gematik
Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH

Einführung der Gesundheitskarte

Spezifikation

OCSP-Proxy

Version:	1.3.0
Revision:	\main\rel_ors1\6
Stand:	11.04.2014
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_OCSP_Proxy

Dokumentinformationen

Änderungen zur Vorversion

Es handelt sich um die die 2. Überarbeitung des Dokumentes.

Dokumentenhistorie

Version	Stand	Kap./ Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
0.0.1	23.12.2013		Initiale Erstellung	AuthentiDate
0.0.2	13.01.2014	6	Erstellung Systemüberblick, TUCs und Anforderungen	AuthentiDate
0.0.3	30.01.2014		Überarbeitung TUCs, Ergänzung Anforderungen, Erstellung Systemkontext, Zerlegung des Produkttyps und Übergreifende Festlegungen	AuthentiDate
0.0.4	02.02.2014		Fachliche QS	arvato
0.0.5	04.02.2014		Einarbeitung Kommentare durch QS	AuthentiDate
1.0.0	06.02.2014		Freigegeben durch Release Board	Martin Mielke, Arndt R. Maas, Dr. Andreas Eisenkolb
1.0.1	07.03.2014		Einarbeitung Kommentare der gematik	AuthentiDate
1.1.0	07.03.2014		Freigabe durch Release-Management	J. Rädisch
1.1.1	25.03.2014		Einarbeitung der Kommentare der gematik nach Abgleich mit Sicherheitskonzept	D. Baron
1.2.0	25.03.2014		Freigabe durch Release-Management	J. Rädisch
			Aufnahme der Anforderungen in das Anforderungsmanagement der gematik (Anforderungsnummern nach Nomenklatur der gematik)	gematik
1.3.0	11.04.2014		freigegeben	gematik

Inhaltsverzeichnis

Dokumentinformationen **2**

Inhaltsverzeichnis **3**

1 Einordnung des Dokumentes **5**

1.1 Zielsetzung **5**

1.2 Zielgruppe **5**

1.3 Geltungsbereich **5**

1.4 Abgrenzungen **5**

1.5 Methodik **6**

1.5.1 Hinweis auf offene Punkte 6

2 Systemüberblick **7**

3 Systemkontext **8**

3.1 Nutzer **8**

3.2 Nachbarsysteme **8**

4 Zerlegung des Produkttyps **9**

5 Übergreifende Festlegungen **12**

5.1 Logging **12**

5.2 Datenschutz **12**

5.3 Sicherheit **13**

6 Funktionsmerkmale **14**

6.1 Funktionsmerkmal OCSP-Proxy-Initialisierung **14**

6.1.1 Schnittstelle I_Init_OCSP_Proxy 14

6.1.1.1 Schnittstellendefinition *14*

6.1.1.2 Umsetzung *14*

6.2 Funktionsmerkmal OCSP-Proxy-Responder **16**

6.2.1 Schnittstelle I_OCSP_Status_Information 16

6.2.1.1 Schnittstellendefinition *16*

6.2.1.2 Umsetzung *17*

6.3 Funktionsmerkmal OCSP-Proxy-Requestor **20**

6.3.1 Schnittstelle I_OCSP_Information_Request 20

6.3.1.1 Schnittstellendefinition *20*

6.3.1.2 Umsetzung *20*

6.4 OCSP-Proxy-Speicher 22
6.5 Testunterstützung 23

Anhang A - Verzeichnisse 24
A1 – Abkürzungen 24
A2 – Glossar 24
A3 – Abbildungsverzeichnis 25
A4 – Tabellenverzeichnis 25
A5 - Referenzierte Dokumente 25
A5.1 – Dokumente der gematik 25
A5.2 – Weitere Dokumente 25

1 Einordnung des Dokumentes

1.1 Zielsetzung

Die vorliegende Spezifikation definiert die Anforderungen zu Herstellung, Test und Betrieb des Produkttyps OCSP-Proxy.

1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter des OCSP-Proxys der TI sowie Hersteller und Anbieter von Produkttypen, die hierzu eine Schnittstelle besitzen.

1.3 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des Deutschen Gesundheitswesens für den Online-Rollout (Stufe 1). Der Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z.B. Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und bekannt gegeben.

Schutzrechts-/Patentrechtshinweis

Die nachfolgende Spezifikation ist von der gematik allein unter technischen Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik GmbH übernimmt insofern keinerlei Gewährleistungen.

1.4 Abgrenzungen

Spezifiziert werden in dem Dokument die von dem Produkttyp bereitgestellten (angebotenen) Schnittstellen. Benutzte Schnittstellen werden hingegen in der Spezifikation desjenigen Produkttypen beschrieben, der diese Schnittstelle bereitstellt. Auf die entsprechenden Dokumente wird referenziert (siehe auch Anhang A5).

Die vollständige Anforderungslage für den Produkttyp ergibt sich aus weiteren Konzept- und Spezifikationsdokumenten, diese sind in dem Produkttypsteckbrief des Produkttyps OCSP-Proxy verzeichnet.

1.5 Methodik

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID in eckigen Klammern sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

⌦ **gemSpec_OCSP_Proxy_AFO_0000 <Titel der Afo>**

Text / Beschreibung⌫

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

1.5.1 Hinweis auf offene Punkte

Hinweis: Für die Anforderungen [TIP1-A_5280] und [TIP1-A_5281] wurde ein CR [L3-005] bei der gematik eingereicht und am 06.03.2014 genehmigt.

2 Systemüberblick

Im Rahmen der Telematikinfrastruktur (TI) kommen qualifizierte Signaturzertifikate zum Einsatz, die von akkreditierten Zertifizierungsdiensteanbietern (ZDA) herausgegeben werden. Der Aussteller der CA-Zertifikate für die akkreditierten ZDAs ist in Deutschland die Bundesnetzagentur (BNetzA). Für Statusprüfungen von QES-Zertifikaten in der Telematikinfrastruktur (TI) muss die gesamte Zertifikatskette vom CA-Zertifikat bis zum QES-Wurzelzertifikat der BNetzA geprüft werden. Der OCSP-Responder der BNetzA ist jedoch (a) nicht innerhalb der TI verfügbar und (b) leistungsmäßig nicht für das erwartete Volumen von OCSP-Requests ausgelegt. Daher wird der OCSP-Proxy (OCSP-Proxy) eingesetzt, der als OCSP-Requestor regelmäßig den OCSP-Responder der BNetzA abfragt und mit den zwischengespeicherten Ergebnissen die Anfragen aus der TI bedient.

