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.

Änderungsbedarf:

Im Test wurden Fehlersituationen bei TI-Produkten erkannt, die kein QES auswerten sollen bzw. können, ausgelöst durch nicht-RSA-QES-CA-Zertifikate in der TSL.

Um diese Fehler zukünftig zu vermeiden, werden QES-CA-Elemente aus der TSL entfernt. Diese waren dort nur vor Inkrafttreten von eIDAS notwendig, werden aber nicht mehr benötigt, da sie in der BNetzA-VL enthalten sind. In der TSL verbleiben (allerdings an anderer Stelle) für die zugelassenen VDAs die Adress-Informationen zu deren OCSP-Respondern in der TI.

Die Entfernung von QES-Zertifikaten in der TSL erfordert geringfügige Anpassungen der QES-Zertifikatsprüfungs-Mechanismen für QES-Konnektoren und stützt sich damit vollständig auf die Einträge in der Vertrauensliste der BNetzA, die im Zuge der TI-Anpassungen für eIDAS (Rel. 1.6.3) bereits für Konnektoren in der TI verfügbar gemacht wurde.

Die klarere Trennung der Vertrauensdomänen (TSL für nonQES / BNetzA-VL für QES) ist dabei das Ziel, dass Sicherheit und Architektur verfolgen und zukunftsweisend umgesetzt werden kann, solange noch kein QES-Konnektor im Feld umgesetzt ist.

Diese Änderung verhindert das Risiko, dass zukünftige QES-CA-Zertifikate, die von VDAs in die TSL eingebracht werden, zu Fehlern bei anderen Systemen in der TI führen. Hintergrund: Verwendete Signatur-Algorithmen können für QES-CA-Zertifikate der VDAs nicht von der gematik vorgegeben werden und sind in der BNetzA-VL enthalten.

QES-Konnektoren werden vorbereitet, um mit allen QES-CA-Zertifikaten in der BNetzA-VL umgehen zu können.

Die Änderungen berücksichtigen ferner die weggefallene Notwendigkeit, Attributzertifikate bei Zertifikatsprüfungen zu berücksichtigen. Siehe als Referenz dazu auch den Änderungseintrag C_6388.

Die folgenden Spezifkation werden dahingehend angepasst:

- gemSpec_PKI
- gemSpec_TSL
- gemSpec_OCSP_Proxy
- gemKPT_PKI_TIP

Änderungen in gemSpec_PKI

[…]

~~3.5 Sperrungen von QES-CAs~~

~~Im Falle von sicherheitskritischen Incidents bei QES-CA-Zertifikaten (s. Definition und Beschreibung in [gemKPT_PKI_TIP#2.3.3.5]) müssen innerhalb der TI besondere Maßnahmen ergriffen werden, wenn die betroffene QES-CA Zertifikate für die TI ausstellt und durch die BNetzA gesperrt wurde.~~

~~⌦ **GS-A_5065 Sperrung einer QES-CA**~~

~~Der Gesamtbetriebsverantwortliche der TI MUSS im Falle der Sperrung einer QES-CA in Kooperation mit der BNetzA die erforderlichen Maßnahmen für die TI festlegen und den TSL-Dienst entsprechend anweisen.⌫~~

[…]

8 Prüfung von Zertifikaten

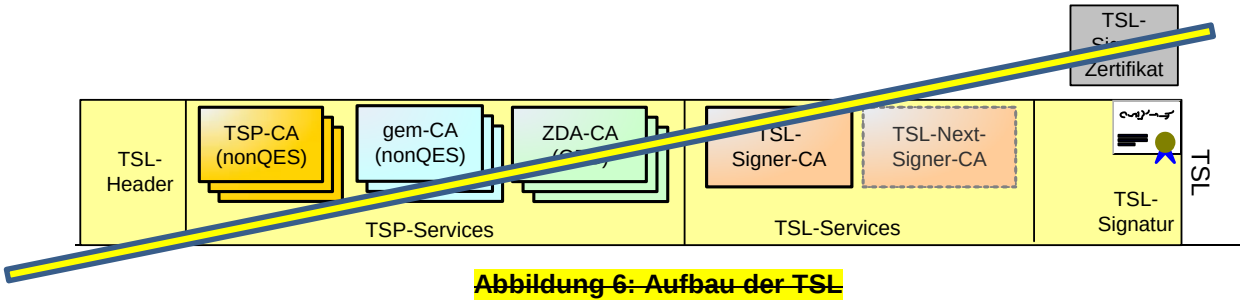
Für die Nutzung und Statusprüfung von Zertifikaten in der TI gilt:

- Das TSL-Signer-CA-Zertifikat bildet den Vertrauensanker für die TI.
- Die TSL stellt (i. S. einer Whitelist) den Vertrauensraum für die in der TI zugelassenen Aussteller-CA.
- nonQES-Aussteller-CA-Zertifikate werden ausschließlich gegen die TSL geprüft
- QES-Aussteller-CA-Zertifikate werden
  ~~(a) hinsichtlich ihrer Zulassung in der TI gegen die TSL und~~
  ~~(b)~~ hinsichtlich ihres VDA Qualifikationsstatus gemäß [eIDAS] gegen die BNetzA-VL geprüft.
- Als Vertrauensanker für die BNetzA-VL fungieren jeweils die aktuell publizierten BNetzA-VL-Signer-Zertifikate. Diese werden mittels TSL in die QES-prüfenden Systeme (Konnektoren) eingebracht und aktualisiert.
- End-Entity-Zertifikate werden gegen den OCSP-Dienst der Aussteller-CA geprüft, außer die Statusprüfung für einen bestimmten Zertifikatstyp ist explizit optional oder nicht vorgesehen.

[…]

8.1 Vertrauensraum der TI

[…]



~~**Abbildung 6: Aufbau der TSL**~~

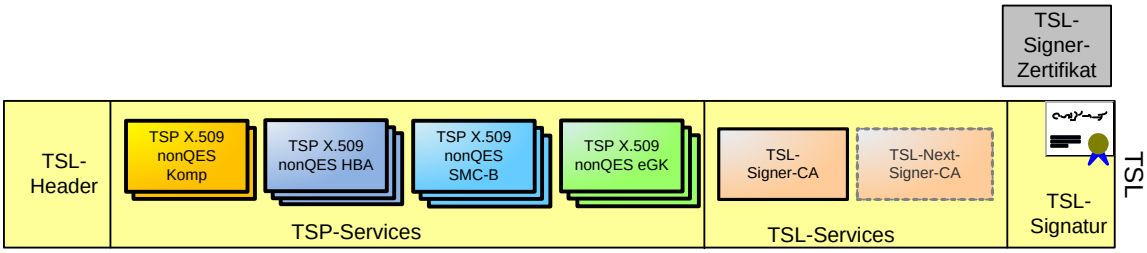


Abbildung 6: Aufbau der TSL

[…]

8.5 Zertifikatsprüfung X.509 QES

[…]

⌦ **GS-A_4750 TUC_PKI_030 „QES-Zertifikatsprüfung“**

Alle Produkttypen, die QES-Zertifikate prüfen, MÜSSEN TUC_PKI_030 zur Prüfung der QES-Zertifikate umsetzen. ⌫

