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.

1. Änderung in [gemSpec_PKI]

⌦ GS-A_4749 TUC_PKI_007: Prüfung Zertifikatstyp

Die Produkttypen der TI, die Zertifikate prüfen, MÜSSEN TUC_PKI_007 zur Prüfung des Zertifikatstyps umsetzen.⌫

Tabelle 100: TUC_PKI_007 "Prüfung Zertifikatstyp"

Element	Beschreibung
Name	TUC_PKI_007 "Prüfung Zertifikatstyp"
Beschreibung	In diesem Use Case wird der Soll-/Ist-Vergleich des Zertifikatstyps im Zuge einer Zertifikatsprüfung beschrieben. Verglichen wird die im Zertifikat enthaltene Zertifikatstyp-OID (abgelegt in einem Element PolicyIdentifier der X.509-Extension CertificatePolicies) mit der als Eingangsparameter dieses TUC übergebenen Liste der erwarteten Zertifikatstyp-OIDs. Zusätzlich wird die Zertifikatstyp-OID aus dem Zertifikat jeweils mit den in der TSL (TSL-Extension "ServiceInformationExtensions") enthaltenen ExtensionOIDs der CA verglichen, die das Zertifikat ausgestellt hat.
Anwendungsumfeld	System, das spezifische Inhalte von Zertifikaten verwendet
Vorbedingungen	Gültiges End-Entity-Zertifikat Aktuelle TSL-Informationen im System.
Auslöser	TUC_PKI_018 "Zertifikatsprüfung in der TI"
Eingangsdaten	• Das zu prüfende Zertifikat • PolicyList
Komponenten	System
Ausgangsdaten	• Status der Prüfung • OID des Zertifikatstyps
Referenzen	[RFC5280], [Common-PKI#Part5#2.2] Für weitere Erläuterungen zum Parameter "PolicyList" siehe [Common-PKI#Part5], Kapitel 2.2 Validating the Certificate Path. In der TSL werden OIDs für Zertifikatstypen benutzt, um anzuzeigen, welche Typen von Zertifikaten unter einer CA ausgestellt werden dürfen. Diese OIDs werden jeweils im Element "ServiceInformationExtensions" eingefügt, s. [gemSpec_TSL#7.3.2.1].
Standardablauf	1. [System:] Start des Prozesses zur Ermittlung des Zertifikatstyps. 2. [System:] Zertifikat laden 3. [System:] Auswahl der CertificatePolicies aus dem Zertifikat 4. [System:] Auswahl des Elements PolicyInformation. Es können mehrere Elemente vorkommen, da es eine SEQUENCE ist. In jedem Schritt wird

Element	Beschreibung
	ein Element aus der SEQUENCE entnommen. 5. [System:] Selektion der CertPolicyId aus dem Element PolicyInformation 6. [System:] Prüfung der Zertifikatstyp-OID aus dem Zertifikat gegen Liste der Zertifikatstyp-OIDs aus dem Parameter PolicyList der Eingangsdaten. 7. [System:] ~~Übereinstimmung der OIDs. und Ende des Use Case mit Rückmeldung des logischen Wertes TRUE. Mit dem ersten OID-Match wird der TUC beendet und die geforderte Bedingung als erfüllt gewertet~~ Die Zertifikatstyp-OID ist in PolicyList enthalten. Aus den TSL-Informationen wird der TSL-Eintrag der passenden CA ermittelt, welche das Zertifikat herausgegeben hat. (TUC_PKI_003 "CA Zertifikat in TSL finden"). 8. [System:] Prüfung der Zertifikatstyp-OID aus dem Zertifikat gegen die im TSL-Eintrag in der TSL-Extension "ServiceInformationExtensions" enthaltenen OIDs. 9. [System:] Die Zertifikatstyp-OID stimmt mit einer ExtensionOID überein. Ende des Use Case mit der Rückgabe der Zertifikatstyp-OID. Mit dem ersten OID-Match wird der Use Case beendet und die gesamte Prüfung als erfolgreich gewertet.
Varianten/Alternativen	6a. [System:] Keine Übereinstimmung, nächstes Element PolicyInformation des Zertifikates wird analysiert. Wiederholung des Vorgangs ab Schritt 4. 7a. Wird die Prüfung der ExtensionOID ausgelassen, endet der Use Case mit der Rückmeldung „Prüfung Zertifikatstyp erfolgreich“ und der Rückgabe der OID des Zertifikatstyps.
Fehlerfälle/Warnungen	4a. [System:] Abbruch und Rückmeldung. Kein Element PolicyIdentifier vorhanden. (CERT_TYPE_INFO_MISSING) 7~~a-b~~. [System:] Abbruch und Fehler~~Rück~~meldung. Ende der SEQUENCE ist erreicht und es wurde keine Übereinstimmung festgestellt. (CERT_TYPE_MISMATCH) 9a. [System:] Es wurde keine Übereinstimmung mit den ExtensionOIDs im Element ServiceInformationExtensions festgestellt. Abbruch mit der Fehlermeldung CERT_TYPE_CA_NOT_AUTHORIZED.
Technische Fehlermeldung	Das System meldet entsprechende Fehlercodes.
Anmerkungen	Der Aufbau der Extension CertificatePolicies ist in Kapitel 4.8.3.3 beschrieben. Für die Speicherung des Zertifikatstyps enthält das Element PolicyInformation kein Unterelement policy-Qualifier. Das TSL-Element ServiceInformationExtensions wird detailliert in [gemSpec_TSL#7.3.2.1] beschrieben.
Zugehörige Diagramme	Abbildung 22: Aktivitätsdiagramm TUC_PKI_007 "Prüfung Zertifikatstyp"

