
C_12257_Anlage

Inhaltsverzeichnis

1 Änderungsbeschreibung.....	2
2 Änderung in gemSpec_PKI.....	3
2.1.1 Kapitel 8.5.2 TUC_PKI_036 „BNetzA-VL Aktualisierung“	3
2.1.2 Kapitel 8.5.1 TUC_PKI_030 „QES-Zertifikatsprüfung“	9
2.1.3 Kapitel 11.5.2 Weitere Dokumente.....	19
3 Änderung in gemKPT_PKI_TIP.....	21
3.1.1 Kapitel 8.5.2 Weitere Dokumente.....	21
4 Änderung in gemSpec_TSL.....	22
4.1.1 8.5.2 Weitere Dokumente.....	22
5 Änderungen in Steckbriefen.....	23
5.1 Änderungen in gemProdT_eRp_FD.....	23
5.2 Änderungen in gemProdT_Kon_Highspeed.....	23
5.3 Änderungen in gemProdT_Kon_PTV5Plus.....	23
5.4 Änderungen in gemProdT_Kon_PTV6.....	24

1 Änderungsbeschreibung

Zur Prüfung und Erstellung qualifizierter Zertifikate gemäß eIDAS-Verordnung wird in Deutschland gemäß Vertrauensdienstegesetz (VDG) die Vertrauensliste der Bundesnetzagentur (BNetzA-VL) verwendet. Die technischen Vorgaben und Rahmenbedingungen für Vertrauenslisten der EU wurden bisher durch den Implementation Act CID 2015/1505 rechtskräftig und verweisen dabei als technische Basis auf den Standard ETSI TS 119 612 in der Version 2.1.1 (von 07/2015). Für Mai 2025 wurde von der EU-Kommission eine Aktualisierung des Implementation Act angekündigt, wodurch als technische Grundlage für die Vertrauenslisten nun die Version 2.3.1 des ETSI-Standards Verwendung finden wird.

Auch die QES-Signaturen und -Zertifikate in der Telematikinfrastruktur (TI) unterliegen diesen technischen Regelungen und müssen verpflichtend eingehalten werden.

Da die Erstellung und Bereitstellung der BNetzA-VL durch die Bundesnetzagentur erfolgt und dabei von der EU-Kommission bereitgestellte Tools verwendet werden, wird nach Inkrafttreten des aktualisierten Implementation Act der aktualisierte Standard ETSI TS 119 612 v.2.3.1 (von 11/2024) bei der nächsten Veröffentlichung der BNetzA-VL sofort zum Einsatz kommen.

Eine Berücksichtigung des neuen Standards ist für alle Produkttypen der TI zwingend notwendig, die QES-Zertifikate prüfen. Ggf. sind dafür Produkt-Anpassungen vorzunehmen.

Die gematik beschreibt in der gemSpec_PKI mit TUC_PKI_036 (GS-A_5484-01), wie QES-prüfende Systeme die BNetzA-VL aktualisieren müssen. In TUC_PKI_030 (GS-A_4750-02) ist geregelt, wie diese Systeme Prüfungen von QES-Zertifikaten durchführen müssen. Dabei wird jeweils auf den zu verwendenden ETSI-Standard verwiesen. Aufgrund der oben beschriebenen Veränderungen werden entsprechende Anpassungen an den Spezifikationen mit Hinweisen auf den neueren Standard ETSI TS 119 612 v.2.3.1 (von 11/2024) vorgenommen.

2 Änderung in gemSpec_PKI

2.1.1 Kapitel 8.5.2 TUC_PKI_036 „BNetzA-VL Aktualisierung“

GS-A_5484-02 -TUC_PKI_036 „BNetzA-VL-Aktualisierung“

Alle Produkttypen, die die BNetzA-VL verwenden, MÜSSEN TUC_PKI_036 zur Aktualisierung umsetzen.

Tabelle 1: TUC_PKI_036 „BNetzA-VL Aktualisierung“

Element	Beschreibung
Name	TUC_PKI_036 „BNetzA-VL Aktualisierung“
Beschreibung	Dieser Use Case beschreibt die Aktualisierung der im System gespeicherten BNetzA-VL.
Anwendungsumfeld	System, das die BNetzA-VL verwendet
Vorbedingungen	Eine aktuell gültige TSL im System
Auslöser	Produktypspezifischer Trigger
Eingangsdaten	<ul style="list-style-type: none">optional: neu eingebrachte BNetzA-VL-Datei
Komponenten	System
Ausgangsdaten	Status des Prozesses
Referenzen	[ETSI TS_119_612]. [XML] [XMLSig]
Standardablauf	<p>Der Standardablauf stellt die Prüfungen dar, die vollzogen werden müssen. Die Reihenfolge der Schritte ist aber nicht normativ. Eine Trennung in zwei Prozesse oder eine Umstrukturierung, bei der alle notwendigen Prüfungen erfolgen, ist zulässig.</p> <ol style="list-style-type: none">1. [System:] System startet die Aktualisierung der BNetzA-VL2. [System:] Primäre BNetzA-VL Hash Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]).3. [System:] Von der im vorherigen Schritt ermittelten Downloadadresse den aktuellen BNetzA-VL Hashwert vom TSL-Dienst