8.5.1 TUC_PKI_030 „QES-Zertifikatsprüfung“

Tabelle 101: TUC_PKI_030 „QES-Zertifikatsprüfung“

Element	Beschreibung
Name	TUC_PKI_030 „QES-Zertifikatsprüfung“
Beschreibung	In diesem Use Case wird die Prüfung von Zertifikaten mit qualifizierter Signatur beschrieben. Die Prüfung von QES-Zertifikaten setzt sich aus den in [Common-PKI#Part5] und [Common-PKI#9 beschriebenen Schritten zusammen], sofern sie den Vorgaben von [eIDAS] nicht widersprechen. ~~Die Prüfungen der korrespondierenden Attributzertifikate (falls übergeben) müssen die Vorgaben gemäß [baekAttr], [RFC5755], [Recommendation ITU-T X.509 | ISO/IEC 9594-8] und [Common-PKI#Part9#2.2] berücksichtigen.~~ Zusätzlich werden folgende Schritte in diesem Technical Use Case (TUC) durchgeführt.
Anwendungsumfeld	System, das Zertifikate verwendet

Element	Beschreibung
Vorbedingungen	aktuelle TSL-Informationen im Truststore (inkl. OCSP-Adressen in der TI für die zugelassenen VDAs), eine aktuell gültige BNetzA-VL.
Auslöser	Zertifikats-Check
Eingangsdaten	• QES-Zertifikat • ~~Liste der korrespondierenden Attributzertifikate (optional, zum QES-Zertifikat als Basis-Zertifikat)~~ • Referenzzeitpunkt (refTime): Zeitpunkt, für den das Zertifikat geprüft werden soll • Offline-Modus (ja/nein) • Beigefügte OCSP-Response, die zur Prüfung des angefragten QES-Zertifikates erforderlich ist (optional; z. B. in Signatur eingebettet) • Nonce (optional; Wert ausschließlich zur Verwendung bei der OCSP-Prüfung des zu prüfenden QES-Zertifikates) • ~~TSL-Informationen (Adressen für OCSP-Abfragen)~~ • Timeout-Parameter für OCSP-Abfragen (Default: 10s)
Komponenten	System
Ausgangsdaten	• Status der Prüfung~~,~~ • OCSP-Response zum angefragten QES-Zertifikat~~,~~ • im Zertifikat enthaltene Rollen-OIDs • im Zertifikat enthaltene QCStatements-Einträge
Standardablauf	~~0.~~ ~~Die QES-Zertifikatsprüfung setzt sich aus den in [Common-PKI#Part5] und [Common-PKI#9] beschriebenen Schritten zusammen.~~ ~~Die Prüfungen der korrespondierenden Attributzertifikate müssen die Vorgaben gemäß [baekAttr], [RFC5755] und [Recommendation ITU-T X.509 | ISO/IEC 9594-8] berücksichtigen.~~ ~~(Zusätzlich zu den in [Common-PKI] beschriebenen Schritten werden folgende Schritte durchgeführt:~~ 1. [System] Auslesen und Ausgabe aller gesetzten Elemente der Extension QCStatements des Zertifikates ~~1~~ 2. [System:] Anhand der End-Entity-Zertifikatsdaten wird die BNetzA-VL durchsucht, um das passende QES-CA-Zertifikat zu finden. *Hinweis: Das Verfahren zum Finden des QES-CA-Zertifikates in BNetzA-VL verläuft analog zum Finden des nonQES-CA-Zertifikates in der TSL mittels TUC_PKI_003.* ~~1~~ 3. [System:] Prüfung, ob das ausstellende QES-CA-Zertifikat für die QES-Prüfung zum Referenzzeitpunkt in der BNetzA-VL gemäß [eIDAS] und [ETSI TS 119 612#5.5.4 und #Annex J] qualifiziert und als gültig gekennzeichnet ist. *Hinweis: Für gültige Status siehe Anmerkungszeile zu diesem TUC* ~~2.~~ ~~[System:] Prüfung, ob das ausstellende QES-CA-Zertifikat des QES-Zertifikates in der TSL enthalten ist (TUC_PKI_003 "CA-Zertifikat in TSL-Informationen finden").~~ ~~3.~~

Element	Beschreibung
	~~[System:] Prüfung, ob das QES-CA-Zertifikat (zum Referenzzeitpunkt) in der TSL als gültig gekennzeichnet ist.~~ ~~4.~~ [System:] Ermittlung der OCSP-Adresse aus ~~der TSL (TUC_PKI_005 "Adresse für Status- und Sperrprüfung ermitteln")~~ dem AIA-Feld des QES-EE-Zertifikates. Dabei handelt es sich um eine öffentlich aufrufbare URL im Internet. Wird für die ermittelte OCSP-URL in der TSL derselbe Wert im InformationValue-Element von AdditionalServiceInformation von BNetzA-VL-Service (mit ServiceTypeIdentifier http://uri.telematik/TrstSvc/Svctype/TrustedList/schemerules/DE) gefunden, so wird die dahinter folgende (nach Leerzeichen) URL als Adresse für die OCSP-Anfrage verwendet. Andernfalls wird die zuvor ermittelte OCSP-Adresse aus dem AIA-Feld für die OCSP-Anfrage verwendet. *Hinweis: Details zu den TSL-Einträgen für URLs für OCSP-Responder in der TI unter gemSpec_TSL# TIP1-A_7219* 5. [System:] Die abzufragenden Statusinformationen zu QES-Zertifikaten werden unter Verwendung der ~~extrahierten~~ ermittelten OCSP-Adresse~~n~~ eingeholt. *Hinweis: Details zur OCSP-Statusprüfung siehe Anmerkungszeile zu diesem TUC* 6. [System:] Ermittlung der Rolle (TUC_PKI_009 "Rollenermittlung") 7. [System:] Ende des Use Case mit Rückgabe des/der im Zertifikat enthaltenen Rollen-OID(s)
Varianten/Alternativen	Der Standardablauf stellt die üblichen Schritte dar, die durchgeführt werden müssen. Eine Trennung in zwei Prozesse oder eine Umstrukturierung, bei der alle notwendigen Schritte erfolgen, ist zulässig. ~~0.~~ 5a. [System:] Wird im optionalen Parameter Nonce ein Wert übergeben, dann muss für QES-Zertifikate dieser Wert als OCSP-Parameter in den OCSP-Request integriert und im Response geprüft werden. ~~4a.~~ 5b. [System:] Der Offline-Modus ist aktiviert. Es werden keine Statusinformationen eingeholt. (Schritte 4 und 5 entfallen.) 5~~a~~ c. [System:] Eine OCSP-Response zu dem zu prüfenden Zertifikat wurde im Aufruf mit übergeben. Falls dieses zum Referenzzeitpunkt gültig ist, werden keine OCSP-Requests erzeugt, sondern die beigefügte OCSP-Response zur weiteren Prüfung verwendet.
Fehlerfälle	In jedem der beschriebenen Schritte können Fehler auftreten. Diese sind durch das System zu melden und der Prozess muss beendet werden. ~~0b.~~ ~~In [Common-PKI#Part5] und [Common-PKI#9] sind Fehlerfälle für die QES-Zertifikatsprüfung und die Prüfung von Attributzertifikaten beschrieben. Diese beinhalten:~~ ~~- Prüfung von QCStatements: QC_STATEMENT_ERROR~~ ~~- Prüfung von QES-Basiszertifikat assoziierten Attributzertifikaten: ATTR_CERT_MISMATCH.~~ ~~0c.~~ ~~Wenn die in einer OCSP-Response zurückgelieferte Nonce nicht mit der~~

