
C_11918_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	3
2 Änderungen in gemSpec_PKI.....	4
2.1 Geänderte Anforderungen:.....	4
2.2 Neue Anforderungs-Zuweisungen:.....	4
2.3 Entfernte Anforderungs-Zuweisungen:.....	4
2.4 Geänderte Prüfverfahren von Anforderungen für TSP-Steckbriefe:.....	4
3 Änderungen in gemSpec_X.509_TSP.....	13
3.1 Geänderte Anforderungen:.....	13
3.2 Geänderte Prüfverfahren von Anforderungen für TSP-Steckbriefe:.....	14
4 Änderungen in gemSpec_Net.....	15
4.1 Entfernte Anforderungs-Zuweisungen:.....	15
5 Änderungen in gemRL_TSL_SP_CP.....	16
5.1 Geänderte Prüfverfahren von Anforderungen für TSP-Steckbriefe:.....	16
5.2 Anforderungen, die komplett gelöscht werden:.....	16
6 Änderungen in gemSpec_OM.....	17
6.1 Geänderte Prüfverfahren von Anforderungen für TSP-Steckbriefe:.....	17
7 Änderungen in Steckbriefen.....	18
7.1 Änderungen in gemProdT_..._PTVx.y.z-n.....	18

1 Änderungsbeschreibung

Die Anforderungen an die Trust Service Provider (TSP) entsprechen nicht den aktuellen Bedarfen oder sind einzelnen TSP-Anbietern noch nicht wirksam zugeordnet. Deshalb ist eine Überarbeitung der Anforderungslage notwendig geworden zur Sicherstellung eines stabilen Betriebs und sind die Voraussetzung für zukünftige Beauftragungen.

Dazu werden hier Anforderungs-Anpassungen und Zuweisungen von Anforderungen vornehmlich aus PKI-Spezifikationen in den Produktypsteckbriefen der TSP-Produkte vorgenommen.

2 Änderungen in gemSpec_PKI

2.1 Geänderte Anforderungen:

Die SOLL-Anforderung GS-A_4685 wird angepasst und dabei durch Anforderung GS-A_4685-01 ersetzt:

GS-A_4685-01 - Statusprüfdienst - Steigerung der Performance

Die Produkttypen TSL-Dienst, gematik Root-CA und TSP-X.509 nonQES MÜSSEN Methoden des Response-Caching anwenden, um die Performance des Statusprüfdienstes zu steigern. Die Caching-Dauer muss vom Betreiber per Konfiguration änderbar sein. Dabei darf eine Caching-Dauer der OCSP-Antworten von 30 Sekunden nicht überschritten werden.

[<=]

2.2 Neue Anforderungs-Zuweisungen:

Afo-ID	Afo-Titel	betroffene(r) TSP-Produkttyp(en)	Prüfverfahren (neu)
GS-A_5043	Auflösung von OCSP-Adressen im Internet	TSP X.509 nonQES - eGK	funkt. Eignung: Test Produkt/FA
GS-A_4722	Belegung der Felder professionInfos	TSP X.509 QES	funkt. Eignung: Test Produkt/FA

2.3 Entfernte Anforderungs-Zuweisungen:

Afo-ID	Afo-Titel	betroffene(r) TSP-Produkttyp(en)
GS-A_4257	Hauptsitz und Betriebsstätte	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC, TSP-CVC