	<p>herunterladen.</p> <p>4.</p> <p>[System:] Heruntergeladenen BNetzA-VL Hashwert mit dem Hashwert der aktuell im System gespeicherten BNetzA-VL (falls vorhanden) vergleichen. Falls die Hashwerte verschieden sind oder im System noch keine BNetzA-VL vorhanden ist muss die BNetzA-VL im System aktualisiert werden.</p> <p>5.</p> <p>[System:] Primäre BNetzA-VL Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]).</p> <p>6.</p> <p>[System:] Von der ermittelten Downloadadresse die aktuelle BNetzA-VL vom TSL-Dienst herunterladen.</p> <p>7.</p> <p>[System:] Die Wohlgeformtheit der BNetzA-VL-Datei prüfen.</p> <p>8.</p> <p>[System:] Die BNetzA-VL-Datei gegen das XML-Schema gem. [ETSI_TS_119_612#Annex C.2] validieren (Hierzu muss das in Annex C.2 referenzierte XML-Schema für die Validierung verwendet werden).</p> <p>9.</p> <p>[System:] Die Aktualität der BNetzA-VL prüfen. Dies geschieht anhand des aktuellen Datums und des Elements „NextUpdate“ aus der BNetzA-VL. Die BNetzA-VL wird als aktuell bezeichnet, wenn ihr NextUpdate nicht in der Vergangenheit liegt.</p> <p>10.</p> <p>[System:] Das verwendete BNetzA-VL-Signer-Zertifikat aus der BNetzA-VL-Datei extrahieren.</p> <p>11.</p> <p>[System:] Prüfen ob das BNetzA-VL-Signerzertifikat in der TSL enthalten ist. Die Identifizierung des Zertifikats erfolgt durch</p> <ul style="list-style-type: none">• Suche nach einem TSPService mit ServiceTypeldentifizier für „BNetzA-VL“ gem. [gemSpec_TSL#7.3.2] und• Vergleich des Elements X509Certificate in zugehöriger DigitalId mit dem BNetzA-VL-Signer-Zertifikat aus Schritt 10 <p>12.</p> <p>[System:] Die XML-Signatur der BNetzA-VL-Datei mittels in der TSL gefundenem BNetzA-VL-Signerzertifikat entweder gem. [XAdES-BES] (depricated) oder gem. [XAdES-B-B] prüfen.</p> <p>13.</p> <p>[System:] Die aktualisierte BNetzA-VL und deren Hashwert (falls vorhanden) sicher im System speichern. Ende des Use Cases.</p>
--	---

Varianten/Alternativen	<p>1a. [System:] Wenn eine BNetzA-VL-Datei als Eingangsparameter eingebracht wurde, dann wird diese Datei validiert und geprüft. Weiter mit Schritt 7.</p> <p>2a. [System:] Das Element ist nicht vorhanden. Weiter mit Schritt 3a.2</p> <p>3a. [System:] Das Herunterladen von der primären Downloadadresse schlägt fehl.</p> <p>3a.1 [System:] Das Herunterladen wird bis zu drei Mal wiederholt versucht (insgesamt wird der Vorgang also maximal vier Mal ausgeführt). Falls erfolgreich, weiter mit Schritt 4.</p> <p>3a.2 [System:] Backup BNetzA-VL Hash Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]). Falls nicht erfolgreich, weiter mit Schritt 5.</p> <p>3a.3 [System:] Das Herunterladen wird von der Backup Downloadadresse ausgeführt. Falls erfolgreich, weiter mit Schritt 4.</p> <p>3a.4 [System:] Das Herunterladen von der Backup Downloadadresse wird bis zu drei Mal wiederholt versucht (insgesamt wird der Vorgang also maximal vier Mal ausgeführt). Falls erfolgreich, weiter mit Schritt 4. Falls nicht erfolgreich, weiter mit Schritt 5.</p> <p>4a. [System:] Die verglichenen Hashwerte sind identisch. In diesem Fall ist die im System gespeicherte BNetzA-VL aktuell. Ende des Use Cases ohne Fehler.</p> <p>5b. [System:] Das Element ist nicht vorhanden. Weiter mit Schritt 6a.2</p> <p>6a. [System:] Das Herunterladen von der primären Downloadadresse schlägt fehl.</p> <p>6a.1 [System:] Das Herunterladen wird bis zu drei Mal wiederholt versucht (insgesamt wird der Vorgang also maximal vier Mal ausgeführt). Falls erfolgreich, weiter mit Schritt 7.</p> <p>6a.2 [System:] Backup BNetzA-VL Download-Adresse aus der TSL extrahieren (s. [gemSpec_TSL#7.5]).</p> <p>6a.3 [System:] Das Herunterladen wird von der Backup Downloadadresse ausgeführt. Falls erfolgreich, weiter mit Schritt 7.</p> <p>6a.4</p>
------------------------	--