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

Alle ZDA-CA-Zertifikate sowie die Cross- und Wurzelzertifikate der BNetzA und die CA-Zertifikate der HBA-Vorläuferkarten werden in die gematik Trust-service Status List (TSL) aufgenommen. Der Fully Qualified Domain Name (FQDN) des OCSP-Proxys wird als OCSP-Responder-Adresse im TSL-Eintrag des jeweiligen Dienstes eingetragen. Der OCSP-Proxy lädt in periodischen Abständen die TSL herunter, identifiziert die relevanten TSL-Einträge anhand des FQDNs, extrahiert diese aus der TSL und legt die erworbenen Informationen im Speicher des OCSP-Proxys ab.

Auf Basis der aus der TSL extrahierten Informationen sendet der OCSP-Proxy in regelmäßigen Abständen OCSP-Anfragen an alle aus der TSL extrahierten ZDA-CA-Zertifikate sowie Cross- und Wurzelzertifikate der BNetzA über das Internet an den OCSP-Responder der BNetzA und speichert die empfangenen OCSP-Antworten (einschließlich der zugehörigen Signatur) zwischen. Der OCSP-Proxy besitzt keine eigene Signaturfunktionalität und verändert die Signatur des OCSP-Responders der BNetzA nicht.

Bei OCSP-Anfragen aus der TI für ZDA-CA-Zertifikate sowie Cross- und Wurzelzertifikate der BNetzA antwortet der OCSP-Proxy mit den zwischengespeicherten OCSP-Antworten des OCSP-Responders der BNetzA. Im Falle von Anfragen für nonQES-End-Entity- und QES-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.

 © gematik - öffentlich

3 Systemkontext

3.1 Nutzer

Nutzer des OCSP-Proxys sind die zertifikatsvalidierenden Komponenten, die

- qualifizierte Zertifikate und/oder
- Endnutzer-Zertifikate (nonQES und QES) der durch die TI unterstützten HBA-Vorläuferkarten

prüfen. Im Vorhaben Online-Rollout (Stufe 1) handelt es sich lediglich um den Konnektor.

3.2 Nachbarsysteme

Nachfolgende Abbildung stellt die Nachbarsysteme und Nutzer des OCSP-Proxys dar.

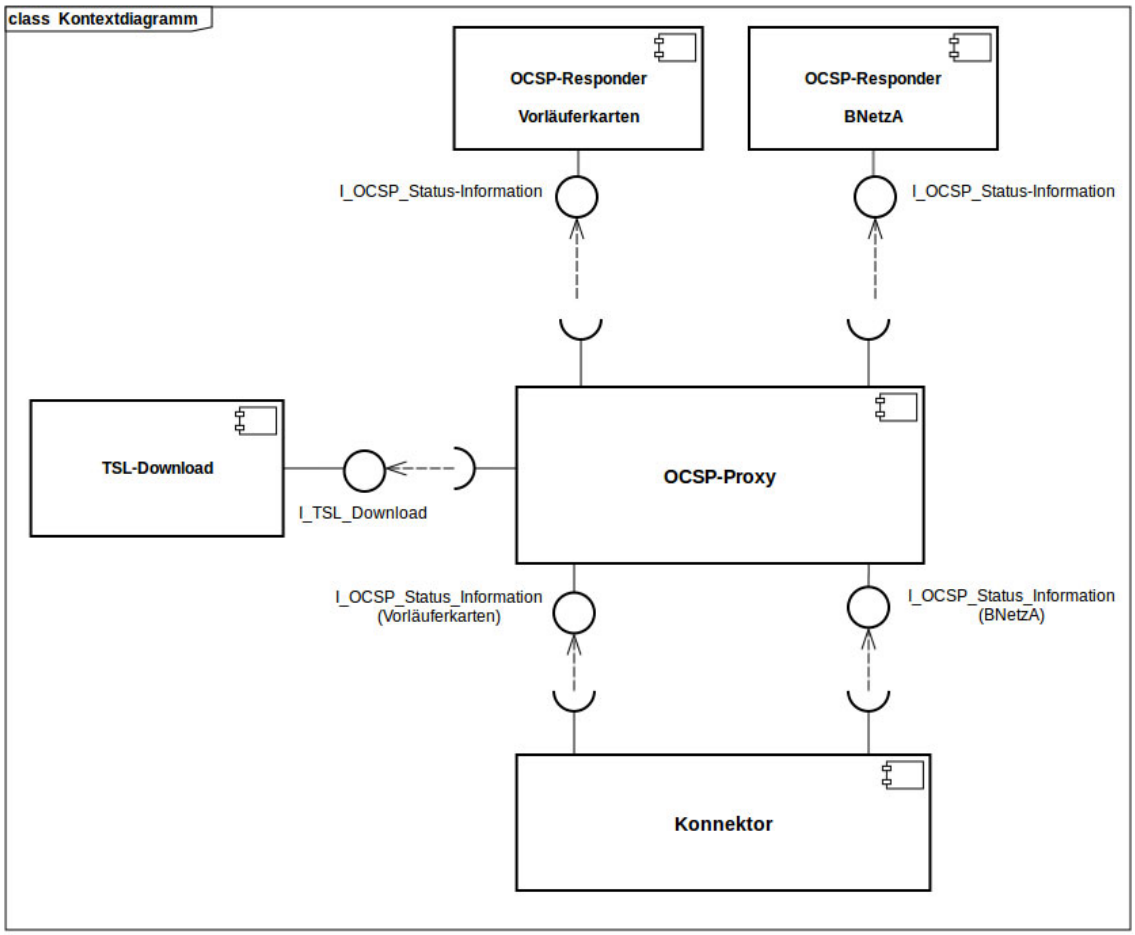

Abbildung 1: Abb_OCSP-Proxy_001 Nachbarsysteme und Nutzer des OCSP-Proxys.

4 Zerlegung des Produkttyps

Der OCSP-Proxy aggregiert die folgenden funktions-spezifischen Komponenten:

Das Modul **OCSP-Proxy-Initialisierung** liest periodisch in festgelegten Intervallen die TSL-Datei ein und extrahiert und speichert die für die Statusabfrage von Zertifikaten der BNetzA (Wurzel-, Cross- und ZDA-CA-Zertifikate – im Folgenden als QES-Root- und QES-CA-Zertifikate bezeichnet) sowie für Zertifikate der unterstützten HBA-Vorläuferkarten erforderlichen Informationen im Speicher des OCSP-Proxys ab.

