
C_12742_Anlage

Inhaltsverzeichnis

1 **Änderungsbeschreibung.....2**

2 **1.1 Änderungen in gemSpec_X.509_TSP.....2**

3 1.1.1 (Kap. 6.6) Erneuerung von Zertifikaten der gSMC-K.....2

4 **1.2 Änderungen in gemSpec_CVC_TSP.....4**

5 1.2.1 (Kap. 5.2) Erneuerung von CV-Zertifikaten der gSMC-K.....4

6 **2 Änderungen in Steckbriefen.....5**

7 **2.1 Änderungen in gemProdT_X509_TSP_nonQES_Komp.....5**

8 **2.2 Änderungen in gemProdT_CVC_TSP.....5**

1 Änderungsbeschreibung

Zur Verlängerung der Lebensdauer von Konnektoren wurde im Jahre 2022 das Feature "Laufzeitverlängerung gSMC-K" spezifiziert. Dazu wurde die Verlängerung von gSMC-K-Zertifikaten um 3 Jahre für den TSP für Komponenten spezifiziert und im Jahre 2023 beim AZPD veranlasst für Konnektoren mit gSMC-K-Zertifikaten, die bis zum Jahresende 2020 ausgegeben wurden.

Dieses Feature wurde bereits im Jahr 2025 auf Konnektoren erweitert, deren Zertifikate in den Jahren 2021 und 2022 ausgegeben wurden.

Um eine Weiterverwendung von Konnektoren zu gewährleisten, die im Jahr 2023 produziert wurden und somit in 2028 unbrauchbar werden würden, wird für diese ergänzend eine Laufzeitverlängerung ermöglicht. Dabei werden allerdings nur die ECC-Zertifikate erneuert, da die Verwendung von RSA-Zertifikaten nicht mehr gegeben sein wird. Das Laufzeitende der erneuerten Zertifikate wird dabei auf Ende 2030 terminiert.

Die Änderungen beschreiben die Anpassungen für den TSP für Komponenten (TSP X.509 und TSP CVC), die sich durch die neuen Daten ergeben und sind damit Basis der erneuten Beauftragung der gSMC-K Zertifikatsverlängerung.

1.1 Änderungen in gemSpec_X.509_TSP

1.1.1 (Kap. 6.6) Erneuerung von Zertifikaten der gSMC-K

Die Anforderung A_21765-03 ersetzt die A_21765-02:

Alte Afo:

A_21765-02 -Erneuerung von gSMC-K-Zertifikaten: Zeitliche Vorgabe

Ein TSP-X.509 nonQES für Komponenten MUSS zur Erneuerung von Zertifikaten der gSMC-K (C.NK.VPN, C.AK.AUT und C.SAK.AUT) den Erneuerungsprozess auf Antrag der gematik einleiten. Dazu MÜSSEN alle Zertifikate der gSMC-K erneuert werden, wenn die Zertifikate der Karte in den Jahren 2020, 2021 oder 2022 ausgegeben wurden. Als Laufzeitende MUSS je nach Ausgabejahr der zu erneuernden Zertifikate das folgende Laufzeitende-Datum gesetzt werden:

- Zertifikate ausgegeben in 2020: Laufzeitende wird auf 31.12.2027 gesetzt.
- Zertifikate ausgegeben in 2021: Laufzeitende wird auf 31.12.2028 gesetzt.
- Zertifikate ausgegeben in 2022: Laufzeitende wird auf 29.11.2029 gesetzt.

[<=,TSP X.509 nonQES - gSMC,funkt. Eignung: Test Produkt/FA]

Neue Afo:

A_21765-03 -Erneuerung von gSMC-K-Zertifikaten: Zeitliche Vorgabe

Ein TSP-X.509 nonQES für Komponenten MUSS zur Erneuerung von Zertifikaten der gSMC-K (C.NK.VPN, C.AK.AUT und C.SAK.AUT) den Erneuerungsprozess auf Antrag der gematik einleiten. Dazu MÜSSEN alle Zertifikate der gSMC-K erneuert werden, wenn die Zertifikate der Karte in den Jahren 2020, 2021 oder 2022 ausgegeben wurden. Es MÜSSEN nur die

ECC-Zertifikate erneuert werden (keine RSA-Zertifikate), wenn die Zertifikate der Karte im Jahr 2023 ausgegeben wurden. Als Laufzeitende MUSS je nach Ausgabejahr der zu erneuernden Zertifikate das folgende Laufzeitende-Datum gesetzt werden:

- Zertifikate ausgegeben in 2020: Laufzeitende wird auf 31.12.2027 gesetzt.
- Zertifikate ausgegeben in 2021: Laufzeitende wird auf 31.12.2028 gesetzt.
- Zertifikate ausgegeben in 2022: Laufzeitende wird auf 29.11.2029 gesetzt.
- Zertifikate ausgegeben in 2023: Laufzeitende wird auf 31.12.2030 gesetzt.

