Einführung der Gesundheitskarte

PKI für X.509-Zertifikate

Registrierung eines Trust Service Provider (TSP)

Version:	1.2.0
Stand:	19.03.2008
Status:	freigegeben

Dokumentinformationen

Änderungen zur Vorversion

Überarbeitung der Beschreibungen der TSL. Hinzugefügt wurden Felder wie ServiceSupplyPoint und PointersToOtherTSL.

Änderung der Abgrenzung des Dokuments.

Aufnahme der Anforderungen in Kapitel 3.

Überarbeitung der Formularstrukturierung in Kapitel 7.

Referenzierung

Die Referenzierung in weiteren Dokumenten der gematik erfolgt unter:

[gemX.509-TSP]	gematik (19.03.2008): Einführung der Gesundheitskarte - PKI für X.509-Zertifikate: Registrierung eines Trust Service Provider Version 1.2.0

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.0.1	21.08.06		Dokument neu erstellt	gematik, AG3
0.0.2	10.11.06		Aktualisierung aufgrund Erfahrungen CVC-Registrierung	gematik, AG3
0.0.3	15.11.06	5,6	Beschreibung TSL eingefügt, Formular-Update	gematik, AG3
0.0.5	21.11.06	4, 5, Anh. B	Update zu PDF-Formularen und TSL-Beschreibung, Anhang B (Leseanleitung XML-Schemata-Fragmente) zugefügt	gematik, AG3
0.0.6	01.12.06		Überarbeitung nach interner QS	gematik, AG3
1.0.0	08.12.06		freigegeben	gematik
1.0.1	23.10.07	5 6	Erweiterung der Struktur der TSL Entfernung der exemplarischen Darstellung der Registrierungsformulare	gematik, AG8
1.0.2	15.11.07	i.W. 4	Einarbeitung der internen Kommentierung	gematik, AG8
1.1.0	22.11.07		freigegeben	gematik
1.1.1	05.03.08	2, 3, 6	Anforderungen wurde aufgenommen. Überarbeitung der Beschreibung der TSL	SPE/ZD

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.1.2	18.03.08		Einarbeitung Kommentare	SPE/ZD
1.2.0	19.03.08		freigegeben	gematik

Inhaltsverzeichnis

1 Zusammenfassung

X.509-Zertifikate für eine eGK, einen HBA oder eine SMC werden im Rahmen der PKI für X.509-Zertifikate durch einen Trust Service Provider (TSP) erzeugt. Die X.509-Zertifikate (sowie die zugehörigen privaten Schlüssel) werden dann während der Kartenherstellung in die Chipkarten eingebracht.

Ein TSP muss in der gematik Trust-service Status List (gematik-TSL) eingetragen sein. Um dies beantragen zu können, muss sich der TSP vorher bei der gematik registrieren lassen. Im Rahmen ihrer Verantwortung für die Gestaltung der PKI für X.509-Zertifikate gibt die gematik die Mindestanforderungen vor, die an die Sicherheit eines TSP gestellt werden. Als Voraussetzung für die Registrierung muss der Trust Service Provider nachweisen, dass er diese Mindestanforderungen erfüllt.

Der TSP arbeitet bei der Kartenherstellung und Kartenauslieferung eng mit dem Kartenherausgeber und dem Kartenhersteller zusammen. Für die Sicherheit der PKI der X.509-Zertifikate ist die Sicherheit des Gesamtprozesses für die Kartenherstellung bis zur Auslieferung an den Karteninhaber von Bedeutung. Entsprechende Anforderungen werden daher von der gematik aufgestellt. Die Zusammenarbeit der Beteiligten kann sehr unterschiedlich organisiert werden. Aus Sicht der PKI für X.509-Zertifikate ist der TSP stellvertretend für alle Beteiligten für die Einhaltung der in diesem Dokument enthaltenen Anforderungen verantwortlich.

Das vorliegende Dokument beschreibt den Prozess der Registrierung eines TSP durch die gematik. Die Mindestanforderungen an einen TSP werden in [gemTSL_SP_CP] beschrieben.

2 Einführung

2.1 Zielsetzung und Einordnung des Dokumentes

Chipkarten der Gesundheitstelematikinfrastruktur benötigen X.509-Zertifikate. Diese werden im Rahmen einer PKI für X.509-Zertifikate erzeugt, die aus vielen Trust Service Providern (TSPs) besteht. Den Vertrauensanker bildet die gematik Trust-service Status List (TSL).

TSPs MÜSSEN sich bei der gematik registrieren lassen. Dabei müssen sie u. a. nachweisen, dass die durch die gematik vorgegebenen Mindestanforderungen (Certificate Policy) an die Sicherheit des TSP erfüllt werden. Dieses Dokument beschreibt den Prozess der Registrierung.

2.2 Zielgruppe

Dieses Dokument richtet sich an Trust Service Provider, die X.509-Zertifikate für eGKs, HBAs oder SMCs generieren.

2.3 Geltungsbereich

Die in diesem Dokument enthaltenen Vorgaben sind für alle Trust Service Provider verbindlich, sofern sie X.509-Zertifikate für eGKs, HBAs oder SMCs generieren, und sich bei der gematik registrieren lassen möchten.

2.4 Arbeitsgrundlagen

Dieses Dokument hat folgende Dokumente als Grundlage:

Tabelle 1: Überblick über die Basisdokumente

Name	Dokument
Zertifikatsprofile für X.509 Basiszertifikate HBA	[BÄK_ZPX.509B]
ETSI Technical Specification TSL	[ETSI]
Certificate Policy AUT/ENC/OSIG	[gemTSL_SP_CP]
PKI-Zertifikatsinfrastruktur (TSL)	[gemX.509_TSL]
X.509-Zertifikate der Versicherten	[gemX.509_eGK]
X.509-Zertifikate der SMC-Typ-B	[gemX.509_SMCB]
Personalisierung kryptografischer Daten der eGK	[gemPersKrypt]

2.5 Abgrenzung des Dokumentes

Aufbau und Inhalt der X.509-Zertifikate werden in den Spezifikationen der Versichertenzertifikate [gemX.509_eGK] und HBA/SMC ([HPC-P2] bzw. [gemX.509_SMCB]) beschrieben. Die dort angegebenen Festlegungen sind verbindlich.

Die langfristige Bestimmung der Hash-Algorithmen, der Schlüssellängen und der Signaturalgorithmen ist nicht Gegenstand der Betrachtung, hier werden jeweils aktuell die Empfehlungen der international relevanten Gremien und die Anforderungen von SigG/SigV [ALGCAT] berücksichtigt. Die Festlegungen zum „Aktivieren qualifizierter Zertifikate“ [gemQES] und die Vorgaben für die Vereinheitlichung der Public-Key-Infrastrukturen, insbesondere hinsichtlich der „Policy-Aspekte“ [gemTSL_SP_CP], werden in gesonderten Dokumenten getroffen.

Im vorliegenden Dokument werden ebenfalls keine Aussagen zum Management der kryptographischen Schlüssel getroffen. Diesbezüglich wird auf das übergreifende Sicherheitskonzept der gematik [gemSiKo] verwiesen, insbesondere auf Abschnitt F5 [gemSi-Ko#AnhF5].

Die für die Verwendung in der TI zulässigen Algorithmen, Schlüssellängen und maximalen Gültigkeitsdauern von Schlüsseln und Zertifikaten werden in [gemSiKo] sowie entsprechend der Technischen Richtlinie für eCard-Projekte der Bundesregierung [BSI-TR03116] normativ vorgegeben. Die freie Auswahl aus den hier zugelassenen Algorithmen durch die Hersteller könnte zu Interoperabilitätsproblemen führen, während die Implementierung aller zulässigen Algorithmen erheblichen Aufwand verursacht. Dieser Konflikt wird durch [gemSpec_Krypt] adressiert. Ziel des Dokumentes „Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur“ [gemSpec_Krypt] ist es, das Spektrum der zulässigen kryptographischen Algorithmen, sofern sie betreiberübergreifend verwendet werden, einzuschränken, um so mit einer minimalen Anzahl von Algorithmen kryptographische Interoperabilität herzustellen.

Deshalb wird als Basis zur Referenzierung der kryptographischen Algorithmen auf o. g. Dokument, Abschnitt 5.1.1 [gemSpec_Krypt#5.1.1] verwiesen.

Die Registrierung von TSPs für Komponentenzertifikate ist in [gemX.509_TCL] beschrieben.

Detaillierte Vorgaben zur Validierung von Zertifikaten und der Listen der vertrauenswürdigen Herausgeber werden in [gemVerw_Zert_TI] gemacht.

2.6 Methodik

2.6.1 Verwendung von Schüsselworten

Für die genauere Unterscheidung zwischen normativen und informativen Inhalten werden die dem RFC 2119 [RFC2119] entsprechenden in Großbuchstaben geschriebenen, deutschen Schlüsselworte verwendet:

- **MUSS** bedeutet, dass es sich um eine absolutgültige und normative Festlegung bzw. Anforderung handelt.
- **DARF NICHT** bezeichnet den absolutgültigen und normativen Ausschluss einer Eigenschaft.

- **SOLL** beschreibt eine dringende Empfehlung. Abweichungen zu diesen Festlegungen sind in begründeten Fällen möglich. Wird die Anforderung nicht umgesetzt, müssen die Folgen analysiert und abgewogen werden.
- **SOLL NICHT** kennzeichnet die dringende Empfehlung, eine Eigenschaft auszuschließen. Abweichungen sind in begründeten Fällen möglich. Wird die Anforderung nicht umgesetzt, müssen die Folgen analysiert und abgewogen werden.
- **KANN** bedeutet, dass die Eigenschaften fakultativ oder optional sind. Diese Festlegungen haben keinen Normierungs- und keinen allgemeingültigen Empfehlungscharakter.

2.6.2 Hinweis auf offene Punkte

Offene Punkte, die bis zur nächsten Dokumentversion bearbeitet werden, sind mit den folgenden Konventionen gekennzeichnet

Offene Punkte, die arbeitsgruppenübergreifend abgestimmt werden müssen, sind Magenta eingerahmt.

Durch die zentrale Dienste / Infrastruktur aufgrund bereits erfolgter Abstimmungen noch zu erweiternde Punkte sind violett markiert.

Formale noch offene Inhalte sind blau markiert.

3 Anforderungen

1) Die Anforderungen müssen noch mit dem Anforderungsmanagement abgestimmt werden. Das Kapitel wird in einer späteren Version des Dokumentes entsprechend überarbeitet.
2) Der Umgang mit den Ausgangsanforderungen muss gemäß den Vorgaben aus dem Handbuch Standards und Konventionen überarbeitet werden.

Die Notwendigkeit für eine PKI für die benötigten X.509-Zertifikate für die Komponenten ergibt sich aus der Gesamtarchitektur [gemGesArch#5.4.4]. Die gematik muss die Interoperabilität zwischen dieser PKI und der sie nutzenden Komponenten/Prozesse sicherstellen.

Die folgende Tabelle enthält die entsprechenden für X.509-Zertifikate relevanten Eingangsanforderungen, wie sie aktuell bereits identifiziert werden können:

Tabelle 2 Bereits erfasste Eingangsanforderungen

Quelle	Anforderungs-nummer	Anforderungs-level	Beschreibung
[gemPolicy]	A_01298	MUSS	gematik MUSS die Interoperabilität aller Telematikkomponenten sicherstellen. Dies gilt im Sinne der: * Spezifikationsverantwortung * Verantwortung für das Test- und Zulassungsverfahren * Betriebsverantwortung (Betriebsprozesse sowie das einzuhaltende Sicherheitsniveau) * Sicherstellung der Interoperabilität über alle PKI-Strukturen der Telematikinfrastruktur des Gesundheitswesens
[gemSiKo]	AS-AI-11110	MUSS	Die Integrität der Infrastrukturdienste sowie der sicherheitsrelevanten technischen Komponenten MUSS gewährleistet werden.
AM	A_00875	MUSS	Das Vertrauensmodell der PKI MUSS auf einer gematik Bridge CA, die als zentrale Instanz agiert und auf die alle Zertifikate zurückführbar sein MÜSSEN, basieren. Die Verbindung zwischen weiteren Root CAs und der gematik Bridge CA MUSS durch Trust-service Status Lists (TSLs) hergestellt werden.
AM	A_00876	MUSS	Die Verbindung zwischen weiteren Root CAs und der gematik Bridge CA MUSS durch Trusted-service Status Lists (TSLs) hergestellt werden, die durch die gematik signiert und herausgegeben werden MÜSSEN. Innerhalb der PKI MÜSSEN zwei getrennte TSLs existieren: die Infrastruktur TSL und die Personen TSL.
AM	A_00877	MUSS	Die Infrastruktur-TSL (Trust-service Status List) MUSS alle CAs enthalten, die Service- und Netzzertifikate ausstellen dürfen.

