
C_12553 - Anbieter TSP eGK: Fortwährende Datenübertragung von Zertifikats-Hashes zum PoPP- Service

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Änderung in gemSpec_X.509_TSP.....	3
2.1 6.7 Übertragung von Zertifikats-Hash-Daten an PoPP-Service durch den Anbieter TSP eGK.....	3
3 Änderung in gemSpec_OLD.....	4
4 Änderungen in Steckbriefen.....	8
4.1 Änderungen in gemAnbT_X509_TSP_eGK.....	8
4.2 Änderungen in gemProdT_X509_TSP_nonQES_Komp.....	8

1 Änderungsbeschreibung

Zur Umsetzung der PoPP-Lösung (Proof of Patient Presence) benötigt der PoPP-Service Informationen zu eGK-Zertifikaten, um diese in einer eGK-Hash-Datenbank zu verwalten. Dazu muss der Anbieter TSP eGK Zertifikatsinformationen über seine ausgegebenen X.509- und CVC-Zertifikate regelmäßig übermitteln. Er muss daher SHA-256 Hashwerte der beiden Zertifikate X.509-AUT und CVC für jede neu ausgegebene eGK übertragen und dabei die vom PoPP-Service bereitgestellte Schnittstelle nutzen. Diese Änderung beschreibt die Anforderungen an den Anbieter TSP eGK, um die CertHash-Schnittstelle des PoPP-Service zur Übertragung zu nutzen.

2 Änderung in gemSpec_X.509_TSP

Es wird ein neues Kapitel 6.7 eingefügt

2.1 6.7 Übertragung von Zertifikats-Hash-Daten an PoPP-Service durch den Anbieter TSP eGK

Zur Umsetzung der PoPP-Lösung (Proof of Patient Presence) benötigt der PoPP-Service Informationen zu eGK-Zertifikaten, um diese in einer eGK-Hash-Datenbank zu verwalten. Dazu muss der Anbieter TSP eGK SHA-256-Hashwerte seiner X.509-AUT- und CVC-Zertifikate regelmäßig übermitteln.

Die Vorgaben zur Bildung und Übertragung der Zertifikats-Hashwerte und damit der Befüllung der im PoPP-Service vorhandenen eGK-Hash-Datenbank ist in der "Spezifikation Proof of Patient Presence (PoPP)-Service (Stufe 1)" - gemSpec_PoPP_Service in Kapitel 6.1.1.9.4 "Use Cases zur Befüllung durch Kostenträger" beschrieben und muss von den Anbietern TSP eGK beachtet werden, die im Sinne der PoPP-Spezifikation als Lieferant die folgende Anforderung erfüllen müssen:

A_28581 -Anbieter TSP eGK: Lieferung von Zertifikats-Hash-Daten an PoPP-Service

Der Anbieter TSP eGK MUSS Zertifikats-Hash-Daten der X.509- und CV-Zertifikate gemäß A_27045 unter Nutzung folgender Zertifikats-Informationen einliefern:

1. Als TSL-Client-Zertifikat wird ein Zertifikat des Typs C.FD.TLS-C (als ECC-NIST) mit der Rolle oid_tsp_egk verwendet.
2. Zum Signieren der Nachrichten wird ein Zertifikat des Typs C.FD.OSIG (als ECC-NIST) mit der Rolle oid_tsp_egk verwendet.

[<=,Anb_X.509_TSP_eGK,organ./betriebl. Eignung: Anbietererklärung]

Hinweis: Beide Zertifikate müssen bei der Komponenten-PKI beantragt werden.

3 Änderung in gemSpec_OID

GS-A_4446-17 -OID-Festlegung für technische Rollen

Ein TSP-X.509 MUSS die technischen Rollen für die Nutzung in X.509-Zertifikaten der TI mit OIDs entsprechend der Tabelle Tab_PKI_406-* referenzieren.