	<p>[System:] Das Herunterladen von der Backup Downloadadresse wird bis zu drei Mal wiederholt versucht (insgesamt wird der Vorgang also maximal vier Mal ausgeführt). Falls erfolgreich, weiter mit Schritt 7.</p>
Fehlerfälle	<p>Ein Abbruch des TUC führt nur dazu, dass keine neue BNetzA-VL gespeichert wird. Er hat keinen Einfluss auf die Gültigkeit der bestehenden BNetzA-VL. Das System muss dies jedoch protokollieren.</p> <p>6a.2a [System:] Das Element ist nicht vorhanden. Ende des Use Case mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>6a.4a [System:] Das Herunterladen der BNetzA-VL ist fehlgeschlagen. Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>7a. [System:] Die XML-Datei ist nicht wohlgeformt. Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>8a. [System:] Die XML-Schema-Validierung liefert einen Fehler. Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>9a. [System:] Die Aktualitäts-Prüfung ergibt, dass die BNetzA-VL abgelaufen ist (nextUpdate < aktuelles Datum). Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>10a. [System:] Das BNetzA-VL-Signer-Zertifikat lässt sich nicht aus der BNetzA-VL-Datei extrahieren. Ende des Use Cases mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>11a. BNetzA-VL-Signerzertifikat ist nicht in der TSL enthalten. Ende des Use Case mit der Fehlermeldung VL_UPDATE_ERROR.</p> <p>12a. [System:] Die Signatur ist nicht gültig. Ende des Use Cases mit der Fehlermeldung XML_SIGNATURE_ERROR.</p>
Sicherheitsanforderungen	<p>Es gelten die allgemeinen Sicherheitsanforderungen an den Produkttypen.</p>
Anmerkungen	<p>Das BNetzA-VL-Signer-Zertifikat wird vor Aufnahme in die TSL geprüft (s. [gemSpec_TSL#6.3]). Diese Prüfschritte werden</p>

	darum nach dem Download innerhalb der TI nicht wiederholt.
Zugehörige Diagramme	

[<=,Konnektor Highspeed, Konnektor PTV5Plus, Konnektor PTV6, eRp_FD,Sich.techn.
 Eignung: CC-Evaluierung, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test
 Produkt/FA, Sich.techn. Eignung: Prüfung durch CC-Prüfstelle]

2.1.2 Kapitel 8.5.1 TUC_PKI_030 „QES-Zertifikatsprüfung“

GS-A_4750-02 -TUC_PKI_030 „QES-Zertifikatsprüfung“

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

Tabelle 2: TUC_PKI_030 „QES-Zertifikatsprüfung“

Element	Beschreibung
Name	TUC_PKI_030 „QES-Zertifikatsprüfung“
Beschreibung	<p>In diesem Use Case wird die Prüfung von Zertifikaten mit qualifizierter Signatur beschrieben.</p> <p>Die Prüfung von QES-Zertifikaten und die Sperrprüfung per OCSP entsprechen den gesetzlichen Vorgaben und relevanten Standards. Die zugrundeliegende Prüfung des Zertifikatspfads (Validation Certificate Path) basiert auf dem Kettenmodell (chain model), siehe Anmerkung [1].</p> <p>Zusätzlich werden folgende Schritte in diesem Technical Use Case (TUC) durchgeführt.</p>
Anwendungsumfeld	System, das Zertifikate verwendet
Vorbedingungen	<p>aktuelle TLS-Informationen im Truststore (inkl. OCSP-Adressen in der TI für die zugelassenen VDAs),</p> <p>eine aktuell gültige BNetzA-VL.</p>
Auslöser	Zertifikats-Check
Eingangsdaten	<ul style="list-style-type: none"> QES-Zertifikat Referenzzeitpunkt (optional; bei Nichtangabe Verwendung der aktuellen Systemzeit): Zeitpunkt, für den das Zertifikat geprüft werden soll, Details siehe