Element	Beschreibung
	~~Nonce des OCSP-Requests für ein QES-Zertifikat übereinstimmt, wird die Prüfung abgebrochen mit der Fehlermeldung OCSP_NONCE_MISMATCH.~~ 1a. Ist die Extension QCStatements nicht auslesbar, leer oder enthält keine auslesbaren Elemente, bricht der TUC mit dem Fehler QC_STATEMENT_ERROR ab ~~1~~ 3a. Ist das QES-CA-Zertifikat in der BNetzA-VL nicht vorhanden oder zum Referenzzeitpunkt nicht mit einem gültigen Status gekennzeichnet, muss der TUC mit einer Fehlermeldung CA_CERTIFICATE_NOT_QES_QUALIFIED abbrechen. 3~~a~~ b. [System:] QES-CA-Zertifikat des QES-Zertifikates ist in der ~~TSL~~ BNetzA-VL als revoked gekennzeichnet und QES-Zertifikat ist nach Sperrzeitpunkt erstellt worden. Abbruch mit Fehlermeldung (CA_CERTIFICATE_REVOKED_IN_~~TSL~~BNETZA-VL). 5b. [System:]. Der zuständige OCSP-Responder ist nicht erreichbar. Abbruch mit Fehlermeldung (OCSP_NOT_AVAILABLE). 5c. [System:] OCSP-Responses zu dem zu prüfenden Zertifikat wurden im Aufruf mit übergeben, ergaben bei den weiteren Prüfschritten jedoch kein gültiges Ergebnis. Eine erneute Prüfung wird in diesem Fall durchgeführt, als wären keine OCSP-Responses beigefügt. In den Rückgabewerten dieses TUC wird die Warnmeldung (PROVIDED_OCSP_RESPONSE_NOT_VALID) an die aufrufende Funktion übergeben. 5d. [System:] Warnmeldung, dass keine Online-Statusprüfung durchgeführt wurde (NO_OCSP_CHECK). 5e. Wenn die in einer OCSP-Response zurückgelieferte Nonce nicht mit der Nonce des OCSP-Requests (vgl. optionalen Eingangsparameter „Nonce“) für ein QES-Zertifikat übereinstimmt, wird die Prüfung abgebrochen mit der Fehlermeldung OCSP_NONCE_MISMATCH.
Technische Fehlermeldung	Das System meldet entsprechende Fehlercodes.
Sicherheits-anforderungen	
Anmerkungen	Gültige Status zu Schritt 1 sind gemäß [ETSI TS 119 612#5.5.4 und #Annex J] *granted, accredited, undersupervision, supervisionincessation* Die Einträge der QES-CA-Zertifikate in der BNetzA-VL besitzen gemäß [ETSI TS 119 612#5.5.1.1] die Extension AdditionalServiceInformation http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures. Die Einträge der QES-CA-Zertifikate in der TSL und der BNetzA-VL besitzen den ServiceTypeIdentifier http://uri.etsi.org/TrstSvc/Svctype/CA/QC. Schritt 2 stellt eine TI-spezifische Sperrprüfung des QES-CA-Zertifikats gemäß Kettenmodell dar. ~~Vgl. Kap. 8.1.1 Initialisierung TI-Vertrauensraum.~~ ~~Schritt 5 enthält die QES-spezifischen Statusprüfungen.~~ Zusätzlich zu den Vorgaben gemäß [eIDAS#Artikel 24, Abs. (2) Buchstabe (k), Abs. (3) und (4)] muss Schritt 5 folgende Anforderungen bei der QES-spezifischen Statusprüfungen erfüllen:

Element	Beschreibung
	• Zur Auswertung der OCSP-Response siehe auch [Common-PKI#Part4#3 und #Part9#4] • Zur Prüfung der certHash-Erweiterung siehe auch [Common-PKI#Part4#3.1.2] und [Common-PKI#Part5#2.3] sowie [gemSpec_Krypt#GS-A_4393] • Zur Prüfung der OCSP-Response auf Integrität (Signatur): Das OCSP-Signer-Zertifikat wird gemäß RFC 6960 durch die ausstellende QES-CA bereitgestellt
Zugehörige Diagramme/Tabelle	

[…]

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

Code	Severity	ErrorType	ErrorText	Detail	Meldungskürzel
…					
1062	Error	Security	Das QES-EE-Zertifikat ist ungültig. Es wurde nach der Sperrung der ausgebenden QES-CA ausgestellt		CA_CERTIFICATE_REVOKED_IN_BNETZA_VL
…					

9.1.1 Schnittstelle I_OCSP_Status_Information

[…]

9.1.1.2 Umsetzung

[…]

⌦ **GS-A_5517 Schlüsselgenerationen der OCSP-Signer-Zertifikate**

Die Produkttypen TSL-Dienst, gematik Root-CA~~, TSP-X.509 QES~~ und TSP-X.509 nonQES MÜSSEN sicherstellen, dass zum Signieren von OCSP-Responses für Zertifikate einer bestimmten Schlüsselgeneration, ausschliesslich ein OCSP-Signer-Zertifikat derselben Schlüsselgeneration (gemäß [gemSpec_Krypt#GS-A_4357] bzw. [gemSpec_Krypt#GS-A_4358]) verwendet wird.⌫

[…]

B5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
…	
~~[baekAttr]~~	~~Zertifikatsprofile für X.509 Attributzertifikate; Version 2.3.1 vom 29.05.2009~~
~~[BÄK_ZPX.509B]~~	~~Bundesärztekammer (28.05.2009):~~

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
	~~Zertifikatsprofile für X.509 Basiszertifikate V 2.3.1; Zertifikatsaufbau und –hierarchie, Gültigkeitsmodell für Zertifikatstypen: ENC, AUT, QES, ATT sowie die Root, Cross- und CA-Zertifikate, die CRL-Signer und die OCSP-Zertifikate~~
…	

[…]

Änderungen in gemKPT_PKI_TIP

[…]

2.3.1 Vertrauensmodell für QES

[…]
~~Außerdem werden die TSP-X.509 QES mit ihren zugelassenen Diensten in den Vertrauensraum der TI aufgenommen~~**~~Fehler! Textmarke nicht definiert.~~**.

