Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

gemKPT_PKI_TIP

6.5.3 Weitere Prüfungen und Auswertungen

[…]

⌦ **TIP1-A_4499 Ermittlung des Zertifikatstyps bei der Zertifikatsprüfung**

Die TI-Plattform MUSS bei der Prüfung von Zertifikaten den Zertifikatstyp aus dem Zertifikat ermitteln und an die aufrufende Anwendung zurückgeben.⌫

Innerhalb des Prozesses zur Zulassung eines TSP-X.509 zur Aufnahme in die TSL können Informationen erfasst werden, für welche Zertifikatstypen dieser TSP mit der jeweiligen CA erstellungsberechtigt ist, z. B. nur für Komponentenzertifikate, oder nur für eGK-Zertifikate. Diese Informationen – hinterlegt im Element „ServiceInformationExtensions“ in der TSL (siehe Tabelle 13) – ergeben sich anhand der Beauftragungen durch die für den jeweiligen Kartentyp verantwortlichen Kartenherausgeber.

Tabelle 13: Zuordnung der (zugelassenen) X.509-Sub-CAs zu Zertifikatstypen

Spezifischer CA-Einsatzbereich	CN (<usage> im Feld DN)	OID-Referenz in anderen Dokumenten	Name des Zertifikatstyp	Zertifikatstyp-OID	Referenz/Anmerkung
Elektronische Gesundheitskarte	<TSP>.eGK-CA<n> *) z.B. ATOS.EGK-CA201	oid_egk_enc	C.CH.ENC	1.2.276.0.76.4.68	[gemSpec_PKI#5.1.3;#5.11] [gemSpec_OID# Tab_PKI_405]
		oid_egk_encv	C.CH.ENCV	1.2.276.0.76.4.69	[gemSpec_PKI#5.1.3;#5.11] [gemSpec_OID# Tab_PKI_405]

Spezifischer CA-Einsatzbereich	CN (<usage> im Feld DN)	OID-Referenz in anderen Dokumenten	Name des Zertifikatstyp	Zertifikatstyp-OID	Referenz/Anmerkung
		oid_egk_aut	C.CH.AUT	1.2.276.0.76.4.70	[gemSpec_PKI#5.1.3;#5.11] [gemSpec_OID# Tab_PKI_405]
		oid_egk_autn	C.CH.AUTN	1.2.276.0.76.4.71	[gemSpec_PKI#5.1.3;#5.11] [gemSpec_OID# Tab_PKI_405]
Heilberufsausweis	<TSP>.HBA-qCA<n> *) D-Trust.HBA-qCA1	oid_hba_qes	C.HP.QES	1.2.276.0.76.4.72	[gemSpec_PKI#5.11;#5.11] [gemSpec_OID# Tab_PKI_405]
	<TSP>.HBA-CA<n> *) z.B. D-Trust.HBA-CA1	oid_hba_enc	C.HP.ENC	1.2.276.0.76.4.74	[gemSpec_PKI#5.11;#5.11] [gemSpec_OID# Tab_PKI_405]
		oid_hba_aut	C.HP.AUT	1.2.276.0.76.4.75	[gemSpec_PKI#5.11;#5.11] [gemSpec_OID# Tab_PKI_405]
Institutionskarten	<TSP>.SMCB-CA<n> *) z.B. D-Trust.SMCB-CA1	oid_smc_b_enc	C.HCI.ENC	1.2.276.0.76.4.76	[gemSpec_PKI#5.3.4;#5.11] [gemSpec_OID# Tab_PKI_405]
		oid_smc_b_aut	C.HCI.AUT	1.2.276.0.76.4.77	[gemSpec_PKI#5.3.4;#5.11] [gemSpec_OID# Tab_PKI_405]
		oid_smc_b_osig	C.HCI.OSIG	1.2.276.0.76.4.78	[gemSpec_PKI#5.3.4;#5.11] [gemSpec_OID# Tab_PKI_405]
Komponenten-PKI	<TSP>.KOMP-CA<n> *) z.B. GEM.KOMP-CA1	oid_fd_tls_s	C.FD.TLS-S	1.2.276.0.76.4.169	[gemSpec_PKI#5.9.3;#5.11] [gemSpec_OID# Tab_PKI_405]
		oid_zd_tls_s	C.ZD.TLS-S	1.2.276.0.76.4.157	[gemSpec_PKI#5.8.3;#5.11] [gemSpec_OID# Tab_PKI_405]
		oid_smkt_aut	C.SMKT.AUT	1.2.276.0.76.4.82	[gemSpec_PKI#5.5.2;#5.11] [gemSpec_OID# Tab_PKI_405]
		oid_nk_vpn	C.NK.VPN	1.2.276.0.76.4.80	[gemSpec_PKI#5.6.4;#5.11]

Spezifischer CA-Einsatzbereich	CN (<usage> im Feld DN)	OID-Referenz in anderen Dokumenten	Name des Zertifikatstyp	Zertifikatstyp-OID	Referenz/Anmerkung
					[gemSpec_OID# Tab_PKI_405]
		oid_sak_aut	C.SAK.AUT	1.2.276.0.76.4.113	[gemSpec_PKI#5.6.4;#5.11] [gemSpec_OID# Tab_PKI_405]
		oid_ak_aut	C.AK.AUT	1.2.276.0.76.4.79	[gemSpec_PKI#5.6.4;#5.11] [gemSpec_OID# Tab_PKI_405]
		oid_cm_tls_c	C.CM.TLS-CS	1.2.276.0.76.4.175	[gemSpec_PKI#5.10.3;#5.11] [gemSpec_OID# Tab_PKI_405]
		oid_fd_tls_c	C.FD.TLS-C	1.2.276.0.76.4.168	[gemSpec_PKI#5.9.3;#5.11] [gemSpec_OID# Tab_PKI_405]
		oid_fd_aut	C.FD.AUT	1.2.276.0.76.4.155	[gemSpec_OID# Tab_PKI_405] (derzeit nicht verwendet)
		oid_zd_tls_c	C.ZD.TLS-C	1.2.276.0.76.4.156	[gemSpec_OID# Tab_PKI_405] (derzeit nicht verwendet)
		oid_zd_aut	C.ZD.AUT	1.2.276.0.76.4.158	[gemSpec_OID# Tab_PKI_405] (derzeit nicht verwendet)
VPN-Zugangsdienst	<TSP>.VPNK-CA<n> *) z.B. GEM.VPNK-CA1	oid_vpnk_vpn	C.VPNK.VPN	1.2.276.0.76.4.81	[gemSpec_PKI#5.7.3;#5.11] [gemSpec_OID# Tab_PKI_405]
		oid_vpnk_vpn_sis	C.VPNK.VPN-SIS	1.2.276.0.76.4.165	[gemSpec_PKI#5.7.3;#5.11] [gemSpec_OID# Tab_PKI_405]

*) Für CA-Zertifikate der zentralen PKI wird für <tsp> die Bezeichnung "GEM" und für <tspName> "gematik GmbH" eingesetzt; für von TSPs betriebene Sub-CAs wird das jeweilige TSP-Kürzel sowie der vollständige TSP-Name eingefügt. Bei laufenden beispielshaften SubCA-Nummern können Abweichungen auftreten.