
C_12723_Anlage

Inhaltsverzeichnis

1	Änderungsbeschreibung.....	3
2	Änderung in gemKPT_PKI_TIP.....	5
2.1	zum Kapitel 2.3 Vertrauensmodelle in der PKI der TI.....	5
2.1.1	zum Kapitel 2.3.5 Vertrauensmodell von Zertifikaten der HBA-Vorläuferkarten in der TI.....	5
2.1.2	zum Kapitel 7.4.1 Geltungsbereich.....	6
2.2	zum Kapitel 4.5.1 OCSP-Responder Proxy.....	6
3	Änderung in gemSpec_PKI.....	8
3.1.1	zum Kapitel 5.3.1 Definition der Organisationsidentität.....	8
3.2	in Kapitel 8.1 Vertrauensraum der TI.....	8
3.3	in Kapitel 8.6 Fehlercodes bei TSL- und Zertifikatsprüfung X.509.....	8
3.4	in Kapitel 9.1 Statusprüfung.....	15
4	Änderung in gemKPT_Betr.....	17
4.1	zum Kapitel 3.5.2 Servicezerlegung.....	17
4.1.1	zum Kapitel 7.1.1 Produkttypen (PDT-IDs).....	17
4.2	zum Kapitel 8.1 Abkürzungen.....	18
5	Änderung in gemSpec_Perf.....	19
5.1.1	zum Kapitel 2.3.1 Wartungsfenster und Servicezeiten.....	19
5.2	zum Kapitel 2.5 Datenliefermodelle.....	19
5.3	zum Kapitel 3.15 OCSP-Responder-Proxy (PDT01).....	20
5.3.1	zum Kapitel 3.15.1 Leistungsanforderungen OCSP-Responder-Proxy.....	20
5.3.1.1	zum Kapitel 3.15.2 Performancevorgaben OCSP-Responder-Proxy.....	20
5.3.2	zum Kapitel 3.15.2 Betriebsdatenerfassung v2 Spezifika OCSP-Responder-Proxy.....	20
5.3.3	zum Kapitel 3.15.3 Performance-Kenngrößen OCSP-Responder-Proxy.....	22
5.3.4	zum Kapitel 3.15.4 Performance-Kenngrößen OCSP-Responder-Proxy.....	23
5.3.4.1	zum Kapitel 3.21.1.1 Lastmodell Zentrales Netz der TI.....	24
5.3.4.2	3.6.1.1 Bearbeitungszeiten VPN-Zugangsdienst.....	25
5.4	zum Kapitel 5.2 Produkttypen der zentralen Zone der TI-Plattform.....	25
5.4.1	zum Kapitel 5.1.2 Produkttyp Konnektor (PDT17, PDT67).....	25
5.5	Änderungen in gemProdT_gematik_Root_CA, gemProdT_NamD, gemProdT_SG_BestNetze, gemProdT_VPN_Zug_D, gemProdT_VZD, gemProdT_VZD_FHIR und gemProdT_X509_TSP_nonQES_Komp.....	26

38	5.6 Änderungen in gemProdT_VPN_Zug_D.....	26
39		
40		

1 Änderungsbeschreibung

Der Wegfall von HBA-Vorläuferkarten (HBA-qSig und ZOD 2.0) führt dazu, dass der OCSP-Responder-Proxy nicht mehr benötigt wird. Im vorliegenden Ticket werden die betroffenen Dokumenten (Konzepte und Spezifikationen) und Produkttypsteckbriefe auf Änderungen in Bezug auf die Abkündigung der Spezifikation [gemSpec_OCSP_Proxy] untersucht. Die Anpassung von betroffenen Dokumenten und Steckbriefen ist ein Teil des QG-Prozesses, welches nicht Gegenstand des vorliegenden Tickets ist.

Hinweis 1: Die folgenden Anforderungen werden als weggefallene Anforderung in Polarion markiert:

gemKPT_PKI_TIP

- TIP1-A_2159 - Leistung des OCSP-Responder Proxy
- TIP1-A_2160 - Erreichbarkeit des OCSP-Responder Proxy
- TIP1-A_5131 - CA-Zertifikate der HBA-Vorläuferkarten im TI-Vertrauensraum
- TIP1-A_5282 - OCSP-Auskünfte der HBA-Vorläuferkarten innerhalb der TI

gemSpec_OCSP_Proxy

- TIP1-A_5831 - FehlerLog (gemSpec_OCSP_Proxy)
- TIP1-A_5832 - OCSP-Proxy Security-Log (gemSpec_OCSP_Proxy)
- TIP1-A_5833 - OCSP-Proxy Performance-Log (gemSpec_OCSP_Proxy)
- TIP1-A_5834 - OCSP-Proxy Debug-Log für Testbetrieb (gemSpec_OCSP_Proxy)
- TIP1-A_5835 - Fehlerprotokollierung
- TIP1-A_5836 - Schutz von Log-Dateien
- TIP1-A_5837 - Technische Datenschutzmaßnahmen
- TIP1-A_5838 - Verwendung von Standards und Best Practices
- TIP1-A_5848 - Erreichbarkeit OCSP-Proxy
- TIP1-A_5849 - OCSP-Anfragen aus der TI beantworten
- TIP1-A_5851 - Weiterleitung von OCSP-Anfragen für nonQES- und QES-EE-Zertifikate der zu unterstützenden HBA-Vorläuferkarten
- TIP1-A_5852 - Verbindungsaufbau zu OCSP-Respondern im Internet
- TIP1-A_5853 - Ablehnung von Anfragen aus dem Internet
- TIP1-A_5855 - Speicherung von OCSP-Anfragen
- TIP1-A_5856 - Speicherung von OCSP-Antworten
- TIP1-A_5857 - Protokollierung von OCSP-Anfragen und OCSP-Antworten

gemSpec_Perf

- A_24159 - Performance - Betriebsdatenlieferung v2 - Spezifika OCSP-Responder-Proxy - Operation (gemSpec_Perf)
- A_24158 - Performance - Betriebsdatenlieferung v2 - Spezifika OCSP-Responder-Proxy - Duration (gemSpec_Perf)