	<p>Anmerkung [2]</p> <ul style="list-style-type: none"> • 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) • Timeout-Parameter für OCSP-Abfragen (Default: 10s)
Komponenten	System
Ausgangsdaten	<ul style="list-style-type: none"> • Status der Prüfung • OCSP-Response zum angefragten QES-Zertifikat • im Zertifikat enthaltene Rollen-OIDs • im Zertifikat enthaltene QCStatements-Einträge
Referenzen	[eIDAS], [VDG], [ETSI TS 119 612] (neue Version 2.3.1 (Stand November 2024), [ETSI EN 319 412-5], [ETSI EN 319 412-2], [ETSI EN 319 102-1], [ETSI TS 119 172-4] [RFC5280], [RFC6960], [RFC5019]
Standardablauf	<ol style="list-style-type: none"> 1. [System:] Auslesen und Ausgabe aller gesetzten Elemente der Extension QCStatements des Zertifikates, Details siehe Anmerkung [3]. 2. [System:] Prüfung der (zeitlichen) Gültigkeit des Zertifikats mittels TUC_PKI_002 "Gültigkeitsprüfung des Zertifikats", Details siehe Anmerkung [4]. 3. [System:] Prüfung der Extension KeyUsage auf Vorhandensein und die richtige Belegung entsprechend [ETSI EN 319 412-2], Details siehe Anmerkung [5]. 4. [System:] Anhand der End-Entity-Zertifikate wird die BNetzA-VL durchsucht, um das passende QES-CA-Zertifikat zu finden. 5. [System:] Prüfung, ob das ausstellende QES-CA-Zertifikat für die QES-Prüfung zum Zeitpunkt der Erstellung des End-Entity-Zertifikats in der BNetzA-VL gemäß [eIDAS] und [ETSI TS 119 612]

	<p>qualifiziert und als gültig gekennzeichnet ist, Details siehe Anmerkung [7].</p> <p>6.</p> <p>[System:] Prüfung der mathematischen Signaturkorrektheit des Signaturzertifikats zum übergebenen Referenzzeitpunkt gegen das CA-Zertifikat aus Schritt 5 nach dem Kettenmodell, Details siehe Anmerkungen [1], [9].</p> <p>7.</p> <p>[System:] Ermittlung der OCSP-Adresse aus 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 TLS derselbe Wert im InformationValue-Element von AdditionalServiceInformation von BNetzA-VL-Service (mit ServiceTypenIdentifier 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, Details siehe Anmerkung [10].</p> <p>8.</p> <p>[System:] Die abzufragenden Statusinformationen zu QES-Zertifikaten werden per OCSP-Requests unter Verwendung der aus der TLS ermittelten OCSP-Adresse aus Schritt 7 eingeholt.</p> <p>9. Prüfung der OCSP-Response auf Integrität</p> <p>[System, OCSP-Responder:] Das dazu benötigte OCSP-Responder-Zertifikat (OCSP-Signer-Zertifikat) wird aus dem URI (markiert mit dem ServiceTypenIdentifier http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP oder http://uri.etsi.org/TrstSvc/Svctype/Certstatus/OCSP/QC) in der BNetzA-VL ermittelt. Die Signatur der OCSP-Response wird zum Referenzzeitpunkt mittels des ermittelten OCSP-Signer-Zertifikats geprüft. Falls keiner der URIs vorhanden ist, wird weiter mit Schritt 10 verfahren, siehe Anmerkung [12].</p> <p>10.</p> <p>[System, OCSP-Responder:] Das OCSP-Signer-Zertifikat aus dem Feld „certs“ in der OCSP-Response ermitteln. Die Signatur des OCSP-Signer-Zertifikats wird entsprechend mittels des im Schritt 6 validierten QES-CA-Zertifikats geprüft. Die Signatur der OCSP-Response wird anschließend mittels des ermittelten OCSP-Signer-Zertifikats geprüft, siehe Anmerkungen [12].</p> <p>11.</p> <p>[System] Auswertung der OCSP-Response. Dies umfasst die Prüfung gemäß Standards (Details</p>
--	---

