Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

- Certificate Policy -

Gemeinsame Zertifizierungs-Richtlinie für Teilnehmer der gematik-TSL zur Herausgabe von X.509-ENC/AUT/OSIG-Zertifikaten

Version:	1.2.0
Stand:	29.11.2007
Status:	freigegeben

Dokumentinformationen

Änderungen zur Vorversion

Im gesamten Dokument wurden Aussagen v.a. hinsichtlich des Schlüsselmanagements auf Einheitlichkeit mit dem Sicherheitskonzept, Anhang Kryptographiekonzept (Anhang F) geprüft und ggf. ergänzt.

Hinsichtlich der kryptographischen Algorithmen wurde anstelle konkreter Festlegungen der Verweis auf das Dokument „Verwendung kryptographischer Algorithmen in der Telematikinfrastruktur“, Abschnitt 5.1.1 [gemSpec_Krypt#5.1.1.] eingefügt.

Weiterhin wurden die Bedingungen für eine Zertifikatssperrung präzisiert.

Bzgl. der Rollenverteilung wurden Inkonsistenzen korrigiert.

Inhaltliche Änderungen gegenüber der letzten freigegebenen Version sind gelb markiert. Sofern ganze Kapitel eingefügt wurden, wurde zur besseren Lesbarkeit lediglich die Überschrift durch gelbe Markierung hervorgehoben.

Die noch in der Diskussion befindliche Frage der OID-Festlegung für diese Policy wurde als offener Punkt aufgenommen.

Referenzierung

Die Referenzierung in weiteren Dokumenten der gematik erfolgt unter:

[gemTSL_SP_CP]	gematik (29.11.2007): Einführung der Gesundheitskarte - Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL zur Herausgabe von X.509-ENC/AUTH/OSIG-Zertifikaten Version 1.2.0

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.1.0	01.04.06		Neufassung	gematik AG3
0.3.1	27.04.06		Grundlegende Überarbeitung aller Kapitel	gematik AG3
0.4.0	03.05.06		Abstimmung der Begrifflichkeiten	gematik AG3
0.5.0	09.05.06		Ergänzung um Institutionszertifikate	gematik AG3
0.6.0	11.05.06	2	Festlegung der Verantwortlichkeiten	gematik AG3
0.7.0	13.05.06		Ergänzung Rollenkonzept	gematik AG3
0.8.0	17.05.06		Festlegung der Begrifflichkeiten	gematik AG3
0.8.9	16.07.06		Editorische Überarbeitung	gematik AG3

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.8.94	25.09.06		Differenzierung der Rollen	gematik AG3
0.8.95	26.09.06		Einarbeitung Reviewergebnisse	gematik AG3
0.8.96	29.09.06	5.2.1	Ergänzung Registrierungsbedingungen	gematik AG3
0.8.97	13.10.06	5.2.1	Präzisierung bezüglich geh. Schlüssel	gematik AG3
1.0.0	16.10.06		Freigabe	gematik
1.0.1	28.02.07		Einarbeitung Kommentare, Zulassung der Suspendierung von Zertifikaten	gematik AG3
1.1.0	04.05.07		freigegeben	gematik
1.1.1	02.11.07		Vereinheitlichung mit Sicherheitskonzept, Anhang Kryptographiekonzept (Anhang F) Korrekturen und Präzisierungen bzgl. Rollen-verteilung und Zertifikatssperrung Editorische Überarbeitung	gematik AG8
1.1.2	26.11.07		Einarbeitung der internen Kommentierung	SPE/ZD
1.2.0	29.11.07		freigegeben	gematik

Inhaltsverzeichnis

1 Zusammenfassung

Für eine Public Key Infrastruktur (PKI) ist die Einschätzung der Vertrauenswürdigkeit der ausgestellten Zertifikate durch die Empfänger von Nachrichten oder Transaktionen von entscheidender Bedeutung. Dieses Dokument beschreibt die dazu notwendigen Sicherheitsrichtlinien (Policy). Die Dokumentenstruktur lehnt sich an die Empfehlungen des [RFC3647] an und vereinigt somit inhaltlich sowohl die Elemente einer Certification Policy als auch eines mehr technisch-organisatorisch orientierten Certificate Practice Statements (CPS).

Aussteller von Zertifikaten (Trust-Service Provider, TSP), die innerhalb der Telematikinfrastruktur eingesetzt werden sollen, **MÜSSEN** die Anforderungen dieser Policy erfüllen und dieses durch die Erstellung eines spezifischen CPS nachweisen.

Der Nachweis erfolgt durch die Vorlage des „Certification Practice Statements“ gegenüber der gematik. Nur nach erfolgter Genehmigung nimmt der gematik-TSL-Service Provider den TSP in die zentrale Trust-Service Status List auf.

Um den jeweiligen TSP größtmögliche Flexibilität einzuräumen, stellen die teilnehmenden TSPs die Einhaltung dieser Anforderungen über vertragliche Vereinbarungen mit der gematik sicher. Darüber hinausreichende Regelungen können die TSPs nach eigenem Ermessen festlegen.

In der jetzigen Ausbaustufe spezifiziert diese Policy in Verbindung mit den entsprechenden Zertifikatsprofilen Leitlinien für die Nutzung der Anwendungsbereiche Verschlüsselung, Authentisierung und elektronischer Signaturen mit „nicht qualifizierten Zertifikaten“ für natürliche Personen und Institutionen.

2 Einführung

2.1 Zielsetzung und Einordnung des Dokumentes

Dieses Dokument definiert die Anforderungen an die Aussteller personen- bzw. organisationsbezogener Zertifikate (Trust-Service Provider, TSP). Hierbei werden die Sicherheitsanforderungen hinsichtlich der Erzeugung, Verwaltung und Sperrung von Zertifikaten definiert.

Das Dokument hat bewusst die umfangreiche Gliederung auf Basis des RFC 3647 beibehalten, um die strukturierte Vergleichbarkeit von Policies, auch im internationalen Kontext, zu ermöglichen. Nur hierdurch wird der komplexe Prozess eines „Policy-Matching“ zur Vergleichbarkeit von Sicherheitsniveaus in verschiedenen technischen und organisatorischen Systemen möglich.

2.2 Zielgruppe

Das Dokument wendet sich an alle Personen und Organisationen, die am Design und Betrieb der IT-Sicherheitsarchitektur der Gesundheitstelematik beteiligt sind, sowie die betroffenen Organisationen gemäß Kapitel 2.3.

2.3 Geltungsbereich

Die getroffenen Festlegungen sind verbindlich für Kartenherausgeber, Betreiber von Kartenmanagementsystemen und Trust-Service Provider, die innerhalb der Gesundheitstelematik tätig sind und die Authentifizierungs-, Verschlüsselungs- und Signaturzertifikate für eGK und SMC-B herausgeben oder die damit verbundenen Verzeichnisdienste betreiben.

2.4 Arbeitsgrundlagen

Die Dokumentenstruktur lehnt sich dabei an die Empfehlungen des RFC 3647 an und berücksichtigt die Empfehlungen der Policy der European Bridge CA [EBCA-CP] und der PKI-1-Verwaltung des Bundes [PKI-1-CP].

2.5 Abgrenzung des Dokumentes

Festlegungen zur Bereitstellung von Verzeichnisdiensten im Internet sind nicht Gegenstand dieser Policy, die für offene Netze geltenden Vorgaben von Datenschutz-, Telekommunikationsdienste- und Signaturgesetz sind bereits sehr umfassend.

Für qualifizierte Signaturzertifikate gelten zusätzlich die spezifischen Vorgaben des Signaturgesetzes für angezeigte und akkreditierte Zertifizierungsdiensteanbieter.

Für CV-Zertifikate gelten aufgrund der beschränkten technischen Funktionalitäten hinsichtlich Gültigkeit und Sperrung gesonderte Vorgaben [gemPKI_CVCGK].

Die Festlegungen zum „Aktivieren qualifizierter Zertifikate“ und die Vorgaben für die Inhalte der X.509-Zertifikate werden in gesonderten Dokumenten getroffen, welche von der gematik (siehe unter www.gematik.de) veröffentlicht werden. Der Zusammenhang zwischen den verschiedenen PKI-relevanten Dokumenten wird im PKI-Grobkonzept [gemFK_X.509] dargestellt.

Die Details zum Ablauf der Registrierungsbedingungen und –Prozesse für die Zertifikate der Versicherten sind durch die Kostenträger zu definieren und im jeweiligen „Certification Practise Statement“ darzulegen.

Für die Zertifikate der HPC gelten zusätzlich die Anforderungen aus [BÄK_POL] in der jeweils gültigen Fassung.

Die genauen Anforderungen an die Durchführung von Audits zum Nachweis der Umsetzung dieser Policy werden noch abschließend durch die gematik definiert.

Maßgeblich für den Einsatz aller PKI-Komponenten sind die im Sicherheitskonzept der gematik [gemSiKo] festgelegten Mindestanforderungen.

2.6 Methodik

2.6.1 Verwendung von Schlüsselworten

Für die genauere Unterscheidung zwischen normativen und informativen Inhalten werden die dem [RFC2119] entsprechenden 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 Empfehlung. Abweichungen zu diesen Festlegungen sind in begründeten Fällen möglich.
- **SOLL NICHT** kennzeichnet die Empfehlung, eine Eigenschaft auszuschließen. Abweichungen sind in begründeten Fällen möglich.
- **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 vorläufig mit den folgenden Konventionen gekennzeichnet

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

Durch die AG8 aufgrund bereits erfolgter Abstimmungen noch zu erweiternde Punkte sind violett markiert.

