

Änderung in gemSpec_PKI

Es wird das Kapitel 5.8.3.2 neu aufgenommen und wie folgt befüllt:

5.8.3.2 C.ZD.SIG Signatur für Zentrale Dienste

A_22834 - Umsetzung Zertifikatsprofil C.ZD.SIG

Der TSP-X.509 nonQES MUSS C.ZD.SIG gemäß Tab_PKI_278 umsetzen.

Tabelle 1: Tab_PKI_278 C.ZD.SIG Signatur Zentrale Dienste

Element	Inhalt	Kar.	
certificate	C.ZD.SIG		
tbsCertificate			
version	2 (v3)		
serialNumber	gemäß [RFC5280#4.1.2.2.]		
signature	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS-A_4359]		
issuer	DN der ausstellenden CA		
validity	Gültigkeit des Zertifikats (von - bis)		
subject			
commonName	Name des Dienstes gemäß Zuweisung	1	
serialNumber	bei Bedarf zur Unterscheidung gleichartiger Instanzen	0-1	
organizationName	Name des verantwortlichen Anbieters	1	
countryName	Land der Anschrift des verantwortlichen Anbieters	1	
andere Attribute		0	
subjectPublicKeyInfo	Algorithmus gemäß [gemSpec_Krypt#GS-A_4359] und individueller Wert des öffentlichen Schlüssels des Zertifikatsinhabers		
extensions			critical
SubjectKeyIdentifier {2 5 29 14}	keyIdentifier = ID des öffentlichen Schlüssels des Zentralen Dienstes	1	FALSE
KeyUsage {2 5 29 15}	<i>nonRepudiation</i>	1	TRUE

SubjectAltNames {2 5 29 17}	bei überlangem organizationName: Langname des Anbieters	0-1	FALSE
BasicConstraints {2 5 29 19}	ca = FALSE	1	TRUE
CertificatePolicies {2 5 29 32}	policyIdentifier = <oid_policy_gem_or_cp> policyQualifierInfo = http://www.gematik.de/go/policies (URL zur Publikation der Zertifikatsrichtlinie) policyIdentifier = <oid_zd_sig>	1 0-1 1	FALSE
CRLDistributionPoints {2 5 29 31}	keine Festlegung	0-1	FALSE
AuthorityInfoAccess {1 3 6 1 5 5 7 1 1}	URL für OCSP-Statusdienst	1	FALSE
AuthorityKeyIdentifier {2 5 29 35}	keyIdentifier = ID des öffentlichen Schlüssels der ausstellenden CA	1	FALSE
Admission {1 3 36 8 3 3}	professionItem = Beschreibung der technischen Rolle gemäß [gemSpec_OID#GS-A_4446] professionOID = OID der technischen Rolle gemäß [gemSpec_OID#GS-A_4446]	1 1	FALSE
ExtendedKeyUsage {2 5 29 37}		0	FALSE
<i>andere Erweiterungen</i>		0	
signatureAlgorithm	zur Signatur des Zertifikats verwendeter Algorithmus gemäß [gemSpec_Krypt#GS- A_4359]		
signature	Wert der Signatur		

[<=]

Änderung in gemSpec_OID

Es wird Kapitel 3.5.3 wie folgt angepasst:

GS-A_4445-06 - OID-Festlegung für Zertifikatstypen

Ein TSP-X.509 MUSS die Zertifikatstypen für die Nutzung in X.509-Zertifikaten der TI mit OIDs entsprechend der Tabelle Tab_PKI_405-03 referenzieren.

[<=]