Quelle	Anforderungs-nummer	Anforderungs-level	Beschreibung
AM	A_00881	MUSS	Jede CA MUSS einen OCSP-Responder betreiben, über den die durch diese CA ausgestellten Zertifikate überprüft werden können. Aus Performanzgründen KÖNNEN zwei Optimierungen eingeführt werden: 1. Die spätere Einführung von CRLs bzw. Caching von OCSP-Anfragen. 2. Die maximalen Caching-Zeiten MÜSSEN bei der Verwendung von Caching vor dem Rollout festgelegt werden.
AM	A_01706	SOLL	Zur besseren Handhabbarkeit und für eine effiziente Umsetzung von Sicherheitsvorgaben SOLL die Rolle in den verschiedenen Zertifikaten einheitlich (d.h. z.B. gleiches Feld/Attribut, gleiches Encoding und Datenformat) kodiert werden.

4 Grundlagen

Hinsichtlich der verwendeten kryptographischen Komponenten in Bezug auf Algorithmengüte, Schlüssellängen, Schutz des privaten Schlüssels und Systemverfügbarkeit sind an alle Signaturerstellungseinheiten und die zugehörigen Zertifikate sehr hohe Anforderungen zu stellen.

Maßgeblich ist hierbei das im Sicherheitskonzept der gematik [gemSiKo] definierte Schutzniveau.

Für Verschlüsselungs-(ENC), Authentisierungs-(AUT) und Organisationszertifikate (OSig) ist das Konzept einer flachen zweistufigen Hierarchie, wie es für qualifizierte elektronische Signaturen mit Anbieterakkreditierung gesetzlich bestimmt wurde, sektorübergreifend nicht durchsetzbar, da eine Vielzahl von Zertifikatsherausgebern zu erwarten ist und bestehende Strukturen einzubinden sind. Abbildung 1 zeigt die beteiligten Akteure in der PKI und unterstreicht die Komplexität des Systems.

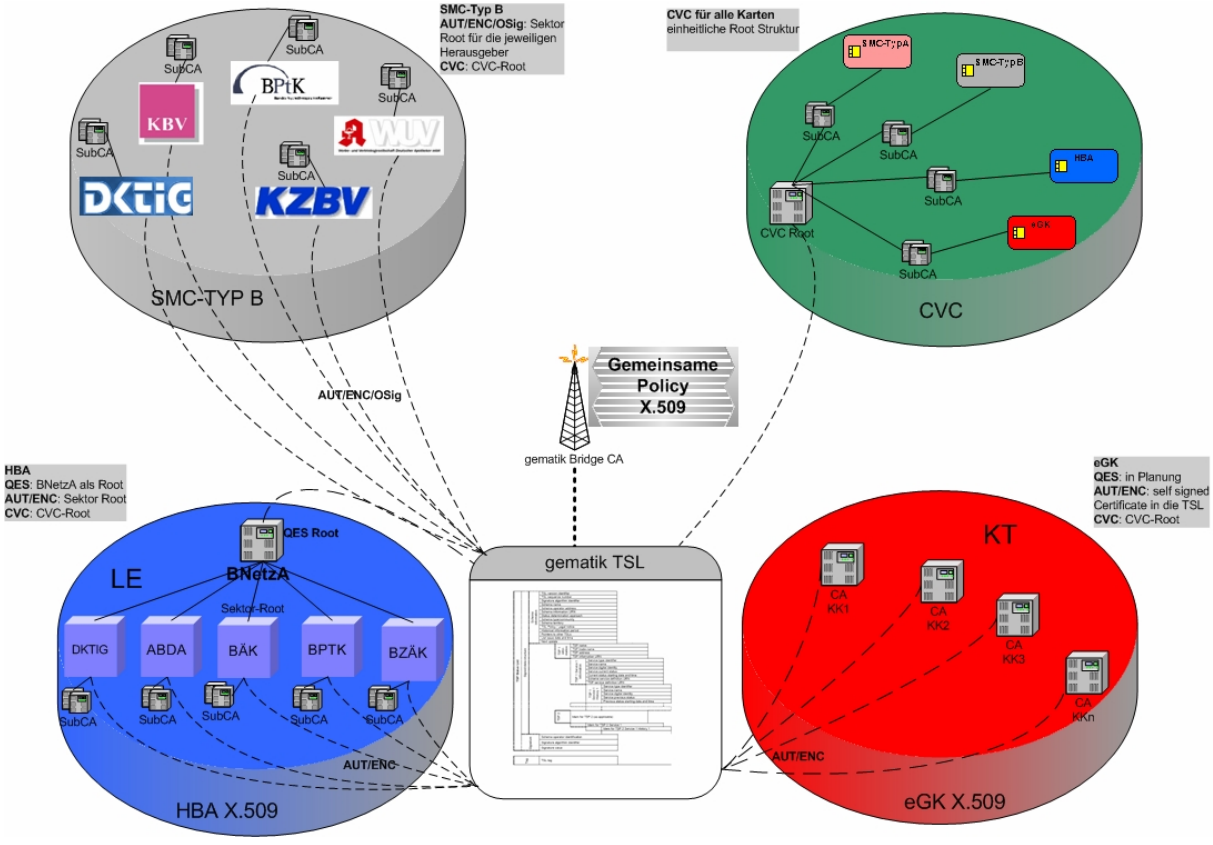


Abbildung 1: Struktur der PKI mit TSL und beteiligten Akteuren

In Hinsicht auf

- Verbraucherschutz,
- Haftungsaspekte,

- Identifizierung und Registrierung durch die Kostenträger,
- einen Mechanismus zum Entschlüsseln der Daten bei Verlust des ENC-Schlüssels
- sowie Dauer und den Kosten der Einführung

bestehen grundsätzliche Unterschiede zu den Regelungen bei qualifizierten Zertifikaten.

Daher wurde entschieden, als Vertrauensmodell eine Bridge-Struktur zu wählen, bei der die individuellen Vertrauensinformationen der verschiedenen TSPs in einer signierten XML-Datei abgelegt werden (ETSI Trust-service Status List). Nähere Informationen zur TSL sind in den Dokumenten [gemX.509_TSL] und [ETSI] veröffentlicht.

Hierzu wurde auf Basis der im Sicherheitskonzept als erforderlich definierten Maßnahmen zur Nutzung von PKI-Komponenten eine übergreifende Certificate Policy für ENC-, AUT- und OSig-Zertifikaten der eGK und der SMC Typ B entwickelt [gemTSL_SP_CP]. Alle beteiligten TSP MÜSSEN in ihrem „Certification Practice Statement“ die Erfüllung dieser Vorgaben zusichern. Die konkrete Umsetzung der Sicherheitsmaßnahmen im laufenden Betrieb des TSP wird durch die gematik, den TSL-Service-Provider oder zugelassene Prüfinstitute begutachtet.

4.1 Aufbau eines X.509-Zertifikats

Für Aufbau und Inhalt der X.509-Zertifikate sind die Vorgaben in [gemX.509_eGK], [HPC-P2] und [gemX.509_SMCB] verbindlich.

4.2 Zuständigkeiten

An der PKI für X.509-Zertifikate sind verschiedene Organisationen bzw. Personen beteiligt. In den folgenden Abschnitten wird ein Überblick über die vorhandenen Rollen und deren Zuständigkeiten bzw. Verantwortlichkeiten in Bezug auf die PKI für X.509-Zertifikate gegeben. Weitere Angaben und Beschreibungen der Zuständigkeiten und der Mindestanforderungen werden in der Policy [gemTSL_SP_CP] getroffen.

Im Rahmen der Gesundheitstelematikinfrastruktur gibt es neben der PKI für X.509-Zertifikate weitere PKIs. Die im Folgenden genannten Rollen haben ggf. auch im Rahmen dieser weiteren PKIs Zuständigkeiten und Verantwortlichkeiten. Hierauf wird im Folgenden jedoch nicht weiter eingegangen.

Bei der folgenden Beschreibung wird von einer Trennung der Organisationen bzw. Personen bei der Ausübung der Rollen ausgegangen. Eine Organisation bzw. Person kann jedoch mehrere Rollen übernehmen.

Übernimmt eine Organisation/Person eine Rolle, so kann sie Teile der zu dieser Rolle gehörenden Zuständigkeiten/Aufgaben an eine andere Organisation/Person übergeben. Hiervon unabhängig bleiben aber die im Folgenden genannten Verantwortlichkeiten bei der die Rolle ausübenden Organisation/Person.

4.2.1 gematik

Die gematik ist verantwortlich für die Gestaltung der PKI der X.509-Zertifikate. Sie übernimmt unter anderem die folgenden Aufgaben:

- Beauftragung und Kontrolle des gematik-TSL-Service-Provider,
- Registrierung eines TSP [gemTSL_SP_CP],
- ggf. Widerruf der Registrierung eines TSP [gemTSL_SP_CP],
- bei Bedarf Kontrolle eines TSP [gemTSL_SP_CP],
- Vorgabe der Algorithmen und Schlüssellängen für das Generieren der X.509-Zertifikate [gemX.509_eGK], [gemX.509_SMCB],
- Entscheidung über Generationswechsel beim gematik-TSL-SP [gemTSL_SP_CP] und
- gematik-Test-TSL.

4.2.2 Betreiber gematik-TSL (gematik TSL-SP)

Der Betreiber der gematik-TSL betreibt als technischer Dienstleister im Auftrage der gematik den folgenden Services:

- gematik-Produktiv-TSL-System (HumanAndOrganisation TSL).

Der gematik TSL-SP veröffentlicht die Wurzel- und Signaturzertifikate des Produktiv-TSL-Systems.

4.2.3 Kartenherausgeber

Der Herausgeber von eGK/HBA/SMC beauftragt einen TSP, die für seine Chipkarten benötigten X.509-Zertifikate zu generieren. Er beauftragt nur solche TSPs, für die aktuell eine gültige Registrierung durch die gematik vorliegt (in der TSL eingetragen sind).

Die Verantwortlichkeiten der Kartenherausgeber sind in [gemTSL_SP_CP] beschrieben.

Für die Ausgabe von HBAs und SMCs können weitere Anforderungen durch die jeweils zuständige berufsständische Organisation vorgegeben werden.

4.2.4 TSP

Ein TSP ist für das Generieren der X.509-Zertifikate für eine Chipkarte (eGK, HBA, SMC) bzw. für einen untergeordneten TSP zuständig. Die dabei einzuhaltenden Anforderungen werden in der Certificate Policy [gemTSL_SP_CP] beschrieben.

Ein TSP muss bei der gematik registriert werden. Dabei ist insbesondere durch ein Sicherheitsgutachten nachzuweisen, dass die in [gemTSL_SP_CP] beschriebenen Mindestanforderungen durch den TSP eingehalten werden.

4.2.5 Kartenhersteller

Im Rahmen der Produktion einer Chipkarte (eGK, HBA, SMC) werden folgende Werte in die Chipkarte eingebracht:

- X.509-Zertifikate der Chipkarte
- private Schlüssel der Zertifikate

Es liegt in der Verantwortung des Kartenherstellers, dass hierbei die korrekten Werte in die Chipkarte eingebracht werden.

Chipkarten, die vor Weitergabe als fehlerhaft erkannt werden, MÜSSEN durch den Kartenhersteller ordnungsgemäß vernichtet und entsorgt werden.

Die vom Kartenhersteller einzuhaltenden Anforderungen werden in der Certificate Policy [gemTSL_SP_CP] beschrieben.

4.3 Unterscheidung Test-TSL – Produktiv-TSL

Bei der PKI für X.509-Zertifikate wird zwischen einer Produktiv-PKI und einer Test-PKI unterschieden.