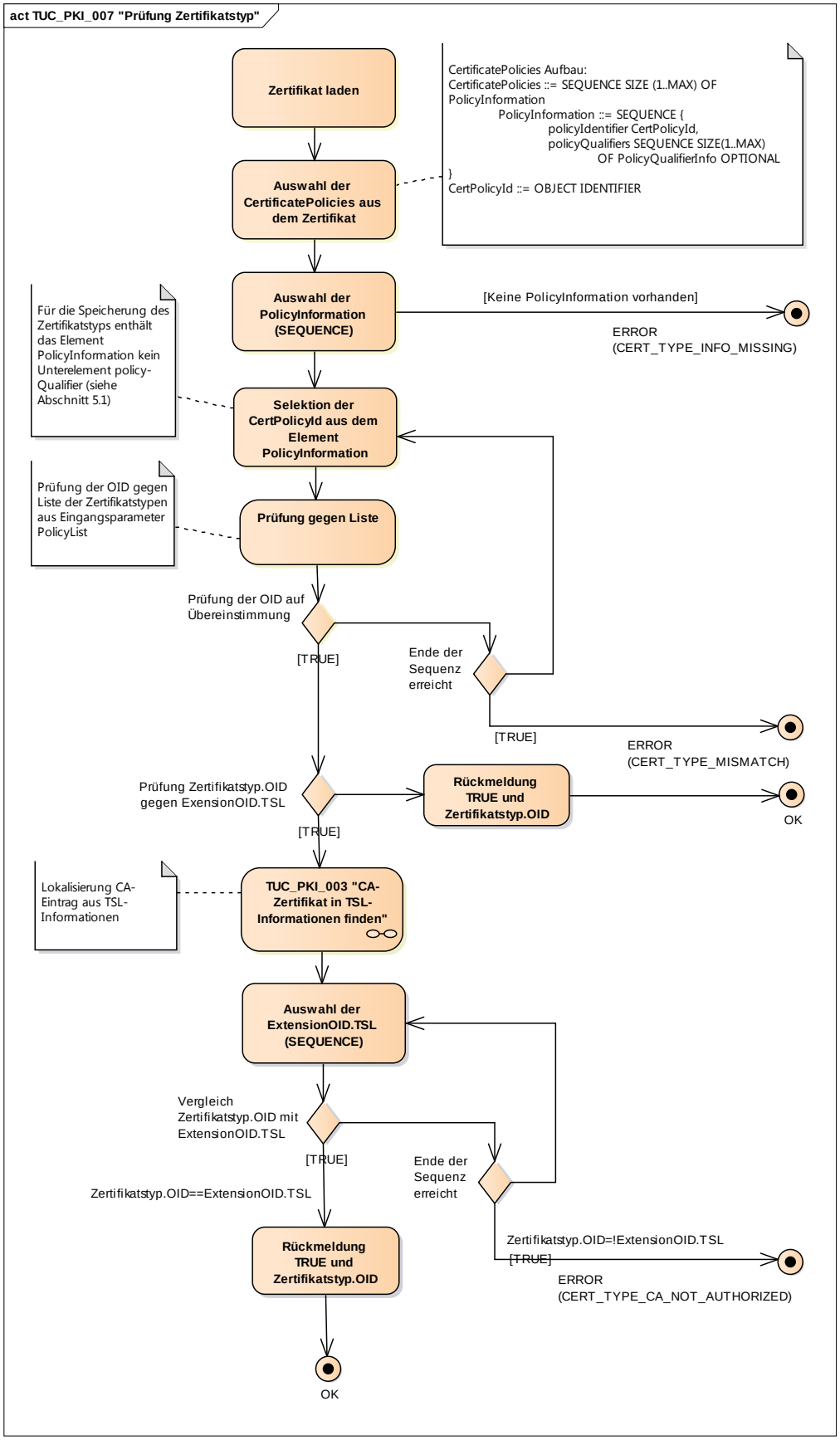

Abbildung 22: Aktivitätsdiagramm TUC_PKI_007 „Prüfung Zertifikatstyp“

⌦ **GS-A_5579 Prüfung Zertifikatstyp-OID - ExtensionOID**

Die Produkttypen der TI, die Zertifikate prüfen, KÖNNEN im Zuge der Prüfung des Zertifikatstyps gemäß TUC_PKI_007 die Prüfung der Zertifikatstyp-OID aus dem Zertifikat gegen die ExtensionOID aus den zugrunde liegenden TSL-Informationen auslassen.

In diesem Fall müssen Schritt 8. und 9. (s. Standardablauf) nicht umgesetzt werden. Der Use Case endet bei Schritt 7. mit der Meldung und der Rückgabe aus Schritt 7a. (s. Varianten/Alternativen). Der Fehlerfall 9a. (s. Fehlerfälle/Warnungen) entfällt.⌫

Hinweis:

Die Anforderung GS-A_5579 wird perspektivisch entfallen. Eine Umsetzung ist demzufolge nicht zu empfehlen.

Tabelle 104: Tab_PKI_274 Fehlercodes des SubCompTyps PKI bei TSL- und Zertifikatsprüfung

Code	Severity	ErrorType	ErrorText	Detail	Meldungskürzel
1061	Error	Security	CA (laut TSL) nicht autorisiert für die Herausgabe dieses Zertifikatstyps		CERT_TYPE_CA_NOT_AUTHORIZED

2. Hinweis zur Zuordnung der zugehörigen Produkttypsteckbriefen

