

## Elektronische Gesundheitskarte und Telematikinfrastruktur

# Spezifikation OCSP-Proxy

|                  |                                      |
|------------------|--------------------------------------|
| Version:         | 1.9. <del>0</del> <u>1</u>           |
| Revision:        | <del>849548770</del>                 |
| Stand:           | <del>14.0509.06.2018</del> <u>23</u> |
| Status:          | freigegeben                          |
| Klassifizierung: | öffentlich                           |
| Referenzierung:  | gemSpec_OCSP_Prox<br>y               |

## Dokumentinformationen

### Änderungen zur Vorversion

Anpassungen gemäß der vorliegenden Änderungsliste P15.2 sind gelb markiertn Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

### Dokumentenhistorie

| Versio<br>n      | Stand                                   | Kap./<br>Seite | Grund der Änderung, besondere<br>Hinweise   | Bearbeitun<br>g |
|------------------|---|----------------|---|-----------------|
| 0.0.1            | 23.12.2013                              |                | Initiale Erstellung   |                 |
| 0.0.2            | 13.01.2014                              | 6              | Erstellung Systemüberblick, TUCs und Anforderungen  |                 |
| 0.0.3            | 30.01.2014                              |                | Überarbeitung TUCs, Ergänzung Anforderungen, Erstellung Systemkontext, Zerlegung des Produkttyps und Übergreifende Festlegungen |                 |
| 0.0.4            | 02.02.2014                              |                | Fachliche QS  |                 |
| 0.0.5            | 04.02.2014                              |                | Einarbeitung Kommentare durch QS  |                 |
| 1.0.0            | 06.02.2014                              |                | Freigegeben durch Release Board   |                 |
| 1.0.1            | 07.03.2014                              |                | Einarbeitung Kommentare der gematik   |                 |
| 1.1.0            | 07.03.2014                              |                | Freigabe durch Release-Management   |                 |
| 1.1.1            | 25.03.2014                              |                | Einarbeitung der Kommentare der gematik nach Abgleich mit Sicherheitskonzept  |                 |
| 1.2.0            | 25.03.2014                              |                | Freigabe durch Release-Management   |                 |
| <u>1.3.0</u>     | <u>11.04.2014</u>                       |                | Aufnahme der Anforderungen in das Anforderungsmanagement der gematik (Anforderungsnummern nach Nomenklatur der gematik)         | gematik         |
| <del>1.3.0</del> | <del>11.04.2014</del>                   |                | freigegeben   | gematik         |
| 1.4.0            | 01.04.2015                              |                | Korrekturen der Verarbeitung von QES-Zertifikaten   |                 |
| <u>1.5.0</u>     | <del>24.04.2015</del> <u>05.05.2015</u> |                | Freigabe d. Release-Management  |                 |
| <del>1.5.0</del> | <del>05.05.2015</del>                   |                | freigegeben   | gematik         |
| 1.6.0            | 24.08.16                                |                | Anpassungen zum Online-Produktivbetrieb (Stufe 1)   | gematik         |
| 1.7.0            | 16.10.16                                |                | Anpassungen gemäß Änderungsliste  |                 |

|                       |                          |                       |  |                         |
|-----------------------|--------------------------|-----------------------|--|-------------------------|
|                       |                          |                       |  |                         |
|                       |                          |                       | Änderungen in Vorbereitung auf das Release 1.6.3 (eIDAS) |                         |
| 1.8.0                 | 06.02.17                 |                       | Anpassungen lt. Änderungsliste                           | gematik                 |
| 1.9.0                 | 14.05.18                 |                       | freigegeben  | gematik                 |
| <a href="#">1.9.1</a> | <a href="#">09.06.23</a> | <a href="#">6.5.2</a> | <a href="#">Einarbeitung<br/>CI_Maintenance_23.1</a>     | <a href="#">gematik</a> |