Der gematik TSL-SP stellt die Produktiv-TSL und die gematik die Test-TSL zur Verfügung. Die beiden Systeme werden technisch, organisatorisch und betrieblich so getrennt, dass keine gegenseitige Beeinflussung und keine Verwechslung möglich sind.

Jeder TSP, der ebenfalls einen Test-TSP betreibt, muss diesen dabei von dem Produktivsystem technisch, organisatorisch und betrieblich so trennen, dass keine gegenseitige Beeinflussung und keine Verwechslung möglich sind.

Ein Test-TSP muss ebenfalls bei der gematik registriert werden. Hierfür gibt es ein verkürztes Verfahren (siehe Abschnitt 5.2.4).

Die Produktiv-TSL verwaltet die TSPs, mit denen Zertifikate mit Echtdaten produziert werden. Im Gegensatz dazu werden in der Test-TSL nur TSPs verwaltet, die Zertifikate mit Testdaten produzieren.

5 Registrierung eines Trust Service Providers

Damit im Rahmen der Gesundheitstelematikinfrastruktur ein TSP an der PKI für X.509-Zertifikate teilnehmen kann, muss er sich bei der gematik registrieren lassen. Dabei wird zwischen der Registrierung eines Produktiv-TSP und der Registrierung eines Test-TSP unterschieden.

Mit dem Antrag auf Registrierung eines Produktiv-TSP oder eines Test-TSP akzeptiert der Betreiber alle Vorgaben und Regelungen dieses und aller referenzierten Dokumente.

5.1 Allgemeine Regelungen

5.1.1 Geltungsbereich

Ein TSP kann von verschiedenen Organisationen betrieben werden. Beispiele sind:

- Kartenpersonalisierer,
- Kartenhersteller,
- Kartenherausgeber,
- ZDAs im Sinne vom SigG.

Für eine Registrierung als TSP kommen nur solche Organisationen in Frage,

- deren Hauptsitz in einem Land der Europäischen Union liegt und
- deren Betriebsstätte für den tatsächlichen Betrieb des TSP in einem Land der Europäischen Union liegt.

5.1.2 Produktiv- und Test-TSP

Bei der Registrierung eines TSP wird zwischen der Registrierung für den Produktivbetrieb und der Registrierung für den Testbetrieb unterschieden. Wesentlicher Unterschied der beiden Verfahren ist, dass bei einer Registrierung für den Testbetrieb noch keine Gutachten über die Sicherheit des Test-TSP benötigt werden.

5.1.3 Registrierung/Widerruf

Eine Registrierung eines Produktiv- bzw. Test-TSP wird auf Antrag des Betreibers durch die gematik durchgeführt.

Ein Widerruf einer vorher durchgeführten Registrierung durch die gematik ist möglich. In Frage kommende Gründe hierfür sind in [gemTSL_SP_CP] sowie in den Abschnitten 5.2.4 und 5.3.4 beschrieben.

5.1.4 Information der gematik für TSL-Service-Provider

Die gematik informiert den TSL-Service-Provider regelmäßig über die aktuell registrierten Produktiv- bzw. Test-TSPs. Dies geschieht

- spätestens fünf Werktage nach einer erfolgreichen Registrierung eines TSP bzw.
- spätestens einen Werktag nach dem Widerruf einer Registrierung.

5.1.5 Notwendigkeit der Registrierung

Der gematik TSL-SP wird einen Eintrag in die Produktiv- bzw. Test-TSL nur dann erzeugen, falls der TSP aktuell als Produktiv- bzw. Test-TSP bei der gematik registriert ist. Eine Ausnahme hiervon ist nicht möglich.

5.1.6 Kosten des Verfahrens

Die eigentliche Registrierung eines TSP durch die gematik ist kostenfrei.

5.2 Verfahren für einen Produktiv-TSP

5.2.1 Antrag auf Registrierung

Für die Registrierung eines Produktiv-TSP muss der Betreiber einen schriftlichen Antrag an die gematik stellen. Zu diesem Antrag gehören

- vollständig ausgefülltes Formular "Unterlagen zur Registrierung als Trust Service Provider Produktiv-TSL" (Vorgaben Formulare),
- vollständig ausgefülltes Formular "Anmeldung als TSL-TSP" (Vorgaben Formulare),
- ausgefülltes Formular "Liste der Kontaktpersonen TSL" (Vorgaben Formulare),
- ausgefülltes Formular "Registrierung eines TSP-Service in der TSL“ (Vorgaben Formulare),
- Kopie des Registerauszugs[1],
- Sicherheitsgutachten (siehe [gemTSL_SP_CP]) und
- zu registrierende Zertifikate (Digitale Identitäten).

Bei akkreditierten CAs sind, anstelle des Sicherheitsgutachtens, folgende Unterlagen zwingend erforderlich:

- Kopie der Akkreditierungsurkunde,

[1] Für Organisationen der Rechtsform „Körperschaft des öffentlichen Rechts“ (K.d.ö.R.) muss anstelle des Registerauszuges eine Bestätigung über die zeichnungsberechtigten Personen eingereicht werden.

- Kopie der Bestätigungsurkunde "Bestätigung für die Umsetzung von Sicherheitskonzepten",
- Selbsterklärung zur Einhaltung des Betriebs TSP unter akkreditierten Bedingungen (Vorgaben Formulare).

In dem Formular "Anmeldung als TSL-TSP" muss unter Firma/Organisation die Adresse der eigentlichen Betriebsstätte des Produktiv-TSP angegeben werden. Zu den Datenfeldern „Allgemeine Angaben in der TSL“ sind die Hinweise unter 6.8.1 zu beachten.

In dem Formular "Liste der Kontaktpersonen TSL" muss für die Rolle "Leiter TSP" ein verantwortlicher Mitarbeiter und ein Stellvertreter genannt werden. Für die Rolle "Sicherheitsbeauftragter" muss ein verantwortlicher Mitarbeiter genannt werden, ein Stellvertreter ist optional. Für die Rolle "Antragsteller TSP-TSL-Eintrag" können bis zu drei Mitarbeiter genannt werden.

Das Formular "Registrierung eines TSP-Service in der TSL“ nimmt die für die TSL notwendigen Detailinformationen bzgl. der vom TSP angebotenen Dienste auf.

Die genannten Formulare sind als PDF-Formulare konzipiert. Sie können von der gematik-Website herunter geladen werden und sind elektronisch auszufüllen. Sie müssen (direkt aus dem Formular heraus) ausgefüllt per Mail vorab an die gematik gesendet werden. Der mit dem Mailversand erstellte Ausdruck ist dann unterschrieben per Post zu senden.

Die Kopie des Registerauszugs muss von dem aktuellen Eintrag des Betreibers in dem zuständigen Register (Handelsregister, Vereinsregister, etc.) stammen. Aus diesem MÜSSEN die folgenden Informationen hervorgehen:

- Hauptsitz des Betreibers (Einschränkungen siehe 5.1.1),
- Gesellschafter des Betreibers,
- Zeichnungsberechtigte Personen.

Das Sicherheitsgutachten muss bestätigen, dass der TSP die Mindestanforderungen aus [gemTSL_SP_CP] erfüllt und dies in einem Sicherheitskonzept ausreichend beschrieben hat. Das Sicherheitsgutachten muss von einem durch die gematik anerkannten Gutachter stammen (Liste der Gutachter ist auf den Seiten der gematik veröffentlicht). Bei akkreditierten CAs bestätigt die Selbsterklärung, dass der Betrieb des TSP unter denselben Sicherheitsbedingungen erfolgt.

Alle Formulare des Antrages und die beigefügten Unterlagen müssen rechtsverbindlich nach Registerauszug (oder entsprechend vorgelegter Vertretungsvollmacht) unterschrieben sein.

5.2.2 Entscheidung über die Registrierung

Über eingehende Anträge auf Registrierung eines Produktiv-TSP entscheidet die gematik innerhalb von fünfzehn Werktagen.

Ein Antrag auf Registrierung eines Produktiv-TSP wird positiv entschieden, falls

- der Antrag gemäß den Vorgaben in Abschnitt 5.2.1 vollständig ist,

- die Kontrolle des Registerauszuges bei dem zuständigen Register die Korrektheit und Aktualität der Kopie bestätigt,
- das Sicherheitsgutachten bestätigt, dass die Mindestanforderungen aus [gemTSL_SP_CP] durch den Betreiber erfüllt werden,
- bei akkreditierten CAs die notwendigen Unterlagen nach Abschnitt 5.2.1 vollständig vorliegen und
- keine sonstigen Gründe gegen die Registrierung sprechen.

Die Gültigkeit der Registrierung ist zeitlich beschränkt. Der Betreiber wird über die Registrierung und deren Gültigkeit informiert (siehe Abschnitt 5.2.5). Der Betreiber muss rechtzeitig vor Ablauf der Gültigkeit seiner Registrierung einen neuen Antrag bei der gematik stellen.

5.2.3 Änderung einer Registrierung

Der Betreiber eines registrierten Produktiv-TSP ist verpflichtet, Änderungen an den für die Registrierung relevanten Informationen unverzüglich der gematik mitzuteilen (siehe Formular "Änderungsmitteilung TSL").

Zurzeit sind die folgenden Änderungen mitteilungspflichtig:

- Einstellung des Betriebs,
- Änderungen an der Gesellschafterstruktur,
- Änderungen bei den zeichnungsberechtigten Personen,
- Verlagerung des Hauptsitzes des Betreibers bzw. der eigentlichen Betriebsstätte des TSP in ein anderes Land,
- Änderungen bei der Zuordnung von Mitarbeitern zu den Rollen "Leiter TSP", "Sicherheitsbeauftragter" oder "Antragsteller TSP-TSL-Eintrag",
- Änderungen an den in dem Sicherheitskonzept beschriebenen technischen, baulichen und organisatorischen Sicherheitsmaßnahmen bzw. bei deren Umsetzung innerhalb des TSP,
- Änderung der TSP-Services und der zugehörigen TSL-Einträge.

Das Formular ist als PDF-Formular konzipiert. Es kann von der gematik-Website herunter geladen werden und ist elektronisch auszufüllen. Es muss (direkt aus dem Formular heraus) ausgefüllt per Mail vorab an die gematik gesendet werden. Der mit dem Mailversand erstellte Ausdruck ist dann unterschrieben (s. u.) per Post zu senden.

Die Änderungen sind durch entsprechende Nachweise, z. B. neuer Registerauszug, nachzuweisen.

Liegen Änderungen vor, die für das Sicherheitskonzept relevant sind, muss der Änderungsmitteilung ein neues Sicherheitsgutachten beigefügt werden. Dieses Sicherheitsgutachten muss bestätigen, dass die Mindestanforderungen aus [gemTSL_SP_CP] auch nach den Änderungen erfüllt werden.

Ggf. können die Änderungen zu einem Widerruf der Registrierung führen (siehe 5.2.4).

Alle Formulare des Antrages und die beigefügten Unterlagen müssen rechtsverbindlich nach Registerauszug (oder entsprechend vorgelegter Vertretungsvollmacht) unterschrieben sein.

5.2.4 Widerruf einer Registrierung

In den folgenden Fällen wird die Registrierung eines TSP durch die gematik widerrufen und der TSP aus der TSL entfernt:

- zeitlicher Ablauf der Gültigkeit der Registrierung, ohne dass rechtzeitig (3 Monate vorher) ein erneuter Antrag durch den TSP gestellt wurde,
- bekannt werden von Änderungen gemäß Abschnitt 5.2.3 ohne dass diese der gematik mit einer Änderungsmitteilung ordnungsgemäß durch den Betreiber mitgeteilt wurden,
- bekannt werden von Sicherheitsproblemen/-verstößen bei dem TSP,
- Verlagerung des Hauptsitzes des TSP oder der eigentlichen Betriebsstätte des TSP in ein Land außerhalb der Europäischen Union,
- Änderungsmitteilung gemäß Abschnitt 5.2.3 über eine für das Sicherheitskonzept relevante Änderung ohne entsprechende positive Einschätzung durch ein Sicherheitsgutachten eines von der gematik anerkannten Gutachters.