2.4 Geänderte Prüfverfahren von Anforderungen für TSP-Steckbriefe:

Afo-ID	Afo-Titel	betroffene(r) TSP- Produkttyp(en)	Prüfverfahren (alt)	Prüfverfahren (neu)
A_17700	TSL-Auswertung ServiceTypeldentifizier "unspecified"	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklärung
GS-A_4588	CA-Namen für Test-PKI der TI	TSP X.509 QES	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklärung
GS-A_4590	Zertifikatsprofile für Test-PKI	TSP X.509 QES, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklärung
GS-A_4637	TUCs, Durchführung Fehlerüberprüfung	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklärung
GS-A_4642	TUC_PKI_001: Periodische Aktualisierung TI- Vertrauensraum	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklärung

		nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC		
GS-A_4643	TUC_PKI_013: Import TI- Vertrauensanker aus TSL	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklär- ung
GS-A_4646	TUC_PKI_017: Lokalisierung TSL Download- Adressen	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklär- ung
GS-A_4647	TUC_PKI_016: Download der TSL-Datei	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklär- ung
GS-	TUC_PKI_019:	TSP X.509	funkt. Eignung:	funkt. Eignung:

A_4648	Prüfung der Aktualität der TSL	QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	Test Produkt/FA	Herstellereklärung
GS-A_4649	TUC_PKI_020: XML-Dokument validieren	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellereklärung
GS-A_4650	TUC_PKI_011: Prüfung des TSL-Signer-Zertifikates	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellereklärung
GS-A_4651	TUC_PKI_012: XML-Signatur-Prüfung	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellereklärung

		X.509 nonQES - gSMC		
GS- A_4652 -01	TUC_PKI_018: Zertifikatsprüfung in der TI	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellereklär ung
GS- A_4653 -01	TUC_PKI_002: Gültigkeitsprüfun g des Zertifikats	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellereklär ung
GS- A_4654 -01	TUC_PKI_003: CA- Zertifikat finden	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellereklär ung
GS- A_4655 -01	TUC_PKI_004: Mathematische Prüfung der Zertifikatssignatur	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellereklär ung

		nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC		
GS-A_4656	TUC_PKI_005: Adresse für Status- und Sperrprüfung ermitteln	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklär ung
GS-A_4657-03	TUC_PKI_006: OCSP-Abfrage	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklär ung
GS-A_4660-02	TUC_PKI_009: Rollenermittlung	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklär ung
GS-	kritische	TSP X.509	funkt. Eignung:	funkt. Eignung:

A_4661-01	Erweiterungen in Zertifikaten	QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	Test Produkt/FA	Herstellereklärung
GS-A_4662	Bedingungen für TLS-Handshake	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellereklärung
GS-A_4663	Zertifikats-Prüfparameter für den TLS-Handshake	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellereklärung
GS-A_4669	Umsetzung Statusprüfdienst	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellereklärung

		X.509 nonQES - gSMC		
GS-A_4687	Statusprüfdienst - Response Status sigRequired	TSP X.509 nonQES - eGK, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellereklär ung
GS-A_4694	Betrieb von OCSP- Responder für Test-PKI-CAs	TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellereklär ung
GS-A_4697	PKI für Test- und Referenzumgebun g	TSP X.509 nonQES - HBA	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellereklär ung
GS-A_4705-01	Verarbeitung von Sonderzeichen in PKI-Komponenten	TSP X.509 nonQES - eGK	funkt. Eignung: Herstellereklärun g	funkt. Eignung: Test Produkt/FA
GS-A_4706	Vorgaben zu SubjectDN von CA- und OCSP- Zertifikaten	TSP X.509 nonQES - eGK	funkt. Eignung: Herstellereklärun g	funkt. Eignung: Test Produkt/FA
GS-A_4714-01	Kodierung der Attribute in X.509-Zertifikaten	TSP X.509 nonQES - eGK	funkt. Eignung: Herstellereklärun g	funkt. Eignung: Test Produkt/FA
GS-A_4715-01	Maximale Stringlänge der Attribute im SubjectDN	TSP X.509 nonQES - eGK	funkt. Eignung: Herstellereklärun g	funkt. Eignung: Test Produkt/FA
GS-A_4717-02	TI-spezifische Vorgabe zur Nutzung der Extension	TSP X.509 nonQES - eGK	funkt. Eignung: Herstellereklärun g	funkt. Eignung: Test Produkt/FA