	<p>siehe Anmerkung [11])</p> <ul style="list-style-type: none"> • Statuscode („OCSPResponseStatus“) auf Belegung mit ‚0‘ (für „successful“), • Zertifikatsidentifizierungs-Informationen („CertID“) auf Identität mit derjenigen aus dem Request und • Konformität/Plausibilität der Zeitangaben („producedAt“, „thisUpdate“ und (sofern vorhanden) „nextUpdate“). <p>12. [System:] Überprüfung der Gültigkeit der Statusinformation anhand des übergebenen Referenzzeitpunkts. Der certStatus „good“ wird gemeldet. Rückmeldung „Das Zertifikat ist gültig“ und Rückgabe der OCSP-Response.</p> <p>13. [System:] Ermittlung der Rolle (TUC_PKI_009 "Rollenermittlung")</p> <p>14. [System:] Ende des Use Case mit Rückgabe des/der im Zertifikat enthaltenen Rollen-OID(s)</p>
Varianten/ Alternativen	<p>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.</p> <p>7a. [System:] Der Offline-Modus ist aktiviert. Es werden keine Statusinformationen eingeholt. (Schritte 8, 9, 10, 11 und 12 entfallen)</p> <p>8a. [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.</p> <p>8b. [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.</p>
Fehlerfälle/ Warnung	<p>In jedem der beschriebenen Schritte können Fehler auftreten. Diese sind durch das System zu melden und der Prozess muss beendet werden.</p> <p>1a. Ist die Extension QCStatements nicht auslesbar, leer oder enthält keine auslesbaren Elemente, bricht der TUC mit dem Fehler</p>

	<p>QC_STATEMENT_ERROR ab.</p> <p>3a. [System:] KeyUsage ist nicht vorhanden bzw. entspricht nicht der vorgesehenen keyUsage (WRONG_KEYUSAGE)</p> <p>5a. 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.</p> <p>5b. [System:] QES-CA-Zertifikat des QES-Zertifikates ist in der BNetzA-VL als revoked gekennzeichnet und QES-Zertifikat ist nach Sperrzeitpunkt erstellt worden. Abbruch mit Fehlermeldung (CA_CERTIFICATE_REVOKED_IN_BNETZA-VL).</p> <p>6a. [System] Die Zertifikats-Signatur ist nicht gültig. Ende des Use Case. Abbruch mit Fehlermeldung (CERTIFICATE_NOT_VALID_MATH)</p> <p>7b. [System:] Warnmeldung, dass keine Online-Statusprüfung durchgeführt wurde (NO_OCSP_CHECK).</p> <p>8c. [System:]. Der zuständige OCSP-Responder ist nicht erreichbar. Abbruch mit Fehlermeldung (OCSP_NOT_AVAILABLE).</p> <p>8d. [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.</p> <p>8e. Wenn die in einer OCSP-Response zurückgelieferte Nonce nicht mit der Nonce des OCSP-Requests für ein QES-Zertifikat übereinstimmt, wird die Prüfung abgebrochen mit der Fehlermeldung OCSP_NONCE_MISMATCH.</p> <p>8f. [System] Nach zeitlichem Ablauf der TSL-Graceperiod ist die aus der TSL zu ermittelnde OCSP-Adresse nicht mehr vertrauenswürdig. Abbruch mit Fehlermeldung (OCSP_CHECK_REVOCATION_ERROR).</p> <p>9a/10a. [System:] OCSP-Signer-Zertifikat nicht in der</p>
--	--

	<p>OCSP-Response enthalten. Abbruch mit Fehlermeldung. (OCSP_CERT_MISSING). 9a1/10a1.</p> <p>[System] Signatur der OCSP-Response ist nicht gültig. Abbruch mit Fehlermeldung (OCSP_SIGNATURE_ERROR) 11a.</p> <p>[System] Die Response enthält einen Statuscode („OCSPResponseStatus“), der ungleich 0 (für „successful“) ist. (Damit zeigt der OCSP-Responder eine Exception an. Beispielsweise kann der Wert für den Status auf 3 für „tryLater“ gesetzt sein.) Abbruch mit Fehlermeldung (OCSP_STATUS_ERROR) 11b.</p> <p>[System] Die Response enthält einen Statuscode („OCSPResponseStatus“), der gleich 0 („successful“) ist. Die ausgewertete OCSP-Response passt aber nicht zum OCSP-Request (z.B. CertID in OCSP-Request und -Response stimmt nicht überein, s. a. Anmerkung [13]). Abbruch mit Fehlermeldung (OCSP_CHECK_REVOCATION_ERROR) 12a.</p> <p>[System:] Das Zertifikat ist für den Referenzzeitpunkt gültig, obwohl der CertStatus "revoked" gemeldet wird, da "revocationTime" > Referenzzeitpunkt. Rückmeldung Zertifikat ist für den Referenzzeitpunkt gültig und Rückgabe der OCSP-Response, siehe Anmerkung [14]. 12b.</p> <p>[System:] Zertifikat ist gesperrt und die Referenzzeit liegt nach dem Sperrzeitpunkt (CertStatus revoked UND revocationTime <= Referenzzeitpunkts). Rückmeldung Zertifikat ist gesperrt und Rückgabe der OCSP-Response. (CERT_REVOKED) 12c.</p> <p>[System:] Zertifikat ist unbekannt (Status unknown) Rückmeldung, dass das Zertifikat ungültig ist und Rückgabe der OCSP-Response. (CERT_UNKNOWN)</p> <p>Weitere Fehlerfälle werden in den jeweiligen referenzierten Use Cases beschrieben.</p>
Sicherheitsanforderungen	Es gelten die allgemeinen Sicherheitsanforderungen an die Produkttypen der TI, die QES-Zertifikate prüfen, siehe auch [RFC6960] Kap. 5.
Anmerkungen	<p>Folgende Hinweise sollen als Hilfestellung für eine Umsetzung des TUC dienen:</p> <p>[1] Kettenmodell (chain model) für die Validierung von QES-X.509-Zertifikatketten: Alle</p>

