

---

## C\_12689\_Anlage

---

# Inhaltsverzeichnis

<b>1</b>	<b>Änderungsbeschreibung.....</b>	<b>2</b>
<b>2</b>	<b>Änderung in gemSpec_OID.....</b>	<b>3</b>
2.1	in Kapitel 3.5.3 OID-Vergabe für den Zertifikatstyp.....	3
2.2	in Kapitel 3.5.4 OID-Vergabe für technische Rollen.....	5
2.3	in Kapitel 5 Anhang B - Nicht mehr verwendete OIDs.....	9
<b>3</b>	<b>Änderungen in Steckbriefen.....</b>	<b>12</b>
3.1	Änderungen in gemProdT_X509_nonQES_Komp.....	12
3.2	Änderungen in gemProdT_X509_TSP_QES, gemProdT_X509_TSP_nonQES_eGK, gemProdT_X509_TSP_nonQES_HBA, gemProdT_X509_TSP_nonQES_SMC-B.....	12

---

## 1 Änderungsbeschreibung

---

Das Zertifikat C.SGD-HSM.AUT ist gemäß dem stattgegebenen C\_12253 abgekündigt. Die Zertifikatstyp-OID "oid\_sgd\_hsm\_aut" (hinterlegt unter Extension Certificatepolicies) und die technischen Rollen-OIDs "oid\_sgd1\_hsm" und "oid\_sgd2\_hsm" (hinterlegt unter Extension Admission) werden nicht mehr benötigt. Die hier referenzierten Tabellen werden entsprechend angepasst.

Hinweis:

Die Zeilen oid\_zeta-policies, oid\_zeta-oci, oid\_ZETA-Policy-Autor, oid\_ZETA-Policy-Freigeber, oid\_ZETA-Policy-Leitstand und oid\_cdc-p15g in "Tab\_PKI\_406-\* OID-Festlegung technische Rolle in X.509-Zertifikaten" gehören zum Änderungseintrag C\_12646. Diese werden aus organisatorischen Gründen hier mit aufgeführt, damit der Suffix der aktuellen Anforderung GS-A\_4446-17 nur einmal erhöht wird.

## 2 Änderung in gemSpec\_OID

### 2.1 in Kapitel 3.5.3 OID-Vergabe für den Zertifikatstyp

#### GS-A\_4445-10 -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-\* referenzieren.

**Tabelle 1: Tab\_PKI\_405-\* 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	[gemSpec_PKI]
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
<del>oid_sgd_hsm_aut</del>	<del>C.SGD-HSM.AUT</del>	<del>1.2.276.0.76.4.214</del>	<del>[gemSpec_PKI]</del>
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	1.2.276.0.76.4.287	[gemSpec_PKI]
oid_hsk_sig	C.HSK.SIG	1.2.276.0.76.4.300	[gemSpec_PKI]
oid_hsk_enc	C.HSK.ENC	1.2.276.0.76.4.301	[gemSpec_PKI]

oid_gem-ver	C.GEM.VER	1.2.276.0.76.4.321	[gemSpec_PKI]
-------------	-----------	--------------------	---------------

39 [ $\leq$ , TSP X.509 nonQES - HBA, TSP X.509 nonQES - eGK, TSP X.509 QES, TSP X.509  
 40 nonQES - SMC-B, TSP X.509 nonQES - gSMC, funkt. Eignung: Herstellererklärung, funkt.  
 41 Eignung: Test Produkt/FA]

## 2.2 in Kapitel 3.5.4 OID-Vergabe für technische Rollen

### GS-A 4446-18 -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 2: 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	1.2.276.0.76.4.1 60	C.ZD.TLS-S
oid_vpnz_ti	VPN-Zugangsdienst-TI	1.2.276.0.76.4.1 61	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 Störungsampel 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	1.2.276.0.76.4.2	C.FD.AUT