Die Anforderung GS-A_5579 gilt für die zertifikatsvalidierenden Produkttypen(*) außer den Produkttypen Konnektor PTV3, Fachdienst KOM-LE, KTR-AdV-Terminal und KTR-AdV.

(*):

Die Zuordnung zu den Prüfverfahren der einzelnen Produkttypen erfolgt wie folgt (analog zu GS-A_4749 - TUC_PKI_007):

Aufnahme der Anforderung GS-A_5579 in das Kapitel 3.1.1 – Tabelle 2 Produkttest / Produktübergreifender Test der folgenden Produkttypsteckbriefe:

- gemProdT_OCSP_Proxy
- gemProdT_gematik-Root-CA
- gemProdT_X.509_TSP_nonQES_eGK
- gemProdT_X.509_TSP_nonQES_HBA
- gemProdT_X.509_TSP_nonQES_Komp
- gemProdT_X.509_TSP_nonQES_SMC-B
- gemProdT_X.509_TSP_nonQES_QES
- gemProdT_VPN_ZugD
- gemProdT_KSR
- gemProdT_NamD
- gemProdT_SG_BestNetze
- gemProdT_VZD
- gemProdT_Intermediaer_VSDM
- gemProdT_FD_KOMLE
- gemProdT_FD_VSDM
- gemProdT_ZeitD
- gemProdT_ZentrNetz.

Die Anforderung GS-A_5579 wird NICHT aufgenommen in folgenden Produkttypsteckbriefen:

- gemProdT_Kon_PTV1/_ PTV2/_ PTV3
- gemProdT_FD_KOMLE
- gemProdT_KTR_AdV
- gemProdT_KTR-AdV-Terminal.

Die Anforderung GS-A_4749 wird aufgenommen in allen o.g. Produkttypsteckbriefen.