- A_24160 - Performance - Betriebsdatenlieferung v2 - Spezifika OCSP-Responder-Proxy - Status (gemSpec_Perf)

- A_24161 - Performance - Betriebsdatenlieferung v2 - Spezifika OCSP-Responder-Proxy - Message (gemSpec_Perf)

Hinweis 2 (*): Das zu den folgenden Anforderungen zugeordneten Prüfverfahren "funkt. Eignung: Test Produkt/FA" bzw. "funkt. Eignung: Herstellererklärung" wird entfernt:

(*) Anpassung weiterer dem OCSP-Responder Proxy zugeordneten Prüfverfahren wird nach der GS-Freigabe anhand des folgenden Tool ermittelt: [Suche nach KonfigElementen zu Prüfverfahren < Zuordnung Produkttypen und Prüfverfahren < Documents & Pages < Mainline](#)

gemSpec_Perf

- GS-A_4145 (funkt. Eignung: Test Produkt/FA)
- GS-A_4155-03 (funkt. Eignung: Herstellererklärung)
- ...

gemSpec_Net

- A_17824 (funkt. Eignung: Test Produkt/FA)
- ...

gemSpec_PKI

- A_17821 (funkt. Eignung: Test Produkt/FA)
- A_17820 (funkt. Eignung: Test Produkt/FA)
- A_17700 (funkt. Eignung: Test Produkt/FA)
- A_17690 (funkt. Eignung: Test Produkt/FA)
- A_17688 (funkt. Eignung: Test Produkt/FA)
- A_17689 (funkt. Eignung: Test Produkt/FA)
- ...

gemSpec_Krypt

- A_17775 (funkt. Eignung: Herstellererklärung)
- A_17322 (funkt. Eignung: Herstellererklärung/Sich.techn. Eignung: Herstellererklärung)
- ...

Hinweis 3: Der Produkttypsteckbrief gemProdT_OCSP_Proxy wird abgekündigt.

2 Änderung in gemKPT_PKI_TIP

2.1 zum Kapitel 2.3 Vertrauensmodelle in der PKI der TI

Ein definierter PKI-Vertrauensraum für die Anwendungsbereiche der Gesundheitskarte bildet den Kern der kryptographisch abgesicherten Geschäftsprozesse des Gesundheitswesens. Gemäß der regulatorischen Hoheit der unterschiedlichen Anwendungsfelder müssen zu deren Abbildung innerhalb und außerhalb der TI verschiedene Vertrauensmodelle implementiert werden für:

- Zertifikate für die Erstellung qualifizierter elektronischer Signaturen (QES), die speziell für die Anwendungsbereiche der Gesundheitskarte zusätzlich unter den Bestimmungen des SGB implementiert werden.
- Digitale Zertifikate, für deren Einsatz innerhalb der TI und des Internets die Regularien einerseits der gematik sowie andererseits die der Vertretungsorganisationen von Leistungserbringern und Kostenträgern bestimmend sind.
- ~~Digitale Zertifikate, die im Kontext des zeitlich begrenzten Bestandsschutzes der HBA-Vorläuferkarten bereits im Feld im Einsatz sind, und deren Funktionsweise (soweit technisch unterstützt) auch innerhalb der TI unterstützt werden soll.~~

2.1.1 zum Kapitel 2.3.5 Vertrauensmodell von Zertifikaten der HBA-Vorläuferkarten in der TI

~~Zur Unterstützung der HBA-Vorläuferkarten qSIG- und ZOD-Karten auch innerhalb der TI müssen weitere Anforderungen berücksichtigt werden:~~

TIP1-A_5131 – CA-Zertifikate der HBA-Vorläuferkarten im TI-Vertrauensraum

~~Die TI-Plattform MUSS die zugehörigen CA-Zertifikate sowie OCSP-Signatur-Zertifikate von zu unterstützenden HBA-Vorläuferkarten (qSIG, ZOD) unter Einhaltung eines geregelten Registrierungsverfahrens in den Vertrauensraum der TI aufnehmen.<=~~

TIP1-A_5282 – OCSP-Auskünfte der HBA-Vorläuferkarten innerhalb der TI

~~Die TI-Plattform MUSS die im Internet verfügbaren OCSP-Dienste von bereits zugelassenen Anbietern der HBA-Vorläuferkarten (qSIG-Karten, ZOD-Karten) innerhalb der TI verwenden.<=~~

~~Die bereits im Internet etablierten PKIs der HBA-Vorläuferkarten (qSIG, ZOD), die im Rahmen des Bestandsschutzes zu unterstützen sind, werden in der TI insoweit berücksichtigt, dass die zugehörigen CAs in den TI-Vertrauensraum (also die TSL) aufgenommen und die im Internet verfügbaren Statusinformationen der zugehörigen EE-Zertifikate in der TI zur Verfügung gestellt werden.~~

2.1.2 zum Kapitel 7.4.1 Geltungsbereich

Verzeichniseinträge müssen einer bereits bestehenden elektronischen Identität zuordenbar sein. Dabei handelt es sich um:

- Natürliche Personen, denen aufgrund ihrer bestätigten Berufszugehörigkeit als Leistungserbringer des deutschen Gesundheitswesens ein HBA/BA (oder HBA-Vorläuferkarte) ausgestellt wurde.
- Juristische Personen (Organisationen/Institutionen) des deutschen Gesundheitswesens denen eine SMC-B ausgestellt wurde.

(...)