Formale noch offene Inhalte sind blau markiert.

3 Einleitung fachlicher Teil

3.1 Überblick

Alle an der Telematikinfrastruktur (TI) beteiligten Trustcenter, genauer ausgedrückt „Trust-Service Provider“ (TSP) **MÜSSEN** aus Gründen des Datenschutzes ein Mindestsicherheitsniveau einhalten. Dieses wird anhand eines vom TSP für diesen Zweck erstellten „Certification Practice Statements“ durch die gematik oder von ihr Beauftragte geprüft. Auf dieser Basis erfolgt die Aufnahme des Root- bzw. des CA-Zertifikats des TSP in eine signierte XML-Liste, die „Trust-Service Status List“ (TSL).

Der von der gematik beauftragte TSL-Service Provider (gematik TSL-SP) signiert die TSL (Format nach [ETSI-TSL]) in einer Hochsicherheitsumgebung und stellt sie allen Konnektoren und Zertifikate prüfenden Instanzen zur Verfügung, ferner wird die Liste auf einem Server des gematik-TSL-SP veröffentlicht. Vor der Prüfung eines Zertifikats in einem Verzeichnisdienst wird von der „lokalen“ Anwendung anhand der TSL (Zertifikat des TSP ist als „digitalIdentity“ eingetragen) geprüft, ob die zu benutzende Verzeichnisdienstadresse (URL, URI) zugelassen ist.

Aufgrund der besonderen Rolle der gematik-TSL als Abbildung eines organisationsübergreifenden Vertrauensraums werden hier technische und organisatorische Sicherheitsanforderungen formuliert.

3.1.1 Ziel dieser Policy

Der Prozess der Aufnahme in die gematik-TSL orientiert sich grundsätzlich an den Wertmaßstäben

- technische Konformität und
- angemessene und vergleichbare Sicherheitslevel.

Das vorliegende Dokument adressiert vorrangig den zweiten Wertmaßstab, da die entsprechenden Vorgaben zur Konformität durch andere Dokumente vorgegeben werden. Ein Herausgeber von Zertifikaten (TSP), der in die „Trust-Service Status List“ der gematik aufgenommen werden will, **MUSS** zukünftig ein eigenes CPS erstellen, das mit dieser Gliederung nach RFC 3647 konform ist. Dieses dient der Erfüllung der folgenden Ziele:

- Der formale Aufbau nach dem international anerkannten Rahmenwerk nach RFC 3647 verbessert die Transparenz und Vergleichbarkeit gegenüber der bisher üblichen Praxis. Durch das Dokument wird eine sichtbare Vergleichbarkeit der Policies und damit der Sicherheitsniveaus erreicht.
- In der Erklärung zur Teilnahme eines TSP in gematik-TSL sind für die teilnehmende PKI und deren Architektur Mindestanforderungen formuliert. Diese CP präzisiert einerseits diese Mindestanforderungen, andererseits bietet diese Policy die Möglichkeit, dass die Selbsterklärung auf die Erfüllung dieser Policy verweist. So kann eine Aktualität der geforderten Sicherheitslevels erzielt werden.

- Das vorliegende Dokument bzw. seine teilnehmerspezifische Ausprägung bietet die Möglichkeit, als Referenzdokument für vertragliche Regelungen zwischen den Nachfragern (z. B. Kostenträgern) und Anbietern (z. B. Kartenpersonalisierern) von Trust-Services zu dienen (geeignet als Basis für Ausschreibungen und Verträge).

3.1.2 Rahmen dieser Policy

Diese Certificate Policy definiert die Vorgaben, die TSPs erfüllen **MÜSSEN**, wenn das zugehörende TSP-Ausstellerzertifikat in die signierte Liste des gematik-TSL-Service Providers aufgenommen werden soll. Der Prozess der Registrierung eines TSP bei der gematik ist im Registrierungsdokument [gemX.509_TSP] ausführlich beschrieben. Im Rahmen dieser CP werden an Personen und Organisationen ausgestellte Zertifikate (End Entity / Endanwender) bzw. die ausstellenden TSP-Zertifikate betrachtet. Die Schlüsselverwendung/Zertifikatsnutzung (*keyUsage*) umfasst:

- Elektronische Signatur (*nonRepudiation* im Sinne von „*contentCommitment*“),
- Authentifizierung (*digitalSignature*) und
- Verschlüsselung (*dataEncipherment*, *keyEncipherment*).

Das vorliegende Dokument ist nach RFC 3647 aufgebaut und ist an dessen Gliederung angelehnt. Die in der Kapitelüberschrift gekennzeichneten Punkte sind verbindliche Vorgaben und Voraussetzungen zur Teilnahme an der gematik-TSL.

3.1.3 Der gematik-TSL-Service Provider und seine Teilnahmebedingungen

Die gematik stellt über den TSL-Service Provider (TSL-SP) eine kostengünstige und verlässliche Dienstleistung zur Prüfung von Zertifikaten der teilnehmenden TSPs in der TI bereit. Als Brücke zwischen den Beteiligten prüft dieser die Root- und TSP-Zertifikate der teilnehmenden Organisationen (TSPs) und bringt sie in die gemeinsam genutzte „Trust-Service Status List“ (TSL) ein. Der Teilnehmer erkennt den gematik-TSL-Service Provider als vertrauenswürdige Instanz an.

Weitere Voraussetzung für die Teilnahme ist die Durchführung eines gematik-TSL-Service Provider-Konformitätstests. Um die gewünschte Kompatibilität der jeweiligen Public Key Infrastruktur (PKI) zu erreichen, ist der TSP gehalten, die auf Grund der Ergebnisse des Konformitätstests erforderlichen technischen und organisatorischen Anpassungen vorzunehmen. Weiterhin **MUSS** die Bereitschaft zur Migration der Komponenten bestehen, falls dies für den gematik-TSL-Service Provider aus Gründen der Interoperabilität, der technischen Fortentwicklung oder anderer Anforderungen erforderlich wird.

Die Anforderungen, die in der eGK-Spezifikation [gemSpec_eGK] und in den Vorgaben zu den Zertifikaten der Versicherten [gemX.509_eGK] dargestellt sind, können durch die gematik aktualisiert und überarbeitet werden. Analog dazu informieren die Leistungserbringerorganisationen die gematik rechtzeitig über Änderungen an der HPC-Spezifikation. Die gematik informiert ihrerseits die TSPs über derartige Veränderungen. Eine angemessene Frist für die Migration wird berücksichtigt.

Die Mindestanforderungen zur Aufnahme in die gematik-TSL **MÜSSEN** durch den TSP in einem eigenen Sicherheitskonzept berücksichtigt sein. Begründete Abweichungen sind nach ausdrücklicher Bestätigung durch die gematik möglich.

Diese Policy trifft Vorgaben sowohl für TSPs, die als Root-Instanz (Root-TSP) fungieren, als auch für TSPs, die innerhalb einer Zertifizierungshierarchie nachgeordnet sind. Des Weiteren werden Aussagen bzgl. der Erstellung von Endnutzer-Zertifikaten getroffen. Der Geltungsbereich der jeweiligen Vorgaben ist aus der Kapitelüberschrift ersichtlich.

Da die gematik die Verantwortung für den TSL-Service-Provider und den damit geschaffenen Vertrauensraum in Form der TSL trägt, ist es nötig, dass sich jeder TSP (Root-Instanz als auch weitere innerhalb der Zertifikatshierarchie nachgeordnete) bei der gematik registrieren lässt. Die gematik bearbeitet die Anträge und aktualisiert daraufhin die TSL. Dies ist zwingend notwendig, da die Zertifikatskette nicht auf der eGK enthalten ist. Der Validierungsdienst überprüft, ob die ausstellende Instanz in der TSL vorhanden ist.

3.1.4 Überblick zur Public Key Infrastruktur

Diese CP dient zur Schaffung TSP-übergreifender (und damit auch organisationsübergreifender) Vertrauensbeziehungen. Hierbei sollen sowohl existierende als auch neu entstehende Public Key Infrastrukturen verwendet werden, um die Sicherheitsanforderungen an die TI abzubilden.

Da der Aufwand für bilaterale Cross-Zertifizierungen ab einer bestimmten Größenordnung unverhältnismäßig groß ist, gewinnt die Verwendung einer gemeinsamen Zertifizierungsstelle, mit der die lokalen Public Key Infrastrukturen (PKI) Zertifikate austauschen, mit steigender Anzahl von Public Key Infrastrukturen an Bedeutung.

Dieses Vorgehen hat den Vorteil, dass jede Public Key Infrastruktur nur eine einzige Zertifizierung durchführen **MUSS** und dennoch in den Genuss umfangreicher Cross-Zertifizierungen kommt. Da die derart gemeinsam genutzte Zertifizierungsstelle einen Brückenschlag zwischen den einzelnen PKI darstellt, wird sie im Allgemeinen als „Bridge-CA“ bezeichnet.

Ausgangspunkt für den Betrieb einer „Bridge-CA“, hier als gematik-TSL-Service Provider bezeichnet, ist diese Certificate Policy, sowie eine Dokumentation der zur Teilnahme erforderlichen Mindestanforderungen. Seitens der gematik ist ein Gremium eingerichtet worden, welches die Erfüllung der Mindestanforderungen überprüft und die Aufnahme neuer Teilnehmer dokumentiert.