	<p>CA-Zertifikate müssen zum Zeitpunkt der Ausstellung eines QES-EE-Zertifikats gültig sein und das Zertifikat war beim Erstellen der qualifizierten Signatur gültig und nicht von der CA gesperrt, s. Artikel 32, Absatz (1), Satz (b) [eIDAS], Definition Kettenmodell s. [ETSI TR 119 001], Verwendung v. Prüfmodellen s. [ETSI EN 319 102-1] Kap. 5.2.6.4.</p> <p>[2] Weiterführende Informationen siehe Glossar aus Kap. 11.2 und Definition der Zeitparameter aus [gemSpec_Kon] Kap. 4.1.8.1.3.</p> <p>[3] Schritt 1: Im Signaturzertifikat muss mindestens ein QCStatement mit dem OID id-etsi-qcs-QcCompliance. (0.4.0.1862.1.1) enthalten sein. Die QC-Statement-Typen werden in ETSI EN 319 412-5, insbesondere Kap. 5 – Table 2 für QES-Zertifikate, bezüglich der Extension QCStatements des Zertifikates beschrieben.</p> <p>[4] Schritt 2: Die (zeitliche) Gültigkeitsprüfung ist nach [eIDAS] Artikel 28 Satz (1) ANHANG I Buchstabe e) auch für die QES-Zertifikatsprüfung gemäß TUC_PKI_030 verpflichtend, s. a. [ETSI EN 319 412-5] Annex A.1 Buchstabe (e).</p> <p>[5] Schritt 3: Die Prüfung der KeyUsage lehnt sich an [RFC5280] Kap. 4.2.1.3 und [ETSI EN 319 412-2] Kap. 4.3.2 – Table 1 (KeyUsage v. Type A) sowie Tab_PKI_270.</p> <p>[6] Schritt 4: 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.</p> <p>[7] Schritt 5: Gültigkeitsstatus einer QES-CA wird gemäß [ETSI TS 119 612] Kap. 5.5.4 und Annex J durch den Servicestatus granted und withdrawn in der BNetzA-VL gekennzeichnet. Pre-eIDAS-relevante Servicestatus (undersupervision, supervisionincession oder accredited) werden in granted bzw. (supervisionceased oder supervisionrevoked") in withdrawn überführt.</p> <p>Historien zum Servicestatus v. VDAs, hinterlegt im Element ServiceHistory in der BNetzA-VL, sind bei der Prüfung der CA zu berücksichtigen.</p> <p>[8] Die Einträge der QES-CA-Zertifikate in der BNetzA-VL besitzen gemäß [ETSI TS 119 612] Kap. 5.5.9.4 die Extension additionalServiceInformation http://uri.etsi.org/TrstSvc/TrustedList/SvcInfoExt/ForeSignatures.</p> <p>[9] Schritt 6: Die Prüfung der Korrektheit der digitalen Signatur des Signaturzertifikats ist z.B. gemäß FDP_DAU.2/QES aus [BSI-CC-PP-0098] ein Bestandteil der QES-Prüfung, welcher sich nicht aus TUC_PKI_004 ableiten lässt.</p>
--	--