	Admission			
GS-A_4718	TI-spezifische Vorgabe zur Nutzung der Extension CertificatePolicies	TSP X.509 nonQES - eGK	funkt. Eignung: Herstellererklärung	funkt. Eignung: Test Produkt/FA
GS-A_4719	TI-spezifische Vorgabe zur Nutzung der Extension SubjectAltNames	TSP X.509 nonQES - eGK	funkt. Eignung: Herstellererklärung	funkt. Eignung: Test Produkt/FA
GS-A_4722	Belegung der Felder professionInfos	TSP X.509 nonQES - eGK	funkt. Eignung: Herstellererklärung	funkt. Eignung: Test Produkt/FA
GS-A_4724	Komplettsperrung aller Zertifikate einer Karte	TSP X.509 nonQES - eGK	funkt. Eignung: Herstellererklärung	funkt. Eignung: Test Produkt/FA
GS-A_4741	Umsetzung Zertifikatsprofil C.GEM.OCSP	TSP X.509 nonQES - eGK	funkt. Eignung: Herstellererklärung	funkt. Eignung: Test Produkt/FA
GS-A_4749-01	TUC_PKI_007: Prüfung Zertifikatstyp	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellerklärung
GS-A_4751	Fehlercodes bei TSL- und Zertifikatsprüfung	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES -	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellerklärung

		gSMC		
GS-A_4829	TUCs, Fehlerbehandlung	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklärung
GS-A_4898	TSL-Grace-Period einer TSL	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklärung
GS-A_4899	TSL Update-Prüfintervall	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklärung
GS-A_4957-01	Beschränkungen OCSP-Request	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklärung

		X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC		
GS- A_5077	FQDN-Prüfung beim TLS- Handshake	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklär- ung
GS- A_5336	Zertifikatsprüfung nach Ablauf TSL- Graceperiod	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklär- ung

3 Änderungen in gemSpec_X.509_TSP

3.1 Geänderte Anforderungen:

Die Anforderung TIP1-A_3638 wird angepasst und dabei durch Anforderung TIP1-A_3638-01 ersetzt:

TIP1-A_3638-01 - Fristen zur Ausführung der Sperrung von nonQES-Personen- und Organisationszertifikaten

Der TSP-X.509 nonQES MUSS nach eindeutiger Identifizierung des berechtigten Sperrantragstellers und Zertifikates die Sperrung des Zertifikates gemäß den in gemRL_TSL_SP_CP in Kap. 5.8.13 definierten Fristen ausführen.

[<=]

Die Anforderung TIP1-A_4244 wird angepasst und dabei durch Anforderung TIP1-A_4244-01 ersetzt:

TIP1-A_4244-01 - Fristen zur Ausführung der Sperrung für Komponenten, Signer-, nonQES-HBA- oder Organisationszertifikate

Der Anbieter der zentralen PKI (TSP-X.509 nonQES) MUSS nach eindeutiger Identifizierung des berechtigten Sperrantragstellers und des Komponenten-, Signer-, nonQES-HBA- oder Organisationszertifikates die Sperrung des Zertifikates gemäß den in gemRL_TSL_SP_CP in Kap. 5.8.13 definierten Fristen ausführen.

[<=]

Die Anforderung TIP1-A_4232 wird angepasst und dabei durch Anforderung TIP1-A_4232-01 ersetzt:

TIP1-A_4232-01 - Löschung von TSP-X.509 nonQES-Zertifikatsstatusinformationen, Zertifikats- und Sperranträge

Der TSP-X.509 nonQES MUSS die Zertifikatsanträge, die Zertifikatsstatusinformationen und die Sperraufträge zu einem X.509-Zertifikat unverzüglich löschen, sobald die gesetzlichen oder vertraglichen Aufbewahrungsfristen erreicht sind.

Als Ausnahmefall hierzu muss der TSP-X.509 nonQES SMC-B Zertifikatsstatusinformationen für Zertifikate des Profils C.HCI.OSIG abweichend dazu 15 Jahre nach Ablauf der Zertifikats-Gültigkeit aufbewahren.

