
C_11920_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	3
2 Änderungen in gemSpec_PKI.....	4
2.1 Geänderte Anforderungen:.....	4
2.2 Entfernte Anforderungs-Zuweisungen:.....	4
3 Änderungen in gemSpec_CVC_TSP.....	5
3.1 Neue Anforderungen.....	5
3.2 Neue Anforderungs-Zuweisungen:.....	5
4 Änderungen in gemSpec_CAN_TI.....	7
4.1 Neue Anforderungs-Zuweisungen:.....	7
5 Änderungen in gemKPT_Test.....	8
5.1 Entfernte Anforderungs-Zuweisungen:.....	8
6 Änderungen in gemSpec_OM.....	10
6.1 Entfernte Anforderungs-Zuweisungen:.....	10
7 Änderungen in gemRL_TSL_SP_CP.....	11
7.1 Neue Anforderungen.....	11
8 Änderungen in Steckbriefen.....	12
8.1 Änderungen in gemAnbT_..._PTVx.y.z-n.....	12

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 Anbietertypsteckbriefen der TSP-Produkte vorgenommen.

2 Änderungen in gemSpec_PKI

2.1 Geänderte Anforderungen:

Die Anforderung **GS-A_4257** wird angepasst und dabei durch Anforderung **GS-A_4257-01** ersetzt. Sie wird so umformuliert, um sie statt bisher den Produkttypen, nun den Anbietern zuzuweisen:

GS-A_4257-01 - Hauptsitz und Betriebsstätte

Der Anbieter der Produkttypen gematik Root-CA, TSP-X.509 nonQES, TSP-X.509 QES, TSP-CVC, CVC-Root und des TSL-Dienstes MÜSSEN ihren Hauptsitz und die Betriebsstätten für den tatsächlichen Betrieb in einem Land der Europäischen Union haben.

Die Anforderung **GS-A_4724** wird angepasst und dabei durch Anforderung **GS-A_4724-01** ersetzt. Sie wird so umformuliert, um sie statt bisher den Produkttypen, nun den Anbietern zuzuweisen:

GS-A_4724-01 - Komplettspernung der Zertifikate einer Karte (RSA bzw. ECDSA)

Die Anbieter der Produkttypen TSP-X.509 MÜSSEN sicherstellen, dass alle Zertifikate einer Schlüsselgeneration (RSA bzw. ECDSA) auf einem Kartenexemplar durch einen Sperrauftrag gesperrt werden können (sofern für die jeweiligen Zertifikatstypen die Statusinformationsbereitstellungen gefordert sind).

2.2 Entfernte Anforderungs-Zuweisungen:

Afo-ID	Afo-Titel	betroffene(r) TSP-Produkttyp(en)	Hinweise
A_23142	TSP-X.509nonQES: OCSP-Responder-Zertifikate nach RFC-6960#4.2.2.2	Anb_X.509_TSP_eGK	Zuweisungen zu entsprechenden Produkttypen bleiben erhalten

3 Änderungen in gemSpec_CVC_TSP

3.1 Neue Anforderungen

Die folgende Anforderung inkl. Hinweis-Text darunter wird in Kap. 4.7 (Beantragung eines CV-Zertifikats für die CVC-CA) hinzugefügt:

A_26820 - Planmäßige Schlüsselerneuerung der TSP-CVC-CAs

Der TSP-CVC MUSS spätestens 3 Jahre nach der letzten Erzeugung des CVC-CA-Zertifikates eine planmäßige Schlüsselerneuerung einleiten und dazu mit geeignetem Vorlauf den Anbieter der CVC-Root kontaktieren, um eine Neu-Beantragung des CVC-CA-Zertifikates mit neuem Schlüssel zu veranlassen.

Hinweis: Damit wird sichergestellt, dass EE-Zertifikate von der TSP-CVC-CA ausgegeben werden können, die eine Maximal-Gültigkeit von 5 Jahren haben.