2.2 zum Kapitel 4.5.1 OCSP-Responder Proxy

Zur Statusprüfung von X.509-Zertifikaten werden die zuständigen OCSP-Responder in der TI betrieben. Ausnahmen hiervon sind die OCSP-Responder

- für Zertifikate der HBA-Vorläuferkarten

Diese werden nicht in der TI betrieben. Um deren Abfrage innerhalb der TI zu ermöglichen, wird ein OCSP-Responder Proxy bereitgestellt.

Ein solcher Proxy verfügt über keine eigene Signaturidentität, somit benötigt er kein X.509-Zertifikat. Aus diesem Grund erfolgt die Erwähnung nur der Vollständigkeit halber hinsichtlich OCSP-Dienste innerhalb der TI.

Die Verfügbarkeit der OCSP-Responder für Zertifikate der HBA-Vorläuferkarten muss für Zertifikatsstatusprüfungen innerhalb der TI durch einen Proxy sichergestellt werden.

TIP1-A_2159 – Leistung des OCSP-Responder Proxy

Der OCSP-Responder Proxy MUSS die OCSP-Statusauskunft für Zertifikate der HBA-Vorläuferkarten in der TI verfügbar machen. <=

TIP1-A_2160 – Erreichbarkeit des OCSP-Responder Proxy

Der OCSP-Responder Proxy MUSS in der TI durch alle Komponenten und Dienste erreichbar sein. <=

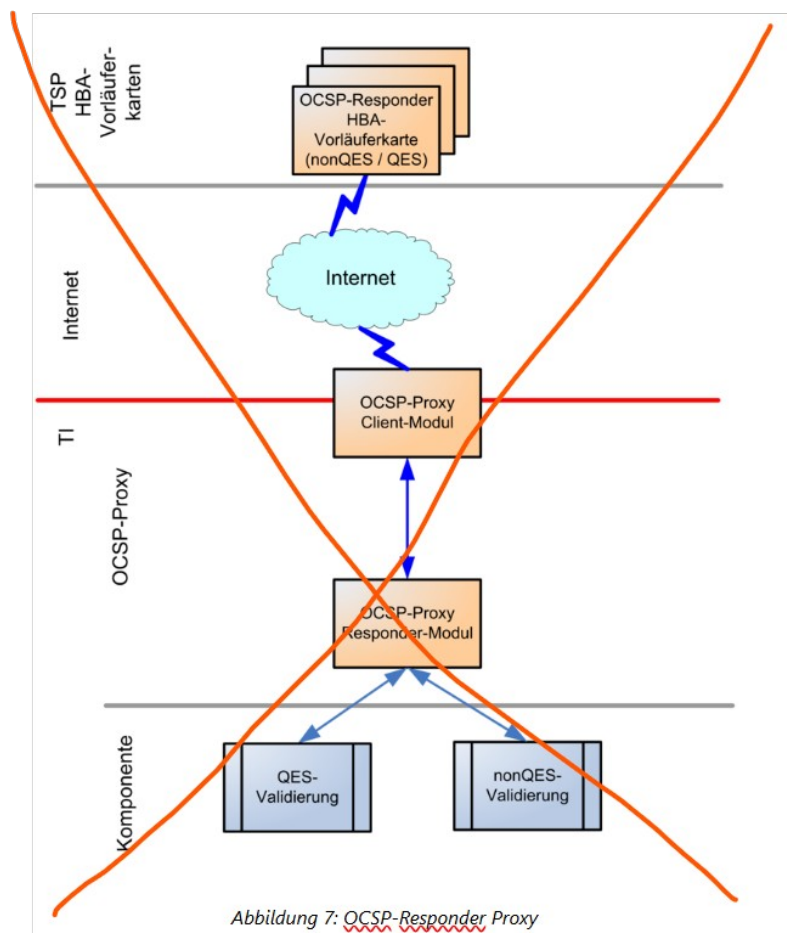


Abbildung 7: OCSP-Responder Proxy

Abbildung 7: OCSP-Responder Proxy

3 Änderung in gemSpec_PKI

3.1.1 zum Kapitel 5.3.1 Definition der Organisationsidentität

(...)

Hinweis 1: Von dieser Regelung sind SM-B ohne CVC (SMC-B ORG) oder mit dem Zugriffsprofil CHAT.0 und CHA.8 [gemSpec_PKI#Tab_PKI_254-*) nicht betroffen, da sie keinen Zugriff auf die entsprechenden Daten erlauben. Ebenso sind SM-B mit Zugriffsprofil CHAT.1 [gemSpec_PKI#Tab_PKI_254-*) nicht betroffen, da sie dem Zugriff des Versicherten selbst in der KTR-AdV-Umgebung dienen.

Hinweis 2: Ein HBA im Sinne dieser Anforderung ist ein HBA oder eine HBA-Vorläuferkarte (HBA-qSig und ZOD_2.0).

3.2 in Kapitel 8.1 Vertrauensraum der TI

Grundlage jeder zertifikatsbasierten Prüfung auf Vertrauenswürdigkeit in der TI ist die gesicherte Information über den aktuell gültigen TI-Vertrauensraum, gegen den eine solche Prüfung erfolgt.

(...)

Die bereits im Internet etablierten PKIs der Vorläuferkarten (qSIG, ZOD), die im Rahmen des Bestandsschutzes zu unterstützen sind, werden in der TI insoweit berücksichtigt, dass die zugehörigen CAs in den TI-Vertrauensraum (also die TSL) aufgenommen und die Statusinformationen der zugehörigen EE-Zertifikate durch Nachnutzung des OCSP-Responder Proxy zur Verfügung gestellt werden (s. Beschreibung in [gemKPT_Arch_TIP#5.4.13]).