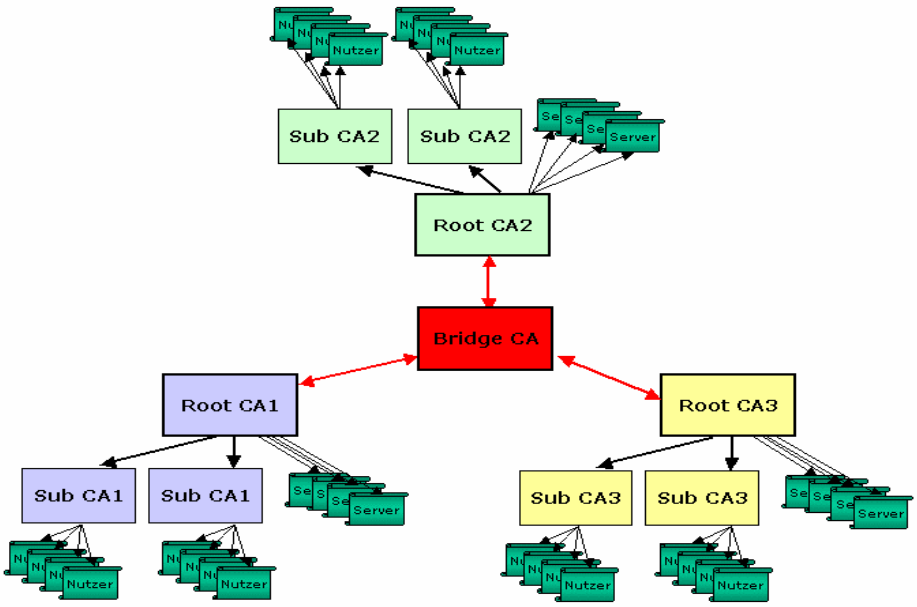

Abbildung 1 - Verwendung einer Bridge-CA

Wie die einzelnen TSPs aus den unterschiedlichen Domänen der Kostenträger und Leistungserbringer in die zentrale TSL aufgenommen werden und die TSL dabei die Funktion der „Bridge-CA“ einnimmt, wird in Abbildung 2 verdeutlicht:

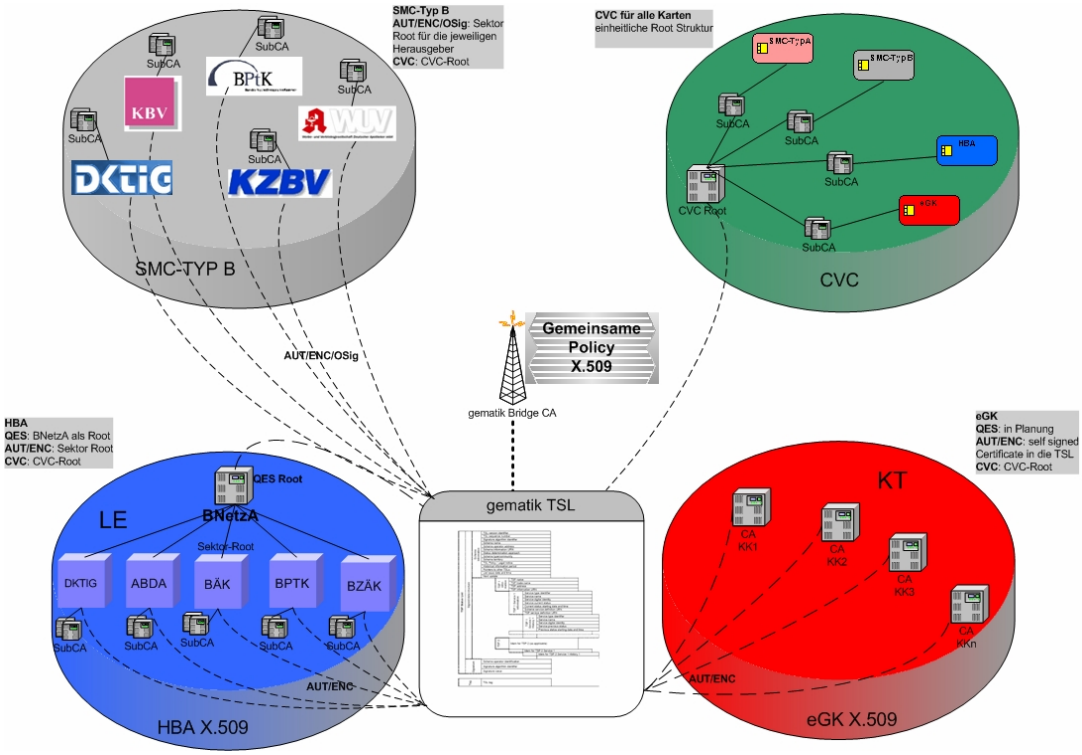

Abbildung 2 - Teilnehmer der gematik Bridge (TSL)

3.2 Name und Kennzeichnung des Dokuments

Diese Certificate Policy trägt den Titel:

> „Gemeinsame Zertifizierungsrichtlinie für Teilnehmer der gematik-TSL zur Herausgabe von X.509-ENC/AUT/OSIG-Zertifikaten“.

Der Object Identifier (OID) für dieses Dokument ist:

> 1.3.36.5.2.1

Bzgl. der OID-Festlegung wird derzeit eine einheitliche Struktur unter dem Dach des DIMDI aufgebaut. Somit wird die derzeitige OID noch geändert werden.

3.3 Teilnehmer

Teilnehmer sind Organisationen, die eine eigene Public Key Infrastruktur betreiben oder einen Trust-Service Provider mit der Ausstellung von Zertifikaten für die Nutzung innerhalb der TI beauftragen.

3.3.1 gematik-TSL-Service Provider

Die gematik beauftragt einen Service Provider zur Erstellung, Verwaltung und Veröffentlichung der TSL.

3.3.2 Trust-Service Provider (TSP)

TSPs sind Stellen, die innerhalb oder im Auftrag der Teilnehmerorganisationen Zertifikate für natürliche oder juristische Personen ausstellen und / oder Verzeichnisdienste betreiben, die mindestens die Vorgaben dieser Policy erfüllen. Die Zertifikate der TSPs, welche in der gematik-TSL eingetragen sind, werden als TSP-Zertifikate bezeichnet.

3.3.3 Registrierungsstellen

Registrierungsstellen (RAs) sind Stellen, die innerhalb oder im Auftrag der Teilnehmerorganisationen Registrierungen von Zertifikatsnehmern durchführen, die mindestens die Vorgaben dieser Policy erfüllen.

3.3.4 Zertifikatsnehmer

Zertifikatsnehmer sind natürliche oder juristische Personen, für die ein TSP innerhalb der gematik-TSL Zertifikate ausstellt. Zertifikatsnehmer **MÜSSEN** innerhalb der gematik-TSL eindeutig einem TSP und der zugehörenden Organisation zugeordnet sein. Zertifikate der Zertifikatsnehmer werden als Endnutzerzertifikate bezeichnet. Bei organisationsbezogenen wie personenbezogenen Zertifikaten **MUSS** stets der für die Nutzung der Zertifikate bzw. der dazugehörigen privaten Schlüssel Verantwortliche bekannt sein.

3.3.5 Zertifikatsnutzer

Zertifikatsnutzer sind alle Personen und Organisationen, die die Zertifikate der in der gematik-TSL enthaltenen TSPs nutzen können und Zugang zu den Diensten des gematik-TSL-Service Providers haben.

3.3.6 Antragsteller

Der Antragsteller ist die natürliche Person, die den Antrag auf ein Zertifikat nach dieser Policy stellt.

Hinweis: Bei personenbezogenen Zertifikaten (der eGK) ist der Antragsteller in der Regel der spätere Zertifikatsnehmer. Bei organisationsbezogenen Zertifikaten können Antragssteller und Zertifikatsnehmer unterschiedlich sein, sofern immer revisionssicher nachvollziehbar ist, wer der haftende Zertifikatsnehmer ist, und dass der Antragsteller berechtigt ist, ein Zertifikat für den späteren Zertifikatsnehmer zu beantragen.

3.3.7 Andere Teilnehmer

Teilnehmer, deren TSP keine Verpflichtungen gegenüber der gematik-TSL eingegangen sind, sind nicht Bestandteil dieser Policy.

3.4 Verwendung von Zertifikaten

3.4.1 Erlaubte Verwendungen von Zertifikaten

Zertifikate bzw. die zugehörigen Schlüsselpaare können von Zertifikatsnehmern für sichere Anwendungen zur Authentisierung, elektronischen Signatur sowie zur Daten- bzw. Nachrichtenentschlüsselung genutzt werden. Zertifikatsnutzer können Zertifikate zur Validierung von Authentisierungen und elektronischen Signaturen sowie zur Daten- und Nachrichtenverschlüsselung nutzen.

4 Allgemeine Maßnahmen

Ist der TSP ein Zertifizierungsdiensteanbieter mit Anbieterakkreditierung nach SigG, genügt statt Vorlage des Sicherheitskonzepts die Vorlage der entsprechenden Akkreditierung sowie eine Erklärung, die Maßnahmen des Sicherheitskonzepts anzuwenden.

Dieser Grundsatz gilt für dieses und alle weiteren Kapitel dieses Dokuments.