---

## Inhaltsverzeichnis

---

|   |           |
|---|-----------|
| <b>1 Einordnung des Dokumentes.....</b>               | <b>5</b>  |
| 1.1 Zielsetzung.....                                  | 5         |
| 1.2 Zielgruppe.....                                   | 5         |
| 1.3 Geltungsbereich.....                              | 5         |
| 1.4 Abgrenzungen.....                                 | 5         |
| 1.5 Methodik.....                                     | 6         |
| <b>2 Systemüberblick.....</b>                         | <b>7</b>  |
| <b>3 Systemkontext.....</b>                           | <b>8</b>  |
| 3.1 Nutzer.....                                       | 8         |
| 3.2 Nachbarsysteme.....                               | 8         |
| 3.3 Anfrageablauf.....                                | 10        |
| <b>4 Übergreifende Festlegungen.....</b>              | <b>11</b> |
| 4.1 Logging.....                                      | 11        |
| 4.2 Datenschutz.....                                  | 11        |
| 4.3 Sicherheit.....                                   | 11        |
| <b>5 Funktionsmerkmale.....</b>                       | <b>13</b> |
| <b>5.1 Funktionsmerkmal OCSP-Proxy-Responder.....</b> | <b>13</b> |
| 5.1.1 Schnittstelle I_OCSP_Status_Information.....    | 13        |
| 5.1.1.1 Schnittstellendefinition.....                 | 13        |
| 5.1.1.2 Umsetzung.....                                | 13        |
| 5.2 Testunterstützung.....                            | 15        |
| <b>6 Anhang A - Verzeichnisse.....</b>                | <b>16</b> |
| 6.1 Abkürzungen.....                                  | 16        |
| 6.2 Glossar.....                                      | 16        |
| 6.3 Abbildungsverzeichnis.....                        | 16        |
| 6.4 Tabellenverzeichnis.....                          | 17        |
| <b>6.5 Referenzierte Dokumente.....</b>               | <b>17</b> |
| 6.5.1 Dokumente der gematik.....                      | 17        |
| 6.5.2 Weitere Dokumente.....                          | 17        |

---

## 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. 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:

**<AFO-ID> - <Titel der Afo>**

Text / Beschreibung

**[<=]**

Dabei umfasst die Anforderung sämtliche innerhalb der Textmarken angeführten Inhalte.