Das Modul **OCSP-Proxy-Requestor** sendet in regelmäßigen Abständen OCSP-Anfragen an den OCSP-Responder der BNetzA und speichert die zurück gegebenen OCSP-Antworten im entsprechenden Eintrag des OCSP-Proxy-Speichers ab (Caching).

Das Modul **OCSP-Proxy-Responder** beantwortet die OCSP-Anfragen der zertifikatsvalidierenden Komponenten aus der TI.

Während der OCSP-Proxy-Responder bei OCSP-Anfragen für QES-Root- und QES-CA-Zertifikate aus der TI die gespeicherte OCSP-Response (einschließlich der Signatur des OCSP-Responders der BNetzA) des angefragten Zertifikats zurück gibt, leitet der OCSP-Proxy-Responder bei Anfragen für nonQES-End-Entity- und QES-End-Entity-Zertifikate (EE-Zertifikate) die OCSP-Anfrage an den OCSP-Responder der HBA-Vorläuferkarten weiter und gibt die vom OCSP-Responder zurück gelieferte OCSP-Antwort an die zertifikatsvalidierende Komponente zurück.

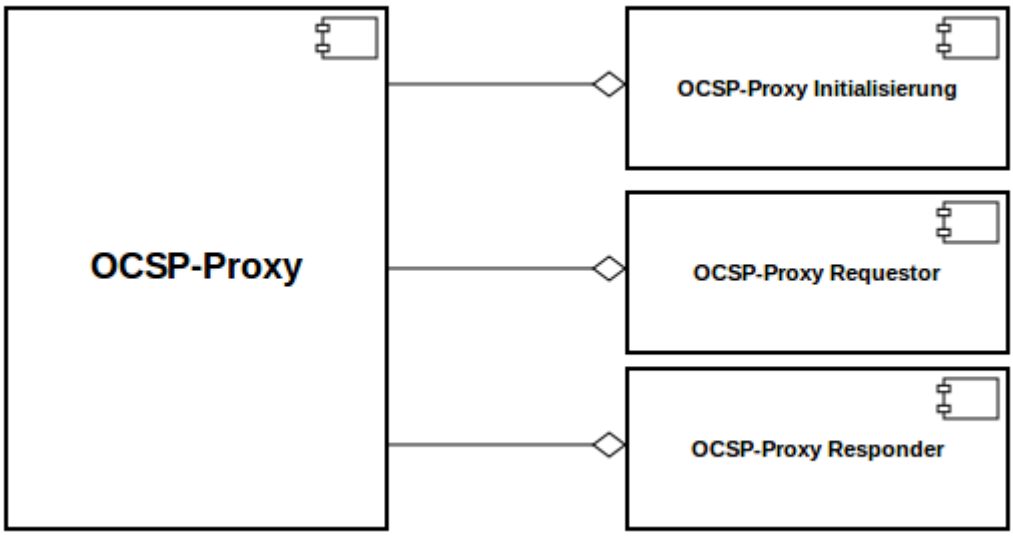

Abbildung 2: Abb_OCSP-Proxy_002 Zerlegung des Produkttyps

Abb_OCSP-Proxy_003 gibt einen Überblick über den Prozess der OCSP-Anfrage an den OCSP-Proxy sowie der OCSP-Antwort durch den OCSP-Proxy:

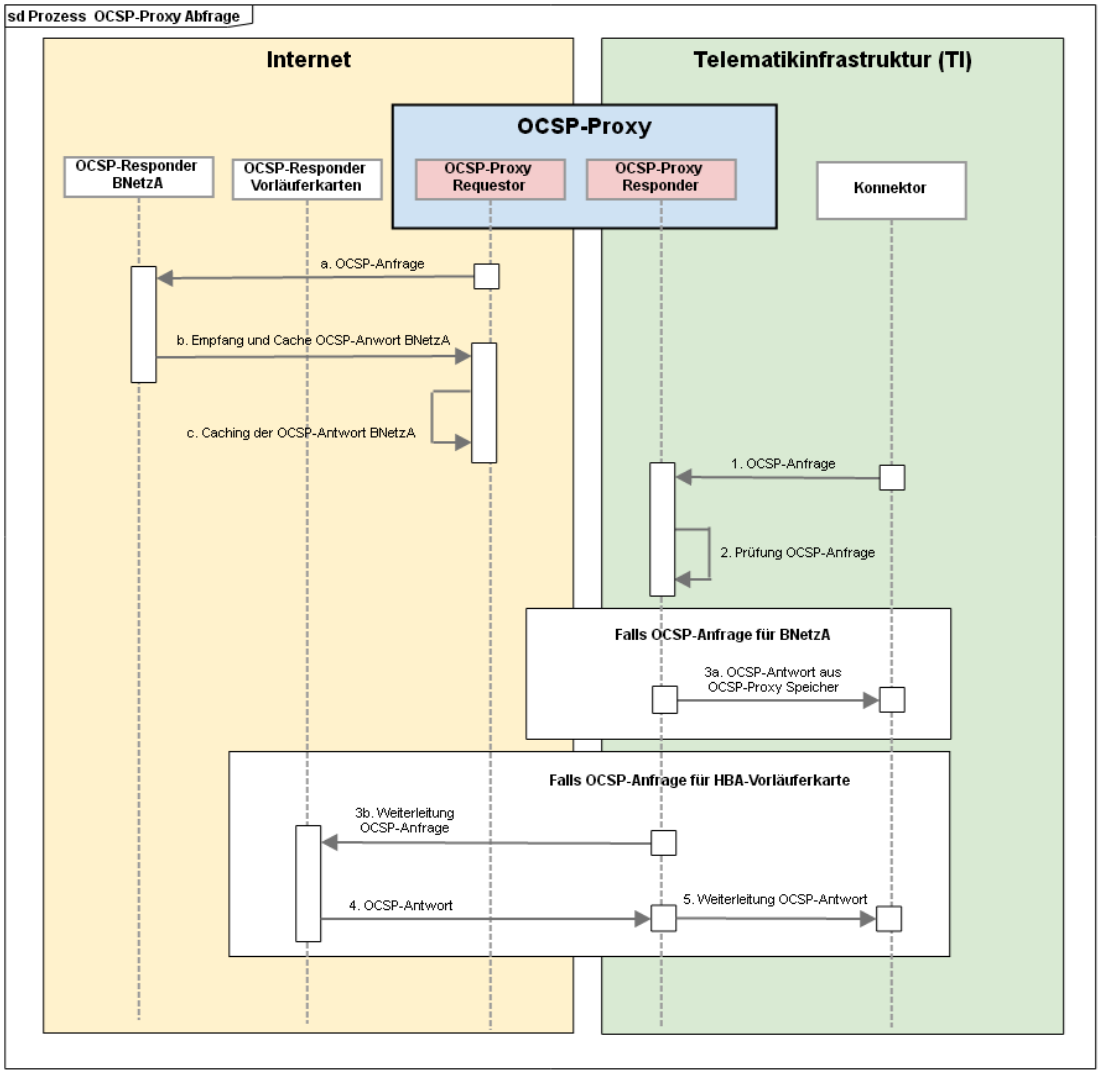

Abbildung 3: Abb_OCSP-Proxy_003 Überblick OCSP-Anfrage aus TI an OCSP-Proxy

Nachfolgende Erläuterung dient dem Verständnis der Abb_OCSP-Proxy_003.

Automatisierte Abfrage des OCSP-Responders der BNetzA (nach OCSP-Proxy-Initialisierung):

(a) Status-Abfrage aller in der TSL enthaltenen QES-Root- und QES-CA-Zertifikate am OCSP-Responder der BNetzA

(b) Empfang der OCSP-Antwort des OCSP-Responders der BNetzA

(c) Caching der OCSP-Antwort BNetzA

Prozessabläufe von OCSP-Anfragen aus der TI:

1. OCSP-Anfrage aus der TI

2. Prüfung der OCSP-Anfrage

Fallunterscheidung:

- OCSP-Anfrage für BNetzA

  3a: Rückgabe der OCSP-Antwort aus OCSP-Proxy-Speicher

- OCSP-Anfrage für Vorläuferkarte

  3b: Weiterleitung der OCSP-Anfrage an OCSP-Responder der Vorläuferkarte im Internet

  4. Empfang der OCSP-Antwort des OCSP-Responders der Vorläuferkarte

  5. Weiterleitung der OCSP-Antwort an anfragende Komponente (Konnektor) in der TI

5 Übergreifende Festlegungen

Im folgenden Kapitel werden übergreifende Anforderungen an den OCSP-Proxy aufgeführt.

5.1 Logging

⌦ **TIP1-A_5831 FehlerLog**

Der OCSP-Proxy MUSS lokal erkannte Fehler und Remote-Fehler im lokalen Protokollspeicher (FehlerLog) protokollieren. ⌫

⌦ **TIP1-A_5832 OCSP-Proxy Security-Log**

Der OCSP-Proxy KANN ein Security-Log für sicherheitsrelevante Ereignisse implementieren. ⌫

⌦ **TIP1-A_5833 OCSP-Proxy Performance-Log**

Der OCSP-Proxy KANN ein Performance-Log implementieren. ⌫

⌦ **TIP1-A_5834 OCSP-Proxy Debug-Log für Testbetrieb**

Der OCSP-Proxy KANN im Testbetrieb ein Debug-Log implementieren, das eine erweiterte Protokollierung für Testzwecke ermöglicht. ⌫

5.2 Datenschutz

⌦ **TIP1-A_5835 Fehlerprotokollierung**

Falls es erforderlich sein sollte, dass der OCSP-Proxy eine Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung durchführt, DARF der OCSP-Proxy NICHT personenenbezogene Daten in den Protokollen speichern. ⌫

⌦ **TIP1-A_5836 Schutz von Log-Dateien**

Falls es erforderlich sein sollte, dass der OCSP-Proxy eine Protokollierung zum Zwecke der Fehler- bzw. Störungsbehebung durchführt, DÜRFEN die Daten NICHT von unautorisierten Personen eingesehen werden. ⌫

⌦ **TIP1-A_5837 Technische Datenschutzmaßnahmen**

Der OCSP-Proxy MUSS zur Gewährleistung der Anforderungen des Datenschutzes technische Maßnahmen umsetzen, wenn deren Aufwand gegenüber organisatorischen Maßnahmen in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. ⌫

© gematik - öffentlich

5.3 Sicherheit

⌦ **TIP1-A_5838 Verwendung von Standards und Best Practices**

Im Rahmen des Designs und der Implementierung des OCSP-Proxys MÜSSEN der

- ISO27002 Standard - Abschnitt 12.2 [ISO27001] zur korrekten Verarbeitung in Anwendungen, d. h.
  - Überprüfung von Eingabedaten,
  - Kontrolle der internen Verarbeitung,
  - Integrität von Nachrichten,
  - Überprüfung von Ausgabedaten

sowie

- Best Practices (Secure Coding Guidelines) bei der Entwicklung von Software
  - OWASP Development Guide Project (Secure Coding Standards) [OWASP]
  - CERT Secure Coding (Secure Coding) [CERT]
  - Common Criteria for Information Technology Security Evaluation, Version 3.1, August 2012 [CC31]

berücksichtigt werden. ⌫

6 Funktionsmerkmale

6.1 Funktionsmerkmal OCSP-Proxy-Initialisierung

Der OCSP-Proxy-Initialisierung liest periodisch in festgelegten Intervallen die TSL-Datei ein und extrahiert und speichert die für die Statusabfrage von Zertifikaten der BNetzA sowie für Zertifikate der unterstützten HBA-Vorläuferkarten erforderlichen Informationen im Speicher des OCSP-Proxys ab.

Die OCSP-Antworten des OCSP-Responders der BNetzA für QES-Root- und QES-CA-Zertifikate (siehe Kapitel 6.3) werden in den entsprechen Einträgen des OCSP-Proxy Speichers abgelegt.

Die Attribute des OCSP-Proxy-Speichers können Tab_OCSP-Proxy_005 entnommen werden.

6.1.1 Schnittstelle I_Init_OCSP_Proxy

6.1.1.1 Schnittstellendefinition

Die Schnittstelle I_Init_OCSP_Proxy setzt den Prozess zur Initialisierung und Befüllung des OCSP-Proxy-Speichers um.