3.3 in Kapitel 8.6 Fehlercodes bei TSL- und Zertifikatsprüfung X.509

GS-A_4751-01 -Fehlercodes bei TSL- und Zertifikatsprüfung

Die Produkttypen der TI, die Zertifikate prüfen und die TSL auswerten MÜSSEN die Fehlercodes gemäß Tab_PKI_274* nutzen. Das Element CompType MUSS belegt werden mit „[Produkttyp]:PKI“, wobei [Produkttyp] zu ersetzen ist durch den konkreten Produkttyp in der umzusetzenden Anforderung

Tabelle 1: Tab_PKI_274* Fehlercodes des SubCompTyps PKI bei TSL- und Zertifikatsprüfung

Co de	Seve rity	ErrorT ype	ErrorText	Detail	Meldungskürzel
10 01	Error	Techni cal	Es liegt keine gültige TSL vor		TSL_INIT_ERROR
10 02	Error	Techni cal	Zertifikate lassen		TSL_CERT_EXTRACTION

			sich nicht extrahieren		_ERROR
1003	Error	Security	Mehr als ein markierter V-Anker gefunden		MULTIPLE_TRUST_ANCHOR
1004	Error	Technical	TSL-Signer-CA lässt sich nicht extrahieren		TSL_SIG_CERT_EXTRACTION_ERROR
1005	Error	Technical	Element „PointersToOtherTSL“ nicht vorhanden		TSL_DOWNLOAD_ADDRESS_ERROR
1006	Error	Technical	TSL-Download-adressen wiederholt nicht erreichbar		TSL_DOWNLOAD_ERROR
1007	Error	Security	Vergleich der ID und Sequence-Number entspricht nicht der Vergleichs-variante 6a		TSL_ID_INCORRECT
1008	Warning	Security	Die TSL ist nicht mehr aktuell		VALIDITY_WARNING_1
1009	Warning	Security	Überschreitung des Elements NextUpdate um TSL-Grace-Period		VALIDITY_WARNING_2
1010	Warning	Security	<i>Veraltet: Diese Warnmeldung ist redundant zu VALIDITY</i>		TSL_NEXTUPDATE_EXPIRED

			<i>_WARNING _1 (Code 1008). Sie soll deshalb nicht mehr verwendet werden.</i>		
10 11	Error	Technical	TSL-Datei nicht wellformed		TSL_NOT_WELLFORMED
10 12	Error	Technical	Schemata der TSL- Datei nicht korrekt		TSL_SCHEMA_NOT_VALID
10 13	Error	Security	Signatur ist nicht gültig		XML_SIGNATURE_ERROR
10 16	Error	Security	KeyUsage ist nicht vorhanden bzw. entspricht nicht der vor- gesehenen KeyUsage		WRONG_KEYUSAGE
10 17	Error	Security	Extended- KeyUsage entspricht nicht der vor- gesehenen Extended- KeyUsage		WRONG _EXTENDEDKEYUSAGE
10 18	Error	Security	Zertifikats- typ-OID stimmt nicht überein		CERT_TYPE_MISMATCH
10 19	Error	Technical	Zertifikat nicht lesbar		CERT_READ_ERROR
10 21	Error	Security	Zertifikat ist zeitlich nicht gültig		CERTIFICATE_NOT_VALID_TIME
10 23	Error	Security	Authority- Key- Identifizier des End- Entity- Zertifikats von		AUTHORITYKEYID_DIFFERENT

			Subject-Key-Identifizier des CA-Zertifikats unterschiedlich		
10 24	Error	Security	Zertifikats-Signatur ist mathematisch nicht gültig.		CERTIFICATE_NOT_VALID_MATH
10 26	Error	Technical	Das Element „Service-Supply Point“ konnte nicht gefunden werden.		SERVICESTSUPPLYPOINT_MISSING
10 27	Error	Technical	CA kann nicht in den TSL-Informationen ermittelt werden.	Keine Adresse hinterlegt.	CA_CERT_MISSING
10 28	Warning	Technical	Die OCSP-Prüfung konnte nicht durchgeführt werden (1)	TOLERATE_OCSP_FAILURE=true	OCSP_CHECK_REVOCATION_FAILED
10 29	Error	Technical	Die OCSP-Prüfung konnte nicht durchgeführt werden (2)	TOLERATE_OCSP_FAILURE=false	OCSP_CHECK_REVOCATION_ERROR
10 30	Error	Security	OCSP-Zertifikat nicht in TSL-Informationen enthalten		OCSP_CERT_MISSING
10 31	Error	Security	Signatur der Response ist nicht gültig.		OCSP_SIGNATURE_ERROR
10 32	Error	Technical	OCSP-Responder nicht		OCSP_NOT_AVAILABLE

			verfügbar		
1033	Error	Security	Kein Element PolicyIdentifier vorhanden		CERT_TYPE_INFO_MISSING
1034	Error	Technical	<i>Veraltet: Diese Fehlermeldung wird nicht mehr verwendet. Stattdessen ist der Fehlercode 1032 zu verwenden.</i>		OCSP_PROXY_NOT_AVAILABLE
1036	Error	Security	Das Zertifikat ist ungültig. Es wurde nach der Sperrung der ausgebenden CA ausgestellt.		CA_CERTIFICATE_REVOKED_IN_TSL
1039	Warning	Security	Warnung, dass Offline-Modus aktiviert ist und keine OCSP-Statusabfrage durchgeführt wurde		NO_OCSP_CHECK
1040	Error	Security	Bei der Online-statusprüfung ist ENFORCE_CERTHASH_CHECK auf 'true' gesetzt, die OCSP-Response enthält jedoch keine certHash-Erweiterung		CERTHASH_EXTENSION_MISSING
10	Error	Security	Der certHash		CERTHASH_MISMATCH