---

## 2 Systemüberblick

---

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

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

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

---

## 3 Systemkontext

---

### 3.1 Nutzer

Nutzer des OCSP-Proxys sind die zertifikatsvalidierenden Komponenten, die

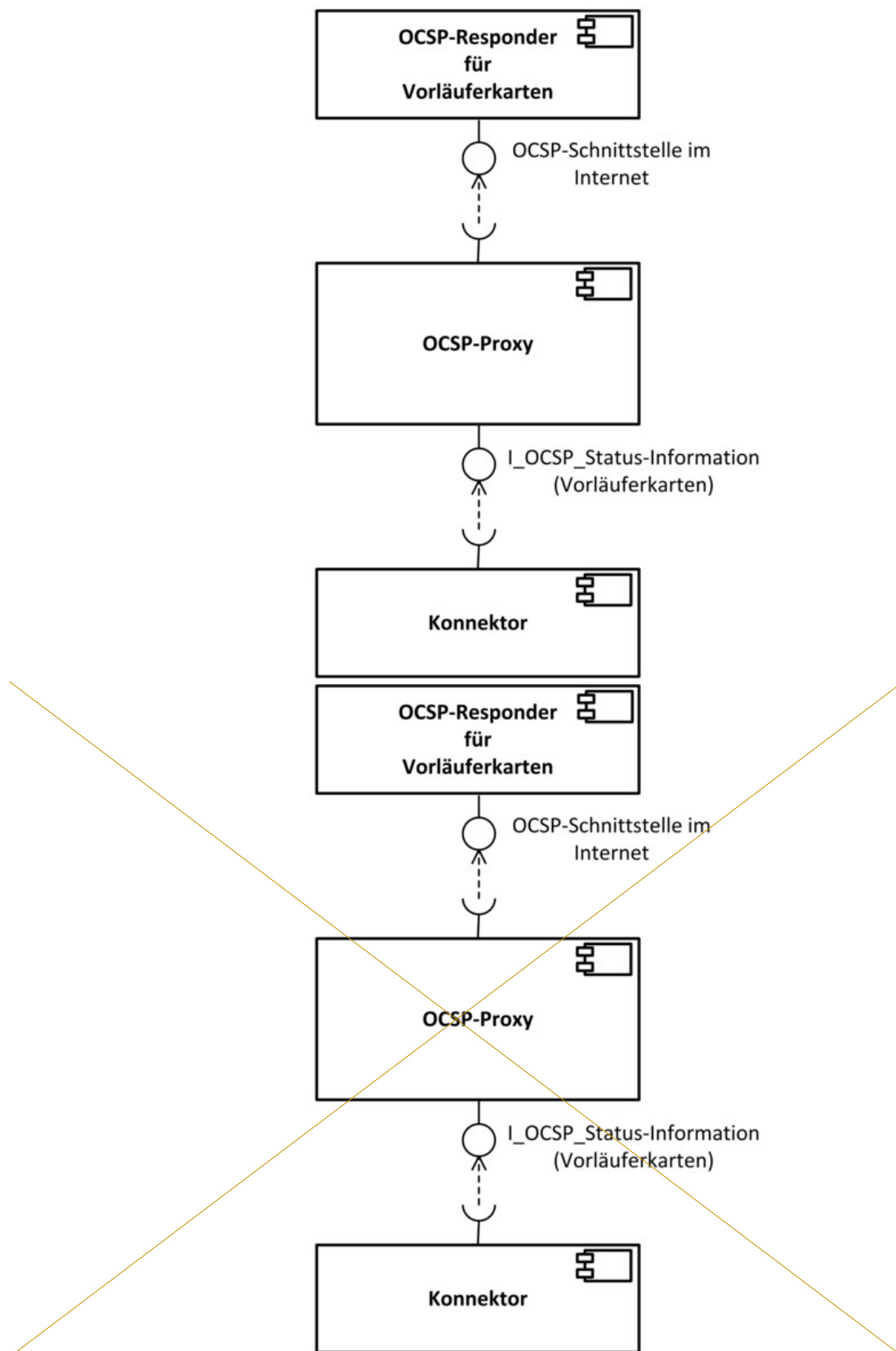
- Endnutzer-Zertifikate (nonQES und QES) der durch die TI unterstützten HBA-Vorläuferkarten

prüfen. Dabei handelt es sich lediglich um den Konnektor.