[<=]

3.2 Geänderte Prüfverfahren von Anforderungen für TSP-Steckbriefe:

Afo-ID	Afo-Titel	betroffene(r) TSP- Produkttyp(en)	Prüfverfahren (alt)	Prüfverfahren (neu)
TIP1-A_3886	OCSP-Adresse im X.509-Zertifikate	TSP X.509 nonQES - eGK	funkt. Eignung: Herstellereklärung	funkt. Eignung: Test Produkt/FA
TIP1-A_3894	Obligatorisch abzuleitende Sub-CAs unterhalb der gematikRoot-CA	TSP X.509 nonQES - gSMC	funkt. Eignung: Herstellereklärung	funkt. Eignung: Test Produkt/FA
A_26192	Prüfung des vom IDP signierten Token	TSP X.509 nonQES - eGK	Sich.techn. Eignung: Gutachten, funkt. Eignung: Test Produkt/FA	Sich.techn. Eignung: Gutachten

4 Änderungen in gemSpec_Net

4.1 Entfernte Anforderungs-Zuweisungen:

Afo-ID	Afo-Titel	betroffene(r) TSP-Produkttyp(en)	Prüfverfahren (alt)
A_20574-02	Beachtung der ISI-LANA für Übergänge zu Fremdnetzen	TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B	Sich.techn. Eignung: Gutachten
GS-A_4054	Paketfilter Default Deny	TSP X.509 nonQES - HBA	funkt. Eignung: Herstellererklärung
GS-A_4054	Paketfilter Default Deny	TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Herstellererklärung , Sich.techn. Eignung: Gutachten
GS-A_4062-01	Sicherheitsanforderungen für Netzübergänge zu Fremdnetzen	TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	Sich.techn. Eignung: Gutachten
GS-A_4879	DNSSEC, Zonen im Namensraum Internet mittels DNSSEC sichern	TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA, funkt. Eignung: Test Produkt/FA

5 Änderungen in gemRL_TSL_SP_CP

5.1 Geänderte Prüfverfahren von Anforderungen für TSP-Steckbriefe:

Afo-ID	Afo-Titel	betroffene(r) TSP-Produkttyp(en)	Prüfverfahren (alt)	Prüfverfahren (neu)
GS-A_4213	Zulässige Nutzungsarten	TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC	funkt. Eignung: Test Produkt/FA	funkt. Eignung: Herstellererklärung

5.2 Anforderungen, die komplett gelöscht werden:

Afo-ID	Afo-Titel	betroffene(r) TSP-Produkttyp(en)
GS-A_4341	Entfall der Verpflichtung für die Bereitstellung einer Statusprüfung bestimmter Komponentenzertifikate	TSP X.509 nonQES - gSMC
GS-A_4349	Obligatorische Gründe für die Sperrung eines selbst signierten Zertifikats eines TSP-X.509 nonQES	TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC
GS-A_4355	Maximale Gültigkeitsdauer des Zertifikats eines TSP-X.509 nonQES bei Erzeugung durch den TSP-X.509 nonQES	TSP X.509 nonQES - eGK

6 Änderungen in gemSpec_OM

6.1 Geänderte Prüfverfahren von Anforderungen für TSP-Steckbriefe:

Afo-ID	Afo-Titel	betroffene(r) TSP-Produkttyp(en)	Prüfverfahren (alt)	Prüfverfahren (neu)
GS-A_5054	Versionierung von Produkten durch die Produktidentifikation erweitert um Klartextnamen	TSP X.509 QES, TSP X.509 nonQES - eGK, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC, TSP-CVC	funkt. Eignung: Test Produkt/FA bzw. nicht prüfrelevant	funkt. Eignung: Herstellererklärung

7 Änderungen in Steckbriefen

7.1 Änderungen in gemProdT_..._PTVx.y.z-n

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_...]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 1: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
	[...]	