	Ausführungsumgebung	09	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 28	C.FD.AUT C.FD.TLS-C
oid_zeta-policies	ZETA PIP/PAP Policies	1.2.276.0.76.4.3 24	C.FD.SIG
oid_zeta-oci	<del>ZETA-OCI-container-image</del> OCI container image für ZETA	1.2.276.0.76.4.3 26	C.FD.SIG
oid_zeta-pol- author	ZETA Policy Autor	1.2.276.0.76.4.3 29	C.FD.SIG
oid_zeta-pol- approv	ZETA Policy Freigeber	1.2.276.0.76.4.3 30	C.FD.SIG
oid_zeta-pol- oper	ZETA Policy Leitstand	1.2.276.0.76.4.3 31	C.FD.SIG
oid_tsp-egk	Technische Zertifikatsausgabestelle eines	1.2.276.0.76.4.3	C.FD.OSIG



	Anbieters EGK	25	C.FD.TLS-C
oid_cdc-p15g	Cyber Defense Center Pseudonymisierung	1.2.276.0.76.4.3 27	C.FD.ENC

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

## 50 **2.3 in Kapitel 5 Anhang B - Nicht mehr verwendete OIDs**

51 Gegenüber der letzten veröffentlichten Version 1.1.0 des Dokumentes wurden eine Reihe  
52 von OIDs aus dem Dokument entfernt. Diese OIDs beziehen sich auf Dienste,  
53 Anwendungen und damit verbundene technische Rollen sowie Zertifikatstypen, die für  
54 den Online-Rollout (Stufe 1) nicht relevant sind.

55 Im Kontext der OIDs für Policy-Dokumente betrifft dies Dokumente, die überarbeitet,  
56 gestrichen oder zusammengefasst wurden. Durch die Bindung der Dokumentenversion an  
57 eine OID sind damit für neue bzw. überarbeitete Dokumente auch neue OIDs notwendig.

58 Einmal zugewiesene OIDs bleiben gültig und werden vom DIMDI nicht zurückgezogen  
59 oder neu vergeben, sie können aber als "nicht mehr zu nutzen" gekennzeichnet werden.

60 Nachfolgend werden die nicht mehr verwendeten OIDs gelistet. Dies erlaubt es, an  
61 anderer Stelle referenzierte OIDs einfach zuzuordnen, ob sie weiterhin verwendet (Listung  
62 im Hauptdokument) oder nicht mehr verwendet (Listung im Anhang) werden.

63  
64 (...)
   
65  
66

**Tabelle 3: Nicht mehr verwendete OIDs - Zertifikatstyp in X.509-Zertifikaten**

OID-Referenz in anderen Dokumenten	Name des Zertifikatstyp	Zertifikatstyp-OID	Früher spezifiziert in
oid_sf_ssl	C.SF.SSL	1.2.276.0.76.4.83	[gemX.509_SD#5.7.2]
oid_sf_ssl_c	C.SF.SSL-C	1.2.276.0.76.4.84	[gemX.509_SD#5.7.2]
oid_sf_ssl_s	C.SF.SSL-S	1.2.276.0.76.4.85	[gemX.509_SD#5.7.2]
oid_sf_aut	C.SF.AUT	1.2.276.0.76.4.86	[gemX.509_SD#5.7.3]
oid_sf_enc	C.SF.ENC	1.2.276.0.76.4.87	[gemX.509_SD#5.7.5]
oid_sks_gcs	C.SKS.GCS	1.2.276.0.76.4.142	[gemPKI_SKS#4.3.7.1]
oid_sgd_hsm_aut	C.SGD-HSM.AUT	1.2.276.0.76.4.214	[gemPKI#5.11]