### 3.2 Nachbarsysteme

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

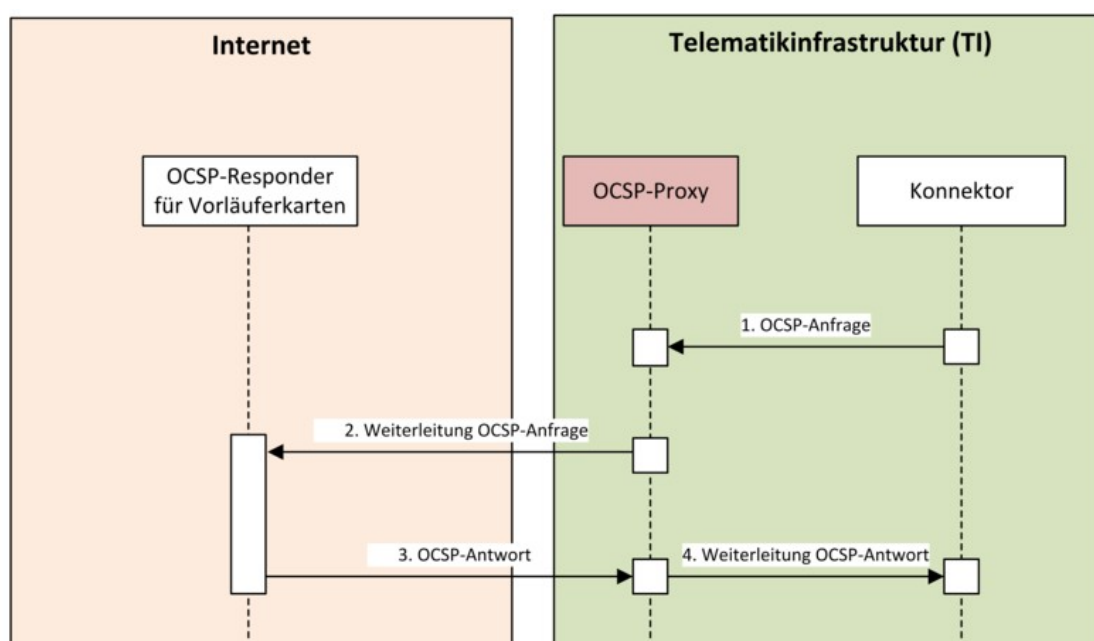




**Abbildung 1: Abb\_OCSP-Proxy\_001 Nachbarsysteme und Nutzer des OCSP-Proxys.**

### 3.3 Anfrageablauf

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 2: Abb\_OCSP-Proxy\_003 Überblick OCSP-Anfrage aus TI an OCSP-Proxy**

Nachfolgende Erläuterung dient dem Verständnis der Abb\_OCSP-Proxy\_003.

Prozessabläufe von OCSP-Anfragen aus der TI:

1. OCSP-Anfrage aus der TI
2. Weiterleitung der OCSP-Anfrage an OCSP-Responder der Vorläuferkarte im Internet
3. Empfang der OCSP-Antwort des OCSP-Responders der Vorläuferkarte
4. Weiterleitung der OCSP-Antwort an anfragende Komponente (Konnektor) in der TI

---

## 4 Übergreifende Festlegungen

---

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

### 4.1 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.

[<=]

### 4.2 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 personenbezogene 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.

[<=]

### 4.3 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.

**[<=]**

---

## 5 Funktionsmerkmale

---

### 5.1 Funktionsmerkmal OCSP-Proxy-Responder

#### 5.1.1 Schnittstelle I\_OCSP\_Status\_Information

##### 5.1.1.1 Schnittstellendefinition

Der OCSP-Proxy muss die technische Schnittstelle I\_OCSP\_Status\_Information gemäß [gemSpec\_PKI#9] implementieren und in der Telematikinfrastruktur anbieten.

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

##### 5.1.1.2 Umsetzung

###### **TIP1-A\_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\_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 zertifikatsvalidierende 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\_5855 - Speicherung von OCSP-Anfragen**

Der OCSP-Proxy DARF OCSP-Anfragen der zertifikatsvalidierenden Komponenten der TI NICHT speichern.

[<=]

###### **TIP1-A\_5856 - Speicherung von OCSP-Antworten**

Der OCSP-Proxy DARF OCSP-Antworten für die zertifikatsvalidierenden Komponenten der TI NICHT speichern.

[<=]

###### **TIP1-A\_5857 - Protokollierung von OCSP-Anfragen und OCSP-Antworten**

Der OCSP-Proxy DARF OCSP-Anfragen und OCSP-Antworten NICHT protokollieren.  
[<=]