41		y	in der OCSP-Response stimmt nicht mit dem certHash des vorliegenden Zertifikats überein.		
1042	Error	Technical	Das TSL-SignerCA-Zertifikat kann nicht aus dem sicheren Speicher des Systems geladen werden.		TSL_CA_NOT_LOADED
1043	Error	Technical	CRL kann aus technischen Gründen nicht ausgewertet werden.		CRL_CHECK_ERROR
1044	Warning	Technical	Warnung, dass zum angefragten Zertifikat keine Statusinformationen verfügbar sind.		CERT_UNKNOWN
1047	Warning	Security	Das Zertifikat wurde vor oder zum Referenzzeitpunkt widerrufen.		CERT_REVOKED
1048	Error	Technical	Es ist ein Fehler bei der Prüfung des QC-Statements aufgetreten (z. B. nicht vorhanden, obwohl gefordert).		QC_STATEMENT_ERROR

10 50	Warnung	Technical	Die einem TUC zur Zertifikatsprüfung beigefügte OCSP-Response zu dem zu prüfenden Zertifikat kann nicht erfolgreich gegen das Zertifikat validiert werden.		PROVIDED_OCSP_RESPONSE_NOT_VALID
10 51	Error	Security	Die in einem OCSP-Response zurückgelieferte Nonce stimmt nicht mit der Nonce des OCSP-Requests überein.		OCSP_NONCE_MISMATCH
10 52	Error	Security	Attribut-Zertifikat kann dem übergebenen Basis-Zertifikat nicht zugeordnet werden.		ATTR_CERT_MISMATCH
10 53	Error	Technical	Die CRL kann nicht heruntergeladen werden.		CRL_DOWNLOAD_ERROR
10 54	Error	Technical	Eine verwendete CRL ist zum aktuellen Zeitpunkt nicht mehr gültig.		CRL_OUTDATED_ERROR
10 55	Error	Security	CRL-Signer-Zertifikat nicht in TSL-Informationen enthalten		CRL_SIGNER_CERT_MISSING
10 57	Error	Security	Signatur der CRL ist nicht gültig.		CRL_SIGNATURE_ERROR
10 58	Error	Technical	Die OCSP-Response enthält eine Exception-Meldung.		OCSP_STATUS_ERROR

1059	Error	Security	CA-Zertifikat für QES-Zertifikatsprüfung nicht qualifiziert		CA_CERTIFICATE_NOT_QES_QUALIFIED
1060	Error	Technical	Die VL kann nicht aktualisiert werden.		VL_UPDATE_ERROR
1061	Error	Security	CA (laut TSL) nicht autorisiert für die Herausgabe dieses Zertifikatstyps.		CERT_TYPE_CA_NOT_AUTHORIZED
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

[<=, TSP X.509 nonQES - HBA, Intermediär VSDM, TSP X.509 nonQES - eGK, Zentrales-Netz, KOM-LE FD, Konfigdienst, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC, NCPeH_FD, gematik Root-CA, Konnektor Highspeed, Basis-Consumer, TSL-Dienst, SigD, VSDD, Zeitdienst, Aktensystem_ePA, Verzeichnisdienst, UFS, SG_BestNetze, TSP X.509 QES, IDP-D, CMS, Namensdienst, eRp_FD, Konnektor PTV5, Konnektor PTV5Plus, TI-Flow_FD, Konnektor PTV6, Zugangsdienst, funkt. Eignung: Herstellererklärung]

3.4 in Kapitel 9.1 Statusprüfung

Gemäß [gemKPT_Arch_TIP] ist zur Statusprüfung die Schnittstelle I_OCSP_Status_Information durch die Produkttypen

- TSL-Dienst,
- gematik Root-CA
- TSP-X.509 nonQES,
- TSP-X.509 QES und
- **OCSP-Responder Proxy**

anzubieten. Darüber können Nutzer, wie z. B. Konnektor und VPN-Zugangsdienst, Statusinformationen zu X.509-Zertifikaten von OCSP-Respondern erhalten. Die Schnittstelle implementiert die logische Operation check_Revocation_Status mit der der Sperrstatus eines X.509-Zertifikats ermittelt werden kann (vgl. auch [gemKPT_PKI_TIP]).

GS-A_4669-01 -Umsetzung Statusprüfdienst

232 Die Produkttypen TSL-Dienst, gematik Root-CA, TSP-X.509 nonQES und TSP-X.509 QES
233 ~~und OCSP-Responder Proxy~~ MÜSSEN die Schnittstelle I_OCSP_Status_Information
234 implementieren.
235 [≤, gematik Root-CA, TSP X.509 nonQES - HBA, TSP X.509 nonQES - eGK, TSL-Dienst,
236 TSP X.509 QES, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - gSMC, funkt. Eignung:
237 Herstellererklärung, funkt. Eignung: Test Produkt/FA]

238

240

241

4 Änderung in gemKPT_Betr

4.1 zum Kapitel 3.5.2 Servicezerlegung

(...)

Tab_gemKPT_Betr_Servicekomponenten

Servicekomponente (SK)	Service Provider (Eigener Service)	Produkttyp	Produkttyp-Name	Anbieter-ausschluss (SK)
Anbindung Bestandsnetze	n/a	n/a	n/a	
...				
OCSP-Responder-Proxy	Anbieter SMC-B, Anbieter X.509-TSP-eGK, Anbieter HBA, Anbieter ZPD	PDT01	OCSP-Proxy	
...				
Proof of Patient Presence-Service	Anbieter Proof of Patient Presence-Service	PDT71	Proof of Patient Presence-Service	n/a

4.1.1 zum Kapitel 7.1.1 Produkttypen (PDT-IDs)

Tab_gemKPT_Betr_Produkttypen

ID	Produkttyp / Anwendungstyp	Produkttyp-Name / Anwendungsname
PDT01	gemProdT_OCSP_Proxy	OCSP-Responder-Proxy
...		
PDT86	gemProdT_PoPP_Client	Proof of Patient Presence-Client

4.2 zum Kapitel 8.1 Abkürzungen

Tabelle 16: Tab_gemKPT_Betr_Abkürzungsverzeichnis

Kürzel	Erläuterung
BDE	Betriebsdatenerfassung / Betriebsdatenlieferung
...	
OCSP-R Proxy	OCSP-Responder Proxy
...	
WANDA Smart	Weitere Anwendungen für den Datenaustausch mit Nutzung der TI oder derer kryptografischen Identitäten für eigene Anwendungszwecke

5 Änderung in gemSpec_Perf

5.1.1 zum Kapitel 2.3.1 Wartungsfenster und Servicezeiten

(...)