[<=,TSP X.509 nonQES - gSMC,funkt. Eignung: Test Produkt/FA]

Die Anforderung A_21769-01 ersetzt die A_21769:

Alte Afo:

A_21769 -Erneuerung von gSMC-K-Zertifikaten: Datei-Namen für X.509-Zertifikate

Ein TSP-X.509 nonQES für Komponenten MUSS zur Erneuerung von Zertifikaten der gSMC-K die Zertifikate jeweils in einer Zertifikats-Datei des Formats PEM bereitstellen und das folgende Namensformat verwenden - die ICCSN wird dabei als Variable für die Zuordnung der jeweiligen gSMC-K mit angegeben:

- C.NK.VPN_RSA_<ICCSN>.pem
- C.AK.AUT_RSA_<ICCSN>.pem
- C.SAK.AUT_RSA_<ICCSN>.pem

Wenn auch X.509-Zertifikate als ECC vorhanden sind und damit erneuert werden, dann werden diese wie folgt bereitgestellt:

- C.NK.VPN_ECC_<ICCSN>.pem
- C.AK.AUT_ECC_<ICCSN>.pem
- C.SAK.AUT_ECC_<ICCSN>.pem

[<=,TSP X.509 nonQES - gSMC,funkt. Eignung: Test Produkt/FA]

Neue Afo:

A_21769-01 -Erneuerung von gSMC-K-Zertifikaten: Datei-Namen für X.509-Zertifikate

Ein TSP-X.509 nonQES für Komponenten MUSS zur Erneuerung von Zertifikaten der gSMC-K die Zertifikate jeweils in einer Zertifikats-Datei des Formats PEM bereitstellen und das folgende Namensformat verwenden - die ICCSN wird dabei als Variable für die Zuordnung der jeweiligen gSMC-K mit angegeben:

- C.NK.VPN_ECC_<ICCSN>.pem
- C.AK.AUT_ECC_<ICCSN>.pem
- C.SAK.AUT_ECC_<ICCSN>.pem

Falls auch X.509-Zertifikate als RSA verlängert werden (nur bei Zertifikatausgabe bis Ende 2022), dann werden diese wie folgt bereitgestellt:

- C.NK.VPN_RSA_<ICCSN>.pem
- C.AK.AUT_RSA_<ICCSN>.pem
- C.SAK.AUT_RSA_<ICCSN>.pem

[<=,TSP X.509 nonQES - gSMC,funkt. Eignung: Test Produkt/FA]

1.2 Änderungen in gemSpec_CVC_TSP

1.2.1 (Kap. 5.2) Erneuerung von CV-Zertifikaten der gSMC-K

Die Anforderung A_21774-03 ersetzt die A_21774-02:

Alte Afo:

A_21774-02 -Erneuerung von CV-Zertifikaten der gSMC-K: Profile, CHR und CXD

Ein TSP-CVC für Komponenten MUSS bei der Erneuerung der CV-Zertifikate der gSMC-K (C.SMC.AUT_CVC und C.SAK.AUTD_CVC) dieselben Zugriffsprofile (0 und 51) und vor allem denselben CHR (inkl. ICCSN-Bezug) verwenden. Als Certificate Expiration Date (CXD) MUSS je nach Ausgabejahr der zu erneuernden Zertifikate das folgende Laufzeitende-Datum gesetzt werden:

- Zertifikate ausgegeben in 2020: Laufzeitende wird auf 31.12.2027 gesetzt.
- Zertifikate ausgegeben in 2021: Laufzeitende wird auf 31.12.2028 gesetzt.
- Zertifikate ausgegeben in 2022: Laufzeitende wird auf 30.11.2029 gesetzt.

[<=,TSP-CVC,funkt. Eignung: Test Produkt/FA]

Neue Afo:

A_21774-03 -Erneuerung von CV-Zertifikaten der gSMC-K: Profile, CHR und CXD

Ein TSP-CVC für Komponenten MUSS bei der Erneuerung der CV-Zertifikate der gSMC-K (C.SMC.AUT_CVC und C.SAK.AUTD_CVC) dieselben Zugriffsprofile (0 und 51) und vor allem denselben CHR (inkl. ICCSN-Bezug) verwenden. Als Certificate Expiration Date (CXD) MUSS je nach Ausgabejahr der zu erneuernden Zertifikate das folgende Laufzeitende-Datum gesetzt werden:

- Zertifikate ausgegeben in 2020: Laufzeitende wird auf 31.12.2027 gesetzt.
- Zertifikate ausgegeben in 2021: Laufzeitende wird auf 31.12.2028 gesetzt.
- Zertifikate ausgegeben in 2022: Laufzeitende wird auf 30.11.2029 gesetzt.
- Zertifikate ausgegeben in 2023: Laufzeitende wird auf 31.12.2030 gesetzt.

[<=,TSP-CVC,funkt. Eignung: Test Produkt/FA]

2 Änderungen in Steckbriefen

2.1 Änderungen in gemProdT_X509_TSP_nonQES_Komp

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments. 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)
A_21765-02	Erneuerung von gSMC-K-Zertifikaten: Zeitliche Vorgabe	gemSpec_X.509_TSP
A_21765-03	Erneuerung von gSMC-K-Zertifikaten: Zeitliche Vorgabe	gemSpec_X.509_TSP

2.2 Änderungen in gemProdT_CVC_TSP

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

Tabelle 2: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_21774-02	Erneuerung von CV-Zertifikaten der gSMC-K: Profile, CHR und CXD	gemSpec_CVC_TSP
A_21774-03	Erneuerung von CV-Zertifikaten der gSMC-K: Profile, CHR und CXD	gemSpec_CVC_TSP