6.1.1.2 Umsetzung

⌦ **TIP1-A_5839 OCSP-Proxy initialisieren**

Der OCSP-Proxy MUSS den technischen Use Case "TUC_OCSP-Proxy_001 OCSP-Proxy Speicher initialisieren" gemäß Tab_OCSP-Proxy_001 umsetzen. ⌫

⌦ **TIP1-A_5840 Sichere Speicherung des TSL-Signer-CA-Zertifikats**

Der OCSP-Proxy MUSS das TSL-Signer-CA-Zertifikat sicher speichern.⌫

⌦ **TIP1-A_5841 Sichere Speicherung des Key Signing Keys des TI Trust Anchors**

Der OCSP-Proxy MUSS den Key Signing Key des TI Trust Anchors sicher speichern. ⌫

⌦ **TIP1-A_5842 Verwaltung des TSL-Signer-CA-Zertifikats**

Das TSL-Signer-CA-Zertifikat MUSS durch autorisierte Administratoren des OCSP-Proxys sicher eingebracht werden. ⌫

⌦ **TIP1-A_5843 Speicherung des Key Signing Keys des TI Trust Anchors**

Der Key Signing Key MUSS im OCSP-Proxy sicher eingebracht und gespeichert werden. ⌫

⌦ **TIP1-A_5844 Identifizierung und Extraktion der relevanten TSL-Einträge**

Der OCSP-Proxy MUSS die relevanten TSL-Einträge (QES-Root-, QES-CA- und CA-Zertifikate der zu unterstützenden HBA-Vorläuferkarten) anhand des FQDN des OCSP-Proxys identifizieren und aus der TSL-Datei extrahieren. ⌫

⌦ **TIP1-A_5845 Attribute des OCSP-Proxy Speichers**

Der OCSP-Proxy MUSS zu jedem relevanten Zertifikat der TSL mindestens die Attribute der in Tab_OCSP-Proxy_005 aufgeführten Zertifikatsinformationen im OCSP-Proxy Speicher speichern. ⌫

⌦ **TIP1-A_5846 OCSP-Anfragen an OCSP-Responder im Internet**

Der OCSP-Proxy DARF NICHT OCSP-Anfragen an andere als in der TSL enthaltenen OCSP-Responder der BNetzA und OCSP-Responder der zu unterstützenden HBA-Vorläuferkarten im Internet senden bzw. weiterleiten. ⌫

⌦ **TIP1-A_5847 Periodische Initialisierung des OCSP-Proxys**

Der OCSP-Proxy MUSS den "TUC_OCSP-Proxy_001 OCSP-Proxy-Speicher initialisieren" periodisch gemäß des in Tab_OCSP-Proxy_003 definierten Parameters Periodische Initialisierung durchführen. ⌫

Tabelle 1: Tab_OCSP-Proxy_001 TUC_OCSP-Proxy_001 OCSP-Proxy-Speicher initialisieren

Element	Beschreibung
Name	TUC_OCSP-Proxy_001 "OCSP-Proxy-Speicher initialisieren"
Beschreibung	Dieser Use Case beschreibt die Ermittlung der QES-Root-, QES-CA-Zertifikate sowie der CA-Zertifikate der unterstützten HBA-Vorläuferkarten aus der TSL-Datei sowie die Befüllung des OCSP-Proxy-Speichers mit den relevanten Informationen.
Auslöser	Periodische Initialisierung
Vorbedingungen	Das TSL-Signer-CA-Zertifikat wurde im OCSP-Proxy hinterlegt. Die TSL ist im TSL-Download-Dienst verfügbar.
Eingangsdaten	FQDN des OCSP-Proxys (Zur Identifizierung der relevanten TSL-Einträge) Konfiguration des Parameters Periodische Initialisierung
Komponenten	TSL-Download-Dienst, OCSP-Proxy
Ausgangsdaten	Zertifikatsinformationen der relevanten QES-Root- und QES-CA-Zertifikate sowie der CA-Zertifikate der unterstützten HBA-Vorläuferkarten
Nachbedingungen	

© gematik - öffentlich

Standardablauf	1. [OCSP-Proxy]: Durchführung des technischen Use Cases "Periodische Aktualisierung TI-Vertrauensraum" gemäß [gemSpec_PKI# TUC_PKI_001]. 2. [OCSP-Proxy]: TSL-Einträge (Element TSPService) der relevanten QES-Root-, QES-CA-Zertifikate sowie CA-Zertifikate der unterstützten HBA-Vorläuferkarten anhand des FQDNs des OCSP-Proxys im Element ServiceSupplyPoint Identifizieren. 3. [OCSP-Proxy]: Benötige Zertifikatsinformationen (siehe Tab_OCSP-Proxy_005) aus identifizierten TSL-Einträgen der TSL extrahieren. 4. [OCSP-Proxy]: Vorhandene Zertifikats- und Statusinformationen aus dem Speicher des OCSP-Proxys löschen. 5. [OCSP-Proxy]: Extrahierte Zertifikatsinformationen im Speicher des OCSP-Proxys ablegen. 6. [OCSP-Proxy]: Initiierung der Durchführung des technischen Use Cases "TUC_OCSP-Proxy_003 OCSP-Abfrage an OCSP-Responder der BNetzA senden" zur Abfrage und Speicherung der OCSP-Antworten des BNetzA-OCSP-Responders für QES-Root- und QES-CA-Zertifikate.
Varianten/Alternativen	1a. [OCSP-Proxy]: Es liegt keine neue TSL-Datei vor. Der Prozess wird beendet. 1b. [OCSP-Proxy]: Es liegt eine neue TSL-Datei vor. Weiter mit Schritt 2.
Fehlerfälle	In jedem der beschriebenen Schritte können Fehler auftreten. Diese werden durch das System protokolliert. Der Prozess wird beendet.
Nichtfunktionale Anforderungen	
Zugehörige Diagramme	
Ergebnisse (Output)	Initialisierter OCSP-Proxy-Speicher.
Anmerkungen	

6.2 Funktionsmerkmal OCSP-Proxy-Responder

6.2.1 Schnittstelle I_OCSP_Status_Information

6.2.1.1 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 des OCSP-Responders der BNetzA sowie für Zertifikate der unterstützten HBA-Vorläuferkarten in der TI-Plattform verfügbar gemacht.