Tabelle 1: Tab_PKI_406-* OID-Festlegung technische Rolle in X.509-Zertifikaten

OID-Referenz in anderen Dokumenten	ProfessionItem (Beschreibung der technischen Rolle)	ProfessionOID (OID der technischen Rolle)	Zertifikatsprofil(e) in denen die ProfessionOID im Element Admission vorkommen darf
oid_vsdd	Versichertenstammdatendienst	1.2.276.0.76.4.97	C.FD.TLS-S
oid_ocsp	Online Certificate Status Protocol	1.2.276.0.76.4.99	In keinem Zertifikatsprofil verwendet.
oid_cms	Card Management System	1.2.276.0.76.4.100	C.FD.TLS-S
oid_ufs	Update Flag Service	1.2.276.0.76.4.101	C.FD.TLS-S
oid_ak	Anwendungskonnektor	1.2.276.0.76.4.103	C.AK.AUT
oid_nk	Netzkonnektor	1.2.276.0.76.4.104	C.NK.VPN
oid_kt	Kartenterminal	1.2.276.0.76.4.105	C.SMKT.AUT
oid_sak	Signaturanwendungskomponente	1.2.276.0.76.4.119	C.SAK.AUT
oid_int_vsdm	Intermediär VSDM	1.2.276.0.76.4.159	C.FD.TLS-S, C.FD.TLS-C
oid_konfigdienst	Konfigurationsdienst	1.2.276.0.76.4.160	C.ZD.TLS-S
oid_vpnz_ti	VPN-Zugangsdienst-TI	1.2.276.0.76.4.161	C.VPNK.VPN C.ZD.TLS-S

oid_vpnz_sis	VPN-Zugangsdienst-SIS	1.2.276.0.76.4.1 66	C.VPNK.VPN-SIS
oid_cmfd	Clientmodul	1.2.276.0.76.4.1 74	C.CM.TLS-CS
oid_vzd_ti	Verzeichnisdienst-TI	1.2.276.0.76.4.1 71	C.ZD.TLS-S C.FD.SIG
oid_komle	KOM-LE Fachdienst	1.2.276.0.76.4.1 72	C.FD.TLS-S C.FD.TLS-C
oid_komle-recipient-emails	KOM-LE S/MIME Attribut recipient-emails	1.2.276.0.76.4.1 73	In keinem Zertifikatsprofil verwendet.
oid_stamp	Betriebsdatenerfassung <i>Hinweis: Wurde ehemals für Störungssampel verwendet</i>	1.2.276.0.76.4.1 84	C.ZD.TLS-S
oid_tsl_ti	TSL-Dienst-TI	1.2.276.0.76.4.1 89	C.ZD.TLS-S
oid_wadg	Weitere elektronische Anwendungen des Gesundheitswesens sowie für die Gesundheitsforschung n. P. 291a Abs. 7 Satz 3 SGB V	1.2.276.0.76.4.1 98	C.FD.TLS-S C.FD.SIG C.FD.AUT C.FD.ENC
oid_epa_authn	ePA Authentisierung	1.2.276.0.76.4.2 04	C.FD.TLS-S C.FD.SIG
oid_epa_authz	ePA Autorisierung	1.2.276.0.76.4.2 05	C.FD.TLS-S C.FD.SIG
oid_epa_dvw	ePA Dokumentenverwaltung	1.2.276.0.76.4.2 06	C.FD.TLS-S
oid_epa_mgmt	ePA Management	1.2.276.0.76.4.2 07	C.FD.TLS-S C.FD.TLS-C
oid_epa_recover y	ePA automatisierter Berechtigungserhalt	1.2.276.0.76.4.2 08	C.FD.ENC
oid_epa_vau	ePA vertrauenswürdige Ausführungsumgebung	1.2.276.0.76.4.2 09	C.FD.AUT C.FD.ENC C.FD.SIG
oid_vz_tsp	Zertifikatsverzeichnis TSP X.509	1.2.276.0.76.4.2 15	In keinem Zertifikatsprofil verwendet.