4.1 Verantwortlichkeit des TSP für Verzeichnisse und Veröffentlichungen

4.1.1 Verzeichnisse (TSP + Root-TSP)

Der TSP **MUSS** den Zertifikatsnutzern einen OCSP-Responder zur Verfügung stellen.

Ein Verzeichnisdienst für die Suche nach Zertifikaten (LDAP) und der Zugriff auf Sperrdaten in Form einer Sperrliste (CRL) **KANN** ebenfalls zur Verfügung gestellt werden.

Der TSP gewährleistet eine ordnungsgemäße Erbringung der Verzeichnisdienstleistungen im Rahmen seines Sicherheitskonzepts und orientiert sich am aktuellen Stand der Technik.

4.1.2 Veröffentlichung von Informationen zur Zertifikatserstellung (TSP + Root-TSP)

Der TSP erklärt sein Einverständnis, dass PKI-betreffende Teile seines Sicherheitskonzepts dem Betreiber des gematik-TSL-SP zugänglich gemacht werden. Der TSP stimmt einer Veröffentlichung seiner Teilnahme an der gematik-TSL und der Weitergabe seines Zertifikats im Rahmen der Vorgaben der gematik zu.

4.1.3 Zeitpunkt und Häufigkeit von Veröffentlichungen (TSP + Root-TSP)

Die Veröffentlichung von Verzeichnisinformationen sowie kritischer Informationen wie eine Betriebseinstellung oder Deregistrierung **MUSS unverzüglich** gegenüber dem gematik-TSL-Service Provider und seinen Teilnehmern erfolgen. Bei CRLs **MUSS** dieses zumindest tagesaktuell erfolgen.

Der TSP **MUSS** rechtzeitig Änderungen an der zugrunde liegenden PKI und deren Architektur gegenüber der gematik bekanntgeben, sofern die Sicherheit verringert oder das Außenverhalten verändert wird.

4.1.4 Zugriffskontrollen auf Verzeichnisse (TSP + Root-TSP)

Der TSP gewährleistet eine ordnungsgemäße Zugriffskontrolle auf die entsprechenden Verzeichnisse.

5 Identifizierung und Authentifizierung

5.1 Namensregeln (TSP + Root-TSP)

5.1.1 Arten von Namen

Für die Namensvergabe für TSP-Zertifikate ist der Standard [X.509] maßgebend. Das Attribut *distinguishedName* ist für die Namensvergabe obligatorisch.

Ist eine E-Mail-Adresse im Zertifikat enthalten, sollte diese unter der X.509-Extension *subjectAltNames* im Format nach RFC 822 hinterlegt sein.

5.1.2 Namensform

Die Namensform der jeweiligen Zertifikate (siehe Kapitel 9) ist bindend für die Struktur der entsprechenden Verzeichnisdienste. Grundsätzlich sind personen- und institutionsbezogene Zertifikatsstrukturen in der gematik-TSL möglich.

5.1.3 Aussagekraft von Namen

Die Details für die Zertifikate der eGK sind in dem Dokument „Festlegungen zu den X.509 Zertifikaten der Versicherten“ [gemX.509_eGK] dargestellt. Die Details der Zertifikate der SMC sind in dem Dokument „Festlegungen zu den X.509 Zertifikaten der SMC-Typ-B“ [gemX.509_SMCB] dargestellt. Details der Zertifikate der Heilberufler sind in dem Dokument „German Health Professional Card and Security Module Card - Part2: HPC Applications and Functions“ [HPC-P2] dargestellt.

5.1.4 Notwendigkeit für aussagefähige und eindeutige Namen

Bei der Vergabe von Namen (Nutzer- oder PKI-Zertifikate) **muss** sichergestellt sein, dass der gewählte *distinguishedName* des Zertifikatsnehmers innerhalb des ausstellenden TSP eindeutig ist. Durch die Verwendung der Namensform in Kapitel 5.1.2 wird die Eindeutigkeit sichergestellt. Der ausstellende TSP **MUSS** sicherstellen, dass die Daten in dieser Form aufbereitet werden. Die Integrität und Vollständigkeit der Daten liegt in der Hoheit der jeweiligen Registrierungsstellen (bei Versicherten ist dies der Kostenträger).

Personen- bzw. organisationsbezogene Zertifikate **MÜSSEN** eindeutig als solche kenntlich sein (Einhaltung der entsprechenden Zertifikatsprofile).

Maschinen-, Rollen- oder pseudonymisierte (nicht personenbezo gene) Zertifikate **MÜSSEN**, um Verwechslungsfreiheit zu garantieren, ebenfalls als solche kenntlich sein.

Zur Unterscheidung von Zertifikaten wird das jeweilige Kennzeichen in die Extension `additionalInformation` gespeichert z. B. C.CH.AUT (C=Certificate, CH=Cardholder, AUT=Authentication)

5.1.5 Anonymität oder Pseudonyme von Zertifikatsnehmern

Pseudonyme-Zertifikate **MÜSSEN** pro TSPs eindeutig sein. Vorgaben sowie Beispiele zur Umsetzung bzgl. der Bildung der pseudonymisierten Versichertenidentität sind in [gemSi-Ko#7.9.1] zu finden

5.1.6 Regeln für die Interpretation verschiedener Namensformen

Maschinen-, Rollen- oder pseudonymisierte (nicht personenbezogene) Zertifikate **MÜSSEN**, um Verwechslungsfreiheit zu garantieren, als solche kenntlich sein. Zur Unterscheidung von Zertifikaten wird das jeweilige Kennzeichen in die Extension additionalInformation gespeichert. Details dazu sind in den jeweiligen Zertifikatsspezifikationen zur SMC-B und eGK zu finden. [gemX.509_eGK] [gemX.509_SMCB]

5.2 Erstmalige Überprüfung der Identität (TSP + Endanwender)

5.2.1 Methoden zur Überprüfung bzgl. Besitz des privaten Schlüssels

Die Registrierungsstelle **MUSS** Prozesse und Vorgaben entsprechend ihres Sicherheitskonzepts definieren, die eine ordnungsgemäße Prüfung auf den Besitz des privaten Schlüssels bei dem Zertifikatsnehmer gewährleisten, bevor das jeweilige Zertifikat im Verzeichnisdienst freigeschaltet und veröffentlicht wird. Bei Authentisierungs- und Verschlüsselungszertifikaten der Endanwender (Versicherte) können die bestehenden Vorgaben bezüglich der Übermittlung der Karten beibehalten werden.

Für die Registrierung der Endanwender **KANN** der TSP die bestehenden Datensätze der Endanwender (Versicherte) beim Kostenträger verwenden, so wie sie im Rahmen der Vorgaben des Sozialgesetzbuches erhoben wurden. Der Kostenträger verantwortet die Korrektheit dieser Daten. Eine erneute Identifizierung der Versicherten nur für die Erstellung von AUT- und ENC-Zertifikaten ist aufgrund der datenschutzrechtlichen Vorgaben nicht geboten.

5.2.2 Authentifizierung von Organisationszugehörigkeiten

Die Vorgaben hierfür, insbesondere zu den X.509-Zertifikaten der SMC-Typ-B, erfolgen in einem gesonderten Dokument [gemX.509_SMCB].

5.2.3 Anforderungen zur Identifizierung und Authentifizierung des Zertifikats-Antragstellers

Die Registrierungsstelle gewährleistet eine zuverlässige Identifizierung und vollständige Prüfung der Antragsdaten im Rahmen der Integritäts-, Authentizitäts- und Vertraulichkeitsanforderungen ihres Sicherheitskonzepts, die sich mindestens an dem aktuellen Stand des IT-Grundschutz-Katalogs [BSI_GK] orientieren **MUSS**.

5.2.4 Ungeprüfte Angaben zum Zertifikatsnehmer

Die Registrierungsstelle hat zu gewährleisten, dass ungeprüfte Angaben nicht die Verbindung der Person zu Schlüsselpaar, Schlüsselaktivierungsdaten und Name betreffen.

5.2.5 Prüfung der Berechtigung zur Antragstellung

Die Berechtigung zur Antragsstellung ist durch den TSP zu prüfen. Näheres **MUSS** der TSP in seinem CPS regeln.

5.2.6 Kriterien für den Einsatz interoperierender Systeme

Bei der Interoperation von Diensten, die zur erstmaligen Prüfung der Identität herangezogen werden, **MÜSSEN** die Integritäts-, Authentizitäts- und Vertraulichkeits-Anforderungen in Abschnitt 6.3 erfüllt bleiben. Dies gilt insbesondere, wenn die Registrierung durch einen externen Dienstleister erfolgt, während andere PKI-Betriebsprozesse ganz oder teilweise im Hause des TSP stattfinden (so kann z. B. die inkonsistente Umwandlung von deutschen Umlauten verhindert werden).

5.3 Identifizierung und Authentifizierung von Anträgen auf Schlüsselerneuerung (Rekeying) (TSP + Endanwender)

5.3.1 Identifizierung und Authentifizierung von routinemäßigen Anträgen zur Schlüsselerneuerung

Die Berechtigung zur Antragsstellung auf Schlüsselerneuerung ist durch den TSP zu prüfen. Näheres **MUSS** der TSP in seinem CPS regeln.