Bei einem Widerruf der Registrierung ist der TSP verpflichtet,

- unverzüglich die Produktion neuer X.509-Zertifikate für die Telematikinfrastruktur einzustellen,
- die Durchführung dieser Maßnahme der gematik schriftlich zu bestätigen.

Die gematik informiert den TSP schriftlich über den Widerruf der Registrierung.

5.2.5 Gültigkeit der Registrierung

Für die Gültigkeit der Registrierung und der Zertifikate sind folgende Aspekte zu beachten:

1) Ein TSP kann die Gültigkeitsdauer seines CA-Zertifikats innerhalb der durch [gemSpec_Krypt#5.1.1.1] gesetzten Grenzen selber festlegen. Das Gültigkeitsende eines CA-Zertifikats sollte immer zum Ende eines Jahres auslaufen.

2) Die Gültigkeit eines End-Entity-Zertifikats kann abhängig von der Einsatzdauer der Komponente gewählt werden. Das Gültigkeitsende eines End-Entity-Zertifikats darf aber das Gültigkeitsende des zugehörigen CA-Zertifikats nicht überschreiten. Die Grenzen aus [gemSpec_Krypt#5.1.1.1] müssen beachtet werden.

3) Ist ein TSP bei der gematik registriert, werden seine CA-Zertifikate (eins oder mehrere) in die TSL eingetragen.

4) Bei der Ausstellung der neuen TSL für das Folgejahr werden alle CA-Zertifikate aus der aktuellen TSL übernommen (d.h. auch solche, die als „revoked“ gekennzeichnet sind), außer es liegt einer der folgenden Gründe vor:

   - Die Gültigkeit des CA-Zertifikats läuft zum Ende des Jahres aus, d.h. das CA-Zertifikat ist im Folgejahr nicht mehr gültig.

5) Wird die Registrierung eines TSP durch die gematik widerrufen (Abs. 5.2.4), wird abhängig von dem Grund wie folgt verfahren:

   a) zeitlicher Ablauf der Gültigkeit der Registrierung, ohne dass rechtzeitig ein erneuter Antrag gestellt wurde

   b) bekannt werden von Änderungen ohne entsprechende Änderungsmitteilung

   c) bekannt werden von Sicherheitsproblemen/-verstößen beim TSP (insbesondere mögliche Kompromittierung des Schlüssels)

   d) Änderungsmitteilung über eine sicherheitsrelevante Änderung ohne positive Einschätzung durch Sicherheitsgutachten

   e) Einstellung des Betriebs

Folgende Auswirkungen haben die beschriebenen Gründe:

a) + e) Die zu dem TSP gehörenden CA-Zertifikate werden in der TSL als „revoked“ gekennzeichnet.

b) Abhängig von der Einschätzung des Vorfalls durch den Sicherheitsbeauftragten der gematik. Ggf. dann fortfahren wie bei c) + d).

c) + d) Alle zu dem TSP gehörenden CA-Zertifikate werden aus der TSL zeitnah entfernt.

Durch die Auswirkungen ergeben sich folgende Aufgaben:

a) + e) erfordern gemäß [gemTSL_SP_CP], dass der Statusauskunftdienst per OCSP des TSP durch einen anderen aufrechterhalten werden kann, und dass der (bzw. die) privaten Schlüssel des TSP sicher zerstört werden. In diesem Fall kann gemäß [gemTSL_SP_CP] auf einen Widerruf aller durch den TSP erzeugten End-Entity-Zertifikate verzichtet werden. Dies bedeutet technisch, dass die CA-zertifikate des TSP in der TSL (und den TSLs der Folgejahre) bis zu ihrem Gültigkeitsende verbleiben müssen.

Bei c) + d) und ggf. b) folgt aus [gemTSL_SP_CP], dass die durch den TSP erzeugten End-Entity-Zertifikate widerrufen werden müssen. Die Reaktionszeit (d.h. wie schnell wird eine neue TSL verteilt), muss dabei durch die gematik (Sicherheitsbeauftragter) für den konkreten Fall festgelegt werden. Eine Information aller Zertifikatsinhaber muss erfolgen. Diesen muss Gelegenheit gegeben werden, neue End-Entity-Zertifikate von einem anderen TSP zu beziehen.

Hinweis zum Status „revoked“

Bei diesem Vorgehen bedeutet die Kennzeichnung „revoked“ für ein CA-Zertifikat innerhalb der TSL nur, dass der TSP keine neuen Zertifikate produziert, nicht aber, dass Zertifikate (sowohl CA-Zertifikate als auch End-Entity-Zertifikate) ihre Gültigkeit vorzeitig verlieren.

5.2.6 Verlängerungsantrag

Der TSL-Service-Provider generiert jedes Jahr eine komplett neue Version der Trust-service Status List. Dazu erhält er von der gematik die Registrierungsanträge (Folgeanträge) der TSPs.

Im laufenden Jahr werden bei Registrierungsanträgen neue TSP-Einträge generiert und der vorhandenen Version der TSL hinzugefügt.

Die Gültigkeit der Erstregistrierung gilt für das Jahr der Registrierung und das Folgejahr. Danach muss spätestens 3 Monate vor Ablauf der registrierte TSP einen Verlängerungsantrag (siehe Vorgaben Formulare) stellen. Dieser bestätigt, dass der Betrieb weiterhin gemäß der bei der Registrierung nachgewiesenen Sicherheitsbedingungen geführt wird. Das Formular muss vollständig ausgefüllt werden. Unter diesen Voraussetzungen kann das Schlüsselpaar des TSP im Kontext „Einführung der Gesundheitskarte“ weiter verwendet werden.

5.3 Verfahren für einen Test-TSP

5.3.1 Antrag auf Registrierung

Für die Registrierung eines Test-TSP muss der Betreiber einen schriftlichen Antrag an die gematik stellen. Zu diesem Antrag gehören:

- vollständig ausgefülltes Formular "Unterlagen zur Registrierung als Trust Service Provider Test-TSL" (Vorgaben Formulare),
- vollständig ausgefülltes Formular "Anmeldung als TSL-TSP" (Vorgaben Formulare),
- ausgefülltes Formular "Liste der Kontaktpersonen TSL" (Vorgaben Formulare),
- ausgefülltes Formular "Registrierung eines TSP-Service in der TSL“ (Vorgaben Formulare),
- Kopie des Registerauszugs,
- zu registrierende Zertifikate (Digitale Identitäten).

In dem Formular "Anmeldung als TSL-TSP" muss unter Firma/Organisation die Adresse der eigentlichen Betriebsstätte des Test-TSP angegeben werden. Zu den Datenfeldern „Allgemeine Angaben in der TSL“ sind die Hinweise unter 6.8.1 zu beachten.

In dem Formular "Liste der Kontaktpersonen TSL" muss für die Rollen "Leiter TSP", "Sicherheitsbeauftragter" und "Antragsteller TSP-TSL-Eintrag" jeweils mindestens eine Person genannt werden. Eine Person kann dabei für mehrere Rollen genannt werden.

Das Formular "Registrierung eines TSP-Service in der TSL“ nimmt die für die TSL notwendigen Detailinformationen bzgl. der vom TSP angebotenen Dienste auf.

Die genannten Formulare sind als PDF-Formulare konzipiert. Sie können von der gematik-Website herunter geladen werden und sind elektronisch auszufüllen. Sie müssen ausgefüllt (direkt aus dem Formular heraus) per Mail vorab an die gematik gesendet

werden. Der mit dem Mailversand erstellte Ausdruck ist dann unterschrieben (s. u.) per Post zu senden.

Die Kopie des Registerauszugs muss von dem aktuellen Eintrag des Betreibers in dem zuständigen Register (Handelsregister, Vereinsregister, etc.) stammen. Aus diesem müssen die folgenden Informationen hervorgehen:

- Hauptsitz des Betreibers (Einschränkungen siehe 5.1.1),
- Gesellschafter des Betreibers,
- zeichnungsberechtigte Personen.

Alle Formulare des Antrages und die beigefügten Unterlagen müssen rechtsverbindlich nach Registerauszug (oder entsprechend vorgelegter Vertretungsvollmacht) unterschrieben sein.

5.3.2 Entscheidung über die Registrierung

Über eingehende Anträge auf Registrierung einer Test-TSP entscheidet die gematik innerhalb von fünf Werktagen.

Ein Antrag auf Registrierung eines Test-TSP wird positiv entschieden, falls

- der Antrag gemäß den Vorgaben in Abschnitt 5.3.1 vollständig ist und
- keine sonstigen Gründe gegen die Registrierung sprechen.

Die Gültigkeit der Registrierung ist zeitlich beschränkt. Der Betreiber wird über die Registrierung und deren Gültigkeit informiert. Der Betreiber muss rechtzeitig (3 Monate vorher) vor Ablauf der Gültigkeit seiner Registrierung einen neuen Antrag bei der gematik stellen.

5.3.3 Änderung einer Registrierung

Der Betreiber eines registrierten Test-TSP ist verpflichtet, Änderungen an den für die Registrierung relevanten Informationen unverzüglich der gematik mitzuteilen (siehe Formular "Änderungsmitteilung TSL" in Abschnitt Vorgaben Formulare).

Zurzeit sind die folgenden Änderungen mitteilungspflichtig:

- Einstellung des Betriebs,
- Änderungen an der Gesellschafterstruktur,
- Änderungen bei den zeichnungsberechtigten Personen,
- Verlagerung des Hauptsitzes des Betreibers bzw. der eigentlichen Betriebsstätte des TSP in ein anderes Land,
- Änderungen bei der Zuordnung von Mitarbeitern zu den Rollen "Leiter TSP", "Sicherheitsbeauftragter" oder "Antragsteller TSP-TSL-Eintrag",
- Änderung der TSP-Services und der zugehörigen TSL-Einträge.

Das Formular ist als PDF-Formular konzipiert. Es kann von der gematik-Website herunter geladen werden und ist elektronisch auszufüllen. Es muss ausgefüllt (direkt aus dem Formular heraus) per Mail vorab an die gematik gesendet werden. Der mit dem Mailversand erstellte Ausdruck ist dann unterschrieben (s. u.) per Post zu senden.

Die Änderungen sind durch entsprechende Nachweise, z. B. neuer Registerauszug, nachzuweisen.

Ggf. können die Änderungen zu einem Widerruf der Registrierung führen (siehe 5.3.4).

Alle Formulare des Antrages und die beigefügten Unterlagen MÜSSEN rechtsverbindlich nach Registerauszug (oder entsprechend vorgelegter Vertretungsvollmacht) unterschrieben sein.

5.3.4 Widerruf der Registrierung

Eine einmal erfolgreich durchgeführte Registrierung eines Test-TSP wird in den folgenden Fällen durch die gematik widerrufen:

- Einstellung des Betriebs,
- ein Jahr nach der Registrierung wurde noch keine erfolgreiche Registrierung des zugehörigen Produktiv-TSP durchgeführt.

Der Widerruf der Registrierung des Test-TSP kann durch die gematik ohne erneute Rücksprache mit dem Betreiber erfolgen. Der Betreiber wird über den Widerruf schriftlich informiert.

5.4 Übertragung/Personalisierung kryptographischer Daten

Sicherheitsrelevante Aspekte beim Transport von Schlüsseln und Zertifikaten behandelt das Dokument [gemPersKrypt]. Die Vorgaben aus diesem Dokument sind verbindlich. Weitere Verfeinerungen liefern das Kryptographiekonzept in dem Übergreifenden Sicherheitskonzept der Telematikinfrastruktur [gemSiKo] und das Kompatibilitäts-Dokument aus der Gesamtarchitektur [gemSpec_Krypt].

6 Architektur der Trust-service Status List

6.1 Logisches Modell der TSL

Ein TSP muss in der gematik Trust-service Status List (gematik-TSL) eingetragen sein. Um dies beantragen zu können, muss sich der TSP vorher bei der gematik registrieren lassen.

Der detaillierte Aufbau der TSL wird im folgenden Kapitel näher erläutert. Damit soll auch eine Hilfestellung für die Beantragung der Registrierung gegeben werden, insbesondere für das Ausfüllen der notwendigen Formulare (s. Abschnitte 5.2.1 und 5.3.1) und der damit verbundenen Beschreibung der zu registrierenden Zertifikate. Die Formulare selbst sind auf der gematik-Website zu finden.