Tabelle 2: Tab_PKI_405-03 OID-Festlegung Zertifikatstyp in X.509-Zertifikaten

OID-Referenz in anderen Dokumenten	Name des Zertifikatstyp	Zertifikatstyp-OID	Spezifiziert in
oid_egk_qes	C.CH.QES	1.2.276.0.76.4.66	[gemSpec_PKI]
oid_egk_sig	C.CH.SIG	1.2.276.0.76.4.67	nur zu Testzwecken
oid_egk_enc	C.CH.ENC	1.2.276.0.76.4.68	[gemSpec_PKI]
oid_egk_encv	C.CH.ENCV	1.2.276.0.76.4.69	[gemSpec_PKI]
oid_egk_aut	C.CH.AUT	1.2.276.0.76.4.70	[gemSpec_PKI]
oid_egk_autn	C.CH.AUTN	1.2.276.0.76.4.71	[gemSpec_PKI]
oid_egk_enc_alt	C.CH.ENC_ALT	1.2.276.0.76.4.211	derzeit nicht verwendet
oid_egk_aut_alt	C.CH.AUT_ALT	1.2.276.0.76.4.212	[gemSpec_PKI]
oid_hba_qes	C.HP.QES	1.2.276.0.76.4.72	[CertsBÄK#1]
oid_hba_sig	C.HP.SIG	1.2.276.0.76.4.73	nur zu Testzwecken
oid_hba_enc	C.HP.ENC	1.2.276.0.76.4.74	[CertsBÄK#1]
oid_hba_aut	C.HP.AUT	1.2.276.0.76.4.75	[CertsBÄK#1]
oid_smc_b_enc	C.HCI.ENC	1.2.276.0.76.4.76	[gemSpec_PKI]
oid_smc_b_aut	C.HCI.AUT	1.2.276.0.76.4.77	[gemSpec_PKI]
oid_smc_b_osig	C.HCI.OSIG	1.2.276.0.76.4.78	[gemSpec_PKI]

oid_ak_aut	C.AK.AUT	1.2.276.0.76.4.79	[gemSpec_PKI]
oid_nk_vpn	C.NK.VPN	1.2.276.0.76.4.80	[gemSpec_PKI]
oid_vpnk_vpn	C.VPNK.VPN	1.2.276.0.76.4.81	[gemSpec_PKI]
oid_smkt_aut	C.SMKT.AUT	1.2.276.0.76.4.82	[gemSpec_PKI]
oid_sak_aut	C.SAK.AUT	1.2.276.0.76.4.113	[gemSpec_PKI]
oid_cm_tls_c	C.CM.TLS-CS	1.2.276.0.76.4.175	[gemSpec_PKI]
oid_fd_tls_c	C.FD.TLS-C	1.2.276.0.76.4.168	[gemSpec_PKI]
oid_fd_tls_s	C.FD.TLS-S	1.2.276.0.76.4.169	[gemSpec_PKI]
oid_fd_aut	C.FD.AUT	1.2.276.0.76.4.155	[gemSpec_PKI]
oid_zd_tls_c	C.ZD.TLS-C	1.2.276.0.76.4.156	derzeit nicht verwendet
oid_zd_tls_s	C.ZD.TLS-S	1.2.276.0.76.4.157	[gemSpec_PKI]
oid_zd_aut	C.ZD.AUT	1.2.276.0.76.4.158	derzeit nicht verwendet
oid_vpnk_vpn_sis	C.VPNK.VPN-SIS	1.2.276.0.76.4.165	[gemSpec_PKI]
oid_fd_sig	C.FD.SIG	1.2.276.0.76.4.203	[gemSpec_PKI]
oid_fd_enc	C.FD.ENC	1.2.276.0.76.4.202	[gemSpec_PKI]
oid_whk_hsm_aut	C.WHK-HSM.AUT	1.2.276.0.76.4.213	derzeit nicht verwendet
oid_sgd_hsm_aut	C.SGD-HSM.AUT	1.2.276.0.76.4.214	[gemSpec_PKI]
oid_vk_pt_enc	C.HP.ENC	1.2.276.0.76.4.62	[BÄK_ePA]
oid_vk_eaa_enc	C.HP.ENC	1.3.6.1.4.1.24796.1.10	[BÄK_eAA]
oid_fd_osig	C.FD.OSIG	1.2.276.0.76.4.283	[gemSpec_PKI]
oid_zd_sig	C.ZD.SIG	1.2.276.0.76.4.xxx	[gemSpec_PKI]

Hinweis: Die Zertifikatstyp-OIDs „oid_vk_pt_enc“ und „oid_vk_eaa_enc“ werden lediglich im Rahmen KIM/QES-Feldtest aufgrund der Zertifikatsprüfung HBA-Vorläuferkarten der Generation 0 (HBAqsig/ZOD2.0) durch den Konnektor verwendet. Für die Zertifikatsausstellung neuer HBA-Karten sind diese OIDs nicht relevant.

Es wird Kapitel 3.5.4 wie folgt angepasst:

GS-A_4446-06 - 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_406-02 referenzieren.