**Tabelle 1: Tab\_OCSP-Proxy\_002 TUC\_OCSP-Proxy\_002 OCSP-Anfragen aus der TI beantworten**

| Element                        | Beschreibung  |
|--------------------------------|---|
| Name                           | TUC_OCSP-Proxy_002 "OCSP-Anfragen aus der TI beantworten"   |
| Beschreibung                   | Dieser Use Case beschreibt den Prozess der Zertifikatsstatusauskunft des OCSP-Proxys bei OCSP-Anfragen für nonQES-EE- und QES-EE-Zertifikate der HBA-Vorläuferkarten und anderer QES-Verfahren.   |
| Auslöser                       | OCSP-Anfrage einer zertifikatsvalidierenden Komponente aus der TI   |
| Vorbedingungen                 |   |
| Eingangsdaten                  | OCSP-Anfrage  |
| Komponenten                    | Zertifikatsvalidierende Komponenten der TI (z. B. Konnektor), OCSP-Proxy, OCSP-Responder (der HBA-Vorläuferkarten, u.a.)  |
| Ausgangsdaten                  | OCSP-Antwort eines OCSP-Responders  |
| Nachbedingungen                |   |
| Standardablauf                 | <ol style="list-style-type: none"> <li>1. [OCSP-Proxy]: OCSP-Anfrage der zertifikatsvalidierenden Komponente empfangen.</li> <li>2. [OCSP-Proxy]: OCSP-Anfrage an den entsprechenden OCSP-Responder im Internet weiterleiten unter Verwendung der Ziel-URL im Internet aus der empfangenen OCSP-Anfrage.</li> <li>3. [OCSP-Proxy]: OCSP-Antwort des OCSP-Responders im Internet empfangen.</li> <li>4. [OCSP-Proxy]: OCSP-Antwort des OCSP-Responders im Internet an zertifikatsvalidierende Komponente zurückgeben.</li> </ol> |
| Varianten/Alternativen         |   |
| Fehlerfälle                    | <ol style="list-style-type: none"> <li>2a [OCSP-Proxy]: Der OCSP-Responder im Internet ist nicht erreichbar: OCSP-Response mit einer unsignierten ErrorResponse des Typs "internalError" (siehe [RFC2560#2.3]) zurückgeben.</li> </ol>  |
| Nichtfunktionale Anforderungen |   |
| Anmerkungen                    | Die URL, mit der der OCSP-Proxy-Responder angesprochen wird, enthält auch die Ziel-URL des OCSP-Responders im   |

|                      |   |
|----------------------|---|
|                      | Internet (s. [gemSpec_VPN_ZugD#TIP1-A_4322]). |
| Zugehörige Diagramme |   |

## 5.2 Testunterstützung

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

---

## 6 Anhang A - Verzeichnisse

---

### 6.1 Abkürzungen

| Kürzel | Erläuterung                             |
|--------|---|
| AIA    | Authority Information Access            |
| 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 Certificate Status Protocol      |
| ORS 1  | Online-Rollout (Stufe 1)                |
| OWASP  | Open Web Application Security Project   |
| QES    | Qualifizierte elektronische Signatur    |
| TI     | Telematikinfrastruktur                  |
| VDA    | Vertrauensdiensteanbieter               |
| URI    | Uniform Resource Identifier             |

### 6.2 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.

### 6.3 Abbildungsverzeichnis

Abbildung 1: Abb\_OCSP-Proxy\_001 Nachbarsysteme und Nutzer des OCSP-Proxys.....10

Abbildung 2: Abb\_OCSP-Proxy\_003 Überblick OCSP-Anfrage aus TI an OCSP-Proxy.....10



## 6.4 Tabellenverzeichnis

|   |    |
|---|----|
| Tabelle 1: Tab_OCSP-Proxy_002 TUC_OCSP-Proxy_002 OCSP-Anfragen aus der TI<br>beantworten..... | 14 |
|---|----|

## 6.5 Referenzierte Dokumente

### 6.5.1 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    |
| [gemSpec_VPN_Zug<br>D] | gematik: Spezifikation VPN-Zugangsdienst    |

### 6.5.2 Weitere Dokumente

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

|  |  |
|--|--|
|  | Syntax <a href="http://tools.ietf.org/html/rfc3986">http://tools.ietf.org/html/rfc3986</a> |
|--|--|