
C_11919_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	3
2 Änderung Zuweisung aus gemSpec_DS_Anbieter.....	4
2.1 Änderung in gemProdT_X509_TSP_nonQES_eGK_PTV.....	4
2.2 Zuweisung der Anforderung GS-A_5324-02 zum gemProdT_X509_TSP_nonQES_Komp und Trust Service Provider CVC.....	4
3 Änderung Zuweisung aus gemSpec_Krypt.....	6
3.1 Anpassung Prüfverfahren.....	6
3.1.1 Entfernen des Prüfverfahrens "Produkttest/Produktübergreifender Test".....	6
3.1.2 Wechsel Prüfverfahren auf "Sicherheitstechnische Eignung Herstellererklärung"	6
3.2 Zuweisung TSP CVC entfernen.....	6
4 Änderung Zuweisung aus gemRL_TSL_SP_CP.....	8
4.1 Ablösung GS-A_4228 durch A_26411.....	8
4.2 Zuordnung zu Produkttypsteckbriefen entfernen.....	8
4.2.1 Zuordnung zu TSP eGK, HBA, SMC-B und Komp entfernen.....	8
4.2.2 Zuordnung zu TSP Komp entfernen.....	16
4.3 Anpassung Prüfverfahren der Anforderung GS-A_4348.....	16
5 Zuweisung aus gemSpec_NET auflösen.....	17
5.1 Zuweisung Anforderung A_20574-02 auflösen.....	17
5.2 Zuweisung Anforderung GS-A_4062-01 auflösen.....	17
5.3 Zuweisung Anforderung GS-A_4054 auflösen.....	17
5.4 Zuweisung Anforderung GS-A_4879 auflösen.....	17

1 Änderungsbeschreibung

Die Anforderungen an die Trust Service Provider (TSP) entsprechen nicht den aktuellen Anforderungen oder sind einzelnen TSP-Anbietern noch nicht wirksam zugeordnet. Deshalb ist eine Überarbeitung der Anforderungen notwendig für einen stabilen Betrieb und eine Voraussetzung für zukünftige Beauftragungen.

Dazu werden Zuweisungen von Anforderungen aus SI-Spezifikationen in den Produkttypsteckbriefen vorgenommen.

2 Änderung Zuweisung aus gemSpec_DS_Anbieter

Im folgenden werden Anforderungen aus der gemSpec_DS_Anbieter bezüglich den verschiedenen TSP's harmonisiert.

2.1 Änderung in gemProdT_X509_TSP_nonQES_eGK_PTV

Die Liste folgender Anforderungen soll auch in dem Produkttypsteckbrief für X509_TSP_nonQES_eGK_PTV übernommen werden.

AFO-ID	Titel	Prüfverfahren
GS-A-3078	Anbieter einer Schlüsselverwaltung: verpflichtende Migrationsstrategie bei Schwächung kryptographischer Primitive	Sich.techn. Eignung: Gutachten
GS-A_3125	Schlüsselinstallation und Verteilung: Dokumentation gemäß Minimalitätsprinzip	Sich.techn. Eignung: Gutachten
GS-A_3130	Krypto_Schlüssel_Installation: Dokumentation der Schlüsselinstallation gemäß Minimalitätsprinzip	Sich.techn. Eignung: Gutachten
GS-A_3139	Krypto_Schlüssel: Dienst Schlüsselableitung	Sich.techn. Eignung: Gutachten
GS-A_3141	Krypto_Schlüssel_Ableitung: Maßnahmen bei Bekanntwerden von Schwächen in der Schlüsselableitungsfunktion	Sich.techn. Eignung: Gutachten
GS-A_3149	Krypto_Schlüssel_Archivierung: Dokumentation der Schlüsselarchivierung gemäß Minimalitätsprinzip	Sich.techn. Eignung: Gutachten

2.2 Zuweisung der Anforderung GS-A_5324-02 zum gemProdT_X509_TSP_nonQES_Komp und Trust Service Provider CVC

AFO-ID	Titel	Prüfverfahren
GS-A_5324-02	kDSM: Teilnahme des Anbieters an Sitzungen des kDSM	Sich.techn. Eignung: Herstellererklärung

Die oben genannte Anforderung wird den folgenden Steckbriefen zugewiesen:

- gemProdT_X509_TSP_nonQES_Komp
- gemProdT_CVC_TSP_PTV

3 Änderung Zuweisung aus gemSpec_Krypt

3.1 Anpassung Prüfverfahren

Die Prüfverfahren in diesem Abschnitt werden werden entweder entfernt, weil sie redundant sind oder aus Gründen der Konsistenz angepasst.