**Tabelle 4: Nicht mehr verwendete OIDs - technische Rolle in X.509-Zertifikaten**

OID-Referenz in	ProfessionItem	ProfessionOID	Früher festgelegt
-----------------	----------------	---------------	-------------------

anderen Dokumenten	(Beschreibung der technischen Rolle)	(OID der technischen Rolle)	in
oid_broker	Broker	1.2.276.0.76.4.88	[gemGesArch#Anh B1]
oid_broker_anonym	Broker Anonymisierungsdienst	1.2.276.0.76.4.89	[gemGesArch#Anh B1]
oid_vpnk	VPN-Konzentrator	1.2.276.0.76.4.90	[gemGesArch#Anh B1]
oid_vpnk_ti	VPN-Konzentrator-TI	1.2.276.0.76.4.91	[gemGesArch#Anh B1]
oid_vpnk_mwdn	VPN-Konzentrator-Mehrwertdienstenetz	1.2.276.0.76.4.92	[gemGesArch#Anh B1]
oid_trusted	Trusted Service	1.2.276.0.76.4.93	[gemGesArch#Anh B1]
oid_audit	Audit Service	1.2.276.0.76.4.94	[gemGesArch#Anh B1]
oid_sds	Service Directory Service	1.2.276.0.76.4.95	[gemGesArch#Anh B1]
oid_vodd	Verordnungsdatendienst	1.2.276.0.76.4.96	[gemGesArch#Anh B1]
oid_amdd	Dienst für die Daten zur Prüfung der Arzneimitteltherapiesicherheit	1.2.276.0.76.4.98	
oid_mgmtss	Management Schnittstelle	1.2.276.0.76.4.106	[gemGesArch#Anh B1]
oid_ths	Treuhand-Service für Datenerhalt	1.2.276.0.76.4.107	[gemGesArch#Anh B1]
oid_krs	Krypto-Service	1.2.276.0.76.4.108	[gemGesArch#Anh B1]
oid_pfdd	Patientenfachdatendienst	1.2.276.0.76.4.109	
oid_gcs	Gematik Code Signing	1.2.276.0.76.4.110	[gemGesArch#Anh B1]

oid_btmd	Betäubungsmitteldatendienst	1.2.276.0.76.4.1 11	
oid_mon_vpnk_ti	Probe-Client VPN-Konzentrator TI	1.2.276.0.76.4.1 14	[gemGesArch#Anh B1]
oid_mon_vpnk_mwd	Probe-Client VPN-Konzentrator Mehrwertdienste	1.2.276.0.76.4.1 15	[gemGesArch#Anh B1]
oid_mon_sds	Probe-Client SDS	1.2.276.0.76.4.1 16	[gemGesArch#Anh B1]
oid_mon_audit	Probe-Client Audit service	1.2.276.0.76.4.1 17	[gemGesArch#Anh B1]
oid_mon_brokerws	Web-Service-Simulator	1.2.276.0.76.4.1 18	[gemGesArch#Anh B1]
oid_mwdd	Mehrwertfachdienst	1.2.276.0.76.4.1 41	[gemGesArch#Anh B1]
oid_sgd1	HSM Schlüsselgenerierungsdienst 1	1.2.276.0.76.4.2 19	C.SGD-HSM.AUT
oid_sgd2	HSM Schlüsselgenerierungsdienst 2	1.2.276.0.76.4.2 20	C.SGD-HSM.AUT

69

70 (...)

71

72

73

## 3 Änderungen in Steckbriefen

### 3.1 Änderungen in gemProdT\_X509\_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 5: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GSA-A_4446-18	OID-Festlegung für technische Rollen	gemSpec:OID

### 3.2 Änderungen in gemProdT\_X509\_TSP\_QES, gemProdT\_X509\_TSP\_nonQES\_eGK, gemProdT\_X509\_TSP\_nonQES\_HBA, gemProdT\_X509\_TSP\_nonQES\_SMC-B

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT\_X509\_TSP\_QES, gemProdT\_X509\_TSP\_nonQES\_eGK, gemProdT\_X509\_TSP\_nonQES\_HBA, gemProdT\_X509\_TSP\_nonQES\_SMC-B]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

**Tabelle 6: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"**

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4445-10	OID-Festlegung für Zertifikatstypen	gemSpec:OID