Der strukturelle Aufbau sowie die ausführliche Beschreibung der einzelnen TSL-Felder sind in [ETSI] zu finden. Daraus entnommen ist die folgende Grafik, die das logische Modell der TSL übersichtlich darstellt.

In den nachfolgenden Abschnitten werden dann die für die Teilnehmer der gematik-TSL besonders relevanten Felder der TSL beschrieben und, wo zutreffend, die möglichen oder erlaubten Inhalte dargelegt.

Die genaue Festlegung der OID wird im Dokument [gemSpec_OID] spezifiziert.

Das entsprechende Schema von [ETSI] (Reference RTS/ESI-000038, ETSI TS 102 231 V2.1.1 (2006-2 03)) mit dem TargetNameSpace "http://uri.etsi.org/02231/v2#" wird in diesem Kapitel verwendet und dargestellt.

In Anhang B findet sich eine Leseanleitung für XML-Schema-Fragmente.

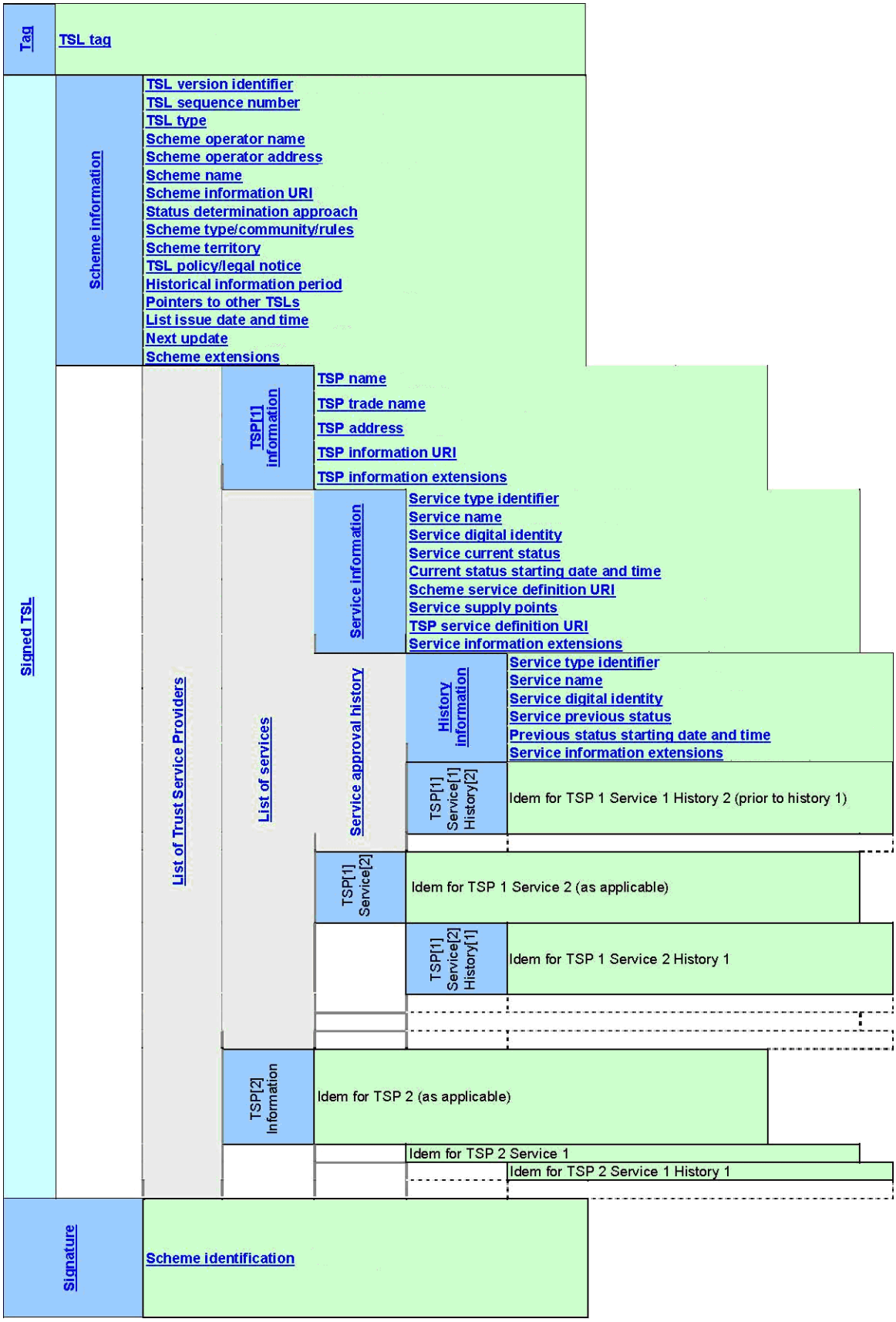


Abbildung 2: Logisches Modell der TSL

6.2 TSL Extension

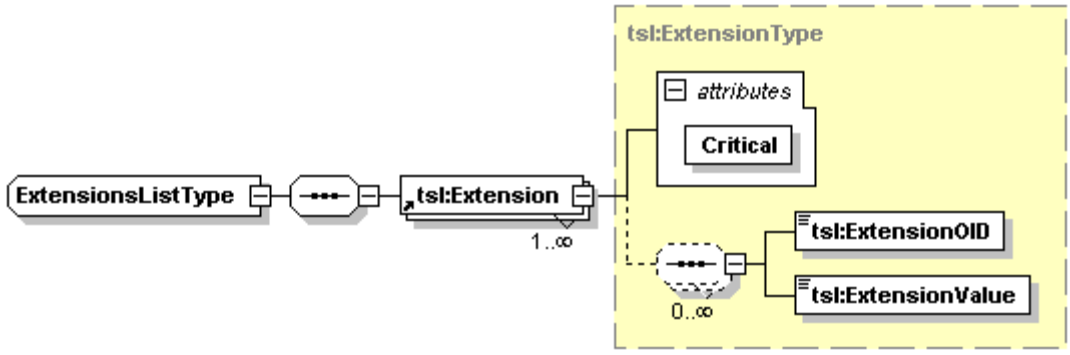
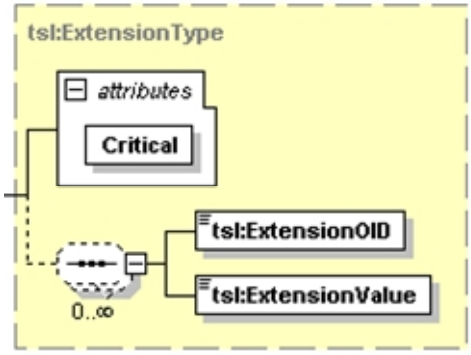


Abbildung 3 Darstellung der TSL-Extension auf Grundlage von [ETSI]

Tabelle 3 element ExtensionType

diagram	
Beschreibung	Der Elementtyp ExtensionType ist eine spezifische Erweiterung der TSL. Nach ETSI müssen Extension mit dem Attribute „Critical“ (true oder false) ausgestattet werden. Die Erweiterung spiegelt sich in dem Paar aus ExtensionOID und ExtensionValue wieder. Ausgewertet wird nur die ExtensionOID. Der ExtensionValue DARF NICHT automatisch interpretiert werden.
Typ	<xsd:element name="ExtensionOID" type="xsd:string"/> <xsd:element name="ExtensionValue" type="xsd:string"/>
Beispiel	ExtensionOID: 1.3.36.15.2.4.4 ExtensionValue: Eintrag für einen TSP, Produzent von eGK-Zertifikaten

Somit ist die TSL durch eine Anwendung differenzierbar. Nicht jeder Service-Eintrag muss interpretiert werden. Es ist möglich, mit einem Filter alle vorhandenen TSP für eGK-Zertifikate anzuzeigen.

Die genaue Festlegung der OID wird im Dokument [gemSpec_OID] spezifiziert.

6.3 Lokalisierung der OCSP-Adresse anhand des Service Supply Point

Der `ServiceSupplyPoint` wird für die Speicherung der OCSP-Responder Adresse verwendet. Zu jedem TSP-CA-Eintrag wird der zugehörige `ServiceSupplyPoint` mit der gültigen Adresse des Responders angelegt.

Die Abfrage des Sperrstatus des zu prüfenden Zertifikats MUSS gegen den im „ServiceSupplyPoint“ der TSL eingetragenen OCSP-Responder gerichtet werden.

Das Element wird in Tabelle 30 element tsl:ServiceSupplyPointsType/ServiceSupplyPoint detailliert beschrieben.

6.4 Lokalisierung der TSL

Die TSL bzw. TCL beinhaltet im Element "PointersToOtherTSL“ die Zugriffsadresse für die jeweilige Liste. Alternativ ist ein Eintrag für die Backup-Liste vorhanden. In der Tabelle 8 element tsl:PointersToOtherTSL wird das Element beschrieben und ein Beispiel aufgelistet.

6.5 TSL-Einträge für die Bereitstellung neuer Vertrauensanker

Dieser Abschnitt wird zum nächsten geplanten Release in das Dokument [gemVerw_Zert_TI] übernommen.

Neue TSL-Service-Provider-Zertifikate werden (bei Generationswechsel) rechtzeitig in der TSL integriert. Dies betrifft konkret die folgenden Zertifikate:

- TSL-Signaturzertifikat
- TSL-Root-Zertifikat

Dadurch wird die Integrität der neuen Schlüssel durch die gültigen alten gesichert. Dazu erzeugt der gematik-TSL-Service Provider einen TSL -Eintrag mit folgenden Eigenschaften (Update-Parameter):

- Service Type Identifier (http://uri.etsi.org/TrstSvc/Svctype/TSLServiceCertChange) signalisiert den Verwendungszweck des Eintrags,
  `<xsd:element name="ServiceTypeIdentifier" type="tsl:NonEmptyURIType"/>`
- das neue Zertifikat (ServiceDigitalIdentity),
  `<xsd:element name="X509Certificate" type="xsd:base64Binary"/>`
- Gültigkeitszeitraum des Eintrags (StatusStartingTime) und
  `<xsd:element name="StatusStartingTime" type="xsd:dateTime"/>`
- Status des Zertifikatswechsels (ServiceInformationExtension).
  `<xsd:element name="ServiceInformationExtensions" type="tsl:ExtensionsListType" minOccurs="0"/>`

Als Vertrauensanker wird das Paar aus Root- und Signaturzertifikat angesehen.

In den folgenden Tabellen werden zwei Beispiele zu den TSL-Einträgen dargestellt, die den Wechsel des Vertrauensraumes bedeuten.