6.2.1.2 Umsetzung

⌦ **TIP1-A_5848 Erreichbarkeit OCSP-Proxy**

Der OCSP-Proxy MUSS in Form eines OCSP-Responders über das Netzwerk der Telematikinfrastruktur erreichbar sein. ⌫

⌦ **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. ⌫

⌦ **TIP1-A_5850 Rückgabe von gecachten OCSP-Antworten für QES-Root- und QES-CA-Zertifikate**

Der OCSP-Proxy MUSS bei Anfragen aus der TI für QES-Root- und QES-CA-Zertifikate mit den gecachten OCSP-Antworten des OCSP-Responders der BNetzA antworten. ⌫

⌦ **TIP1-A_5851 Weiterleitung von OCSP-Anfragen für nonQES- und QES-EE-Zertifikate der zu unterstützenden HBA-Vorläuferkarten.**

Der OCSP-Proxy MUSS OCSP-Anfragen der zertifikatsvalidierenden Komponenten der TI für nonQES- und QES-EE-Zertifikate der zu unterstützenden HBA-Vorläuferkarten unverändert an den entsprechenden OCSP-Responder im Internet weiterleiten und die Antwort des OCSP-Responders an die zertifikatsvalidierenden Komponente unverändert zurückgeben. ⌫

⌦ **TIP1-A_5852 Verbindungsaufbau zu OCSP-Respondern im Internet**

Ein Verbindungsaufbau zu den OCSP-Respondern im Internet MUSS vom OCSP-Proxy initiiert werden. ⌫

⌦ **TIP1-A_5853 Ablehnung von Anfragen aus dem Internet**

Anfragen aus dem Internet MÜSSEN vom OCSP-Proxy abgelehnt werden. ⌫

⌦ **TIP1-A_5854 Beschränkung der ausgehenden Verbindungen**

Der OCSP-Proxy MUSS gewährleisten, dass OCSP-Anfragen in das Internet nur an den OCSP-Responder der BNetzA und an die OCSP-Responder der HBA-Vorläuferkarten gesendet werden. ⌫

⌦ **TIP1-A_5855 Speicherung von OCSP-Anfragen**

Der OCSP-Proxy DARF OCSP-Anfragen der zertifikatsvalidierenden Komponenten der TI für nonQES- und QES-EE-Zertifikate der zu unterstützenden HBA-Vorläuferkarten NICHT speichern. ⌫

⌦ **TIP1-A_5856 Speicherung von OCSP-Antworten**

Der OCSP-Proxy DARF OCSP-Antworten für die zertifikatsvalidierenden Komponenten der TI für nonQES- und QES-EE-Zertifikate der zu unterstützenden HBA-Vorläuferkarten NICHT speichern. ⌫

⌦ **TIP1-A_5857 Protokollierung von OCSP-Anfragen und OCSP-Antworten**

Der OCSP-Proxy DARF OCSP-Anfragen und OCSP-Antworten NICHT protokollieren. ⌫

Tabelle 2: 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 QES-Root- und QES-CA- sowie nonQES-EE- und QES-EE-Zertifikate der HBA-Vorläuferkarten.
Auslöser	OCSP-Anfrage einer zertifikatsvalidierenden Komponente aus der TI
Vorbedingungen	Der OCSP-Proxy wurde initialisiert (siehe Tab_OCSP-Proxy_001).
Eingangsdaten	OCSP-Anfrage
Komponenten	Zertifikatsvalidierende Komponenten der TI (z. B. Konnektor), OCSP-Proxy, OCSP-Responder der HBA-Vorläuferkarten
Ausgangsdaten	OCSP-Antwort des BNetzA-OCSP-Responders oder eines OCSP-Responders von HBA-Vorläuferkarten
Nachbedingungen	
Standardablauf	1. [OCSP-Proxy]: OCSP-Anfrage der zertifikatsvalidierenden Komponente empfangen. 2. [OCSP-Proxy]: IssuerNameHash und IssuerKeyHash aus der OCSP-Anfrage der zertifikatsvalidierenden Komponente extrahieren. 3. [OCSP-Proxy]: Anhand des IssuerNameHashs und IssuerKeyHashs den relevanten Eintrag aus dem Speicher des OCSP-Proxys selektieren. 4. [OCSP-Proxy]: OCSP-Antwort an zertifikatsvalidierende Komponente zurückgeben.

Varianten/Alternativen	3a. [OCSP-Proxy]: IssuerNameHash und IssuerKeyHash im Speicher vorhanden und Seriennummer nicht im Speicher vorhanden (es handelt sich um eine Anfrage für ein nonQES-EE- oder QES-EE-Zertifikat der HBA-Vorläuferkarten). 3a 1. [OCSP-Proxy]: OCSP-Anfrage unter Verwendung von "ServiceSupplyPoint Internet" an den entsprechenden OCSP-Responder im Internet weiterleiten. 3a 2. [OCSP-Proxy]: OCSP-Antwort des OCSP-Responders im Internet empfangen. 3a 3. [OCSP-Proxy]: OCSP-Antwort des OCSP-Responders im Internet an die zertifikatsvalidierende Komponente weiterleiten. Der Prozess ist beendet. 3b. [OCSP-Proxy]: IssuerNameHash und IssuerKeyHash und Seriennummer im Speicher vorhanden und ServiceTypeIdentifier = `http://uri.etsi.org/TrstSvc/Svctype/CA/QC` (es handelt sich um QES-Root- oder QES-CA-Zertifikat): OCSP-Antwort des OCSP-Responders der BNetzA aus Speicher des OCSP-Proxys selektieren
Fehlerfälle	3c. [OCSP-Proxy]: IssuerNameHash und IssuerKeyHash nicht im Speicher vorhanden: OCSP-Antwort mit einer unsignierten Error-Response des Typs "internalError" (siehe [COMMON-PKI#Part4]) zurückgeben. 3a 1a [OCSP-Proxy]: Der OCSP-Responder im Internet ist nicht erreichbar: OCSP-Response mit einer unsignierten Error-Response des Typs "tryLater" (siehe [RFC2560#2.3]) zurückgeben. 3b a. Keine OCSP-Antwort im Speicher des OCSP-Proxys vorhanden: OCSP-Response mit einer unsignierten Error-Response des Typs "tryLater" (siehe [RFC2560#2.3]) zurückgeben. 3b b. [OCSP-Proxy]: Die OCSP-Anfrage besitzt die Extension "nonce": OCSP-Response mit einer unsignierten Error-Response des Typs "malformedRequest" (siehe [RFC2560#2.3]) zurückgeben.
Nichtfunktionale Anforderungen	
Zugehörige Diagramme	

6.3 Funktionsmerkmal OCSP-Proxy-Requestor

6.3.1 Schnittstelle I_OCSP_Information_Request

6.3.1.1 Schnittstellendefinition

Die Schnittstelle I_OCSP_Information_Request setzt den Prozess zur Abfrage des OCSP-Responders der BNetzA und Speicherung der erhaltenen OCSP-Antworten im Speicher des OCSP-Proxy um.