Tabelle 3: Tab_PKI_406-02 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	1.2.276.0.76.4.16 1	C.VPNK.VPN C.ZD.TLS-S
oid_vpnz_sis	VPN-Zugangsdienst-SIS	1.2.276.0.76.4.16 6	C.VPNK.VPN-SIS
oid_cmfd	Clientmodul	1.2.276.0.76.4.17 4	C.CM.TLS-CS
oid_vzd_ti	Verzeichnisdienst-TI	1.2.276.0.76.4.17 1	C.ZD.TLS-S
oid_komle	KOM-LE Fachdienst	1.2.276.0.76.4.17 2	C.FD.TLS-S C.FD.TLS-C
oid_komle-recipient-emails	KOM-LE S/MIME Attribut recipient-emails	1.2.276.0.76.4.17 3	In keinem Zertifikatsprofil verwendet.
oid_stamp	Störungssampel	1.2.276.0.76.4.18 4	C.ZD.TLS-S
oid_tsl_ti	TSL-Dienst-TI	1.2.276.0.76.4.18 9	C.ZD.TLS-S
oid_wadg	Weitere elektronische Anwendungen des Gesundheitswesens sowie für die Gesundheitsforschung n. P. 291a Abs. 7 Satz 3 SGB V	1.2.276.0.76.4.19 8	C.FD.TLS-S C.FD.SIG C.FD.AUT C.FD.ENC
oid_epa_authn	ePA Authentisierung	1.2.276.0.76.4.20 4	C.FD.TLS-S C.FD.SIG
oid_epa_authz	ePA Autorisierung	1.2.276.0.76.4.20 5	C.FD.TLS-S C.FD.SIG
oid_epa_dvw	ePA Dokumentenverwaltung	1.2.276.0.76.4.20 6	C.FD.TLS-S
oid_epa_mgmt	ePA Management	1.2.276.0.76.4.20 7	C.FD.TLS-S C.FD.TLS-C
oid_epa_recover_y	ePA automatisierter Berechtigungserhalt	1.2.276.0.76.4.20 8	C.FD.ENC
oid_epa_vau	ePA vertrauenswürdige Ausführungsumgebung	1.2.276.0.76.4.20 9	C.FD.AUT C.FD.ENC C.FD.SIG

oid_vz_tsp	Zertifikatsverzeichnis TSP X.509	1.2.276.0.76.4.215	In keinem Zertifikatsprofil verwendet.
oid_whk1_hsm	HSM Wiederherstellungskomponente 1	1.2.276.0.76.4.216	In keinem Zertifikatsprofil verwendet.
oid_whk2_hsm	HSM Wiederherstellungskomponente 2	1.2.276.0.76.4.217	In keinem Zertifikatsprofil verwendet.
oid_whk	Wiederherstellungskomponente	1.2.276.0.76.4.218	In keinem Zertifikatsprofil verwendet.
oid_sgd1_hsm	HSM Schlüsselgenerierungsdienst 1	1.2.276.0.76.4.219	C.SGD-HSM.AUT
oid_sgd2_hsm	HSM Schlüsselgenerierungsdienst 2	1.2.276.0.76.4.220	C.SGD-HSM.AUT
oid_sgd	Schlüsselgenerierungsdienst	1.2.276.0.76.4.221	C.FD.TLS-S
oid_erp-vau	E-Rezept vertrauenswürdige Ausführungsumgebung	1.2.276.0.76.4.258	C.FD.ENC
oid_erezept	E-Rezept	1.2.276.0.76.4.259	C.FD.TLS-S C.FD.SIG C.FD.OSIG
oid_idpd	IDP-Dienst	1.2.276.0.76.4.260	C.FD.TLS-S C.FD.SIG
oid_epa_logging	ePA-Aktensystem-Logging	1.2.276.0.76.4.261	C.FD.SIG
oid_bestandsnetze	Bestandsnetze.xml Signatur	1.2.276.0.76.4.xx x	C.ZD.SIG

[<=]

Änderungen in gemProdT_X509_TSP_nonQES_Komp_PTV

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 4: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_22834	Umsetzung Zertifikatsprofil C.ZD.SIG	gemSpec_PKI
GS-A_4445-03	OID-Festlegung für Zertifikatstypen	gemSpec_OID
GS-A_4445-06	OID-Festlegung für Zertifikatstypen	gemSpec_OID
GS-A_4446-05	OID-Festlegung für technische Rollen	gemSpec_OID
GS-A_4446-06	OID-Festlegung für technische Rollen	gemSpec_OID