3.1.1 Entfernen des Prüfverfahrens "Produkttest/Produktübergreifender Test"

Entfernen des Prüfverfahrens "Produkttest/Produktübergreifender Test" für die zwei Anforderung

- A_17124-03 - TLS-Verbindungen (ECC-Migration)
- GS-A_4384-03 - TLS-Verbindungen

aus den Steckbriefen:

- TSP X.509 nonQES - eGK
- TSP X.509 nonQES - HBA
- TSP X.509 nonQES - SMC-B
- gemProdT_X509_TSP_nonQES_Komp
- TSP X.509 QES

3.1.2 Wechsel Prüfverfahren auf "Sicherheitstechnische Eignung Herstellererklärung"

Das Prüfverfahren für die Anforderung A_18464 (TLS-Verbindungen, nicht Version 1.1) wird analog zu den anderen TSPs (eGK, HBA und KOMP) von derzeit "Sich.techn. Eignung: Gutachten" auf "Sich.techn. Eignung: Herstellererklärung" im Steckbrief "gemProdT_X509_TSP_nonQES_Komp" gewechselt.

3.2 Zuweisung TSP CVC entfernen

Die Zuweisung der folgenden vier Anforderungen soll aus dem Steckbrief "gemProdT_CVC_TSP" entfernt werden, weil sie nicht zum Produkt passen:

- A_21275-01 - TLS-Verbindungen, zulässige Hashfunktionen bei Signaturen im TLS-Handshake
- GS-A_5541 - TLS-Verbindungen als TLS-Klient zur Störungsampel oder SM
- GS-A_5580-01 - TLS-Klient für betriebsunterstützende Dienste
- GS-A_5581 - "TUC vereinfachte Zertifikatsprüfung" (Komponenten-PKI)

4 Änderung Zuweisung aus gemRL_TSL_SP_CP

4.1 Ablösung GS-A_4228 durch A_26411

Die AFO GS-A_4228 wird abgelöst durch folgende neue AFO. Die AFO definiert, dass die Produkte die technische Möglichkeit bereitstellen müssen, dass Sperranträge innerhalb von 60 Minuten bearbeitet werden können. Die Verpflichtung gegenüber des Anbieters dies zu tun findet sich in AFO A_26412, welche den Anbietern zugeordnet wird via C_11942.

A_26411 - Technische Voraussetzung zur Umsetzung der Sperrfrist

Die Produkttypen gematik Root-CA und TSP-X.509 nonQES MÜSSEN die technischen Voraussetzungen schaffen, dass eine Zertifikatssperrung binnen 60 Minuten umgesetzt werden kann.[<=]

Zuordnung zu funkt. Eignung: Test Produkt/FA - gematik Root-CA, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC

4.2 Zuordnung zu Produkttypsteckbriefen entfernen

Bei den Anforderungen in diesem Kapitel handelt es sich um Anforderungen, die sich im Grunde an den Anbieter richten. Aus diesem Grund wird die Zuweisung zu einigen Produkten hier aufgelöst und im Steckbrief C_11942 den entsprechenden Anbietertypsteckbriefen zugewiesen.

4.2.1 Zuordnung zu TSP eGK, HBA, SMC-B und Komp entfernen

Die Zuweisung der Anforderung aus der Tabelle werden aus den folgenden Produkttypsteckbriefen abgelöst:

- TSP X.509 nonQES - eGK
- TSP X.509 nonQES - HBA
- TSP X.509 nonQES - SMC-B
- gemProdT_X509_TSP_nonQES_Komp

AFO-ID	Titel
GS-A_4279	Fortbestand von Archiven und die Abrufmöglichkeit einer vollständigen Widerrufsliste
GS-A_4191	Einsatz interoperabler Systeme durch einen externen Dienstleister