[…]

~~⌦ **TIP1-A_2035 Bereitstellung QES-CAs durch TSL-Dienst**~~

~~Der TSL-Dienst MUSS im Kontext der QES die CA-Zertifikate der VDA für QES in der TSL bereitstellen.⌫~~

2.3.3 Vertrauensraum mittels TSL – Umsetzung in der TI

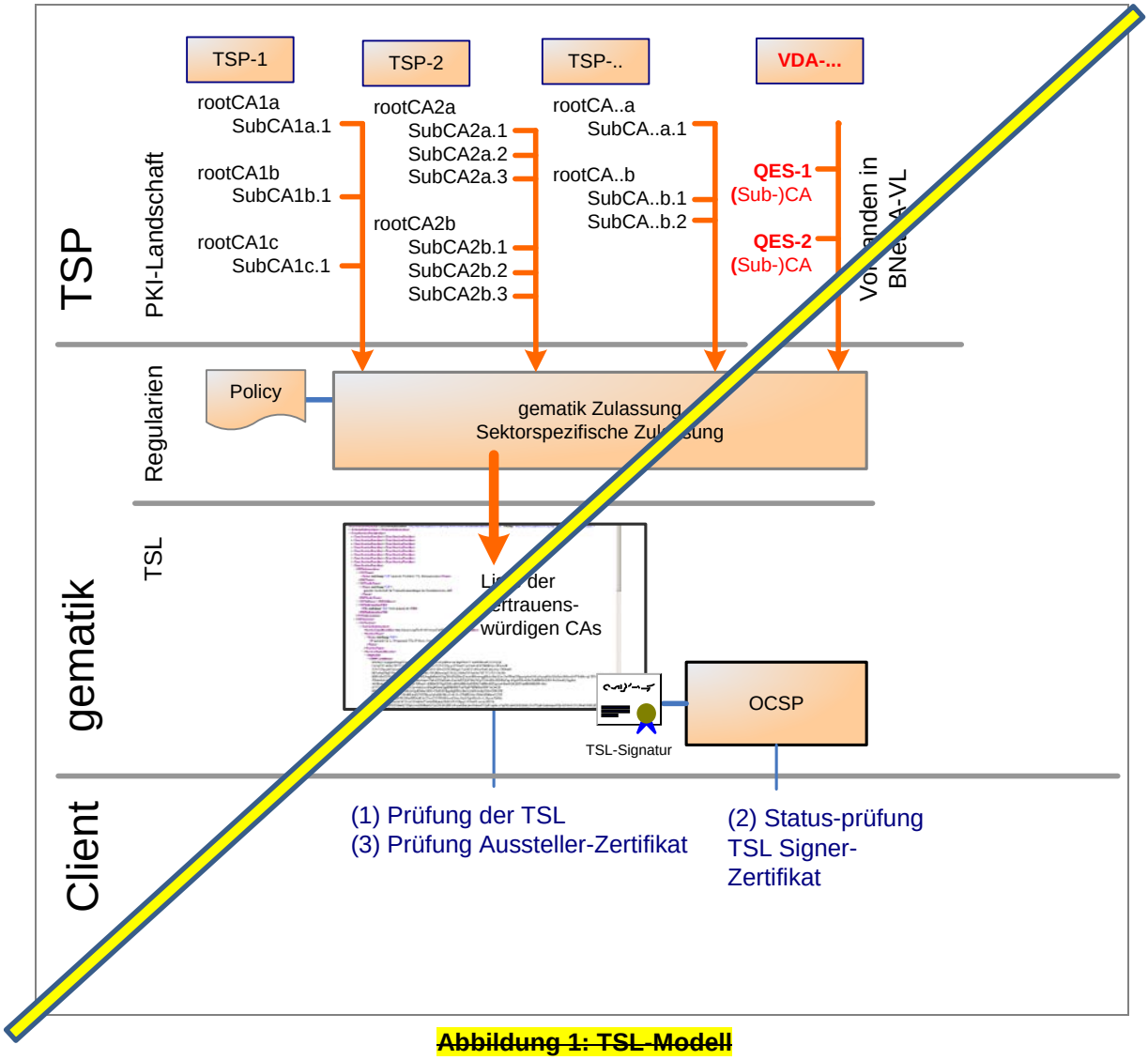
[…]

~~Die Aufnahme eines QES-CA-Zertifikates in die TSL repräsentiert die TI-Zulassung dieses VDA, um QES-Zertifikate für HBA in der TI für einen oder mehrere Sektoren produzieren zu dürfen. Für die Nutzung von QES-Zertifikaten außerhalb der TI hat die TSL keine Relevanz.~~

[…]

2.3.3.2 Struktur, Signatur und Inhalt der TSL

Die folgende Abbildung verdeutlicht die Anwendung der TSL in der TI.



~~Abbildung 1: TSL-Modell~~

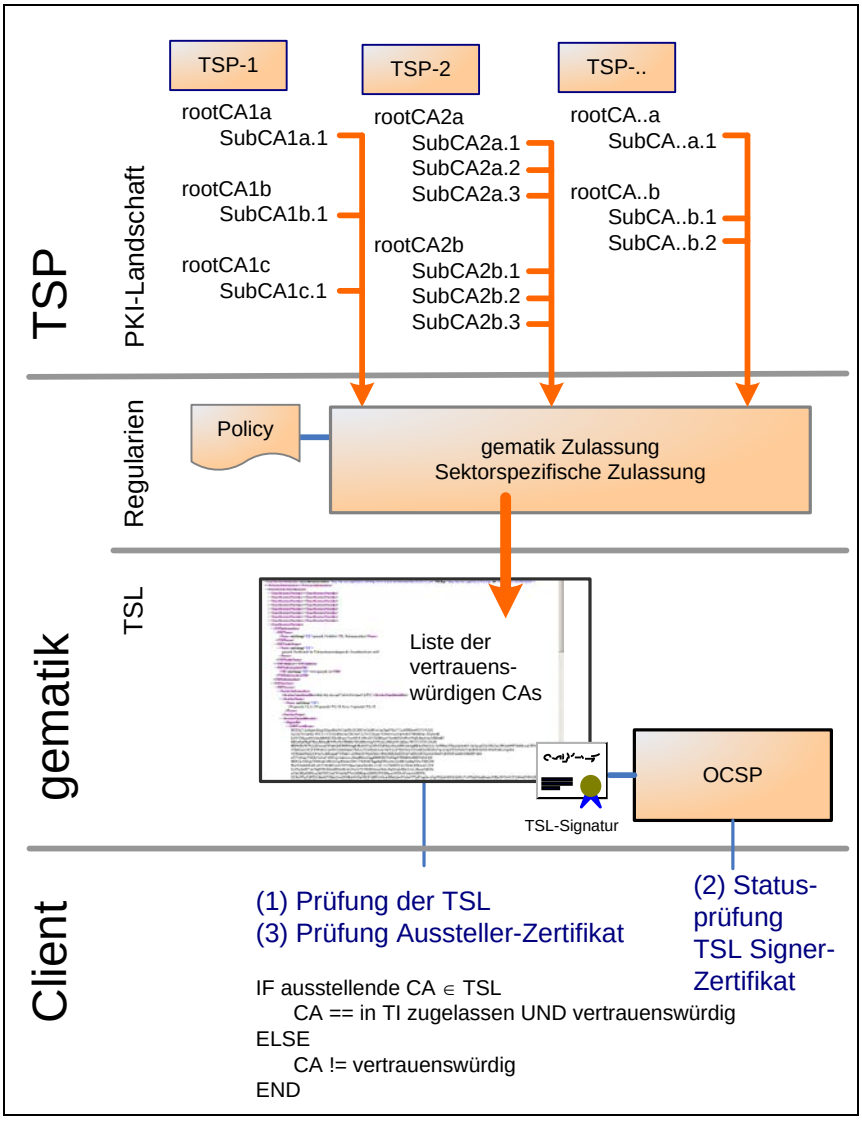


Abbildung 2: TSL-Modell

Abbildung 2 zeigt die grundsätzlichen Hierarchiestufen der Zertifikate und soll verdeutlichen, dass jeweils die CA-Zertifikate in die TSL als Vertrauensraum aufzunehmen sind, unabhängig davon, ob diese aus einer übergeordneten Root-CA abgeleitet sind oder es sich um sog. „self-signed“ CAs handelt.