5.3.2 Identifizierung und Authentifizierung zur Schlüsselerneuerung nach Sperrungen

Die Registrierungsstelle gewährleistet eine zuverlässige Identifizierung und vollständige Prüfung der bisherigen Antragsdaten im Rahmen ihres Sicherheitskonzepts, das sich mindestens an dem aktuellen Stand des [BSI_GK] orientiert.

5.4 Identifizierung und Autorisierung von Sperranträgen (TSP + Endanwender)

Die Registrierungsstelle gewährleistet eine zuverlässige Identifizierung und Autorisierung des Sperrantragstellers, die sich an den Vorgaben ihres Sicherheitskonzepts orientiert.

6 Betriebliche Maßnahmen

6.1 Zertifikatsantrag durch TSP (TSP + Root-TSP)

Der Zertifikatsantrag **MUSS** die zweifelsfreie Identifizierung des Antragstellers unterstützen und **MUSS** das Ergebnis des Antragsprozesses dokumentieren. Er sollte dazu geeignete Felder enthalten.

TSP beantragen schriftlich die Aufnahme ihres (Root-) Zertifikats bei der gematik.

Dem Antrag sind beizufügen:

(1) die aktuell geltenden Sicherheitsleitlinien des TSP,

(2) die Selbsterklärung des TSP,

(3) ein aktueller Handelsregisterauszug oder vergleichbare Dokumente,

(4) die Erklärung, dass gegenwärtig kein Insolvenzverfahren gegen den Antragsteller eröffnet worden ist oder dessen Eröffnung beantragt worden ist.

Auf Verlangen der gematik sind die für sie relevanten Teile der technischen Dokumentationen und Betriebskonzepte vorzulegen.

Es ist vom TSP ein Sicherheitskonzept zu erstellen, welches die konkrete Umsetzung des Schutzbedarfs der verarbeiteten Information in Sicherheitsmaßnahmen regelt. Die für den operativen Betrieb notwendigen Sicherheitsmaßnahmen sollten zusätzlich in einem Betriebskonzept dargelegt werden.

Ist der TSP ein Zertifizierungsdiensteanbieter mit Anbieterakkreditierung nach SigG, genügt statt Vorlage des Sicherheitskonzepts die Vorlage der entsprechenden Akkreditierung sowie die Erklärung, die Maßnahmen des Sicherheitskonzepts anzuwenden.

6.1.1 Wer kann einen Zertifikatsantrag stellen?

Der TSP legt fest, wer in seinem Namen einen Zertifikatsantrag stellen darf und benennt diese Personen gegenüber seinem Root-TSP.

Der Root-TSP legt fest, wer in seinem Namen einen Zertifikatsantrag stellen darf und benennt diese Personen gegenüber der gematik (die dies dem TSP-SP mitteilt).

6.1.2 Registrierungsprozess und Zuständigkeiten

Die Registrierung **MUSS** ein dokumentierter Prozess sein, der die Anforderungen der Identifizierung nach Kapitel 5.2 erfüllt.

Der Zertifikatsantrag **MUSS** Angaben enthalten, die dem Anspruch auf zweifelsfreie Identifizierung des Zertifikatsnehmers und des Antragstellers entsprechen.

6.2 Verarbeitung des Zertifikatsantrags (TSP + Root-TSP)

6.2.1 Durchführung der Identifizierung und Authentifizierung

Vor der Registrierung ist der Zertifikatsnehmer und der Antragsteller zuverlässig nach einem dokumentierten Prozess zu identifizieren.

6.2.2 Annahme oder Ablehnung von Zertifikatsanträgen

Das Vorgehen zur Annahme oder Ablehnung eines Zertifikatsantrages ist zu dokumentieren. Eine Annahme darf nur für identifizierte Antragsteller mit berechtigtem Antrag erfolgen.

6.2.3 Fristen für die Bearbeitung von Zertifikatsanträgen

Keine Vorgaben

6.3 Zertifikatsausgabe

Ausgabe- und Ausstellungsprozess für ein TSP-Zertifikat sind unmittelbar miteinander verbunden. Für Zertifikate für Zertifikatsnehmer sind dieses getrennte Prozesse.

6.3.1 Ausgabe eines Zertifikats für einen nachgeordneten TSP (Root-TSP)

Eine Wurzelzertifizierungsstelle erzeugt im Rahmen ihrer Verpflichtungen nach Vorliegen eines vollständigen und geprüften Antrags und nach erfolgter Identifizierung Zertifikate für ihre nachgeordneten TSP. Dazu **MUSS** ein signierter Zertifikats-Antrag (Certificate Request) des beantragenden TSP der Wurzelzertifizierungsstelle persönlich überbracht werden.

Die Beantragung und die Zustimmung können elektronisch erfolgen, wenn eine sichere Methode zur Authentifizierung der vertretenden Person zur Verfügung steht, hierfür kommt eine qualifizierte elektronische Signatur der vertretenden Person in Betracht.

Eine Wurzelzertifizierungsstelle prüft den signierten Zertifikatsantrag mit dem vorgelegten öffentlichen Signatur-Schlüssel. Hiermit wird sichergestellt, dass der vorgelegte Signatur-Schlüssel mit den Signaturerstellungsdaten korrespondiert.

Die Wurzelzertifizierungsstelle behält sich vor, bei dem Wechsel des Zertifikats der Wurzelzertifizierungsstelle neue Zertifikate für die TSP auszustellen.

Durch das Ausstellen eines Root-Zertifikats für einen TSP erhält dieser die Möglichkeit, eigene Zertifikate mit seinem Schlüsselpaar nicht nur zu erzeugen, sondern Chipkarten auch mit diesem korrekt zu personalisieren. Erst durch Ausstellung des Zertifikats durch einen Root-TSP wird ein TSP in die Lage versetzt, (zusammen mit einem Kartenhersteller) eGKs bzw. SMCs Typ-B zu erstellen, die in dem Gesamtsystem im Rahmen einer Zertifikatsprüfung als „echt“ erkannt werden. Der Prozess des Ausstellens eines Zertifikats für einen TSP ist daher für die Sicherheit des Gesamtsystems von entscheidender Bedeutung. Es **MUSS** sichergestellt werden,

- dass der dabei zertifizierte öffentliche Schlüssel authentisch ist und
- dass der TSP auch wirklich den zugehörigen privaten Schlüssel besitzt.

Im Folgenden wird der Prozess für das Ausstellen eines Zertifikats für einen TSP musterhaft näher beschrieben. Die einzelnen Schritte sind keine verbindlichen Vorgaben:

(1) Der TSP erzeugt mit seinem HSM (bzw. SSEE) einen signierten PKCS#10-Request für seinen öffentlichen Schlüssel. Dieser wird ausgegeben und auf einem geeigneten Medium (z. B. USB-Stick oder CD) gespeichert.

(2) Über den öffentlichen Schlüssel wird ein Fingerprint berechnet und in einem Begleitschreiben dokumentiert und in Schriftform an die Wurzelinstanz gesendet.

(3) Ein Mitarbeiter des TSP überbringt das Medium der Wurzelinstanz (TSP mit Root-Funktion), bzw. übermittelt es auf gesichertem elektronischem Wege. Dieser Mitarbeiter **MUSS** für die Ausübung dieser Rolle (TSP-Zertifikat Beauftragter) berechtigt sein. Dies wurde der Wurzelinstanz im Rahmen der Registrierung mitgeteilt.

(4) Die Wurzelinstanz überprüft die Personalien des Mitarbeiters des TSP. Dadurch wird sichergestellt, dass der TSP authentisch in dem Prozess vertreten wird.

(5) Die Wurzelinstanz überprüft, ob der TSP aktuell gültig registriert ist.

(6) Von dem Medium wird der signierte PKCS#10-Request des TSP ausgelesen. Die Signatur wird mit dem (in dem Request enthaltenen) öffentlichen Schlüssel überprüft. Dadurch wird sichergestellt, dass der TSP tatsächlich über den zugehörigen privaten Schlüssel verfügt.

(7) Über den (in dem Request enthaltenen) öffentlichen Schlüssel wird ein Fingerprint berechnet und mit dem Fingerprint verglichen, der vorher in Schriftform in dem Begleitschreiben an die Wurzelinstanz gesendet wurde. Dadurch wird sichergestellt, dass der öffentliche Schlüssel authentisch ist.

(8) Das TSP-Zertifikat über den öffentlichen Schlüssel wird durch das HSM der Wurzelinstanz berechnet und ausgegeben. Das TSP-Zertifikat wird auf ein Medium (USB-Stick, CD, E-Mail (signiert & verschlüsselt)) geschrieben und dem Mitarbeiter des TSP übergeben.

(9) Nach Rückkehr wird das TSP-Zertifikat von dem Medium ausgelesen und in die entsprechenden Systeme des TSP eingebracht. Das eingebrachte TSP-Zertifikat wird mit dem veröffentlichten öffentlichen Schlüssel der Wurzelinstanz verifiziert. Dadurch wird die Korrektheit des TSP-Zertifikats sichergestellt.

6.3.2 Erstellen eines TSP Zertifikats (self signed Root)

Für die Ausgabe gelten die gleichen Sicherheitsbedingungen wie für die Ausgabe von TSP Zertifikaten.

6.3.3 Ausgabe eines Zertifikats für Zertifikatsnehmer (an Endnutzer)

Der TSP **MUSS** die Anforderungen an die Ausgabe in seinem CPS beschreiben.