Folgende Tabelle "Tab_gemSpec_Perf_Servicekomponente->Servicezeit, Wartungsfenster" stellt in einer Übersicht alle Servicekomponenten bzw. Produkttypen und ihre serviceverantwortlichen Anbieter dar, die bereits auf die generischen Festlegungen in diesem Kapitel umgestellt wurden.

Tabelle 1: Tab_gemSpec_Perf_Servicekomponente->Servicezeit, Wartungsfenster

Servicekomponente	Servicezeit	Wartungsfenster
CVC-Root	-	-
...		
OCSP-Responder-Proxy	A_23350 - HZ Mo bis So eingeschränkt	A_23347* A_23615
...		
Zentrales Netz der TI	A_23350 - HZ Mo bis So eingeschränkt	A_23347* A_23615

5.2 zum Kapitel 2.5 Datenliefermodelle

(...)

Tabelle 3: Tab_gemSpec_Perf_Zuordnung_Datenliefermodelle

PDT-ID	Name des Produkttyps	Aktuelle Datenliefermodelle
PDT01	OCSP-Responder-Proxy	BDEv2, Selbstauskunft v1
PDT79	VSDM 2 Fachdienst	Telemetriedaten
...		
PDT83	TI-Messenger Pro Fachdienst	Ereignisdaten, Selbstauskunft v2

5.3 zum Kapitel 3.15 OCSP-Responder-Proxy (PDT01)

Im Folgenden werden die spezifischen Leistungsanforderungen und Anforderungen an die Betriebsdatenlieferung des OCSP-Responder-Proxy aufgeführt.

5.3.1 zum Kapitel 3.15.1 Leistungsanforderungen OCSP-Responder-Proxy

5.3.1.1 zum Kapitel 3.15.2 Performancevorgaben OCSP-Responder-Proxy

Es gelten die zugeordneten Performancevorgaben aus Kapitel 5.2 Produkttypen der zentralen Zone der TI-Plattform:

- GS_A_3058 Performance – zentrale Dienste – lineare Skalierbarkeit
- GS_A_4145 Performance – zentrale Dienste – Robustheit gegenüber Lastspitzen
- GS_A_4155-03 Performance – zentrale Dienste – Verfügbarkeit

5.3.2 zum Kapitel 3.15.2 Betriebsdatenerfassung v2 Spezifika OCSP-Responder-Proxy

In Ergänzung an die allgemeinen Anforderungen an die Betriebsdatenerfassung befinden sich nachfolgend die produktspezifischen Anforderungen:

A_24159 – Performance – Betriebsdatenlieferung v2 – Spezifika OCSP-Responder-Proxy – Operation

Der Produkttyp OCSP-Responder-Proxy MUSS bei Betriebsdatenlieferungen bzgl. des "operation" Feldes die Angabe der Spalte "Operation / Usecase" aus Tabelle Tab_gemSpec_Perf_Berichtsformat_OCSP-Responder-Proxy berücksichtigen. <=, OCSP-Proxy, funkt. Eignung: Test Produkt/FA

A_24158 – Performance – Betriebsdatenlieferung v2 – Spezifika OCSP-Responder-Proxy – Duration

Der Produkttyp OCSP-Responder-Proxy MUSS bei Betriebsdatenlieferungen bzgl. des "duration_in_ms" Feldes die Hinweise der Spalte "Duration" aus Tabelle Tab_gemSpec_Perf_Berichtsformat_OCSP-Responder-Proxy berücksichtigen. <=, OCSP-Proxy, funkt. Eignung: Test Produkt/FA

Tabelle 89: Tab_gemSpec_Perf_Berichtsformat_OCSP-Responder-Proxy

Operation / Usecase	Duration
OCSPPX	Bei Aufruf der Operation "check_Revocation_Status" beginnt die Messung der Bearbeitungszeit mit der Annahme der Nachricht durch den OCSP-Responder-Proxy, wird mit der Weiterleitung an den Ziel-OCSP im Internet pausiert, läuft mit Erhalt der Antwort vom Ziel-OCSP im Internet weiter und endet mit dem Versand der Antwort an den Client.

A_24160 - Performance - Betriebsdatenlieferung v2 - Spezifika OCSP-Responder-Proxy - Status

Der Produkttyp OCSP-Responder-Proxy MUSS bei Betriebsdatenlieferungen bzgl. der "status"-Felder die Angabe der Spalte "Statuscode" aus Tab_gemSpec_Perf_Statuscodes_OCSP-Responder-Proxy berücksichtigen, sofern ein spezifischer Statuscode bestimmt werden kann. Ist dies nicht möglich MUSS ein definierter Standard-Statuscode gemäß A_22500 * für interne bzw. externe Fehler verwendet werden. <=, OCSP-Proxy, funkt. Eignung: Test Produkt/FA