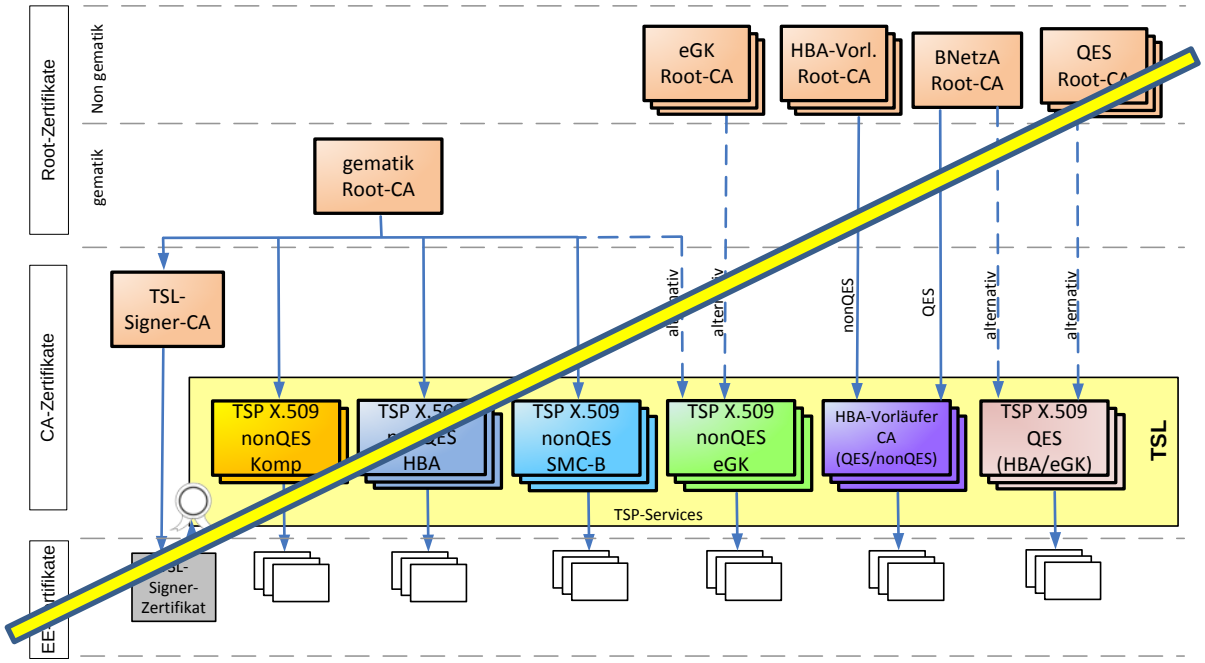


Abbildung 3: Zertifikatshierarchien und deren Abbildung in der TSL

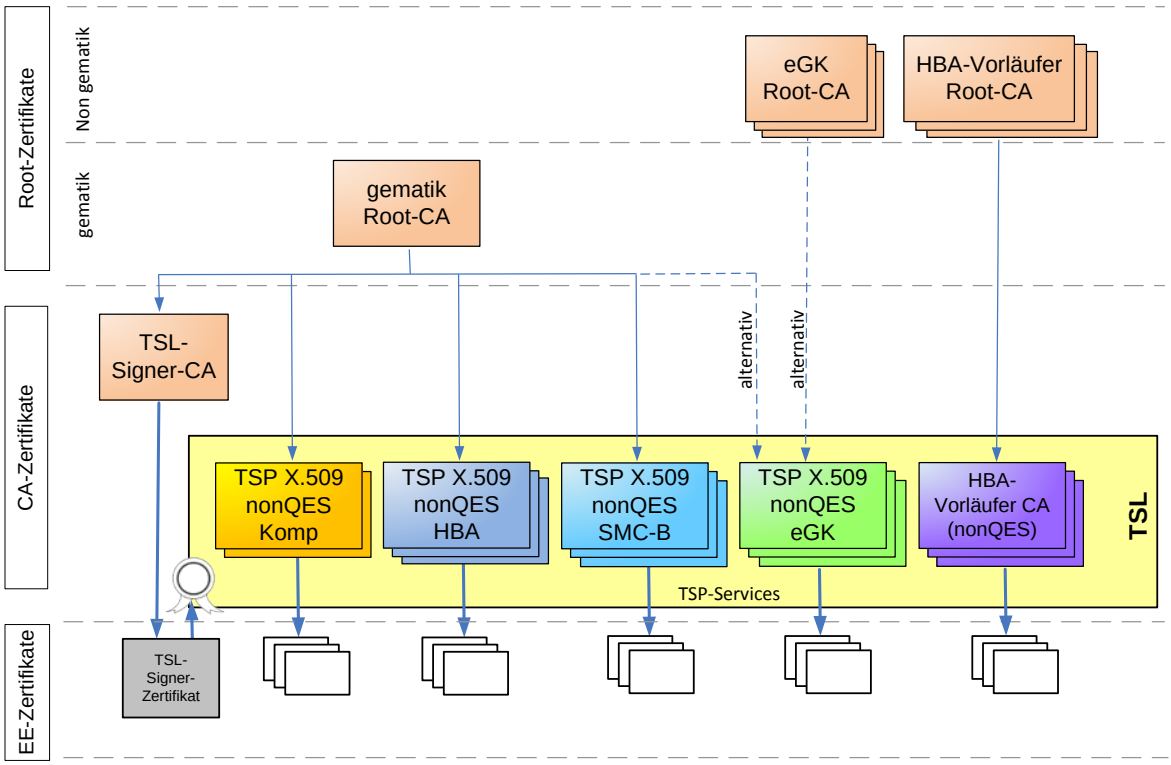
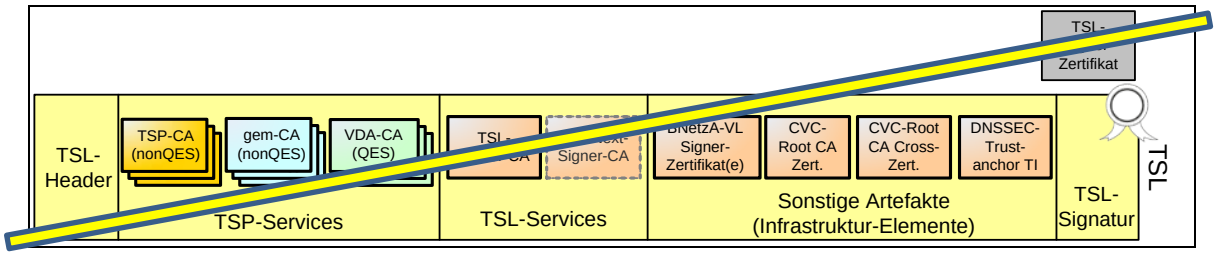


Abbildung 4: Zertifikatshierarchien und deren Abbildung in der TSL

In Abbildung 3 ist der interne Aufbau der TSL gezeigt. Nach Verwaltungsinformationen im TSL-Header werden die CA-Zertifikate der TSP-X.509, ob self-signed oder aus überge-

ordneter Root, als „TSP-Services“ in die TSL aufgenommen. „TSL-Services“ sind die Zertifikate, die zur Absicherung der TSL selbst erforderlich sind, z. B. das TSL-Signer-CA-Zertifikat. Im Falle der Aktualisierung des Vertrauensankers wird auch der neue, zukünftige Vertrauensanker aufgenommen. Das TSL-Signerzertifikat ist in die XML-Signatur der TSL eingebettet. Das TSL-Signerzertifikat wird ausgegeben von der TSL-Signer-CA, die wiederum von der gematik Root-CA zertifiziert wird.