3.2 Neue Anforderungs-Zuweisungen:

Afo-ID	Afo-Titel	betroffene(r) TSP-Produkttyp(en)	Prüfverfahren (neu)
TIP1-A_2579	Korrektur privater Schlüssel in der Chipkarte	Anb_CVC_TSP_eGK	Sich.techn. Eignung: Gutachten (Anbieter)
TIP1-A_2580	Erzeugung des privaten Schlüssels der Chipkarte	Anb_CVC_TSP_eGK	Sich.techn. Eignung: Gutachten (Anbieter)
TIP1-A_2582	Vertraulichkeit des privaten Schlüssels der Chipkarte	Anb_CVC_TSP_eGK	Sich.techn. Eignung: Gutachten (Anbieter)
TIP1-A_2583	Zuordnung des privaten Schlüssels zu Identitäten	Anb_CVC_TSP_eGK	Sich.techn. Eignung: Gutachten (Anbieter)
TIP1-A_2584	Schlüsselpaare und CV-Zertifikate	Anb_CVC_TSP_eGK	Sich.techn. Eignung: Gutachten (Anbieter)
TIP1-	Vernichtung fehlerhafter	Anb_CVC_TSP_eGK	Sich.techn.

A_2590	Chipkarten vor deren Ausgabe		Eignung: Gutachten (Anbieter)
TIP1-A_2591	Ausgabe fehlerfreier Chipkarten	Anb_CVC_TSP_eGK	Sich.techn. Eignung: Gutachten (Anbieter)
TIP1-A_2630	Protokollierung pro Bestellung/Produktionslauf (Profil gleich 0)	Anb_SMC-B	Sich.techn. Eignung: Gutachten (Anbieter)
TIP1-A_2631	Nachvollziehbarkeit bei Produktion mit Profil 0	Anb_SMC-B	Sich.techn. Eignung: Gutachten (Anbieter)
TIP1-A_2692	Protokollierung durch den TSP- CVC – Profil gleich 0	Anb_SMC-B	Sich.techn. Eignung: Gutachten (Anbieter)
TIP1-A_4222	Authentizität des öffentlichen Root-Schlüssels	Anb_CVC_TSP_eGK	Sich.techn. Eignung: Gutachten (Anbieter)

4 Änderungen in gemSpec_CAN_TI

4.1 Neue Anforderungs-Zuweisungen:

Afo-ID	Afo-Titel	betroffene(r) TSP-Produkttyp(en)	Prüfverfahren (neu)
GS-A_5115	Schutzbedarf der CAN	Anb_SMC-B	Sich.techn. Eignung: Gutachten (Anbieter)
GS-A_5116	Zufällige CAN-Erzeugung	Anb_SMC-B	Sich.techn. Eignung: Gutachten (Anbieter)
GS-A_5117	Anforderungen an Zufallsgenerator für CAN-Erzeugung	Anb_SMC-B	Sich.techn. Eignung: Gutachten (Anbieter)
GS-A_5118	CAN-Speicherung nur für die Personalisierung der Karte	Anb_SMC-B	Sich.techn. Eignung: Gutachten (Anbieter)
GS-A_5119	Sicherer Transport und Speicherung der CAN beim Kartenherausgeber bzw. Kartenpersonalisierer	Anb_SMC-B	Sich.techn. Eignung: Gutachten (Anbieter)
GS-A_5120	Verteilung der CAN auf das erforderliche Maß beschränken	Anb_SMC-B	Sich.techn. Eignung: Gutachten (Anbieter)
GS-A_5121	Karteninhaber über Umgang mit CAN informieren	Anb_SMC-B	Sich.techn. Eignung: Gutachten (Anbieter)

