* „+" Symbol and die Box angehangen ist). Die horizontalen Linien am linken oberen Ende sind ein Indikator dafür, dass jedes Element nicht-leer ist.

Kardinalität – Null bis einmal

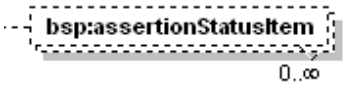
Ein Element, das durch eine gepunktete Linie dargestellt ist, ist OPTIONAL. Ist außerdem keines der weiter unten beschriebenen Kardinalitätsmerkmale angefügt, bedeutet es, dass dieses Element keinmal oder maximal einmal enthalten ist.

Kardinalität – Genau einmal



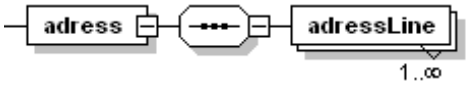
Eine durchgezogene Linie und keine weiteren Kardinalitätsmerkmale bedeutet, dass das Element genau einmal enthalten sein MUSS.

Kardinalität – Optional und wiederholt



Das Element *assertionStatusItem* ist optional und KANN beliebig oft enthalten sein. Die genaue Anzahl, wie oft das Element verwendet werden kann, wird durch die angehängten Zahlen definiert, in diesem Beispiel Null (0) bis Unendlich (∞).

Kardinalität – Verpflichtend und wiederholt



Das Element *adressLine* MUSS mindestens einmal und KANN beliebig oft enthalten sein.