6.3.4 Aktionen des TSPs bei der Ausgabe von Zertifikaten

Eine Ausgabe von Zertifikaten darf nur für angenommene Zertifikatsanträge erfolgen. Die Aktionen bei der Zertifikatsausgabe **MÜSSEN** anhand dokumentierter Prozesse erfolgen. Dabei **MUSS** sicher gestellt sein, dass die eindeutige Verbindung von Zertifikatsnehmer und privatem Schlüssel besteht.

6.3.5 Benachrichtigung des Zertifikatsnehmers über die Ausgabe des Zertifikats durch den TSP

Die Benachrichtigung des Zertifikatsnehmers erfolgt entsprechend dokumentierter Prozesse.

6.4 Zertifikatsannahme (TSP + Root-TSP)

Ein Zertifikat gilt als angenommen, wenn der gesamte Prozess für Antragstellung, Ausstellung des Zertifikats und Zertifikatsausgabe erfolgreich durchlaufen und vom TSP geprüft ist.

6.4.1 Verhalten für eine Zertifikatsannahme

Der TSP dokumentiert die Prozesse für die sichere Ausgabe und die Bedingungen, die zu einer Annahme des Zertifikats führen.

6.4.2 Veröffentlichung des TSP-Zertifikats

Die TSP-Zertifikate **MÜSSEN** der gematik durch den TSP zur Verfügung gestellt werden.

6.4.3 Benachrichtigung anderer Zertifikatsnutzer über die Zertifikatsausgabe

Keine Vorgaben.

6.5 Verwendung des Schlüsselpaars und des Zertifikats (TSP + Root-TSP)

6.5.1 Verwendung des privaten Schlüssels und des Zertifikats durch den Zertifikatsnehmer

Die Verantwortlichkeiten des Zertifikatsnehmers **MÜSSEN** durch den Trust-Service Provider dokumentiert und dem Zertifikatsnehmer mitgeteilt werden.

Der private Schlüssel des Zertifikatsnutzers darf nur für Anwendungen benutzt werden, die in Übereinstimmung mit den im Endnutzerzertifikat angegebenen Nutzungsarten (*keyUsage*) stehen. Folgende Nutzungsarten sind vorgesehen:

- Authentifizierung von Benutzer- oder Anwendungsdaten (Nutzungsart *digitalSignature*)
- Entschlüsselung von Benutzer- oder Anwendungsdaten oder von symmetrischen Schlüsseln, welche in dem so genannten Hybridverfahren für die Verschlüsselung solcher Daten dienen (Nutzungsarten *dataEncipherment* bzw. *keyEncipherment*)
- Kennzeichnung der Verbindlichkeit (Nutzungsart *nonRepudiation*) einer elektronischen Signatur durch den Zertifikatsnehmer.

6.5.2 Verwendung des öffentlichen Schlüssels und des Zertifikats durch Zertifikatsnutzer

Der Zertifikatsnehmer darf seine öffentlichen Schlüssel beliebig veröffentlichen. Eine Veröffentlichung durch Zertifikatsnutzer gegen den Willen des Zertifikatnehmers ist nicht zulässig.

6.6 Zertifikatserneuerung (TSP + Root-TSP)

6.6.1 Bedingungen für eine Zertifikatserneuerung

Eine Zertifikatserneuerung durch den TSP unter Beibehaltung des asymmetrischen Schlüsselpaares darf nur dann erfolgen, wenn die bisher eindeutige Verbindung von Zertifikatsnehmer und privatem Schlüssel erhalten bleibt. Der Schlüssel **MUSS** den aktuellen Vorgaben des [ALGCAT] und [gemSpec_Krypt#5.1.1.1] entsprechen.

Die Registrierungsstelle **MUSS** im Rahmen ihres Sicherheitskonzepts die Bedingungen für eine Zertifikatserneuerung dokumentieren.

6.6.2 Wer darf eine Zertifikatserneuerung beantragen?

Nur der Zertifikatsnehmer bzw. von ihm befugte Personen dürfen einen Erneuerungsantrag stellen.

6.6.3 Bearbeitungsprozess eines Antrags auf Zertifikatserneuerung

Die Bearbeitung eines Antrags auf Zertifikatserneuerung **MUSS** ein dokumentierter Prozess sein, der die Anforderungen der Identifizierung nach Kapitel 5.3 erfüllt.

6.6.4 Benachrichtigung des Zertifikatsnehmers über die Zertifikatserneuerung

Die Benachrichtigung des Zertifikatsnehmers erfolgt entsprechend den dokumentierten Prozessen.

6.6.5 Verhalten für die Annahme einer Zertifikatserneuerung

Der TSP beschreibt anhand dokumentierter Prozesse die sichere Ausgabe und Bedingungen, die zu einer Annahme des Zertifikats führen.

6.6.6 Veröffentlichung der Zertifikatserneuerung durch den TSP

Ein erneuertes TSP-Zertifikat **MUSS** gegenüber der gematik unverzüglich bekannt gemacht werden.

6.7 Zertifizierung nach Schlüsselerneuerung (TSP + Root-TSP)

6.7.1 Bedingungen für eine Zertifizierung nach Schlüsselerneuerung

Der TSP **muss** Bedingungen beschreiben, unter welchen Umständen ein neu erzeugtes Schlüsselpaar zusammen mit den bisherigen Nutzerdaten zertifiziert wird. Mögliche Voraussetzungen sind:

- Zertifikatsrücknahme aufgrund einer Schlüsselkompromittierung,
- Ablauf des bestehenden Zertifikats,
- Ablauf des Schlüssels, oder der Schlüsselparameter.

6.7.2 Wer darf Zertifikate für Schlüsselerneuerungen beantragen?

Siehe Kapitel 6.6.2

6.7.3 Bearbeitung von Zertifikatsanträgen für Schlüsselerneuerungen

Siehe Kapitel 6.6.3

6.7.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines Nachfolgezertifikats

Siehe Kapitel 6.6.4

6.7.5 Verhalten für die Annahme von Zertifikaten für Schlüsselerneuerungen

Der TSP beschreibt anhand dokumentierter Prozesse die sichere Ausgabe und Bedingungen, die zu einer Annahme des Zertifikats führen.

6.7.6 Veröffentlichung von Zertifikaten für Schlüsselerneuerungen durch den TSP

Ein erneuertes TSP-Zertifikat **muss** gegenüber der gematik unverzüglich durch den TSP bekannt gemacht werden.

6.7.7 Benachrichtigung anderer Zertifikatsnehmer über die Ausgabe eines Nachfolgezertifikats

Keine Vorgaben

6.8 Zertifikatsänderung (TSP + Root-TSP)

6.8.1 Bedingungen für eine Zertifikatsänderung

Der TSP **MUSS** Bedingungen beschreiben, unter welchen Umständen eine Zertifikatsänderung durchgeführt wird.

6.8.2 Wer darf eine Zertifikatsänderung beantragen?

Nur der Zertifikatsnehmer bzw. von ihm befugte Personen dürfen eine Zertifikatsänderung beantragen (vergleichbar mit Kapitel 6.6.2).

6.8.3 Bearbeitung eines Antrags auf Zertifikatsänderung

Die Bearbeitung eines Antrags auf Zertifikatsänderung **MUSS** ein dokumentierter Prozess sein, der die Anforderungen der Identifizierung nach Kapitel 5.3 erfüllt (vergleichbar mit Kapitel 6.6.3).

6.8.4 Benachrichtigung des Zertifikatsnehmers über die Ausgabe eines neuen Zertifikats

Die Benachrichtigung des Zertifikatsnehmers erfolgt entsprechend den dokumentierten Prozessen.

6.8.5 Verhalten für die Annahme einer Zertifikatsänderung

Die Ausgabestelle beschreibt anhand dokumentierter Prozesse die sichere Ausgabe und Bedingungen, die zu einer Annahme des Zertifikats führen.

6.8.6 Veröffentlichung der Zertifikatsänderung durch den TSP

Ein geändertes TSP-Zertifikat **muss** gegenüber der gematik unverzüglich durch den TSP bekannt gemacht werden.

6.8.7 Benachrichtigung anderer Zertifikatsnutzer über die Ausgabe eines neuen Zertifikats

Keine Vorgaben

6.9 Sperrung und Suspendierung von Zertifikaten (TSP + Root-TSP + Endanwender)

Es wird die Sperrung und Suspendierung von Zertifikaten näher beschrieben.

6.9.1 Bedingungen für eine Sperrung

Der TSP **MUSS** Bedingungen beschreiben, unter welchen Umständen eine Zertifikatssperrung durchgeführt wird. Eine Sperrung **MUSS** erfolgen, wenn:

- eine Kompromittierung des Schlüssels vorliegt,
- die eindeutige Zuordnung des Zertifikatsnehmers zu seinem Zertifikat nicht mehr gegeben ist,
- Das Zertifikat enthält Angaben, die nicht oder nicht mehr gültig sind.
- die eindeutige Verbindung zwischen Zertifikat und Schlüssel nicht mehr gegeben ist,

Eine Kompromittierung des privaten Signaturschlüssels des TSP ist dem gematik-TSL-Service Provider unverzüglich anzuzeigen.