Tabelle 90: Tab_gemSpec_Perf_Berichtsformat_OCSP-Responder-Proxy

Statuscode	Definition	Beschreibung	Bewertung
200	OK	Anfrage wurde erfolgreich verarbeitet	SUCCESS
413	Payload too large	Die Datenmenge der Anfrage ist größer als der Server verarbeiten kann.	FAILED_OTHER
415	Unsupported Media Type	Die Daten liegen in einem Format vor, welches auf dem Zielsystem nicht unterstützt wird.	FAILED_OTHER
500	Internal Error	Ein unerwarteter Fehler ist aufgetreten	FAILED_SERVICE
504	Gateway Timeout	Der Ziel-OCSP im Internet antwortet nicht auf die Anfrage des OCSP-Responder-Proxys.	FAILED_SERVICE
79875	OCSP_ERROR_WRONG_DATA	Format der OCSP-Anfrage fehlerhaft	FAILED_OTHER

A_24161 - Performance - Betriebsdatenlieferung v2 - Spezifika OCSP-Responder-Proxy - Message

Der Produkttyp OCSP-Responder-Proxy MUSS bei Betriebsdatenlieferungen in den "message"-Feldern die folgenden Daten im JSON-Format übermitteln: { "bkdur": \$backendDuration, "zOcs": "\$ziel-ocsp" } - \$backendDuration = Zeit in ms für Abfragen an den Ziel-OCSP im Internet, Datentyp Integer \$ziel-ocsp = OCSP-gematik-ID des Ziel-OCSP im Internet basierend auf der Zuordnungstabelle Tab_gemSpec_Perf_OCSP-Responder-Proxy_Ziel-URLs, Datentyp String Bei der Erstellung des message-Feldes ist darauf zu achten, dass weder Whitespaces noch Newlines zwischen JSON-Elementen enthalten sind (kein Indenting) und Vorgaben nach [RFC7493] eingehalten werden. <=, OCSP-Proxy, funkt. Eignung: Test Produkt/FA

Tabelle 91: Tab_gemSpec_Perf_OCSP-Responder-Proxy_Ziel-URLs

OCSP Proxy: Ziel URL	OCSP-gematik-ID
----------------------	-----------------

http://ocsp.d-trust.net	ZIELURL_1
http://ocsp-qes.egk-tsp.de	ZIELURL_2
http://qocsp-eA.medesign.de:8080/ocsp	ZIELURL_3
http://qocsp-eZAA.medesign.de:8080/ocsp	ZIELURL_4
http://ocsp.bzaek.de:8080/ocsp-ocspresponder	ZIELURL_5
http://qocsp.hba.telesec.de/ocspr	ZIELURL_6
http://qocsp-ea.medesign.de:8080/ocsp	ZIELURL_7
http://ocsp-qes.egk-test-tsp.de	ZIELURL_8
http://qocsp.hba.test.telesec.de/ocspr	ZIELURL_9
http://ehca.gematik.de/ecc-ocsp	ZIELURL_10
http://ehca.gematik.de/ecc-ocsp	ZIELURL_11
http://ehca.gematik.de/ecc-qocsp	ZIELURL_12
http://d-trust-hba-qca4.ocsp.d-trust.net/	ZIELURL_13
http://d-trust-hba-qca5.ocsp.d-trust.net/	ZIELURL_14
http://staging.ocsp.d-trust.net	ZIELURL_15
Andere Zieladressen	Vollständige URL

Hinweis: EinMapping auf OSCP-gematik-ID muss auch erfolgen, wenn der FQDN Escape-Sequenzen enthält, z.B. %3A oder %2F.

5.3.3 zum Kapitel 3.15.3 Performance-Kenngrößen OSCP-Responder-Proxy

nicht definiert

5.3.4 zum Kapitel 3.15.4 Performance-Kenngrößen OSCP-Responder-Proxy

Schnittstellen::Operation bzw. Anwendungsfall

329 **Tabelle 92: Tab_gemSpec_Perf_OCSP-Responder-Proxy_Operationen/Anwendungsfälle**

Produkttyp / Anwendungstyp	S/A-ID	Schnittstellen::Operation / Anwendungsfall	Beschreibung	Berichtsformat-Alias (sofern von Schnittstellen::Operation bzw. Anwendungsfall abweichend)
PDT01	S01	I*	verwendet für Verfügbarkeitsrechnung	
PDT01	S02	I_OCSP_Status_Information::check_Revocation_Status	Ermitteln des Sperrstatus eines Zertifikats (gesperrt, nicht gesperrt oder unbekannt).	OCSPPX

330 **Performance-Kenngrößen / SL-Werte**331 Der Betrachtungszeitraum T für die aufgeführten Soll-Werte beträgt ein Kalendermonat.

332 Die Bildung der Performance-Kenngrößen basiert auf folgenden PG-Schemata: PG-Schema-I

334 **Tabelle 93: Tab_gemSpec_Perf_OCSP-Responder-Proxy_Performance-Kenngrößen**

Performance-Kenngröße (PKG-ID)	Beschreibung	berechnet aus (Betriebsdaten, Probing)	SL-Wert (Soll-Wert)	min / max	Normative Referenz
OCSP-Responder-Proxy (PDT01) - I*					
PDT01-S01-D3-G14	Relative Verfügbarkeit im Betrachtungszeitraum zur Hauptzeit exkl. Wartung. [%*1000]	Probing	99900	min	GS-A_4155
PDT01-S01-D3-G16	Relative Verfügbarkeit im Betrachtungszeitraum zur Nebenzeit exkl. Wartung. [%*1000]	Probing	99000	min	GS-A_4155
OCSP-Responder-Proxy (PDT01) - I_OCSP_Status_Information::check_Revocation_Status					

336 **5.3.4.1 zum Kapitel 3.21.1.1 Lastmodell Zentrales Netz der TI**

(...)

