

---

## **C\_11973\_Anlage**

---

---

## Inhaltsverzeichnis

---

<b>1 Änderung in gemSpec_NCPeH_FD.....</b>	<b>3</b>
1.1 Änderung an Kapitel "4.1.1 Konfigurationsparameter" .....	3
1.2 Änderung an Kapitel "4.2.1 Schnittstellen zu Diensten der zentralen TI" ..	3
1.3 Änderung an Kapitel "4.2.2.1 TLS-Verbindungsaufbau zu Diensten der TI über das zentrale Netz der TI" .....	4
1.4 Änderung an Kapitel "4.2.3 Prüfung von nonQES-Zertifikaten" .....	4
1.4.1.1 Änderung an Kapitel "4.2.3.1 Prüfung von X.509 nonQES Zertifikaten der TI" .....	5
<b>2 Änderungen in Steckbriefen.....</b>	<b>7</b>
2.1 Änderungen in gemProdT_NCPeH_FD_PTV_2.0.0-0.....	7

---

## 1 Änderung in gemSpec\_NCPeH\_FD

---

### 1.1 Änderung an Kapitel "4.1.1 Konfigurationsparameter"

[...]

**Tabelle 1: TAB\_NCPeH\_Konfigurationsparameter**

Konfigurationsparameter	Wert
[...]	
OCSP_CACHE_REFRESH_PERIOD	<del>60 Minuten</del> 12 Stunden  Der Wert des Parameters bestimmt den Aktualisierungszeitraum für den lokalen Cache der OCSP-Antwort eines Zertifikats (bezogen auf die eindeutige Zertifikatsseriennummer) und stellt die Gültigkeitsdauer der darin zwischengespeicherten OCSP-Antwort dar.
[...]	

[...]

### 1.2 Änderung an Kapitel "4.2.1 Schnittstellen zu Diensten der zentralen TI"

[...]

**Tabelle 2: TAB\_NCPeH\_Schnittstellen\_TI-Dienste**

Schnittstellen der TI-Plattform	Spezifikation
[...]	
Authorization-Endpunkt des IDP-Dienstes	Der IDP-Dienst führt über den Authorization-Endpunkt die Authentisierung des Nutzers durch. Die Beschreibung und Vorgaben zur Nutzung der Schnittstelle sind in [gemSpec_IDP_Dienst#Authorization-Endpunkt] enthalten.
Token-Endpunkt des IDP-Dienstes	Der IDP-Dienst prüft am Token-Endpunkt die Identität zwischen Aufrufer und Initiator und gibt bei Erfolg neben dem ID_TOKEN den ACCESS_TOKEN zur Nutzung am E-Rezept-

	Fachdienst aus [gemSpec_IDP_Dienst#Token-Endpunkt].
--	---

[...]

### 1.3 Änderung an Kapitel "4.2.2.1 TLS-Verbindungsaufbau zu Diensten der TI über das zentrale Netz der TI"

Wenn der NCPeH-FD TLS-gesicherte Verbindungen zu Diensten der TI über das zentrale Netz der TI aufbaut, dann MUSS er folgende Vorgaben zur sicheren Nutzung von TLS beachten:

Beim Aufbau von TLS-gesicherten Verbindungen zu Diensten der TI über das zentrale Netz der TI MUSS der NCPeH-FD die Vorgaben zur sicheren Nutzung von TLS aus:

- [gemSpec\_Krypt] in Kapitel 3.3.2 "TLS-Verbindungen" allgemein,
- beim Verbindungsaufbau zu ePA-Aktensystemen zusätzlich [gemSpec\_Krypt#Kapitel 3.15.3 ePA-spezifische TLS-Vorgaben], ergänzend für den Zugriff auf Dienste der ePA-Aktensysteme und
- beim Verbindungsaufbau zum E-Rezept-Fachdienst zusätzlich [gemSpec\_Krypt#A\_21332\*] (unter Beachtung des Verbots von RSA-basierten Ciphersuiten für den NCPeH-FD nach A\_25639),
- [gemSpec\_PKI#Kapitel 8.4.1 TLS-Verbindungsaufbau].

umsetzen.

Hinweis: Umzusetzende Anforderungen aus diesen Dokumenten werden zusätzlich im Produkttypsteckbrief [gemProdT\_NCPeH\_FD] aufgeführt.

[...]

### 1.4 Änderung an Kapitel "4.2.3 Prüfung von nonQES-Zertifikaten"

[...]

Tabelle 3: TAB\_NCPeH\_nonQES\_Zertifikatsübersicht

Auslöser der Zertifikatsprüfung	Zertifikat der TI	Zertifikatsprofil	Rollen-OID	Nutzung
TLS-Verbindungsaufbau zum TSL-Dienst	ja	C.ZD.TLS-S	oid_tsl_ti	aktiv
TSL-Signaturzertifikat	ja	C.TSL.SIG	n/a	aktiv
TLS-Verbindungsaufbau zur Betriebsdatenerfassung	ja	C.ZD.TLS-S	(keine Vorgabe)	aktiv
TLS-Verbindungsaufbau zum zentralen IDP-Dienst	nein	TLS Internet-Zertifikat	n/a	aktiv

Signaturprüfung des Discovery Document vom IDP-Dienst Signatur-Prüfung des ACCESS_TOKEN vom IDP-Dienst für den E-Rezept-Fachdienst	ja	C.FD.SIG	oid_idpd	aktiv
TLS-Verbindungsaufbau zum ePA-Aktensystem	ja	C.FD.TLS-S	oid_epa_dvw	aktiv
TLS-Verbindungsaufbau zum E-Rezept-Fachdienst	nein	TLS Internet Zertifikat	n/a	aktiv
Aufbau sicherer Kanal zur VAU des E-Rezept-Fachdienstes	ja	C.FD.ENC	oid_erp-vau	aktiv

[...]