Sperrgründe:

Ein TSP-Zertifikat **MUSS** aus folgenden Gründen gesperrt werden:

- Nach dem Wirksamwerden der Kündigung des Vertrages durch eine der Vertragsparteien wird das entsprechende Zertifikat gesperrt, wenn die Deaktivierung des zugehörigen privaten Schlüssels nicht gewährleistet werden kann.
- Der TSP beantragt die Sperrung seines Zertifikats. Er **KANN** die Sperrung jederzeit vornehmen lassen.
- Der geheime Signaturerstellungsschlüssel ist nicht mehr verfügbar oder kompromittiert.
- Das TSP-Zertifikat enthält Angaben, die nicht oder nicht mehr gültig sind.
- Erhebliche Schwächen (nach Einschätzung des BSI) eines verwendeten Kryptoalgorithmus samt zugehörigem Schlüssel werden bekannt.
- Erhebliche Schwächen (nach Einschätzung des BSI) der eingesetzten Hard- oder Software werden bekannt.

Ein TSP-Zertifikat **KANN** aus folgenden Gründen gesperrt werden:

- Der TSP kommt seinen vertraglichen Verpflichtungen in wesentlichen Punkten nicht nach.

Ein Endanwender-Zertifikat **MUSS** aus folgenden Gründen gesperrt werden:

- Der Karteninhaber kündigt den Vertrag.

- Das Zertifikat wurde suspendiert und die Suspendierung wurde nicht innerhalb von 14 Tagen durch eine Desuspendierung aufgehoben (siehe Abschnitt 6.9.16).

6.9.2 Wer kann eine Sperrung beantragen?

Nur Sperrberechtigte dürfen eine Sperrung vornehmen. Der TSP beschreibt in seinem CPS, wer Sperrberechtigter ist. Grundsätzlich sind immer der Zertifikatsnehmer und der ausstellende TSP Sperrberechtigte.

6.9.3 Verfahren für einen Sperrantrag

Der Sperrantragsteller ist durch den TSP hinreichend zu identifizieren und **MUSS** seine Sperrberechtigung entsprechend dem CPS des TSP legitimieren. Der TSP hat den Sperrantragsteller auf die Konsequenzen einer Sperrung hinzuweisen. Der Zertifikatsnehmer **MUSS** immer über die Sperrung seines Zertifikats informiert werden. Der TSP **MUSS** das Verfahren für einen Sperrantrag dokumentieren.

6.9.4 Fristen für einen Sperrantrag

Der TSP **SOLL** Fristen für einen Sperrantrag gegenüber dem Zertifikatsnehmer dokumentieren.

6.9.5 Fristen/Zeitspanne für die Bearbeitung des Sperrantrags durch den TSP

Eine Zertifikatssperrung **MUSS** unverzüglich erfolgen.

6.9.6 Verfügbare Methoden zum Prüfen von Sperrinformationen

Die verfügbaren Methoden zum Prüfen von Sperrinformationen **MÜSSEN** den Konformitätskriterien des gematik-TSL-Service Providers entsprechen.

6.9.7 Frequenz der Veröffentlichung von Sperrlisten

Die Frequenz der Veröffentlichung von Sperrlisten **MUSS** vom TSP dokumentiert werden. Dabei soll eine zeitnahe Verfügbarkeit von aktuellen Sperrinformationen gewährleistet sein.

6.9.8 Maximale Latenzzeit für Sperrlisten

Die maximale Latenzzeit für Sperrlisten **MUSS** vom TSP dokumentiert sein.

6.9.9 Online-Verfügbarkeit von Sperrinformationen

Der TSP **MUSS** Sperrinformationen online zur Verfügung stellen. Die Verfügbarkeit dieser Online-Dienstleistung **MUSS** dokumentiert werden.

6.9.10 Anforderungen zur Online-Prüfung von Sperrinformationen

Der Trust-Service Provider **MUSS** gegenüber den Zertifikatsnutzern eine Beschreibung des Nutzens und der Notwendigkeit einer Online-Prüfung abgeben.

6.9.11 Andere Formen zur Anzeige von Sperrinformationen

Die gematik **MUSS** unverzüglich über die Sperrung eines TSP- bzw. eines Root-Zertifikats informiert werden. Die gematik informiert dann die anderen TSPs (Teilnehmer der TSL) und veranlasst die unverzügliche Aktualisierung der TSL/TCL. Über weitere Maßnahmen wird im Einzelfall entschieden.

6.9.12 Spezielle Anforderungen bei Kompromittierung des privaten Schlüssels

Keine Vorgaben.

6.9.13 Bedingungen für eine Suspendierung (Endanwender)

Suspendierungen (vorübergehende Sperrungen) von Zertifikaten werden für Endanwender-Zertifikate der Typen AUT, ENC, AUTN und ENCV der eGK vorgesehen. Hierzu sind in der Facharchitektur Kartenmanagement eGK [gemFA_CMSeGK] entsprechende Anwendungsfälle beschrieben.

Der zuständige Kartenherausgeber **MUSS** Bedingungen beschreiben, unter welchen Umständen eine Zertifikatssuspendierung durchgeführt wird. Eine Suspendierung **KANN** anstelle einer Sperrung erfolgen, wenn:

- der Versicherte seine eGK verloren hat,
- die eGK des Versicherten entwendet wurde

und in beiden Fällen ein Wieder finden der eGK mitsamt Zertifikaten möglich erscheint.

6.9.14 Wer kann eine Suspendierung beantragen? (Endanwender)

Nur Sperrberechtigte dürfen eine Suspendierung vornehmen. Der TSP beschreibt in seinem CPS, wer Sperrberechtigter ist. Grundsätzlich sind immer der Zertifikatsnehmer und der ausstellende TSP Sperrberechtigte.

6.9.15 Verfahren für Anträge auf Suspendierung (Endanwender)

Der Antragsteller **MUSS** durch den TSP hinreichend zu identifiziert werden und **MUSS** seine Berechtigung zur Suspendierung entsprechend dem CPS des TSP legitimieren. Der TSP hat den Antragsteller auf die Konsequenzen einer Suspendierung hinzuweisen. Der Zertifikatsnehmer **MUSS** immer über die Suspendierung seines Zertifikats informiert werden. Der TSP **MUSS** das Verfahren für einen Sperrantrag dokumentieren.

6.9.16 Begrenzungen für die Dauer von Suspendierungen (Endanwender)

Eine Suspendierung ist auf die maximale Dauer von 14 Tagen begrenzt. Ist das suspendierte Zertifikat nicht innerhalb dieser Frist wieder aktiviert (Desuspendierung) worden, wird es automatisch vom Zustand „on hold“ in den Zustand „gesperrt“ überführt.

6.10 Statusabfragedienst für Zertifikate (TSP + Root-TSP)

6.10.1 Funktionsweise des Statusabfragedienstes

Der TSP **MUSS** die Funktionsweise des Statusabfragedienstes beschreiben. Entsprechend den Konformitätskriterien **MUSS** der Statusabfragedienst interoperabel mit den Vorgaben der gematik für den OCSP-Responder sein.

6.10.2 Verfügbarkeit des Statusabfragedienstes

Die Verfügbarkeit des Statusabfragedienstes **MUSS** dokumentiert werden. Dabei **SOLL** eine zeitnahe Verfügbarkeit von aktuellen Statusinformationen gewährleistet sein.

6.10.3 Optionale Leistungen

Keine Vorgaben.

6.11 Kündigung durch den Zertifikatsnehmer (TSP + Endanwender)

Im Fall einer Kündigung durch den Zertifikatsnehmer **MUSS** das Zertifikat am Ende der Kündigungsfrist gesperrt werden.

6.12 Schlüsselhinterlegung und Wiederherstellung (TSP + Root-TSP)

6.12.1 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung privater CA-Schlüssel

Im Fall einer Schlüsselhinterlegung von Root- bzw. CA-Schlüsseln **MUSS** der TSP die Prozesse der Schlüsselhinterlegung dokumentieren. Diese **MÜSSEN** dem eigenen Sicherheitskonzept und dem aktuellen Stand der Technik entsprechen. Die Hinterlegung darf nur in einem geeigneten HSM erfolgen. Eine Schlüsselhinterlegung **DARF NICHT** für qualifizierte Signaturschlüssel erfolgen.

6.12.2 Bedingungen und Verfahren für die Hinterlegung und Wiederherstellung von Sitzungsschlüsseln

Keine Vorgaben.

6.13 Grundlagen für die Sicherheit der Zertifikatserstellung (TSP + Root-TSP)

Die Sicherheit der PKI für X.509-Zertifikate ist für die Sicherheit des Gesamtsystems von entscheidender Bedeutung. Durch das Ausstellen von X.509-Zertifikaten ermöglicht ein TSP (in Zusammenarbeit mit einem Kartenhersteller und bei Vorhandensein der sonstigen für die Produktion benötigten Daten) die Herstellung

- echter eGKs für Versicherte und
- echte SMCs Typ-B mit beliebigen Profilen (Arztpraxis, Apotheke, etc.).

In diesem Abschnitt werden Grundlagen für die Sicherheit „aus qualitativer Sicht“ angegeben. Dabei werden

- technische Vorgaben für die Sicherheit,
- organisatorische Vorgaben für die Sicherheit und
- betriebliche Vorgaben für die Sicherheit

unterschieden. Die Vorgaben für die Sicherheit **MÜSSEN** in den Feinspezifikationen und Betriebskonzepten des gematik-TSL-Service Providers und den TSPs umgesetzt werden. Über die Umsetzung **MUSS** ein Sicherheitskonzept erstellt werden.