Tabelle 4 Beispiel für den TSL-Eintrag zum Wechsel des Root-Zertifikats

```
<tsl:TSPService>
	<tsl:ServiceInformation>
	<tsl:ServiceTypeIdentifier>
		http://uri.etsi.org/TrstSvc/Svctype/TSLServiceCertChange
	</tsl:ServiceTypeIdentifier>
	<tsl:ServiceName>
		<tsl:Name xml:lang="DE">Neues Root Zertifikat der TSL</tsl:Name>
	</tsl:ServiceName>
	<tsl:ServiceDigitalIdentity>
		<tsl:DigitalId>
			<tsl:X509Certificate>UjBsR09EbGhjZ0dTQUxNQUFBUUNBR
			U1tQ1p0dU1GUXhEUzhi</tsl:X509Certificate>
		</tsl:DigitalId>
	</tsl:ServiceDigitalIdentity>
	<tsl:ServiceStatus>http://uri.etsi.org/TrstSvc/Svcstatus/inaccord
	</tsl:ServiceStatus>
	<tsl:StatusStartingTime>2008-04-01T09:30:47.0Z</tsl:StatusStartingTime>
	<tsl:ServiceSupplyPoints>
		<tsl:ServiceSupplyPoint>http://tsl.ocsp.gematik.de
		</tsl:ServiceSupplyPoint>
	</tsl:ServiceSupplyPoints>
	<tsl:ServiceInformationExtensions>
		<tsl:Extension Critical="true">
			<ExtensionOID>1.3.36.15.2.4.9.1</ExtensionOID>
			<ExtensionValue>Change of Root Certificate</ExtensionValue>
		</tsl:Extension>
	</tsl:ServiceInformationExtensions>
	</tsl:ServiceInformation>
</tsl:TSPService>
```

Tabelle 5 Beispiel für den TSL-Eintrag zum Wechsel des Signatur-Zertifikats

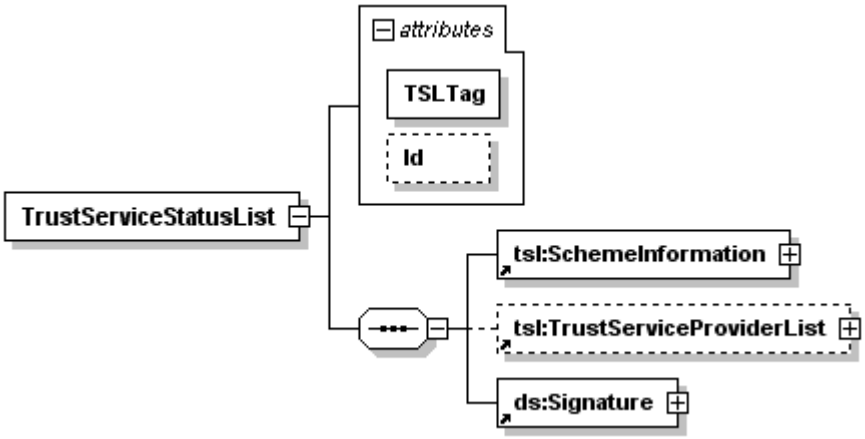
```
<tsl:TSPService>
	<tsl:ServiceInformation>
	<tsl:ServiceTypeIdentifier>
		http://uri.etsi.org/TrstSvc/Svctype/TSLServiceCertChange
	</tsl:ServiceTypeIdentifier>
	<tsl:ServiceName>
		<tsl:Name xml:lang="DE">Neues Signatur-Zertifikat der TSL</tsl:Name>
	</tsl:ServiceName>
	<tsl:ServiceDigitalIdentity>
		<tsl:DigitalId>
			<tsl:X509Certificate>UjBsF09EbGhjZ0dTQUxNQUFBUUNBR
			U1tQ1p0dU1GUXhEUzhi</tsl:X509Certificate>
		</tsl:DigitalId>
	</tsl:ServiceDigitalIdentity>
	<tsl:ServiceStatus>http://uri.etsi.org/TrstSvc/Svcstatus/inaccord
	</tsl:ServiceStatus>
	<tsl:StatusStartingTime>2008-04-01T09:30:47.0Z</tsl:StatusStartingTime>
	<tsl:ServiceSupplyPoints>
		<tsl:ServiceSupplyPoint>http://tsl.ocsp.gematik.de
		</tsl:ServiceSupplyPoint>
	</tsl:ServiceSupplyPoints>
	<tsl:ServiceInformationExtensions>
		<tsl:Extension Critical="true">
			<ExtensionOID>1.3.36.15.2.4.9.2</ExtensionOID>
			<ExtensionValue>Change of Signer Certificate</ExtensionValue>
		</tsl:Extension>
	</tsl:ServiceInformationExtensions>
	</tsl:ServiceInformation>
</tsl:TSPService>
```

Die genaue Festlegung der OID wird im Dokument [gemSpec_OID] spezifiziert.

6.6 XML-Schema der TSL

Tabelle 6 element TrustServiceStatusList

diagram



Beschreibung

Grundstruktur der TSL. Die Schema-Informationen geben Auskunft u. a. über den Herausgeber der TSL. Die "TrustServiceProviderList“ beinhaltet die Angaben der registrierten TSPs. Die Integrität und Authentizität der Inhalte wird durch die Signatur am Ende der Datei gewahrt.

Entgegen der Beschreibung von [ETSI] ist das Attribute "Id" ein Pflichtfeld.

6.7 TSL-Schema Informationen

Tabelle 7 element tsl:SchemeInformation
diagram

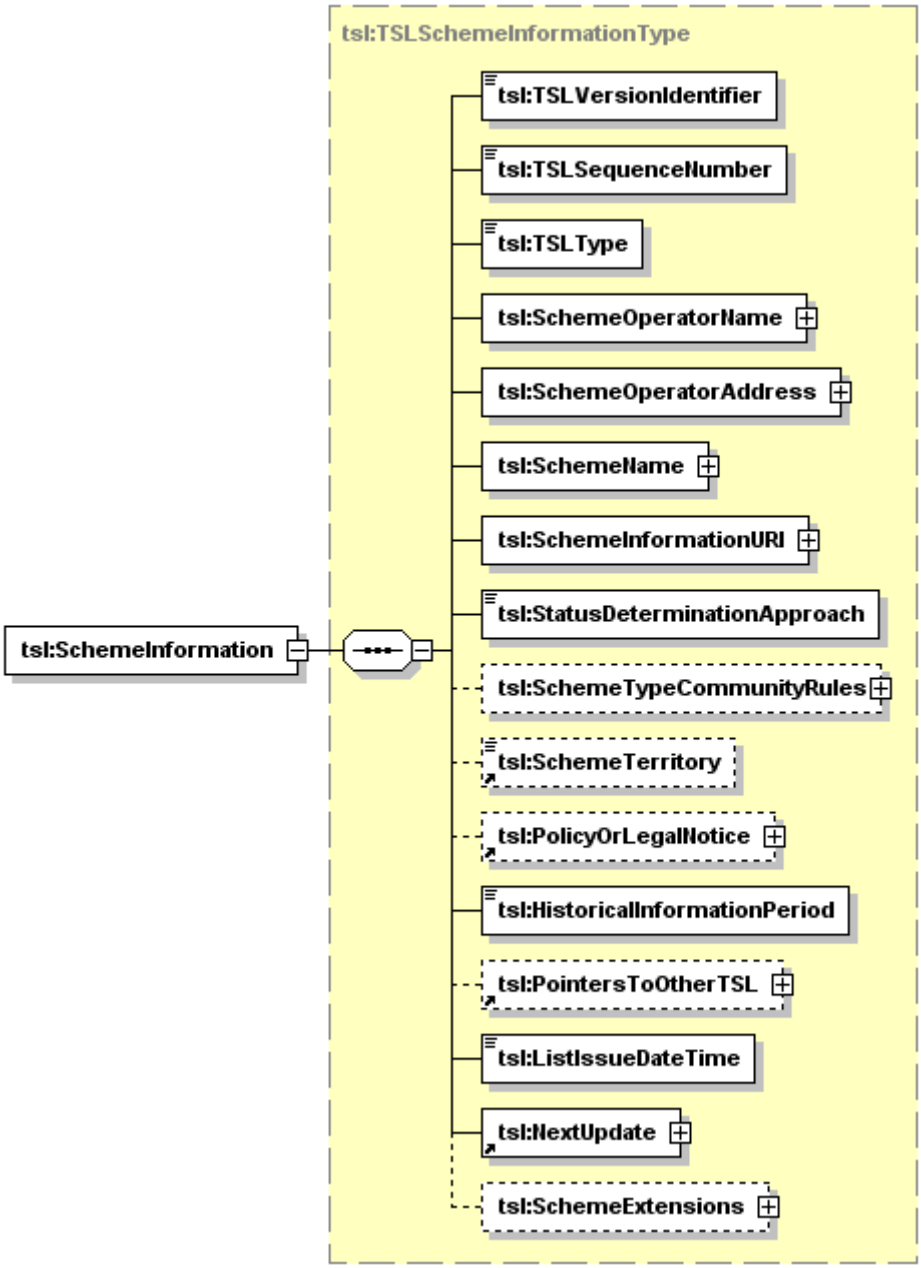
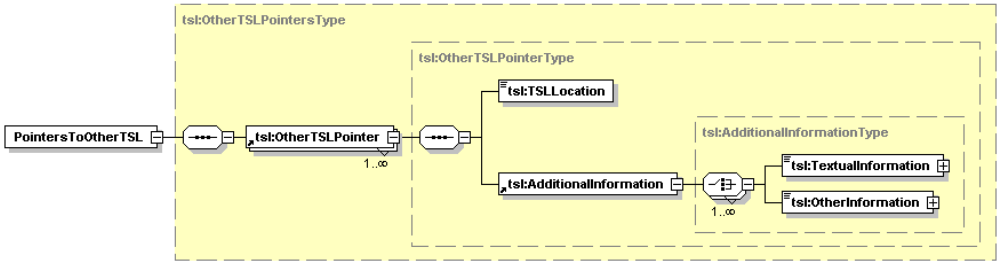


Tabelle 8 element tsl:PointersToOtherTSL
diagram



Beschreibung: Hier wird die Zugriffsadresse für die jeweilige Liste gespeichert. Zusätzlich ist ein Eintrag für die Backup-Liste vorhanden. Die Unterscheidung der Primär- und Backup-Liste erfolgt anhand von OIDs im Element tsl:TextualInformation.

Die genaue Festlegung der OID wird im Dokument [gemSpec_OID] spezifiziert.

Bespiel

```
<PointersToOtherTSL>
        <OtherTSLPointer>
                <TSLLocation>http://test.tsl.gematik.de/TSL_T.xml</TSLLocation>
                <AdditionalInformation>
                <TextualInformation xml:lang="DE">1.3.36.15.2.4.2</TextualInformation>
                </AdditionalInformation>
        </OtherTSLPointer>
        <OtherTSLPointer>
        <TSLLocation>http://backuptest.tsl.gematik.de/TSL_T.xml</TSLLocation>
                <AdditionalInformation>
                <TextualInformation xml:lang="DE">1.3.36.15.2.4.3</TextualInformation>
                </AdditionalInformation>
                </OtherTSLPointer>
</PointersToOtherTSL>
```

6.8 Angaben zum Trust Service Provider

Tabelle 9 element tsl:TrustServiceProviderList

diagram

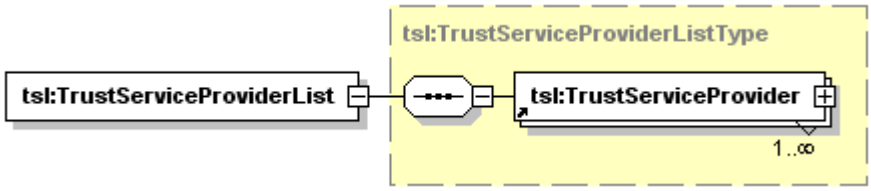
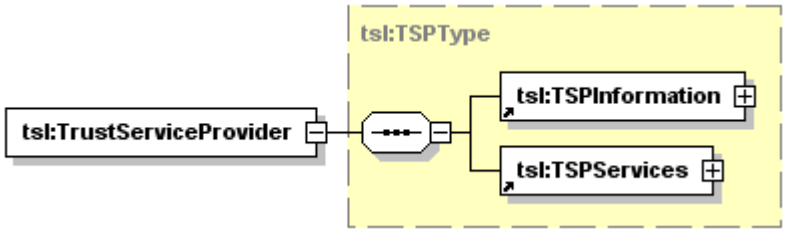


Tabelle 10 element tsl:TrustServiceProvider

diagram



6.8.1 TSP Informationen

Die TSP-Informationen sind in den Formularen in den Bereich „Allgemeine Angaben in der TSL“ einzutragen.

Tabelle 11 element tsl:TSPInformation

diagram

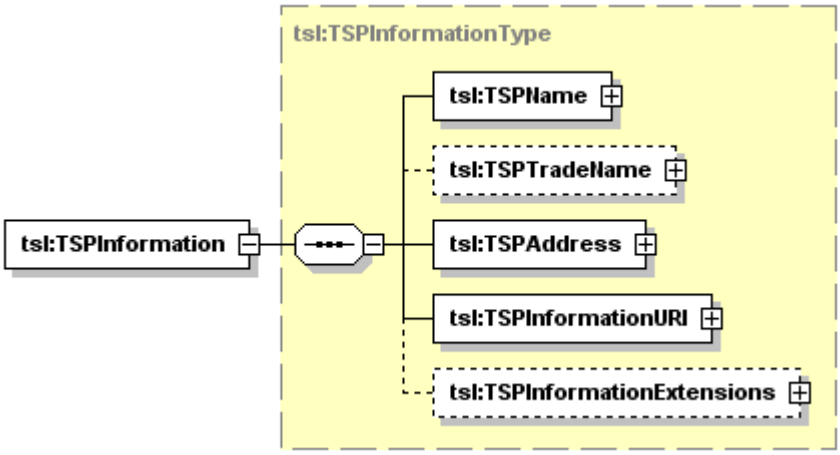
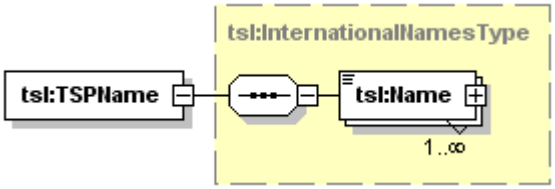


Tabelle 12 element tsl:TSPInformationType/TSPName

diagram



Beschreibung

Der Name der für die TSP verantwortlichen juristischen Person, deren TSP-Dienste über das Schema anerkannt werden. Dabei MUSS es sich um den Namen handeln, unter dem alle formalen rechtlichen Registrierungen erfolgen und an den jegliche formale Kommunikation, unabhängig ob physisch oder elektronisch, gerichtet wird.