	<p>[10] Schritt 7:</p> <ul style="list-style-type: none"> • Details zu den TSL-Einträgen für URLs für OCSP-Responder in der TI unter gemSpec_TSL#TIP1-A_7219. Das Verfahren zur Weiterleitung der OCSP-Anfrage an die zuvor ermittelte OCSP-Adresse aus dem AIA-Feld ist analog zur Weiterleitung von OCSP-Anfragen für QES-Zertifikate der Vorläuferkarten (HBAqSig/ZOD2). • Die Bereitstellung von Statusprüfdiensten durch die VDAs richtet sich nach den Vorgaben gemäß [eIDAS] Artikel 24, Abs. (2) Buchstabe k), Abs. (3) und (4). Die technische Umsetzung des Statusprüfdienstes per OCSP basiert auf [RFC6960]. <p>[11] Schritt 11: Die Response enthält einen Statuscode („OCSPResponseStatus“), der gleich 0 („successful“) ist:</p> <ul style="list-style-type: none"> • Die Prüfung der certHash-Erweiterung richtet sich nach GS-A_4693 und [gemSpec_Krypt#GS-A_4393] • Die Auswertung der OCSP-Responses (Signatur der OCSP-Responses) gemäß [RFC6960] Kap. 4.1, 4.2 und 4.4 und Kap. 9.1.2 aus [gemSpec_PKI] <p>[12] Schritt 9, 10: Zur Prüfung der OCSP-Response auf Integrität (Signatur):</p> <ol style="list-style-type: none"> 1. Die gematik trifft hierzu keine Vorgabe zum Prüfmodell für die Validierung der Signatur von im TUC verwendeten OCSP-Signer-Zertifikaten. 2. Schritt 9: Das OCSP-Signer-Zertifikat kann gemäß [RFC6960] von der ausstellenden QES-CA selbst signiert sein oder von einer beliebigen aktuell qualifizierten CA (vgl. gemKPT_PKI_TIP#4.5). In Bezug auf die Anmerkung aus [ETSI TS 119 612] Kap. 5.5.1.1 (a) NOTE - können OCSP-Signer-Zertifikate aufgrund der Komplexitätsreduzierung nicht direkt als Statusprüfdienst in die BNetzA-VL eingetragen sein (s. URIs in Schritt 9), siehe Schritt 10. 3. Schritt 10: Falls keiner der URIs in der BNetzA-VL vorhanden ist, muss die Prüfung der Signatur der Response technisch gemäß [RFC6960] mittels des OCSP-Signer-Zertifikats erfolgen, welches von der ausstellenden QES-CA selbst signiert und im Feld „certs“ der „BasicOCSPResponse“
--	---

	<p>hinterlegt ist (Festlegung dazu siehe Vorgabe aus Kapitel 9.1.2.7). Der Vertrauensstatus des OCSP-Signer-Zertifikats muss somit über die BNetzA-VL prüfbar sein</p> <p>[13] Schritt 11b: Die OCSP-Response muss gemäß [RFC6960] Kap. 4.2 verarbeitet werden, unabhängig davon, ob das Feld "parameters" der Sequenz AlgorithmIdentifier innerhalb der CertID mit NULL belegt oder nicht gesetzt ist, siehe Tab_PKI_290. Der in [RFC5754] Kap. 2 empfohlene SHA2 als HashAlgorithmus für die Bildung von certID wird nicht von allen OCSP-Responder-Produkten unterstützt.</p> <p>[14] Schritt 12a: Falls die Referenzzeit nicht übergeben wird, wird die aktuelle Systemzeit verwendet. Die Variante 12a. ist unter diesen Umständen nicht möglich; sie wird also nicht berücksichtigt.</p>
Zugehörige Diagramme/Tabell e	

[<=,Konnektor Highspeed, Konnektor PTV5Plus, Konnektor PTV6, eRp_FD,Sich.techn. Eignung: CC-Evaluierung, Sich.techn. Eignung: Produktgutachten, funkt. Eignung: Test Produkt/FA, Sich.techn. Eignung: Prüfung durch CC-Prüfstelle]

2.1.3 Kapitel 11.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
...	
[ETSI TS 119 612]	<p>ETSI (2024-11): ETSI TS 119 612 'Electronic Signatures and Infrastructures (ESI); Trusted Lists', Version 2.3.1 https://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.03.01_60/ts_119612v020301p.pdf Hinweis: Das in Annex C.2 referenzierte XML-Schemamuss für die Validierung verwendet werden https://forge.etsi.org/rep/esi/x19_612_trusted_lists/-/raw/v2.3.1/19612_xsd.xsd https://forge.etsi.org/rep/esi/x19_612_trusted_lists/-/raw/v2.3.1/19612_sie_xsd.xsd https://forge.etsi.org/rep/esi/x19_612_trusted_lists/-/raw/v2.3.1/19612_addition_altypes_xsd.xsd</p>

...	
[XAdES-BES]	ETSI (2010-12): ETSI TS 101 903 Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES), Version 1.4.2 https://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.02_60/ts_101903v010402p.pdf
[XAdES-B-B]	ETSI (2024-07): ETSI EN 319 132-1 'Electronic Signatures and Trust Infrastructures (ESI); XAdES digital signatures; Part 1: Building blocks and XAdES baseline signatures, Version 1.3.1 Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES), Version 1.4.2 https://www.etsi.org/deliver/etsi_en/319100_319199/31913201/01.03.01_60/en_31913201v010301p.pdf
...	