5 Änderungen in gemKPT_Test

5.1 Entfernte Anforderungs-Zuweisungen:

Afo-ID	Afo-Titel	betroffene(r) TSP-Produkttyp(en)	Hinweise
TIP1-A_6517-01	Eigenverantwortlicher Test: TBI	Anb_CVC_TSP_eGK	Redundanz wird entfernt. Zuweisung zu Produkttypen bleibt bestehen
TIP1-A_6519	Eigenverantwortlicher Test: Hersteller und Anbieter	Anb_CVC_TSP_eGK	Redundanz wird entfernt. Zuweisung zu Produkttypen bleibt bestehen
TIP1-A_6523	Zulassungstest: Hersteller und Anbieter	Anb_CVC_TSP_eGK	Redundanz wird entfernt. Zuweisung zu Produkttypen bleibt bestehen
TIP1-A_6524-01	Testdokumentation gemäß Vorlagen	Anb_CVC_TSP_eGK	Redundanz wird entfernt. Zuweisung zu Produkttypen bleibt bestehen
TIP1-A_6526	Produkttypen: Bereitstellung	Anb_CVC_TSP_eGK	Redundanz wird entfernt. Zuweisung zu Produkttypen bleibt bestehen
TIP1-A_6529	Produkttypen: Mindestumfang der Interoperabilitätsprüfung	Anb_CVC_TSP_eGK	Redundanz wird entfernt. Zuweisung zu Produkttypen bleibt bestehen
TIP1-A_6532	Zulassung eines neuen Produkts: Aufgaben der TDI	Anb_CVC_TSP_eGK	Redundanz wird entfernt. Zuweisung zu Produkttypen bleibt bestehen
TIP1-A_6533	Zulassung eines neuen Produkts: Aufgaben der Hersteller und Anbieter	Anb_CVC_TSP_eGK	Redundanz wird entfernt. Zuweisung zu Produkttypen

			bleibt bestehen
TIP1-A_6536	Zulassung eines geänderten Produkts: Aufgaben der TDI	Anb_CVC_TSP_eGK	Redundanz wird entfernt. Zuweisung zu Produkttypen bleibt bestehen
TIP1-A_6537	Zulassung eines geänderten Produkts: Aufgaben der Hersteller und Anbieter	Anb_CVC_TSP_eGK	Redundanz wird entfernt. Zuweisung zu Produkttypen bleibt bestehen
TIP1-A_6538	Durchführung von Produkttests	Anb_CVC_TSP_eGK	Redundanz wird entfernt. Zuweisung zu Produkttypen bleibt bestehen
TIP1-A_6539	Durchführung von Produktübergreifenden Tests	Anb_CVC_TSP_eGK	Redundanz wird entfernt. Zuweisung zu Produkttypen bleibt bestehen
TIP1-A_6772	Partnerprodukte bei Interoperabilitätstests	Anb_CVC_TSP_eGK	Redundanz wird entfernt. Zuweisung zu Produkttypen bleibt bestehen

6 Änderungen in gemSpec_OM

6.1 Entfernte Anforderungs-Zuweisungen:

Afo-ID	Afo-Titel	betroffene(r) TSP-Produkttyp(en)	Hinweise
GS-A_3813	Datenschutzvorgaben Fehlermeldungen	Anb_CVC_TSP_eGK	Zuweisungen zu entsprechenden Produkttypen bleiben erhalten

7 Änderungen in gemRL_TSL_SP_CP

7.1 Neue Anforderungen

Die folgende Anforderung inkl. Hinweis-Text darunter wird in Kap. 7.3.2 (Gültigkeitsperioden von Zertifikaten und Schlüsselpaaren) hinzugefügt:

A_26821 - Planmäßige Schlüsselerneuerung der TSP-X.509 Sub-CAs

Die Anbieter der Produkttypen TSP-X.509 nonQES MÜSSEN spätestens 3 Jahre nach der Erzeugung des letzten Sub-CA-Zertifikates für den jeweiligen Produkttypen eine planmäßige Schlüsselerneuerung einleiten und dazu mit geeignetem Vorlauf den Anbieter der gematik Root-CA kontaktieren, um eine Neu-Beantragung des jeweiligen Sub-CA-Zertifikates mit neuem Schlüssel zu veranlassen.

Hinweis: Damit wird sichergestellt, dass EE-Zertifikate von der Sub-CA ausgegeben werden können, die eine Maximal-Gültigkeit von 5 Jahren haben.

8 Änderungen in Steckbriefen

8.1 Änderungen in gemAnbT_..._PTVx.y.z-n

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemAnbT_...]. 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)
	[...]	