Tabelle 13 element tsl:TSPInformationType/TSPTradeName

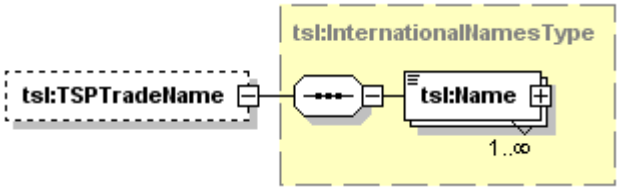
diagram	
Beschreibung	Alternativer (Marken-)Name, unter dem die für die TSP verantwortliche juristische Person am Markt auftritt und die über diese TSL referenzierten Dienste anbietet.

Tabelle 14 element tsl:TSPInformationType/TSPInformationURI

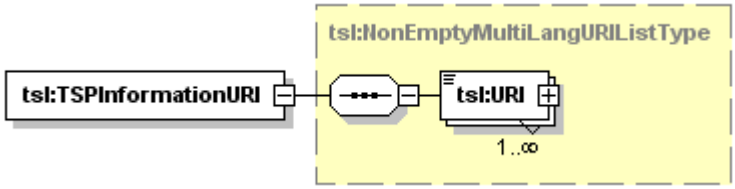
diagram	
Beschreibung	Spezifiziert die URI(s), unter der die Teilnehmer TSP-spezifische Informationen zu allgemeinen Geschäftsbedingungen, Haftung und ähnlichem erhalten können
Beispiel	www.<firmenname>.de/informationen/tsp

Tabelle 15 element tsl:TSPInformationType/TSPAddress

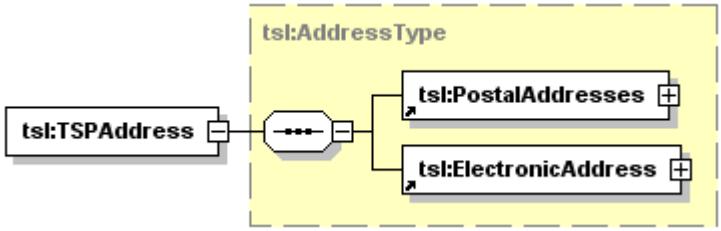
diagram	
Beschreibung	Spezifiziert die postalische sowie die elektronische Adresse des TSP

Tabelle 16 element tsl:PostalAddresses

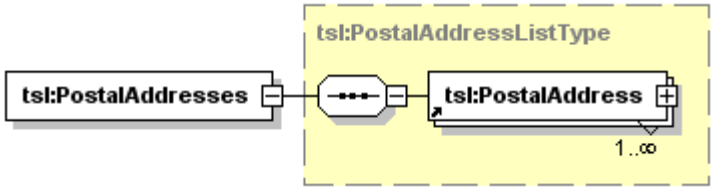
diagram	

Tabelle 17 complexType tsl:PostalAddressType

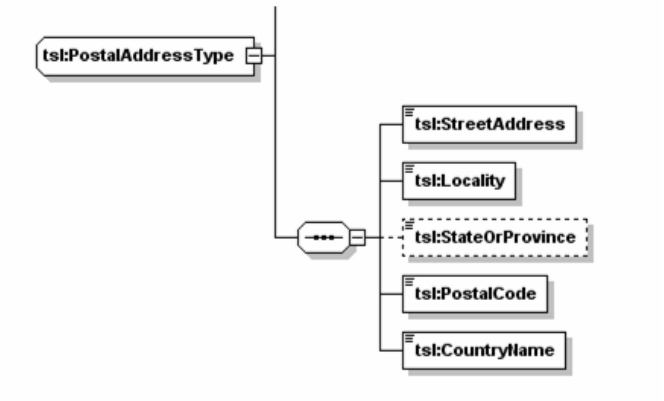
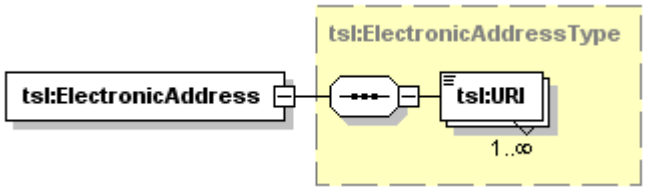
diagram	
Beschreibung	Aufbau der postalischen Adresse

Tabelle 18 element tsl:ElectronicAddress

diagram	
Beschreibung	Elektronische Adresse des TSP
Zugelassene Werte	Kontakt-Email-Adresse des TSP

6.8.2 TSP-Dienst-Informationen

Die TSP-Dienst-Informationen sind in dem entsprechenden Formular in den Bereich „Spezielle Angaben – Service Information" einzutragen.

Tabelle 19 element tsl:TSPServices

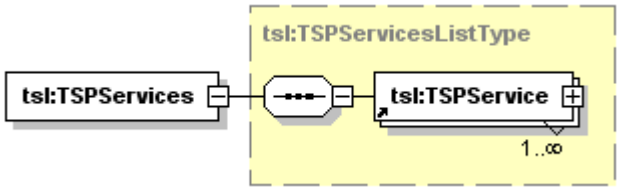
diagram	

Tabelle 20 element tsl:TSPService

diagram

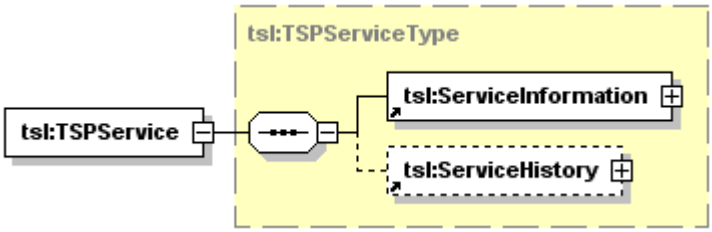
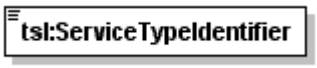


Tabelle 21 element tsl:ServiceInformation

diagram

Tabelle 22 element tsl:ServiceTypeIdentifier

diagram



Beschreibung	Die zitierte URI muss einem der in Anhang D.2 [ETSI] beinhalteten und unten aufgeführten Werte entsprechen. Sie spezifiziert den Identifier des Diensttyps.
Zugelassene Werte	http://uri.etsi.org/TrstSvc/Svctype/CA/PKC (TSP, der Zertifikate ausstellt) http://uri.etsi.org/TrstSvc/Svctype/CA/QC (TSP, der qualifizierte Zertifikate ausstellt) http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP (TSP, der einen OSCP-Dienst betreibt) http://uri.etsi.org/TrstSvc/Svctype/Certstatus/CRL (TSP, der einen CRL-Dienst betreibt) http://uri.etsi.org/TrstSvc/Svctype/RA (Registrierungsstelle)

http://uri.etsi.org/TrstSvc/Svctype/TSA (Zeitstempeldienst)

Tabelle 23 element tsl:TSPServiceInformationType/ServiceName

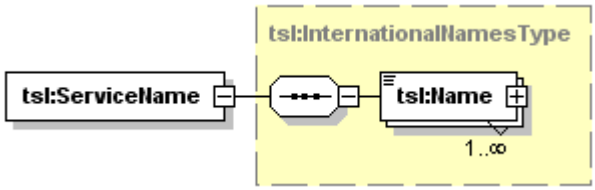
diagram	
Beschreibung	Spezifiziert den Namen, unter dem der TSP den mit „Service Type Identifier“ identifizierten Dienst anbietet.
Beispiel	TSL-SP-Root-CA-Produktivsystem für die X.509-TSL der gematik

Tabelle 24 element tsl:ServiceDigitalIdentity

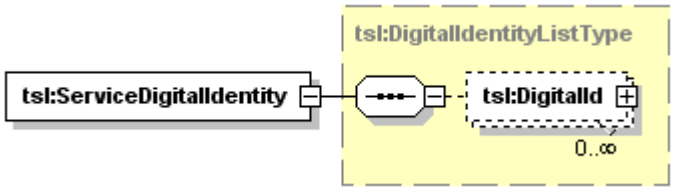
diagram	

Tabelle 25 complexType tsl:DigitalIdentityListType

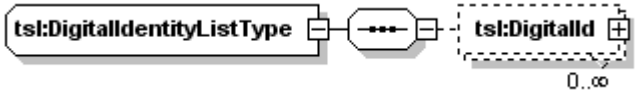
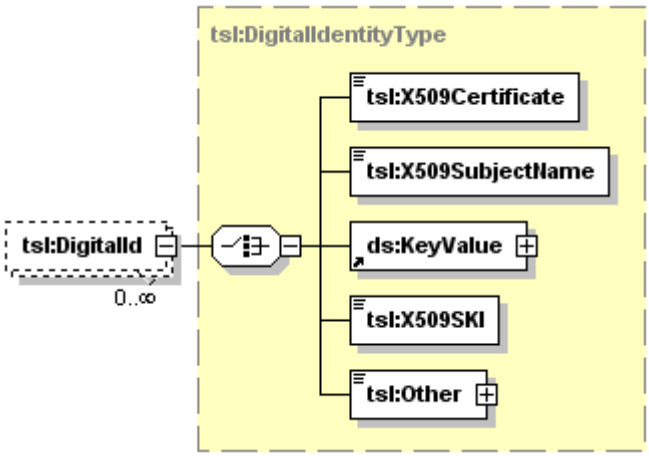
diagram	

Tabelle 26 element tsl:DigitalIdentityListType/DigitalId

diagram	
Beschreibung	Die digitale Identität identifiziert den Service anhand eines Zertifikates oder einer ähnlichen kryptografischen Identität.

Zugelassene Werte	tsl:X509Certificate ds:KeyValue

Tabelle 27 element tsl:ServiceStatus

diagram	
Beschreibung	Die zitierte URI muss einem der in Anhang D.2 [ETSI] beinhalteten und unten aufgeführten Werte entsprechen. Sie spezifiziert den Identifier des Dienststatus.
Zugelassene Werte	http://uri.etsi.org/TrstSvc/Svcstatus/inaccord http://uri.etsi.org/TrstSvc/Svcstatus/revoked

Tabelle 28 element tsl:TSPServiceInformationType/StatusStartingTime

diagram	
Beschreibung	Spezifiziert Datum und Uhrzeit, zu dem der jetzige Status eintrat.

Tabelle 29 complexType tsl:ServiceSupplyPointsType

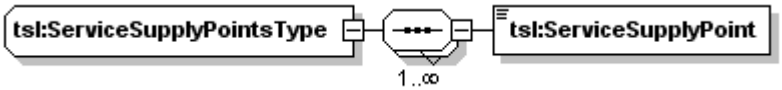
diagram	

Tabelle 30 element tsl:ServiceSupplyPointsType/ServiceSupplyPoint

diagram	
Beschreibung	Spezifiziert eine oder mehrere URIs, unter der Benutzer (Teilnehmer, vertraute Parteien) den Dienst nutzen können. Der `ServiceSupplyPoint` wird für die Speicherung der OCSP-Responder Adresse verwendet. Zu jedem TSP-CA-Eintrag wird der zugehörige `ServiceSupplyPoint` mit der gültigen Adresse des Responders angelegt. Im Fall der VPN-Konzentratoren steht anstelle der OCSP-Adresse analog die CRL-Downloadadresse.
Beispiel	**<ServiceSupplyPoint>http://ocsp.gematik.de:8080/CMOCSP/OCSP</ServiceSupplyPoint>**

6.8.3 Erläuterung der möglichen Dateiformate der digitalen Identitäten

Tabelle 31: Mögliche Dateiformate für digitale Zertifikate

.cer	DER-kodiertes Zertifikat oder Zertifikatsfolgen
.der	DER-kodiertes Zertifikat
.crt	DER- oder Base64-kodiertes Zertifikat
.pem	Base64-kodiertes Zertifikat, umschlossen von “-----BEGIN CERTIFICATE-----" und “-----END CERTIFICATE-----"

Tabelle 32: Mögliche Dateiformate für öffentliche Schlüssel (ds:keyValue)

.cer	DER-kodierter öffentlicher Schlüssel
.der	DER-kodierter öffentlicher Schlüssel
.pem	Base64-kodierter öffentlicher Schlüssel, umschlossen von “-----BEGIN PUBLIC KEY-----" und “-----END PUBLIC KEY -----"

7 Vorgaben Formulare

Die Formulare zur Beantragung der Zulassung als Trust Service Provider werden von der gematik bereitgestellt.