3 Änderung in gemKPT_PKI_TIP

In Erstellung

3.1.1 Kapitel 8.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
...	
[ETSI_TS_119_612]	<p>ETSI (2024-11): ETSI TS 119 612 'Electronic Signatures and Infrastructures (ESI); Trusted Lists', Version 2.3.1 https://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.03.01_60/ts_119612v020301p.pdf Hinweis: Das in Annex C.2 referenzierte XML-Schemamuss für die Validierung verwendet werden https://forge.etsi.org/rep/esi/x19_612_trusted_lists/-/raw/v2.3.1/19612_xsd.xsd https://forge.etsi.org/rep/esi/x19_612_trusted_lists/-/raw/v2.3.1/19612_sie_xsd.xsd https://forge.etsi.org/rep/esi/x19_612_trusted_lists/-/raw/v2.3.1/19612_additionaltypes_xsd.xsd</p>
...	

4 Änderung in gemSpec_TSL

4.1.1 8.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
...	...
[ETSI_TS_119_612]	<p>ETSI (2024-11): ETSI TS 119 612 'Electronic Signatures and Infrastructures (ESI); Trusted Lists', Version 2.3.1 https://www.etsi.org/deliver/etsi_ts/119600_119699/119612/02.03.01_60/ts_119612v020301p.pdf</p> <p>Hinweis: Das in Annex C.2 referenzierte XML-Schema muss für die Validierung verwendet werden https://forge.etsi.org/rep/esi/x19_612_trusted_lists/-/raw/v2.3.1/19612_xsd.xsd https://forge.etsi.org/rep/esi/x19_612_trusted_lists/-/raw/v2.3.1/19612_sie_xsd.xsd https://forge.etsi.org/rep/esi/x19_612_trusted_lists/-/raw/v2.3.1/19612_additionaltypes_xsd.xsd</p>
...	...

5 Änderungen in Steckbriefen

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT...]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

5.1 Änderungen in gemProdT_eRp_FD

Tabelle 3:

Afo-ID (gemSpec_P KI)	Afo-Bezeichnung	Prüfverfahren
GS-A_5484-01	TUC_PKI_036 „BNetzA-VL-Aktualisierung“	Anforderungen zur Sich.techn. Eignung: Produktgutachten
GS-A_4750-02	TUC_PKI_030 „QES-Zertifikatsprüfung“	Anforderungen zur funktionalen Eignung: Test Produkt/FA und zur Sich.techn. Eignung: Produktgutachten

5.2 Änderungen in gemProdT_Kon_Highspeed

Tabelle 4:

Afo-ID (gemSpec_PKI)	Afo-Bezeichnung	Prüfverfahren
GS-A_5484-01	TUC_PKI_036 „BNetzA-VL-Aktualisierung“	Anforderungen zur funktionalen Eignung: Test Produkt/FA
GS-A_4750-02	TUC_PKI_030 „QES-Zertifikatsprüfung“	Anforderungen zur funktionalen Eignung: Test Produkt/FA und zur Sich.techn. Eignung: Prüfung durch CC-Prüfstelle

5.3 Änderungen in gemProdT_Kon_PTV5Plus

Tabelle :

Afo-ID (gemSpec_P KI)	Afo-Bezeichnung	Prüfverfahren
GS-A_5484-01	TUC_PKI_036 „BNetzA-VL-Aktualisierung“	Anforderungen zur funktionalen Eignung: Test Produkt/FA
GS-A_4750-02	TUC_PKI_030 „QES-Zertifikatsprüfung“	Anforderungen zur funktionalen Eignung: Test Produkt/FA und zur Sich.techn. Eignung: CC-Evaluierung

5.4 Änderungen in gemProdT_Kon_PTV6

Tabelle :

Afo-ID (gemSpec_P KI)	Afo-Bezeichnung	Prüfverfahren
GS-A_5484-01	TUC_PKI_036 „BNetzA-VL-Aktualisierung“	Anforderungen zur funktionalen Eignung: Test Produkt/FA
GS-A_4750-02	TUC_PKI_030 „QES-Zertifikatsprüfung“	Anforderungen zur funktionalen Eignung: Test Produkt/FA und zur Sich.techn. Eignung: CC-Evaluierung