GS-A_4230	Gewährleistung der Online-Verfügbarkeit von Sperrinformationen
GS-A_4247	Obligatorische Vorgaben für das Rollenkonzept
GS-A_4249	Standort für Backup-HSM
GS-A_4255	Nutzung des HSM im kontrollierten Bereich
GS-A_4259	Vorgaben für die informationstechnische Trennung sicherheitskritischer Bestandteile der Systemumgebung
GS-A_4260	Manipulationsschutz veröffentlichter Daten
GS-A_4261	Vorgaben zur Betriebsumgebung für sicherheitskritische Bestandteile des Systems
GS-A_4268	Anforderungen an den Einsatz freier Mitarbeiter
GS-A_4271	Aufzeichnung von organisatorischen Ereignissen
GS-A_4272	Aufbewahrungsfrist für sicherheitsrelevante Protokolldaten
GS-A_4274	Archivierung von für den Zertifizierungsprozess relevanten Daten
GS-A_4276	Aktionen und Verantwortlichkeit im Rahmen der Notfallplanung
GS-A_4284	Beachtung des betreiberspezifischen Sicherheitskonzepts bei der Erzeugung von Schlüsselpaaren
GS-A_4285	Sicherheitsniveau bei der Generierung von Signaturschlüsseln
GS-A_4287	Sichere Aufbewahrung des privaten Schlüssels einer CA
GS-A_4288	Verwendung eines Backup-HSM zum Im-/Export von privaten Schlüsseln
GS-A_4289	Unterstützung des sicheren Löschen von Schlüsseln durch HSM

GS-A_4290	Generieren und Löschen von Schlüsselpaaren gemäß Vier-Augen-Prinzip
GS-A_4291	Berechnungen mit dem privaten Schlüssel gemäß Vier-Augen-Prinzip
GS-A_4292	Protokollierung der HSM-Nutzung
GS-A_4294	Bedienung des Schlüsselgenerierungssystems
GS-A_4295	Berücksichtigung des aktuellen Erkenntnisstands bei der Generierung von Schlüsseln
GS-A_4304	Speicherung und Anwendung von privaten Schlüsseln
GS-A_4305	Ordnungsgemäße Sicherung des privaten Schlüssels
GS-A_4306	Verwendung von privaten Schlüsseln
GS-A_4307	Vorgaben an HSM-Funktionalität
GS-A_4308	Speicherung und Auswahl von Schlüsselpaaren im HSM
GS-A_4309	Verwendung von zertifizierten kryptographischen Modulen
GS-A_4310	Vorgaben an die Prüftiefe der Evaluierung eines HSM
GS-A_4311	Hinterlegung des privaten Signaturschlüssels
GS-A_4314	Sichere Übermittlung von Aktivierungsdaten
GS-A_4315	Konformität zum betreiberspezifischen Sicherheitskonzept
GS-A_4316	Härtung von Betriebssystemen
GS-A_4317	Obligatorische Sicherheitsmaßnahmen

GS-A_4396	Speicherung hinterlegter Root- und CA-Schlüssel
GS-A_4906	Zuordnung von Schlüsseln zu Identitäten
GS-A_4186	Prüfung auf den Besitz des privaten Schlüssels bei dem Zertifikatsnehmer
GS-A_4201	Dokumentation des Registrierungsprozesses
GS-A_4202	Identifikation des Zertifikatsnehmers im Rahmen der Registrierung
GS-A_4203	Dokumentationspflichten für die Beantragung von Zertifikaten
GS-A_4188	Zuverlässige Identifizierung und vollständige Prüfung der Antragsdaten
GS-A_4190	Regelung für die Berechtigung zur Antragstellung
GS-A_4345	Automatisierte Zertifikatsanträge für Komponentenzertifikate
A_17860	OCSP-Statusauskunft bei Übernahme durch einen anderen TSP-X.509 nonQES
GS-A_4250	Verwendung des Backup-HSM gemäß Vier-Augen-Prinzip
GS-A_4252	Besetzung von Rollen und Informationspflichten
GS-A_4254	Rollenzuordnung unter Wahrung der Vier-Augen-Prinzips
GS-A_4256	Zugang zu Systemen für die Zertifikatserzeugung
GS-A_4262	Gewährleistung des Zugangs zur Betriebsstätte
GS-A_4263	Rollenunterscheidung im organisatorischen Konzept
GS-A_4264	Mitteilungspflicht für Zuordnung der Rollen