6.3.1.2 Umsetzung

⌦ **TIP1-A_5858 OCSP-Anfrage an OCSP-Responder der BNetzA senden**

Der OCSP-Proxy MUSS den technischen Use Case "TUC_OCSP-Proxy_003 OCSP-Anfrage an OCSP-Responder der BNetzA senden" gemäß Tab_OCSP-Proxy_004 umsetzen. ⌫

⌦ **TIP1-A_5859 Konfigurierbares Intervall für OCSP-Anfragen an den BNetzA-OCSP-Responder**

Der OCSP-Proxy MUSS den OCSP-Responder der BNetzA zu konfigurierbaren periodischen Zeitpunkten abfragen. ⌫

⌦ **TIP1-A_5860 Gültigkeit OCSP-Antworten der BNetzA**

Die gecachten OCSP-Antworten des BNetzA-OCSP-Responders MÜSSEN nach Ablauf der konfigurierten Gültigkeitsdauer gemäß Tab_OCSP-Proxy_003 aus dem Cache entfernt werden. ⌫

⌦ **TIP1-A_5861 Abfrage-Intervall BNetzA-OCSP-Responder**

Der OCSP-Proxy MUSS den OCSP-Responder der BNetzA periodisch gemäß des in Tab_OCSP-Proxy_003 definierten Abfrage-Intervalls abfragen. ⌫

⌦ **TIP1-A_5862 Nicht-Erreichen des OCSP-Responders der BNetzA**

Sofern der OCSP-Responder der BNetzA nicht erreichbar ist, SOLL dieser unmittelbar gemäß der in Tab_OCSP-Proxy_003 definierten Anzahl an Wiederholungen wiederholt angefragt werden. ⌫

⌦ **TIP1-A_5863 Einhaltung der zugelassenen Wertebereiche**

Der OCSP-Proxy MUSS beim Hochfahren überprüfen, dass die in Tab_OCSP-Proxy_003 zugelassenen Wertebereiche eingehalten werden. Sofern die im OCSP-Proxy konfigurierten Werte nicht den in Tab_OCSP-Proxy_003 zugelassenen Wertebereichen entsprechen, DARF der OCSP-Proxy NICHT hochfahren. ⌫

⌦ **TIP1-A_5864 Änderung von Konfigurationsparametern**

Der OCSP-Proxy MUSS gewährleisten, dass die in Tab_OCSP-Proxy_003 definierten Konfigurationsparameter nicht im laufenden Betrieb des OCSP-Proxys geändert werden können. ⌫

Tabelle 3: Tab_OCSP-Proxy_003 Konfigurations-Parameter und Default-Werte des OCSP-Proxys

Parameter	Defaultwert	Zugelassener Wertebereich
BNetzA-Abfrage-Intervall	2 Stunden	1 Stunde – 4 Stunden
Caching-Dauer	4 Stunden	1 Stunde – 4 Stunden
Anzahl Wiederholungen (bei Nicht-Erreichen des OCSP-Responders der BNetzA)	3	1 - 5
Timeout (Zeitraum bevor die Anfrage an den OCSP-Responder der BNetzA wegen Zeitüberschreitung abgebrochen wird)	30 Sekunden	1 Sekunde – 60 Sekunden
Periodische Initialisierung	24 Stunden	1 Stunde – 24 Stunden

Tabelle 4: Tab_OCSP-Proxy_004 TUC_OCSP-Proxy_003 OCSP-Anfrage an den OCSP-Responder der BNetzA senden

Element	Beschreibung
Name	TUC_OCSP-Proxy_003 OCSP-Anfrage an OCSP-Responder der BNetzA senden
Beschreibung	Dieser Use Case beschreibt den Prozess zur Statusabfrage der QES-Root- und QES-CA-Zertifikate beim OCSP-Responder der BNetzA und die Speicherung der empfangenen OCSP-Responses im Speicher des OCSP-Proxys.
Auslöser	BNetzA-Abfrage-Intervall
Vorbedingungen	OCSP-Proxy Zertifikatsinformationen wurden im Rahmen des technischen Use Cases" TUC_OCSP-Proxy_001 OCSP-Proxy initialisieren" gespeichert.
Eingangsdaten	Im OCSP-Proxy-Speicher abgelegte Zertifikatsinformationen Konfiguration des Parameters BNetzA-Abfrage-Intervall Konfiguration des Parameters Anzahl Wiederholungen (bei Nicht-Erreichen des OCSP-Respondes der BNetzA) Konfiguration des Parameters Timeout
Komponenten	OCSP-Proxy, OCSP-Responder der BNetzA
Ausgangsdaten	Aktualisierte OCSP-Antworten im OCSP-Proxy-Speicher (siehe Tab_OCSP-Proxy_005).
Nachbedingungen	

Standardablauf	1. [OCSP-Proxy]: Iteration über die im OCSP-Proxy-Speicher vorhandenen Zertifikatsinformationen und Selektion aller für die OCSP-Anfrage erforderlichen Daten. Es werden lediglich Einträge selektiert, die im Attribut "ServiceTypeIdentifier" den Wert `http://uri.etsi.org/-TrstSvc/Svctype/CA/QC` besitzen. Für die Abfrage des OCSP-Responders der BNetzA muss der Wert aus dem Attribut "AIA" des Zertifikats verwendet werden. 2. [OCSP-Proxy]: OCSP-Anfrage generieren und an den OCSP-Responder der BNetzA senden. 3. [OCSP-Responder der BNetzA]: OCSP-Antwort an OCSP-Proxy senden. 4. [OCSP-Proxy]: OCSP-Antwort empfangen und den Statusinformationen des entsprechenden Eintrags (einschließlich der zugehörigen Signatur) im Speicher des OCSP-Proxys hinzufügen.
Varianten/Alternativen	
Fehlerfälle	2a. [OCSP-Proxy]: Der OCSP-Responder der BNetzA ist nicht erreichbar (Timeout erreicht). Der Vorgang wird protokolliert. a. [OCSP-Proxy]: Anzahl Wiederholungen gemäß Tab_OCSP-Proxy_003 erreicht: Der Prozess wird beendet. b. [OCSP-Proxy]: Anzahl Wiederholungen gemäß Tab_OCSP-Proxy_003 nicht erreicht: Erneute OCSP-Anfrage an den OCSP-Responder der BNetzA senden.
Nichtfunktionale Anforderungen	
Zugehörige Diagramme	

6.4 OCSP-Proxy-Speicher

Der OCSP-Proxy legt für jeden notwendigen und damit aus der TSL extrahierten Dienst einen Eintrag mit den benötigten Informationen im Speicher des OCSP-Proxys ab. Die OCSP-Antwort des OCSP-Responders der BNetzA wird dem entsprechenden Eintrag hinzugefügt.