Neben diesen Basis-Elementen, werden in der TSL auch noch weitere Infrastruktur-Elemente als Artefakte[1] mitgeführt. Dazu gehören vor allem auch die publizierten Signer-Zertifikate der BNetzA-VL[2].



~~**Abbildung 5: Aufbau der TSL**~~

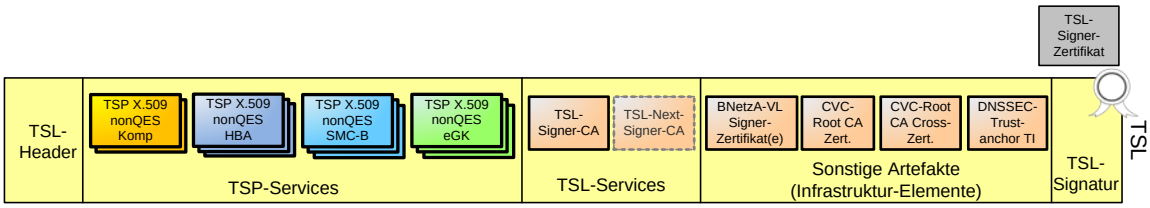


Abbildung 6: Aufbau der TSL

[…]

~~**TIP1-A_2044 Beibehalten von abgelaufenen QES-CA-Zertifikaten in der TSL**~~

~~Der TSL-Dienst MUSS QES-CA-Zertifikate, deren Gültigkeitszeitraum überschritten ist, noch 30 Jahre in der TSL belassen, nachdem das letzte von dieser CA ausgestellte QES-EE-Zertifikat zeitlich abgelaufen ist.~~

[…]

2.3.3.5 Sperrung von CA-Zertifikaten in der TSL

[…]

~~**TIP1-A_5172 Vorkehrungen bei Sperrung einer QES-CA**~~

[1] Siehe auch Hinweis in Kapitel 2.3.3 „Vertrauensraum mittels TSL – Umsetzung in der TI“.

[2] Siehe auch Kapitel 2.3.1 „Vertrauensmodell für QES“

~~Die TI-Plattform MUSS Vorkehrungen treffen, welche Maßnahmen in der TI im Falle der Sperrung einer QES-CA durch die BNetzA getroffen werden.~~ ⌫

[…]

Bei ~~QES-CAs und~~ nonQES-CAs für HBA und SMC-B wird eine solche Sperrung gemäß ~~QES-Kettenmodell (s. Kap. 2.4.3) bzw. dem~~ Kompromissmodell (s. Kap. 2.4.2) umgesetzt, indem diese CAs in der TSL auf den Status „revoked“ gesetzt werden.

[…]

⌦ **TIP1-A_2066 Verhinderung der Neuausstellung von EE-Zertifikaten bei Incidents**

~~TSP-X.509QES und~~ Ein TSP-X.509nonQES ~~MÜSSEN~~ MUSS ab dem Zeitpunkt der Feststellung eines nicht-sicherheitskritischen Incidents sicherstellen, dass von der betroffenen CA keine neuen EE-Zertifikate für den Einsatz in der TI ausgestellt werden.⌫

[…]

⌦ **TIP1-A_2069 Bestätigung des Widerrufs von CA-Zertifikaten in der TSL**

Bei dem Widerruf einer CA-Zulassung durch die gematik ~~MÜSSEN~~ MUSS der betroffene ~~TSP-X.509QES und~~ TSP-X.509nonQES den Widerruf sowie die korrekte Durchführung der Auflagen (z. B. Sperrung von CA- und EE-Zertifikaten oder Sicherstellung des weiteren Betriebs von OCSP- und Sperrdienst) schriftlich gegenüber der gematik dokumentieren und die Umsetzung bestätigen.⌫

2.3.3.6 Aktualisierung des Vertrauensraumes

[…]

Änderungen im Inhalt der TSL können sich ergeben durch:

- Initiale Aufnahme eines ~~TSP-X.509QES oder~~ TSP-X.509nonQES mit erstem CA-Zertifikat
- Aufnahme neuer CA-Zertifikate für einen bereits enthaltenen ~~TSP-X.509QES oder~~ TSP-X.509nonQES
- Update bestehender Aussteller-CA-Zertifikate nach Ablauf deren Gültigkeitszeitraumes
- Wechsel des Status eines bestehenden Aussteller-CA-Zertifikates auf „revoked“ wegen eines nicht-sicherheitskritischen Wegfalls der Zulassung für den ~~TSP-X.509QES oder~~ TSP-X.509nonQES und die betreffende CA ab einem bestimmten Datum.
- Entfernen eines Aussteller-CA-Zertifikates im Status „revoked“ nach Ablauf des regulären Gültigkeitszeitraumes
- Entfernen eines Aussteller-CA-Zertifikats aufgrund eines sicherheitskritischen Incidents
- Aufnahme oder Entfernung von BNetzA-VL-Signerzertifikaten aufgrund Änderungen der EU-LOTL

[…]

6.6.1 Konzeptionelle Festlegungen zur QES-Zertifikatsprüfung

[…]

~~Die CA-Zertifikate der QES-VDAs werden in die TSL eingebracht als Nachweis, dass diese das Zulassungsverfahren der gematik erfolgreich durchlaufen haben.~~ Die Gültigkeitsprüfung ~~eines in der TSL enthaltenen~~ ~~QES-CA-Zertifikates~~ von CA-Zertifikaten der QES-VDAs erfolgt durch die Prüfung auf sein Vorhandensein in der BNetzA-VL und seines Servicestatus in der ~~TSL und~~ BNetzA-VL.

[…]

Generelle Prüfschritte gemäß [Common-PKI] und [RFC5280], wie die Prüfung der zeitlichen Gültigkeit ~~sowie die unter 6.5.3 genannten Schritte der Prüfung von Verwendungszweck und Zertifikatsrichtlinie~~, sind auch bei der QES-Prüfung obligatorisch. Sie sind in der folgenden Übersicht zwecks Vereinfachung und Übersichtlichkeit nicht aufgeführt. ~~Die Prüfung von qualifizierten Attributzertifikaten in der TI wird unterstützt~~.