GS-A_4265	Obligatorische Rollen für sicherheitsrelevante Tätigkeiten
GS-A_4266	Ausschluss von Rollenzuordnungen
GS-A_4267	Rollenaufteilung auf Personengruppen
GS-A_4269	Einsicht in Dokumente für Mitarbeiter
GS-A_4277	Anzeigespflicht bei Beendigung der Zertifizierungsdienstleistungen
GS-A_4278	Maßnahmen zur Einstellung des Zertifizierungsbetriebs
GS-A_4281	Fristen bei der Einstellung des Zertifizierungsbetriebs für einen TSP-X.509 nonQES
GS-A_4282	Erforderliche Form bei Einstellung des Zertifizierungsbetriebs
GS-A_4283	Gültigkeit der Zertifikate bei Einstellung des Zertifizierungsbetriebs
GS-A_4296	Anlass für den Wechsel von Schlüsselpaaren
GS-A_4297	Behandlung einer Kompromittierung eines Schlüsselpaares
GS-A_4318	Maßnahmen zur Beurteilung der Systemsicherheit
GS-A_4319	Prüfpflichten vor Nutzung neuer Software im Wirkbetrieb
GS-A_4321	Bereitstellung eines Certificate Policy Disclosure Statements
GS-A_4322	Zusicherung der Dienstqualität
GS-A_4323	Wahrung der Vertraulichkeit
GS-A_4324	Zusicherung der Dienstgüte

GS-A_4325	Zweckbindung von Zertifikaten
GS-A_4326	Dokumentationspflicht für beschränkte Gültigkeit
GS-A_4327	Transparenz für Nachträge zum Certificate Policy Statement
GS-A_4328	Informationspflicht bei Änderung des CPS
GS-A_4332	Dokumentation der Pflichten des Antragstellers eines Komponentenzertifikats
GS-A_4394	Dokumentation der Zertifikatsausgabeprozesse
A_17861	Aufnahme der OCSP- und CRL-Signerzertifikate der TI in die TSL
GS-A_4174	Veröffentlichung von CA- und Signer-Zertifikaten
GS-A_4175	Veröffentlichungspflicht für kritische Informationen
GS-A_4176	Mitteilungspflicht bei Änderungen
GS-A_4177	Zugriffskontrolle auf Verzeichnisse
GS-A_4178	Standardkonforme Namensvergabe in Zertifikaten
GS-A_4179	Format von E-Mail-Adressen in Zertifikaten
GS-A_4180	Gestaltung der Struktur der Verzeichnisdienste
GS-A_4181	Eindeutigkeit der Namensform des Zertifikatsnehmers
GS-A_4183	Kennzeichnung von maschinen-, rollenbezogenen oder pseudonymisierten (nicht personenbezogenen) Zertifikaten
GS-A_4185	Unterscheidung von Zertifikaten
GS-	Prüfung der Berechtigung zur Antragstellung auf Schlüsselerneuerung

A_4192	
GS-A_4195	Schriftform für Aufnahme eines Zertifikats in die TSL
GS-A_4199	Berechtigung für Beantragung von CA-Zertifikaten
GS-A_4207	Vorgaben für die Ausgabe von Endnutzerzertifikaten
GS-A_4211	Bereitstellung von CA-Zertifikaten bei Aufnahme in die TSL
GS-A_4212	Verwendung des privaten Schlüssels durch den Zertifikatsnehmer
GS-A_4214	Veröffentlichung der öffentlichen Schlüssel durch den TSP-X.509 nonQES
GS-A_4219-01	Sperrung von Anwenderzertifikaten
GS-A_4221	Anzeige der Kompromittierung des privaten Signaturschlüssels
GS-A_4227	Dokumentation der Fristen für einen Sperrantrag
GS-A_4231	Anforderungen zur Online-Prüfung von Sperrinformationen
GS-A_4238	Funktionsbeschreibung des Statusabfragedienstes
GS-A_4245	Anzeige von Änderung an der Gesellschafterstruktur des Betreibers
GS-A_4248	Bereitstellung der Protokollierungsdaten
GS-A_4299	Zulassung/Abnahme und Aufnahme in den Vertrauensraum der TI
GS-A_4300	Zweckbindung von Schlüsselpaaren
GS-A_4302	Transportmedium für die Übergabe des privaten Schlüssels eines Schlüsselpaars