Nachfolgende Tabelle stellt die Attribute des OCSP-Proxy Speichers dar.

Tabelle 5: Tab_OCSP-Proxy_005 Beschreibung der Attribute des OCSP-Proxy Speichers

Informationsobjekt	Attribute

Zertifikatsinformation	• ServiceName
	• ServiceTypeIdentifier
	• X509Certificate
	• IssuerNameHash (aus X509Certificate)
	  o Für alle zu unterstützenden Hash-Algorithmen gemäß [gemSpec_Krypt]
	• IssuerKeyHash (aus X509Certificate)
	  o Für alle zu unterstützenden Hash-Algorithmen gemäß [gemSpec_Krypt]
	• Seriennummer (aus X509Certificate)
	• ServiceSupplyPoint Internet (Extrahierte Adresse des OCSP-Responders im Internet (BNetzA-OCSP-Responder oder OCSP-Responder der HBA-Vorläuferkarten) aus dem Path der OCSP-Proxy-URI im Element ServiceSupplyPoint).
	• Authority Information Access (AIA) (aus X509Certificate)

Statusinformationen	• OCSP-Antwort des BNetzA-OCSP-Responders

6.5 Testunterstützung

Neben dem OCSP-Proxy für die Produktivumgebung (PU) wird ein davon separierter OCSP-Proxy für Test- und Referenzzwecke betrieben.

Da kein BNetzA-COSP-Responder für Testzwecke zur Verfügung steht, wird in der RU/TU ein OCSP-Responder für Pseudo-QES-CA-Zertifikate im Internet bereit gestellt.

Der OCSP-Proxy ermittelt die Adresse des OCSP-Responders der BNetzA (PU) bzw. des OCSP-Responders für Pseudo-QES-CA-Zertifikate (RU/TU) aus den QES-CA-Zertifikaten aus der TSL.

Im Rahmen der RU/TU werden die Pseudo-QES-CA-Zertifikate mit dem ServiceTypeIdentifier `http://uri.etsi.org/TrstSvc/Svctype/CA/QC` in die TSL eingestellt. Die Adresse des OCSP-Responders für Pseudo-QES-CA-Zertifikate ist im Feld `Authority Information Access` des Pseudo-QES-CA-Zertifikats vorhanden.

Anhang A - Verzeichnisse

A1 – Abkürzungen

Kürzel	Erläuterung
AIA	Authority Information Access
BNetzA	Bundesnetzagentur
CA	Certificate Authority
CERT	Computer Emergency Response Team
DNS	Domain Name System
DNSSEC	Domain Name System Security Extensions
EE	End Entity
FQDN	Fully Qualified Domain Name
HBA	Heilberufsausweis
ISO	Internationale Organisation für Normung
OCSP	Online Certficate Status Protocol
ORS 1	Online-Rollout (Stufe 1)
OWASP	Open Web Application Security Project
QES	Qualifizierte elektronische Signatur
TI	Telematikinfrastruktur
TSL	Trust-service Status List
URI	Uniform Resource Identifier
ZDA	Zertifizierungsdiensteanbieter

A2 – Glossar

Begriff	**Erläuterung**
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.

Das Glossar wird als eigenständiges Dokument, vgl. [gemGlossar] zur Verfügung gestellt.

© gematik - öffentlich

A3 – Abbildungsverzeichnis

Abbildung 1: Abb_OCSP-Proxy_001 Nachbarsysteme und Nutzer des OCSP-Proxys. 8
Abbildung 2: Abb_OCSP-Proxy_002 Zerlegung des Produkttyps.....9
Abbildung 3: Abb_OCSP-Proxy_003 Überblick OCSP-Anfrage aus TI an OCSP-Proxy ..10

A4 – Tabellenverzeichnis

Tabelle 1: Tab_OCSP-Proxy_001 TUC_OCSP-Proxy_001 OCSP-Proxy-Speicher initialisieren.....15
Tabelle 2: Tab_OCSP-Proxy_002 TUC_OCSP-Proxy_002 OCSP-Anfragen aus der TI beantworten.....18
Tabelle 3: Tab_OCSP-Proxy_003 Konfigurations-Parameter und Default-Werte des OCSP-Proxys 21
Tabelle 4: Tab_OCSP-Proxy_004 TUC_OCSP-Proxy_003 OCSP-Anfrage an den OCSP-Responder der BNetzA senden.....21
Tabelle 5: Tab_OCSP-Proxy_005 Beschreibung der Attribute des OCSP-Proxy Speichers 23

A5 - Referenzierte Dokumente

A5.1 – Dokumente der gematik

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastruktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert, Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument passende jeweils gültige Versionsnummer sind in der aktuellsten, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur
[gemSpec_PKI	gematik: Übergreifende Spezifikation PKI

A5.2 – Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[CC31]	Common Criteria for Information Technology Security Evaluation, Version 3.1, September 2012
[CERT]	CERT Secure Coding; http://www.cert.org/secure-coding/
[COMMON-PKI]	T7 & TeleTrust (20.01.2009): Common PKI Spezifikation, Version 2.0 http://www.t7ev.org/themen/entwickler/common-pki-v20-spezifikation.html
[ISO27001]	Information technology – Security techniques – Information security management systems – Requirements
[OWASP]	OWASP Development Guide Project; http://www.owasp.org/index.php/Category:OWASP_Guide_Project
[RFC 3986]	RFC 3986 (Januar 2005): Uniform Resource Identifier (URI): Generic Syntax http://tools.ietf.org/html/rfc3986