Sie sind als PDF-Formulare konzipiert und sind elektronisch auszufüllen. Sie müssen (direkt aus dem Formular heraus) ausgefüllt per Mail vorab an die gematik gesendet werden. Der mit dem Mailversand erstellte Ausdruck ist dann mit den restlichen benötigten Unterlagen per Post zu senden.

Alle Formulare des Antrages und die beigefügten Unterlagen müssen rechtsverbindlich nach Registerauszug (oder entsprechend vorgelegter Vertretungsvollmacht) unterschrieben sein.

Die Abbildung 4 zeigt eine Übersicht der Formulare und ihre Abhängigkeit untereinander für den Anwendungsfall Anmeldung eines TSP.

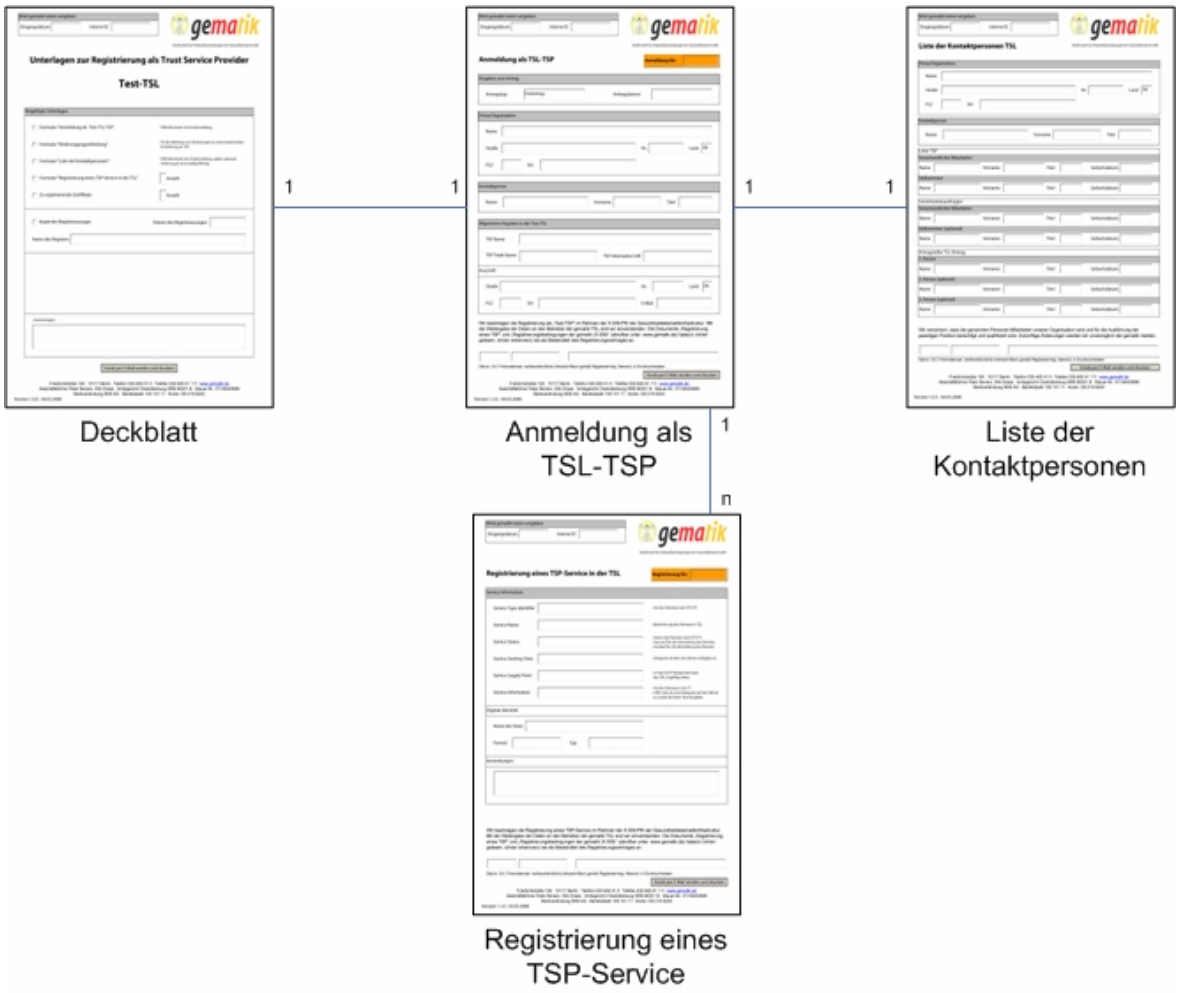


Abbildung 4 Übersicht der Formulare zur Anmeldung eines TSP in die TSL

Anhang A

A1 – Abkürzungen

Kürzel	Erläuterung
AUT	Authentication
CA	certification authority
eGK	Elektronische Gesundheitskarte
ENC	Encryption
ETSI	Europäisches Institut für Telekommunikationsnormen
HBA	Heilberufsausweis
HPC	Oberbegriff für HBA und SMC
OSig	Organizational Signature
PKI	Public Key Infrastructure
SigG	Signaturgesetz
SMC	Security Module Card
SRQ	Specified Related Question
TCL	Trusted Component List
TSL	Trust-service Status List
TSP	Trust Service Provider
ZDA	Zertifizierungsdiensteanbieter

A2 – Glossar

Das Projektglossar wird als eigenständiges Dokument zur Verfügung gestellt.

A3 – Abbildungsverzeichnis

A4 – Tabellenverzeichnis

A5 – Referenzierte Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel

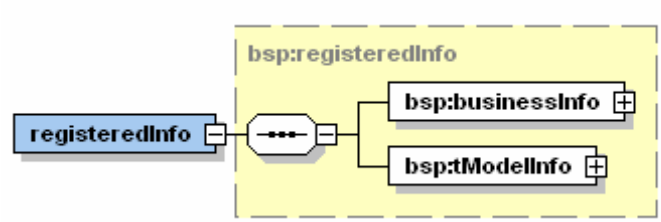
[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[ALGCAT]	Bundesanzeiger Nr. 59, S. 4695-4696 (30. März 2005): Suitable Cryptographic Algorithms Geeignete Algorithmen zur Erfüllung der Anforderungen nach §17 Abs. 1 bis 3 SigG vom 22. Mai 2001 in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV vom 22. November 2001, http://www.bundesnetzagentur.de/media/archive/1507.pdf (zuletzt geprüft am 13.12.2006) NEU: Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) vom 17. Dezember 2007 Geeignete Algorithmen zur Erfüllung der Anforderungen nach § 17 Abs. 1 bis 3 SigG in Verbindung mit Anlage 1 Abschnitt I Nr. 2 SigV Veröffentlicht am 05.Februar 2008 im Bundesanzeiger Nr. 19, Seite 376 http://www.bundesnetzagentur.de/media/archive/12198.pdf
[BSI-TR03116]	BSI TR-03116 (23.03.2007): Technische Richtlinie für die eCard-Projekte der Bundesregierung Version: 1.0 http://www.bsi.de/literat/tr/tr03116/BSI-TR-03116.pdf
[BÄK_ZPX.509B]	Bundesärztekammer (19.04.2006): Zertifikatsprofile für X.509 Basiszertifikate V 0.89; Zertifikatsaufbau und –hierarchie, Gültigkeitsmodell für Zertifikatstypen: ENC, AUT, QES, ATT sowie die Root, Cross- und CA-Zertifikate, die CRL-Signer und die OCSP-Zertifikate
[ETSI]	ETSI (ETSI TS 102 231 V2.1.1 (2006-03)): ETSI Technical Specification TS 102 231 (‘Provision of harmonized Trust Service Provider (TSP) status information’)
[gemPersKrypt]	gematik (21.12.2006): Einführung der Gesundheitskarte - Personalisierung kryptographischer Daten der eGK, Version 1.0.0, www.gematik.de
[gemSiKo]	gematik (10.03.2008): Einführung der Gesundheitskarte – Übergreifendes Sicherheitskonzept der Telematikinfrastruktur Version 2.2.0
[gemSpec_MK]	gematik (22.02.2008): Einführung der Gesundheitskarten - Spezifikation für Musterkarten und Testkarten (eGK, HBA, SMC), Version 2.6.0, www.gematik.de
[gemSpec_Krypt]	gematik (26.03.2008): Einführung der Gesundheitskarte – Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur, Version 1.3.0

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[gemSpec_OID]	gematik (Draft 2008): Einführung der Gesundheitskarte - Spezifikation: Festlegung von OIDs (in Vorbereitung)
[gemTSL_SP_CP]	gematik (29.11.2007): Einführung der Gesundheitskarte - Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL zur Herausgabe von X.509-ENC/AUT/OSIG-Zertifikaten Version 1.2.0, www.gematik.de
[gemVerw_Zert_TI]	gematik (28.02.2008): Einführung der Gesundheitskarte - Verwendung von Zertifikaten in der Telematikinfrastruktur Version 1.1.0
[gemX.509_eGK]	gematik (26.11.2007): Einführung der Gesundheitskarte - Festlegungen zu den X.509-Zertifikaten der Versicherten Version 1.4.0; www.gematik.de
[gemX.509_SMCB]	gematik (18.03.2008): Einführung der Gesundheitskarte - Festlegung zu den X.509-Zertifikaten der SMCTyp B Version 1.3.0; www.gematik.de
[gemX.509_TCL]	gematik (19.03.2008): Einführung der Gesundheitskarte - PKI für X.509-Zertifikate: Konzept und Registrierungsanforderungen für die Trusted Component List (TCL) Version 1.2.0
[gemX.509_TSL]	gematik (15.12.2005): Einführung der Gesundheitskarte – Festlegung einer einheitlichen X.509-Zertifikatsinfrastruktur (TSL) Version 1.0.0
[gemQES]	gematik (15.12.2005): Einführung der Gesundheitskarte - Aktivierung der qualifizierten elektronischen Signatur Version 1.0.0, www.gematik.de
[HPC-P2]	Bundesärztekammer et al. (in Vorbereitung): German Health Professional Card and Security Module Card Part 2: HPC Applications and Functions Version 2.x.x
[RFC2119]	RFC 2119 (März 1997): Key words for use in RFCs to Indicate Requirement Levels S. Bradner, http://www.ietf.org/rfc/rfc2119.txt (zuletzt geprüft am 14.12.2006)

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.

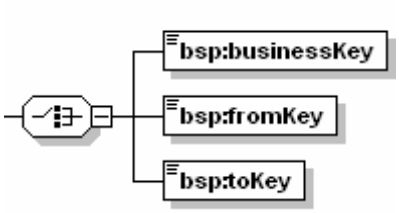
Struktur - Sequenz



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.

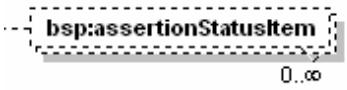
Kardinalität – Null bis einmal

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

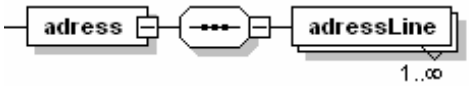
Eine durchgezogene Linie und keine weiteren Kardinalitätsmerkmale bedeutet, dass das Element genau einmal enthalten sein MUSS.

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.