GS-A_5083	Zertifikatsantragstellung im Vier-Augen-Prinzip
GS-A_5084	Zugang zu HSM-Systemen im Vier-Augen-Prinzip
GS-A_4182	Kennzeichnung von personen- bzw. organisationsbezogenen Zertifikaten
GS-A_4187	Nutzung bestehender SGB-Datensätze bei Registrierung für Endanwender (Versicherte)
GS-A_4234	Zusammenhang zwischen Zertifikatssperrung und -suspendierung
GS-A_4235	Festlegung zu Verantwortlichkeit für Suspendierung
GS-A_4236	Verfahren für Anträge auf Suspendierung
GS-A_4237	Festlegung zu maximaler Dauer von Suspendierungen
GS-A_4189	Prüfungspflicht für Person, Schlüsselpaar, Schlüsselaktivierungsdaten und Name
GS-A_4241	Sperrung von Zertifikaten bei Kündigung durch den Zertifikatsnehmer
GS-A_4210	Dokumentation der Annahme eines Zertifikatsantrags und der sicheren Ausgabe des Zertifikats
GS-A_4215	Bedingungen für eine Zertifizierung nach Schlüsselerneuerung
GS-A_4218	Beschreibung der Bedingungen für die Sperrung eines Anwenderzertifikats
GS-A_4226	Verfahren für einen Sperrantrag
GS-A_4229	Methoden zum Prüfen von Sperrinformationen
GS-A_4242	Dokumentationspflicht für Prozesse der Schlüssel hinterlegung
GS-A_4251	Backup-Konzept

GS-A_4208	Ausgabe von Zertifikaten
GS-A_4225	Festlegung eines Sperrberechtigten für Endanwenderzertifikate
GS-A_4395	Benachrichtigung des Zertifikatsnehmer

4.2.2 Zuordnung zu TSP Komp entfernen

Die Zuweisung der Anforderung aus der Tabelle werden aus den folgenden Produkttypsteckbriefen abgelöst:

- gemProdT_X509_TSP_nonQES_Komp

AFO-ID	Titel
GS-A_4331	Sicherstellungspflicht des Antragstellers eines Komponentenzertifikats
GS-A_4337	Sonderregelung für die Sperrung von Komponentenzertifikaten
GS-A_4340	Befristung von Sperranträgen für Komponentenzertifikate
GS-A_4344	Sperrung von Komponentenzertifikate bei Schließung eines TSP-X.509 nonQES
GS-A_4333	Informationspflicht gegenüber Antragsteller bei Sperrung eines Komponentenzertifikats
GS-A_4336	Sperranträge der gematik für Komponentenzertifikate

4.3 Anpassung Prüfverfahren der Anforderung GS-A_4348

Das Prüfverfahren der Anforderung GS-A_4348 (Verbot der Erneuerung von Zertifikaten), wird von 'funkt. Eignung: Test Produkt/FÄ' auf 'sich.techn. Eignung: Herstellererklärung' gewechselt.

5 Zuweisung aus gemSpec_NET auflösen

5.1 Zuweisung Anforderung A_20574-02 auflösen

Die Zuweisung der Anforderung A_20574-02 (Beachtung der ISI-LANA für Übergänge zu Fremdnetzen) wird aus den folgenden Steckbriefen aufgelöst:

- TSP X.509 nonQES - HBA
- TSP X.509 nonQES - SMC-B

5.2 Zuweisung Anforderung GS-A_4062-01 auflösen

Die Zuweisung der Anforderung GS-A_4062-01 (Sicherheitsanforderungen für Netzübergänge zu Fremdnetzen) wird aus den folgenden Steckbriefen aufgelöst:

- TSP X.509 nonQES - HBA
- TSP X.509 nonQES - SMC-B
- TSP X.509 nonQES - gSMC-x, FD, ZD

5.3 Zuweisung Anforderung GS-A_4054 auflösen

Die Zuweisung der Anforderung GS-A_4054 (Paketfilter Default Deny) wird aus den folgenden Steckbriefen aufgelöst:

- TSP X.509 nonQES - HBA
- TSP X.509 nonQES - SMC-B
- TSP X.509 nonQES - gSMC-x, FD, ZD

5.4 Zuweisung Anforderung GS-A_4879 auflösen

Die Zuweisung der Anforderung GS-A_4879 (DNSSEC, Zonen im Namensraum Internet mittels DNSSEC sichern) wird aus den folgenden Steckbriefen aufgelöst:

- TSL-Dienst
- TSP X.509 nonQES - gSMC-x, FD, ZD