Der TSP **MUSS** prüfen, dass nur explizit zugelassene Zertifikate erstellt werden, z.B. ein TSP, der nur eGK-Zertifikate erstellt, **DARF NICHT** HBA-Zertifikate erstellen.

6.13.1 Sicherheit eines TSP

Ein TSP wird im Auftrag eines Kartenherausgebers einer eGK bzw. einer SMC-Typ-B betrieben. Der Betreiber eines TSP **KANN** in Abstimmung mit dem ihn beauftragenden Kartenherausgeber Konzeption, Realisierung und Betrieb seines TSP weitestgehend gemäß eigener Vorgaben durchführen.

Probleme bei der Sicherheit eines TSP können die Sicherheit der gesamten PKI für X.509-Zertifikate und somit des gesamten Systems der elektronischen Gesundheitskarte gefährden. Für die Sicherheit eines TSP werden daher durch die gematik Vorgaben erstellt, die als Mindeststandard bei der Sicherheit des TSP umgesetzt werden **MÜSSEN**. Im Folgenden werden diese Vorgaben für den Mindeststandard beschrieben.

Für einen TSP **MUSS** in einem Sicherheitskonzept dargestellt werden, wie die Vorgaben der gematik für den Mindeststandard der Sicherheit umgesetzt werden. Ein TSP **MUSS** sich bei der gematik registrieren lassen. Im Rahmen dieser Registrierung **MÜSSEN** das Sicherheitskonzept sowie seine Umsetzung beim Betrieb des TSP durch die gematik überprüft und abgenommen werden. Der Prozess der Registrierung eines TSP bei der gematik ist im Registrierungsdokument [gemX.509_TSP] ausführlich beschrieben. Die dazu notwendigen Formulare sind unter www.gematik.de zu finden.

Ist der TSP ein Zertifizierungsdiensteanbieter mit Anbieterakkreditierung nach SigG, genügt statt Vorlage des Sicherheitskonzepts die Vorlage der entsprechenden Akkreditierung sowie eine Erklärung, die Maßnahmen des Sicherheitskonzepts anzuwenden.

Technische Vorgaben:

- Das Schlüsselpaar des TSP zum Signieren von Zertifikaten **MUSS** in einem HSM generiert werden. Als HSM **KANN** auch eine geeignete Chipkarte eingesetzt werden. Die genauen Sicherheitsanforderungen an das HSM werden in Kapitel 8.2.1 beschrieben.
- Der private Schlüssel des TSP **DARF** das HSM im Klartext **NICHT** verlassen. Ausnahme ist nur die gesicherte Ausgabe für das Erzeugen eines Backup HSM.
- Es **MUSS** ein Backup-HSM existieren. HSM und Backup-HSM **MÜSSEN** die gleichen Sicherheitsanforderungen erfüllen. Zwischen HSM und Backup-HSM **MUSS** ein kryptographisch gesicherter Transportkanal hergestellt werden können, um den privaten Schlüssel des Root-TSP aus dem HSM gesichert zu exportieren und in das Backup-HSM zu importieren. Alternativ **KANN** in dem Backup-HSM auch ein eigenes Schlüsselpaar generiert werden. In diesem Fall **MUSS** ein entsprechendes Paar an Cross -Zertifikaten erstellt werden.
- Das HSM **MUSS** eine Funktion unterstützen, mit der ein Schlüsselpaar in dem HSM gelöscht werden kann. Das Löschen kann dabei durch ein Überschreiben mit einem vorgegebenen Wert oder durch das interne dauerhafte Sperren aller Zugriffe auf den Schlüssel realisiert werden.
- Das Generieren eines neuen Schlüsselpaares und das Löschen eines Schlüsselpaares **DÜRFEN** nur nach Benutzerauthentifikation **zweier** hierfür autorisierter Nutzer (Vier-Augenprinzip) ausführbar sein. Die Benutzerauthentifikation **MUSS** durch das Verifizieren einer PIN oder gleichartiges Verfahren realisiert werden.
- Alle kryptographischen Berechnungen mit dem privaten Schlüssel des TSP für das Erstellen eines TSP-Zertifikats **MÜSSEN** innerhalb des HSM erfolgen. Das HSM darf diese Berechnungen nur nach Benutzerauthentifikation **zweier** hierfür autorisierter Nutzer (Vier-Augenprinzip) durchführen. Die Benutzerauthentifikation **MUSS** durch das Verifizieren einer PIN oder gleichartiges Verfahren realisiert werden.
- Die Nutzung des HSM **MUSS** revisionssicher protokolliert werden. Dabei **MUSS** insbesondere protokolliert werden für welche Rolle/Person wann für welche Funktion das HSM genutzt hat und für welche Profile das HSM konfiguriert ist.
- Der öffentliche Schlüssel des TSP wird auf der Internetseite der gematik veröffentlicht. Ein zugehöriger Fingerprint (bzw. der öffentliche Schlüssel selber) wird auf Anfrage in Schriftform versendet.

Organisatorische Vorgaben:

- Der TSP **MUSS** sich bei der gematik registrieren lassen. Die Gültigkeit einer Registrierung ist zeitlich begrenzt.
- Durch die Beantragung der Registrierung erkennt der TSP an, dass er für den, durch einen Missbrauch seines durch die gematik als vertrauensvoll eingestuften Schlüsselpaares, entstehenden Schaden haftet.
- Jede Änderung an der Gesellschafterstruktur des Betreibers des TSP **MUSS** der gematik unverzüglich angezeigt werden. Die Gültigkeit der Registrierung **KANN** in diesem Fall ggf. durch die gematik widerrufen werden.

- Bei der Registrierung des TSP wird das dafür angefertigte Sicherheitskonzept und seine Umsetzung (in Bezug auf die durch die gematik vorgegebenen Mindeststandards) durch die gematik überprüft und abgenommen. Jede nachträgliche Änderung an diesem Sicherheitskonzept und seiner Umsetzung **MÜSSEN** der gematik unverzüglich angezeigt werden. Die Gültigkeit der Registrierung **KANN** in diesem Fall ggf. durch die gematik beendet werden.
- Ein Root-TSP **MUSS** immer über eine aktuelle Liste der zurzeit bei ihm registrierten TSPs verfügen. Diese Liste stellt er zeitnah der gematik zur Verfügung.
- Die genauen Aufgaben der Rollen **MÜSSEN** in dem Sicherheitskonzept des TSP beschrieben werden. Geklärt werden **MUSS** dabei, welche verschiedenen Rollen nicht durch eine einzelne Person ausgeübt werden dürfen (Rollenausschlussmatrix, siehe Kapitel 7.2.3). Dabei **MUSS** insbesondere festgelegt werden, welche Rolle auf welche Weise das HSM des TSP nutzen kann.
- Auf Antrag **MUSS** der TSP der gematik Einblick in die revisionssichere Protokollierung der Zertifikatserzeugung für diesen Kontext gewähren.

Betriebliche Vorgaben:

- Das Backup-HSM **MUSS** an einem sicheren Ort außerhalb des primären Standorts des Root-TSP aufbewahrt werden.
- Zugriff auf das Backup-HSM und sein Freischalten im Rahmen des Einbringens in das eigentliche Produktivsystem des Root-TSP darf nur im Vier-Augenprinzip möglich sein. Das genaue Vorgehen **MUSS** in dem Sicherheitskonzept beschrieben werden. Insbesondere **MUSS** festgelegt werden, welcher Personenkreis über die Nutzung des Backup HSM entscheiden kann.
- Für die bei der Arbeit des Root-TSP notwendige Hardware, Software und Daten **MUSS** ein Backup-Konzept erstellt und umgesetzt werden. Dadurch **MUSS** sichergestellt werden, dass bei einem Ausfall der aktuellen Realisierung des Root-TSP diese kurzfristig wieder neu aufgesetzt werden kann.
- Zu jeder der oben genannten Rollen **MÜSSEN** mindestens ein verantwortlicher Mitarbeiter sowie ein Stellvertreter ernannt werden. Diese Zuordnung wird der gematik mitgeteilt. Änderungen bei der Zuordnung werden ebenfalls mitgeteilt.
- Zu jedem Zeitpunkt der festgelegten Betriebszeit des TSP **MUSS** für jede der oben genannten Rollen mindestens ein für diese Rolle verantwortlicher Mitarbeiter bzw. sein Stellvertreter kurzfristig erreichbar sein.
- Durch die tatsächliche Zuordnung von Rollen zu Personen darf nicht ermöglicht werden, dass eine einzelne Person zwei Rollen ausüben kann, die Zugriffe auf das HSM im Vier-Augenprinzip für diese einzelne Person ermöglicht.
- Das den TSP realisierende System (inklusive des HSMs) **MUSS** in einen geschützten Bereich der Betriebsstätte untergebracht sein. Der Zugang zu diesem Bereich **MUSS** nur für berechtigte Personen möglich sein.
- Den Mitarbeitern der gematik bzw. durch die gematik beauftragten Personen **MUSS** nach Ankündigung (ggf. in Begleitung eines Mitarbeiters des Betreibers des TSP) Zugang zu den für die Zertifikatserzeugung für diesen Kontext relevanten Systemen des

TSP gewährt werden. Genaue Regelungen (Vorlaufzeit für die Ankündigung, Mitteilung der berechtigten Personen) **MÜSSEN** noch festgelegt werden.

- Alle zum TSP gehörenden Systeme **MÜSSEN** in Betriebsstätten betrieben werden, die in einem Land der Europäischen Union liegen.