Tabelle 11: Tab_PKI_106 Ablaufschritte der QES-Zertifikatsprüfung

Ablaufschritte der QES-Zertifikatsprüfung **Anmerkung: Die Sequenz der Ablaufschritte ist funktional hergeleitet, kann jedoch auch anders gestaltet werden, sofern das Ergebnis der Prüfung qualitativ äquivalent ist.**	
Ablaufschritt 1	Prüfung ob „qualifiziert“
Beschreibung	Prüfung, ob das QES-Zertifikat das spezifische QES-Attribut („QCStatement“) als Merkmal enthält
Vorbedingung	keine
~~Anmerkungen~~	~~Für QES-Zertifikat und optional für Attributzertifikate.~~
~~Ablaufschritt 2~~	~~Prüfung des QES-CA-Zertifikates in der TSL~~
~~Beschreibung~~	~~Ermittlung des QES-CA-Zertifikates in der TSL und Prüfung des Status dieses QES-CA-Zertifikates in der TSL zum Referenzzeitpunkt.~~
~~Vorbedingung~~	~~QES-Zertifikat, TSL~~
~~Anmerkungen~~	~~Zum prüfenden Zertifikat wird das QES-CA-Zertifikat zunächst in der TSL ermittelt. Der Status dieses QES-CA-Zertifikates wird anschließend geprüft.~~
Ablaufschritt ~~3~~ 2	Prüfung des QES-CA-Zertifikates gegen die BNetzA-VL
Beschreibung	Das ~~in der TSL enthaltene~~ QES-CA-Zertifikat wird gegen die BNetzA-VL zum Referenzzeitpunkt geprüft (Prüfung auf Vorhandensein und gültigen Servicestatus des QES-CA-Zertifikates)
Vorbedingungen	BNetzA-VL
Anmerkungen	Gültiger Servicestatus des QES-CA-Zertifikates gemäß [ETSI TS 119 612#Annex J] zum Referenzzeitpunkt
Ablaufschritt ~~4~~ 3	Validierung der Zertifikatssignatur

Ablaufschritte der QES-Zertifikatsprüfung **<u>Anmerkung</u>: Die Sequenz der Ablaufschritte ist funktional hergeleitet, kann jedoch auch anders gestaltet werden, sofern das Ergebnis der Prüfung qualitativ äquivalent ist.**	
Beschreibung	Prüfung der mathematischen Korrektheit des QES-Zertifikats (Ableitung vom ermittelten QES-CA-Zertifikat)
Vorbedingungen	QES- und QES-CA-Zertifikat vorhanden
Anmerkungen	Die Prüfung erfolgt über Verifikation der Signatur
Ablaufschritt ~~5~~ 4	Prüfung des Sperrstatus
Beschreibung	Prüfung, ob Zertifikat gesperrt ist durch Abfrage des OCSP-Responders, ggf. durch Auswertung von in Signatur eingebetteter OCSP-Response.
Vorbedingung	QES-Zertifikat vorhanden
Anmerkungen	OCSP-Dienste für QES-Zertifikate müssen den Vorgaben von [eIDAS] genügen. Die Ableitung des OCSP-Signer-Zertifikates erfolgt gemäß [RFC6960]

Änderungen in gemSpec_TSL

[…]

2.1 Zweck der TSL

[…]

Um den Vertrauensraum für X.509-Zertifikate in der Telematikinfrastruktur technisch abzubilden, wird die TSL verwendet. Die TSL-Datei ist eine signierte Whitelist der zugelassenen Zertifikatsherausgeber. Das heißt, die TSL-Datei enthält sämtliche nonQES-~~ und QES~~-X.509-CA-Zertifikate, die in der TI verwendet werden.

[…]

6.1.2 Schnittstelle P_TSL-Management

[…]

6.1.2.2.4 Prüfung

⌦ **TIP1-A_4044 Prüfung auf ungültige Einträge**

Der Anbieter des TSL-Dienstes MUSS sicherstellen, dass in der aktuellen Version keine zum Zeitpunkt der TSL-Erstellung abgelaufenen Einträge enthalten sind~~, mit Ausnahme von X.509 QES-CA-Zertifikaten~~. Der Anbieter des TSL-Dienstes MUSS abgelaufene Einträge und andere Normabweichungen an gematik melden. ⌫

~~⌦ **TIP1-A_4851 Beibehalten von abgelaufenen QES-CA-Zertifikaten in der TSL**~~

~~Der TSL-Dienst MUSS QES-CA-Zertifikate, deren Gültigkeitszeitraum überschritten ist, noch 30 Jahre in der TSL belassen, nachdem das letzte von dieser CA ausgestellte QES-EE-Zertifikat zeitlich abgelaufen ist. ⌫~~

[…]

7.3.2 Angaben zum TSP-Dienst

[…]

Es bestehen die folgenden Möglichkeiten hinsichtlich URI im ServiceSupplyPoint-Element:

- Bei Einträgen von X.509-CA-Zertifikaten wird die Adresse des OCSP-Responder (oder CRL-Verteilungspunktes) eingetragen, der die Status- bzw. Sperrinformationen zu den von der CA ausgegebenen Zertifikaten zur Verfügung stellt (sofern vorhanden).

~~Wenn sich ein OCSP-Responder außerhalb der TI befindet, wird die Adresse des OCSP-Proxy eingetragen.~~

[…]

7.5 BNetzA-VL

[…]

⌦ TIP1-A_6767 BNetzA-VL ServiceInformationExtensions

Der TSL-Dienst MUSS für die BNetzA-VL im Element ServiceInformationExtensions ein Element Extension eintragen, welches den Platzhalter-OID (oid_tsl_placeholder) gemäß [gemSpec_OID#Tab_PKI_407] enthält. ⌫

Im Rahmen der QES-Zertifikatsprüfung benötigen zertifikatsprüfende Komponenten neben den Informationen in der BNetzA-VL zu CA-Zertifikaten von VDAs auch Referenzen zu deren OCSP-Respondern in der TI, wenn diese von in der TI zugelassenen VDAs bereitgestellt wurden. Die URLs der OCSP-Responder in der TI werden in der TSL anhand von Einträgen im Feld AdditionalServiceInformation als Tupel der Elemente URI und InformationValue innerhalb des Services mit ServiceTypeIdentifier für die BNetzA-VL-Signer realisiert.

⌦ TIP1-A_7219 BNetzA-VL AdditionalServiceInformation für Umleitung von OCSP-Responder-Adressen in der TI

Der TSL-Dienst MUSS für jede von der gematik bereitgestellte OCSP-Responder-URL für QES-Zwecke je ein Element AdditionalServiceInformation innerhalb des ServiceInformationExtensions Elementes als Tupel der Elemente URI und InformationValue erstellen.

Das URI Element MUSS dabei jeweils folgenden Eintrag enthalten: <URI>http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures/</URI>.

Das InformationValue Element MUSS jeweils den von der gematik bereitgestellten Text-Eintrag als String (URLs getrennt durch Leerzeichen) enthalten.⌫

Der Text-Eintrag für das InformationValue Element enthält demnach als Umsetzung der OCSP-Responder-Adresse die Quell-URL (aus dem Zertifikat in der Extension AIA) und die Ziel-URL (URL aus dem Namensraum der TI, unter der der OCSP-Responder in der TI erreichbar ist).