oid_whk1_hsm	HSM Wiederherstellungskomponente 1	1.2.276.0.76.4.2 16	In keinem Zertifikatsprofil verwendet.
oid_whk2_hsm	HSM Wiederherstellungskomponente 2	1.2.276.0.76.4.2 17	In keinem Zertifikatsprofil verwendet.
oid_whk	Wiederherstellungskomponente	1.2.276.0.76.4.2 18	In keinem Zertifikatsprofil verwendet.
oid_sgd1_hsm	HSM Schlüsselgenerierungsdienst 1	1.2.276.0.76.4.2 19	C.SGD- HSM.AUT
oid_sgd2_hsm	HSM Schlüsselgenerierungsdienst 2	1.2.276.0.76.4.2 20	C.SGD- HSM.AUT
oid_sgd	Schlüsselgenerierungsdienst	1.2.276.0.76.4.2 21	C.FD.TLS-S
oid_erp-vau	E-Rezept vertrauenswürdige Ausführungsumgebung	1.2.276.0.76.4.2 58	C.FD.ENC C.FD.AUT
oid_erezept	E-Rezept	1.2.276.0.76.4.2 59	C.FD.TLS-S C.FD.SIG C.FD.OSIG C.FD.TLS-C
oid_idpd	IDP-Dienst	1.2.276.0.76.4.2 60	C.FD.TLS-S C.FD.SIG
oid_epa_logging	ePA-Aktensystem-Logging	1.2.276.0.76.4.2 61	C.FD.SIG
oid_bestandsnetze	Bestandsnetze.xml Signatur	1.2.276.0.76.4.2 88	C.ZD.SIG
oid_epa_vst	ePA Vertrauensstelle	1.2.276.0.76.4.2 89	C.FD.TLS-S C.FD.ENC C.FD.AUT
oid_epa_fdz	ePA Forschungsdatenzentrum	1.2.276.0.76.4.2 90	C.FD.TLS-S C.FD.ENC C.FD.AUT
oid_tim	TI-Messenger	1.2.276.0.76.4.2 94	C.FD.SIG
oid_hsk	Highspeed-Konnektor	1.2.276.0.76.4.3 02	C.HSK.SIG C.HSK.ENC

oid_idpd_sek	sektoraler IDP	1.2.276.0.76.4.3 07	C.FD.SIG
oid_tigw_zugm	TI-Gateway Zugangsmodul	1.2.276.0.76.4.3 09	C.FD.OSIG C.FD.TLS-S
oid_zert_smb	Technische Zertifikatsausgabestelle eines Anbieters SMC-B	1.2.276.0.76.4.3 10	C.FD.TLS-C
oid_popp	Proof of Patient Presence (PoPP) Dienst	1.2.276.0.76.4.2 93	C.ZD.SIG
oid_popp-token	Token-Signatur-Identität für Proof of Patient Presence	1.2.276.0.76.4.3 20	C.ZD.SIG
oid_pki-ver	PKI Change Verifikation	1.2.276.0.76.4.3 22	C.GEM.VER
oid_dipag-vau	Digitale Patientenrechnung vertrauenswü rdige Ausführungsumgebung	1.2.276.0.76.4.3 23	C.FD.AUT
oid_zeta-guard	ZETA Guard	1.2.276.0.76.4.3 24	C.FD.AUT C.FD.TLS-C
oid_tsp_egk	Technische Zertifikatsausgabestelle eines Anbieters EGK	1.2.276.0.76.4.3 xx	C.FD.OSIG C.FD.TLS-C

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

4 Änderungen in Steckbriefen

4.1 Änderungen in gemAnbT_X509_TSP_eGK

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments gemAnbT_X509_TSP_eGK. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 2: Festlegungen zur betrieblichen Eignung "Anbietererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_28581	Anbieter TSP eGK: Lieferung von Zertifikats-Hash-Daten an PoPP-Service	gemSpec_X.509_TSP

4.2 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 gemProdT_X509_TSP_nonQES_Komp. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 3: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4446-17	OID-Festlegung für technische Rollen	gemSpec_OID
GS-A_4446-16	OID-Festlegung für technische Rollen	gemSpec_OID