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.

Reaktion auf OCSP-Antwort durch Konnektor (Revoked, Unknown)

Es ist für den Konnektor nicht für alle Fälle ausspezifiziert, wie er agieren muss, wenn die OCSP-Abfrage "REVOKED" liefert, der Sperrzustand nach einem OCSP-Abfrageversuch unbekannt ist oder die OCSP-Abfrage im Online-Fall nicht erfolgen konnte.

Nachzuschärfen sind folgende Fälle:

* TLS-Verbindung wird vom Konnektor zu einem zentralen Dienst der TI-Plattform oder zu einem fachanwendungsspezifischen Dienst aufgebaut.

* Dokumentverschlüsselung

* QES-Erstellung

Änderungsbedarf in gemSpec_Kon

3 Übergreifende Festlegungen

[in Kapitel 3 vor 3.1 wird Folgendes ergänzt]

Übergreifende PKI-Festlegungen

⌦ TIP1-A_7254 Reaktion auf OCSP-Abfrage beim TLS-Verbindungsaufbau

Der Konnektor MUSS beim Aufbau von TLS-gesicherten Verbindungen zu einem zentralen Dienst der TI-Plattform oder zu einem fachanwendungsspezifischen Dienst, bei denen eine OCSP-Abfrage des Serverzertifikats nach TUC_PKI_006 erfolgt, neben Fehlerfällen bei folgenden Warnungen gemäß [gemSpec_PKI#Tab_PKI_274]

- CERT_REVOKED
- CERT_UNKNOWN
- OCSP_CHECK_REVOCATION_FAILED

mit Abbruch des Verbindungsaufbaus reagieren.⌫

4.1.7.4.1. TUC_KON_070 ”Daten hybrid verschlüsseln”

Ausgangsdaten:

~~ocspChecked [Boolean] (Ergebnis des OCSP-Checks)~~

…

Standardablauf/Schritt 4:

Falls Zertifikate übergeben oder referenziert wurden, werden diese durch Aufruf von TUC_KON_037 „Zertifikat prüfen“ geprüft.
Als Parameter des TUC-Aufrufs gilt für Zertifikate, die mit Zertifikaten aus CERT_IMPORTED_CA_LIST geprüft werden:

TUC_KON_037 „Zertifikat prüfen“ {
  certificate =Zertifikat;
  qualifiedCheck = not_required;
  offlineAllowNoCheck = true;
  intendedKeyUsage = keyEncipherment;
  validationMode = NONE }

Für alle anderen Zertifikate gilt: {
  certificate = [C.CH.ENC];
  qualifiedCheck=not_required;
  offlineAllowNoCheck= false; ~~true;~~
  policyList =[oid_egk_enc];
  intendedKeyUsage= keyEncipherment ;
  validationMode=OCSP }
oder
{
  certificate = [C.CH.ENCV];
  qualifiedCheck=not_required;
  offlineAllowNoCheck= false; ~~true;~~
  policyList =[oid_egk_encv];
  intendedKeyUsage= keyEncipherment ;
  validationMode=OCSP }
oder
{
  certificate = [C.HCI.ENC];
  qualifiedCheck=not_required;
  offlineAllowNoCheck= false; ~~true;~~
  policyList =[oid_smc_b_enc];
  intendedKeyUsage= keyEncipherment ;
  validationMode=OCSP }
oder
{
  certificate = [C.HP.ENC];
  qualifiedCheck=not_required;
  offlineAllowNoCheck= false; ~~true;~~
  policyList =[oid_hba_enc];
  intendedKeyUsage= keyEncipherment;
  validationMode=OCSP }

~~Sollte die Prüfung eines der Zertifikate dieses als nicht gültig ausweisen, bricht der TUC ab.~~

~~Wenn eine Online-Prüfung des Status der Zertifikate erfolgen konnte wird ocspChecked=True gesetzt.~~
~~Wenn eine Online-Prüfung des Status der Zertifikate nicht erfolgen konnte wird ocspChecked=False gesetzt, der Fehlercode 1028 (Warning CHECK_REVOCATION_FAILED gemäß gemSpec_PKI#Tab_PKI_274) in die GERROR:Trace-Struktur aufgenommen und mit Schritt 5 fortgefahren.~~

Fehlerfälle:

Siehe Tabelle 172: TAB_KON_740 Fehlercodes TUC_KON_070 „Daten hybrid verschlüsseln“.

Wenn im Ablauf des TUCs ein anderer Fehler als die in Tabelle 172 beschriebenen Fehler auftritt, wird Fehler 4105 gemeldet.

(→4) Schritt 4 – Zertifikatsprüfung „für alle anderen Zertifikate“

Für MGM_LU_ONLINE=Enabled gilt:

Liefert die Zertifikatsprüfung (OCSP-Abfrage) mdt. eine der folgenden Warnungen gemäß [gemSpec_PKI#Tab_PKI_274]

- CERT_REVOKED
- CERT_UNKNOWN

dann wird der TUC mit Fehler 4105 abgebrochen.

4.1.8.3.4. TUC_KON_152 ”Signaturvoraussetzung für QES prüfen”

Fehlerfälle:
~~Keine~~

(→3) Für MGM_LU_ONLINE=Enabled gilt:

Liefert die Zertifikatsprüfung (OCSP-Abfrage) die Warnung CERT_REVOKED

gemäß [gemSpec_PKI#Tab_PKI_274], dann wird der TUC mit Fehler 4123 abgebrochen.

4.1.9.4.1. TUC_KON_037 „Zertifikat prüfen"

Eingangsdaten	[…] • offlineAllowNoCheck [Boolean] – *optional; default: false* (Angabe, ob es als Fehler (false) oder als Warnung (true) interpretiert werden soll, wenn eine OCSP-Prüfung nicht durchgeführt werden konnte ~~im Offlinefall der Check entfallen darf~~.) […]
Standardablauf	[…] Als TOLERATE_OCSP_FAILURE wird beim Aufruf von TUC_PKI_018 offlineAllowNoCheck verwendet. […]