Ein TSL-Eintrag für ~~ein~~ die BNetzA-VL Referenzierung inklusive der URLs für OCSP-Responder für VDAs in der TI sieht also dergestalt aus:

```
<TrustServiceProvider>
   <TSPInformation>
      <TSPName>
         <Name xml:lang="de">Bundesnetzagentur für Elektrizität, Gas, Telekommunikation,
Post und Eisenbahnen</Name>
      </TSPName>
      <TSPTradeName>
         <Name xml:lang="de">Bundesnetzagentur</Name>
      </TSPTradeName>
```

```
        <TSPAddress>
            <PostalAddresses>
                <PostalAddress xml:lang="de">
                    <StreetAddress>Canisiusstr. 21</StreetAddress>
                    <Locality>Mainz</Locality>
                    <StateOrProvince>NW</StateOrProvince>
                    <PostalCode>55122</PostalCode>
                    <CountryName>DE</CountryName>
                </PostalAddress>
            </PostalAddresses>
            <ElectronicAddress>
                <URI>mailto:eIDAS@bnetza.de</URI>
            </ElectronicAddress>
        </TSPAddress>
        <TSPInformationURI>
            <URI xml:lang="en">http://www.bundesnetzagentur.de</URI>
        </TSPInformationURI>
    </TSPInformation>
    <TSPServices>
        <TSPService>
            <ServiceInformation>
                <ServiceTypeIdentifier>
                    http://uri.telematik/TrstSvc/Svctype/TrustedList/schemerules/DE
                </ServiceTypeIdentifier>
                <ServiceName>
                    <Name xml:lang="de">
                      {z.B.“CN=14R-TSL 1:PN,O=Bundesnetzagentur,C=DE”}
                    </Name>
                </ServiceName>
                <ServiceDigitalIdentity>
                    <DigitalId>
                      <X509Certificate>
                            Base64-codiertes BNetzA-VL-Signer-Zertifikat}
                      </X509Certificate>
                    </DigitalId>
                    {weitere DigitalId-Elemente mit Signer-Zertifikaten}
                </ServiceDigitalIdentity>
                <ServiceStatus>
                    http://uri.etsi.org/TrstSvc/Svcstatus/inaccord
                </ServiceStatus>
                    <StatusStartingTime>
                    {z.B. “ 2016-07-01T00:00:01Z”}
                    </StatusStartingTime>
                <ServiceSupplyPoints>
                    <ServiceSupplyPoint>
                    {primäre TI-Download-Adresse der BNetzA-VL}
                    </ServiceSupplyPoint>
                    <ServiceSupplyPoint>
                    {sekundäre TI-Download-Adresse der BNetzA-VL}
                    </ServiceSupplyPoint>
                </ServiceSupplyPoints>
                <ServiceInformationExtensions>
                    <Extension Critical="false">
                      <ExtensionOID>{oid_tsl_placeholder}</ExtensionOID>
                      <ExtensionValue>oid_tsl_placeholder</ExtensionValue>
                    </Extension>
                    <Extension Critical="false">
                      <AdditionalServiceInformation>
```

```
                                <URI>
                                    http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures
                                </URI>
                                <InformationValue>
                                    {TextFeld: Quell-URL1 Ziel-URL1}
                                 </InformationValue>
                            </AdditionalServiceInformation>
                            <AdditionalServiceInformation>
                                <URI>
                                    http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures
                                </URI>
                                <InformationValue>
                                    {TextFeld: Quell-URL2 Ziel-URL2}
                                 </InformationValue>
                            </AdditionalServiceInformation>
                            {ggf. weitere AdditionalServiceInformation-Elemente}
                           </Extension>
                      </ServiceInformationExtensions>
                 </ServiceInformation>
            </TSPService>
        </TSPServices>
</TrustServiceProvider>
```

Änderungen in gemSpec_OCSP_Proxy

[…]

2 Systemüberblick

Der Produkttyp OCSP-Proxy wird eingesetzt, um die Statusinformation der Zertifikate der zeitlich begrenzt durch die TI unterstützten HBA-Vorläuferkarten in der TI-Plattform verfügbar zu machen.

Zusätzlich ermöglicht er das Weiterleiten von OCSP-Anfragen aus der TI an andere im Internet erreichbare OCSP-Responder für QES-Zwecke.

Im Falle von OCSP-Anfragen für End-Entity- Zertifikate leitet der OCSP-Proxy die Anfrage an den zuständigen OCSP-Responder im Internet weiter und gibt die vom OCSP-Responder zurück gelieferte OCSP-Antwort an die zertifikatsvalidierende Komponente zurück.

[…]

5.1.1.1 Schnittstellendefinition

Der OCSP-Proxy muss die technische Schnittstelle I_OCSP_Status_Information gemäß [gemSpec_PKI#9] implementieren und in der Telematikinfrastruktur anbieten.

Über diese Schnittstelle werden die Statusinformation für Zertifikate der unterstützten HBA-Vorläuferkarten und anderer QES-Verfahren in der TI-Plattform verfügbar gemacht.

[…]

5.1.1.2 Umsetzung

[…]

⌦ **TIP1-A_5849 OCSP-Anfragen aus der TI beantworten**

Der OCSP-Proxy MUSS den technischen Use Case "TUC_OCSP-Proxy_002 OCSP-Anfragen aus der TI beantworten" gemäß Tab_OCSP-Proxy_002 umsetzen. ⌫

[…]

Tabelle 1: Tab_OCSP-Proxy_002 TUC_OCSP-Proxy_002 OCSP-Anfragen aus der TI beantworten

Element	Beschreibung
Name	TUC_OCSP-Proxy_002 "OCSP-Anfragen aus der TI beantworten"

Beschreibung	Dieser Use Case beschreibt den Prozess der Zertifikatsstatusauskunft des OCSP-Proxys bei OCSP-Anfragen für nonQES-EE- und QES-EE-Zertifikate der HBA-Vorläuferkarten und anderer QES-Verfahren.
Auslöser	OCSP-Anfrage einer zertifikatsvalidierenden Komponente aus der TI
Vorbedingungen	
Eingangsdaten	OCSP-Anfrage
Komponenten	Zertifikatsvalidierende Komponenten der TI (z. B. Konnektor), OCSP-Proxy, OCSP-Responder (der HBA-Vorläuferkarten, u.a.)
Ausgangsdaten	OCSP-Antwort eines OCSP-Responders ~~von HBA-Vorläuferkarten~~
Nachbedingungen	
Standardablauf	1. [OCSP-Proxy]: OCSP-Anfrage der zertifikatsvalidierenden Komponente empfangen. 2. [OCSP-Proxy]: OCSP-Anfrage ~~unter Verwendung von "ServiceSupplyPoint Internet"~~ an den entsprechenden OCSP-Responder im Internet weiterleiten unter Verwendung der Ziel-URL im Internet aus der empfangenen OCSP-Anfrage. 3. [OCSP-Proxy]: OCSP-Antwort des OCSP-Responders im Internet empfangen. 4. [OCSP-Proxy]: OCSP-Antwort des OCSP-Responders im Internet an zertifikatsvalidierende Komponente zurückgeben.
Varianten/Alternativen	
Fehlerfälle	2a [OCSP-Proxy]: Der OCSP-Responder im Internet ist nicht erreichbar: OCSP-Response mit einer unsignierten Error-Response des Typs "internalError" (siehe [RFC2560#2.3]) zurückgeben.
Nichtfunktionale Anforderungen	
Anmerkungen	Die URL, mit der der OCSP-Proxy-Responder angesprochen wird, enthält auch die Ziel-URL des OCSP-Responders im Internet (s. [gemSpec_VPN_ZugD#TIP1-A_4322]).
Zugehörige Diagramme	

Änderungen in Produkttypsteckbriefen

Die Änderung betrifft die folgenden Produkttypsteckbriefe:

- gemProdT_TSL
- gemProdT_Kon
- gemProdT_X.509_TSP_QES
- gemProdT_OCSP_Proxy