In der Tabelle Tab_gemSpec_Perf_Netzlast_1 sind die Spitzenlastvorgaben am VPN-Zugangsdienst (Punkt 1) aufgelistet.

Tabelle 122: Tab_gemSpec_Perf_Netzlast_1 Spitzenlasten am VPN-Zugangsdienst (Punkt 1)

Datenstrom	Zusammensetzung		Spitzenlast Mbit/sec
VPN-Zugangsdienst zur zentralen Zone	Summe		3.417
	Bestandsnetz		150
	VSDM Intermediär		8
	OCSP-Responder + OCSP-Proxy		8
	KIM-Fachdienst		3.248
	Verzeichnisdienst		3
zentrale Zone zu VPN-Zugangsdienst	Summe		4.016
	KSR (Download Softwarepakete)		100
	Bestandsnetz		150
	OCSP-Responder + OCSP-Proxy		104
	VSDM Intermediär		13
	TSL-Dienst (Download TSL, BNetzA_VL)		360
	KIM-Fachdienst		3.248
	Verzeichnisdienst		41

5.3.4.2 3.6.1.1 Bearbeitungszeiten VPN-Zugangsdienst

A_23610-01 -Performance - VPN-Zugangsdienst - Bandbreite - VPN-Konzentratoren

Der VPN-Zugangsdienst MUSS eine Anbindungsbandbreite ab VPN-Konzentrator in das interne Netz mit folgenden Eigenschaften bereitstellen:

- mindestens eine Bandbreitenanbindung der "Summe aus der Spitzenlastsumme gemäß Tab_gemSpec_Perf_Netzlast_1" mal Anzahl der registrierten und diesem Standort zugeordneten Konnektoren geteilt durch Gesamtanzahl der Konnektoren gemäß gemSpec_Perf#M21.

[<=, Zugangsdienst, funkt. Eignung: Herstellererklärung]

5.4 zum Kapitel 5.2 Produkttypen der zentralen Zone der TI-Plattform

GS-A_4155-04 -Performance - zentrale Dienste - Verfügbarkeit

Die Produkttypen Namensdienst, Sicherheitsgateway Bestandsnetze, VPN-Zugangsdienst, ~~OCSP-Proxy~~, TSP X.509 nonQES - Komp (Komponente OCSP-Responder /CRL-Dienst und Komponente Provisioning/Revocation), gematik-Root-CA (Komponente OCSP-Responder), Verzeichnisdienst und Signaturdienst MÜSSEN zur Hauptzeit eine Verfügbarkeit von 99,9% und zur Nebenzeit von 99% für alle Operationen der technischen Schnittstellen aufweisen.

Der Anschluss an das zentrale Netz muss über die Anschlussoption „redundante Anbindung“ erfolgen.[<=, gematik Root-CA, VZD_FHIR, Verzeichnisdienst, SG_BestNetze, Zugangsdienst, Namensdienst, TSP X.509 nonQES - gSMC, funkt. Eignung: Herstellererklärung]

5.4.1 zum Kapitel 5.1.2 Produkttyp Konnektor (PDT17, PDT67)

(...)

Alle übrigen Aufrufe liegen im Verantwortungsbereich des Konnektors. Tatsächlich verantworten kann er nur die Koordination der Aufrufe nicht das tatsächliche Antwortzeitverhalten, das von den koordinierten dezentralen Produkttypen (Kartenterminals und Smartcards) abhängt. Für die Antwortzeitvorgaben wurden daher dezentrale Produkttypen mit einem normierten Verhalten gewählt, das wie folgt definiert ist:

- Kartenterminal und Karten mit normierten Bearbeitungszeiten gemäß Tabelle "Tab_gemSpec_Perf_Konnektorbearbeitungszeiten_pro_Komponente".
- (...)
- Für die Abfrage der Sperrstatusinformation wird von folgenden normierten Bearbeitungszeiten ausgegangen, welche die Übertragungszeiten des Netzes inkludieren: 1095 msec für OCSP-Responder des TSP-X.509nonQES, ~~600 msec für OCSP-Proxy~~, 2105 msec für OCSP-Responder des TSP-X.509QES....)
- (...)
- Für die Operationen ReadMP und WriteMP wird davon ausgegangen, dass jeweils eine Card-to-Card-Authentisierung (C2C) zwischen SM-B und eGK erforderlich ist. Werden für eine gesteckte eGK ReadMP und WriteMP in Folge (innerhalb einer eGK-

Kartensitzung) ausgeführt, wird davon ausgegangen, dass C2C nur einmal in der Operation ReadMP durchgeführt wird.

(...)

5.5 Änderungen in gemProdT_gematik_Root_CA, gemProdT_NamD, gemProdT_SG_BestNetze, gemProdT_VPN_Zug_D, gemProdT_VZD, gemProdT_VZD_FHIR und gemProdT_X509_TSP_nonQES_Komp

Anmerkung: Die Anforderungen der folgenden Tabelle stellen einen Auszug dar und verteilen sich innerhalb der Tabelle des Originaldokuments [gemProdT_gematik_Root_CA, gemProdT_NamD, gemProdT_SG_BestNetze, gemProdT_VPN_Zug_D, gemProdT_VZD, gemProdT_VZD_FHIR, gemProdT_X509_TSP_nonQES_Komp]. Alle Anforderungen der Tabelle des Originaldokuments, die in der folgenden Tabelle nicht ausgewiesen sind, bleiben unverändert bestehenden.

Tabelle 2: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
GS-A_4155-04	Performance - zentrale Dienste - Verfügbarkeit	gemSpec_Perf

5.6 Änderungen in gemProdT_VPN_Zug_D

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

Tabelle 3: Anforderungen zur funktionalen Eignung "Herstellererklärung"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_23610-01	Performance - VPN-Zugangsdienst - Bandbreite - VPN-Konzentratoren	gemSpec_Perf