Hinweis: Hier nicht aufgeführte Zertifikatsprofile (z. B. VAU-Zertifikat des ePA Aktensystems im "signierten öffentlichen VAU-Schlüssel") durchlaufen einen separat beschriebenen Prüfvorgang.

[...]

#### 1.4.1.1 Änderung an Kapitel "4.2.3.1 Prüfung von X.509 nonQES Zertifikaten der TI"

[...]

**Tabelle 4: TAB\_NCPeH\_Prüfparameter\_nonQES\_Zertifikate\_TI**

Parameter	Wert
[...]	
intendedKeyUsage	Zertifikatsprofile C.ZD.TLS-S, C.FD.TLS-S oder C.FD.SIG: digitalSignature Zertifikatsprofil C.FD.ENC: keyAgreement
intendedExtendedKeyUsage	Zertifikatsprofil C.ZD.TLS-S oder C.FD.TLS-S: id-kp-serverAuth Zertifikatsprofil C.FD.SIG oder C.FD.ENC: leer oder nicht vorhanden
[...]	

Der NCPeH-FD MUSS die Vorgaben zur Prüfung der Sperrinformation von Zertifikaten nach [gemSpec\_PKI#A\_23225\*] umsetzen. Der NCPeH-FD KANN auf eine Zwischenspeicherung der Sperrinformation von Zertifikaten verzichten, wenn das definierte Prüfintervall eines Zertifikats gleich oder größer als OCSP\_CACHE\_REFRESH\_PERIOD ist. Der Konfigurationswert OCSP\_CACHE\_REFRESH\_PERIOD entspricht dem in A\_23225\*, Punkt 2 definierten Wert "D".

Hinweis: Siehe dort auch die Erläuterungen zur Umsetzung der Anforderung in [gemSpec\_Krypt], z. B. auch im Falle der Bereitstellung von Sperrinformationen mittels OCSP-Stapling oder im VAU-Verbindungsaufbau (Nachricht 2, siehe [gemSpec\_Krypt] A\_24608\* und A\_24425\*).

Da die Quellen für Sperrinformationen von Zertifikaten teilweise unterschiedlich vorgegeben sind und der Sinn des Caching sich aus Quelle und Prüfintervall ergibt, folgt hier eine informative Übersicht:

**Tabelle 5: TAB\_NCPeH\_OCSP\_Übersicht\_für\_Zertifikate\_TI**

Auslöser der Zertifikatsprüfung	Quelle der Sperrinformation	Caching ist sinnvoll?
TLS-Verbindungsaufbau zum TSL-Dienst	OCSP-Responder zur CA	nein (Prüfintervall 24h)
TSL-Signaturzertifikat	OCSP-Responder zur CA	nein (Prüfintervall 24h)
TLS-Verbindungsaufbau zur Betriebsdatenerfassung	OCSP-Responder zur CA	ja
Signaturprüfung des Discovery Document vom IDP-Dienst	OCSP-Responder zur CA	ja, falls es das gleiche Zertifikat ist, dass zur Signatur des ACCESS_TOKEN genutzt wird
Signatur-Prüfung des ACCESS_TOKEN vom IDP für den E-Rezept-Fachdienst	OCSP-Responder zur CA	ja
TLS-Verbindungsaufbau zum ePA-Aktensystem	Primär: OCSP-Stapling im TLS-Handshake Backup: OCSP-Responder zur CA	Primär: nein Backup: ja (siehe A_24913*)
Aufbau sicherer Kanal zur VAU des ePA-Aktensystems	ePA VAU-Protokoll (siehe [gemSpec_Krypt#A_24624*])	nein
Aufbau sicherer Kanal zur VAU des E-Rezept-Fachdienstes	E-Rezept-Fachdienst (siehe [gemSpec_Krypt#A_21216*])	ja

Hinweis: Im Rahmen einer Zertifikatsprüfung nach TUC\_PKI\_018 beschreibt der untergeordnete TUC\_PKI\_005 die Ermittlung der Adresse des OCSP-Responders der Zertifikats-herausgebenden CA aus der TSL (siehe [gemSpec\_PKI#Statusprüfung]).

---

## 2 Änderungen in Steckbriefen

---

### 2.1 Änderungen in gemProdT\_NCPeH\_FD\_PTV\_2.0.0-0

<<Hinweis:

Neue Anforderungen mit Zuordnung zu Prüfverfahren für den NCPeH-FD aus gemILF\_PS\_eRp und gemSpec\_Krypt sind im Rahmen der Kommentierung in gemF\_eRp\_EU, Kapitel "Anforderungen an den NCPeH-FD" beschrieben

>>