
gemSpec_Perf - Anpassungen

Vorabinformation zum Änderungseintrag:

Folgende Änderungen sind Bestandteil des Änderungseintrages:

- Zuweisen der Anforderungen zum Senden und Erkennen eines TI-User-Agents zu den Produkttypen "TSL-Dienst", "gematik Root-CA" und "TSP X.509 Komp"
- TSP Komp - Erweitern der Message-Block Anforderung, zur Berücksichtigung des TI-User-Agents in den Betriebsdaten
- TSL-Dienst - Erweitern der Message-Block Anforderung, zur Berücksichtigung des TI-User-Agents in den Betriebsdaten
- Root-CA - Erweitern der Message-Block Anforderungen, zur Berücksichtigung des TI-User-Agents in den Betriebsdaten

Die Nummerierung der Kapitel entspricht nicht der Nummerierung aus den referenzierenden Dokumenten, da diese durch die Formatierung automatisch erzeugt wird. Dies wird bei der Einarbeitung der Änderungen entsprechend beachtet.

Hinweise zur Lesart:

Text, der zur Erklärung der Änderung dient - wird nicht mit eingearbeitet/übernommen.

Text, der neu ist oder aktualisiert wurde.

Text, der entfernt wird.

1 Leistungsanforderungen an die Produkttypen der TI

1.1 User-Agent

Die Produkttypen "TSL-Dienst", "gematik Root-CA" und "TSP X.509 Komp" werden den Anforderungen zum Senden und Erkennen eines TI-User-Agent zugewiesen.

A_27783 -User-Agent - Senden eines User-Agents (Zentrale Dienste der TI)

Der Produkttyp MUSS in allen HTTP-Requests an die in "Tab_gemSpec_Perf_UserAgent_Dienste" aufgeführten Schnittstellen der Produkttypen ein zusätzliches Header-Feld namens "TI-User-Agent" im Format <Client-ID>/<Version> erstellen und wie folgt befüllen:

- <Client-ID>: Alphanumerische Zeichen a-z,A-Z,0-9, sowie dem Trennzeichen "-" mit Länge von 3 bis 20 Zeichen → vergeben durch die gematik
- <Version>: Numerische Zeichen 0-9, sowie dem Trennzeichen "." und "-" mit Länge von 5 bis 15 Zeichen → Produktversion gem. gemSpec_OM::Tab_ProdIdentZ

Beispiel: "CLIENTID1234567890AB/2.1.12-45"

Tabelle 1: Tab_gemSpec_Perf_UserAgent_Dienste

PDT-ID	Produkttyp	Schnittstellen
PDT02	TSP X.509 QES	I_OCSP_Status_Information
PDT03	TSP X.509 nonQES - eGK	I_OCSP_Status_Information
PDT04	TSL-Dienst	I_OCSP_Status_Information I_BNetzA_VL_Download I_TSL_Download
PDT22	gematik-Root-CA	I_OCSP_Status_Information
PDT36	TSP X.509 nonQES - HBA	I_OCSP_Status_Information
PDT37	TSP X.509 nonQES - Komponenten	I_OCSP_Status_Information I_CRL_Download
PDT38	TSP X.509 nonQES - SMC-B	I_OCSP_Status_Information

【<=, Aktensystem_ePA, SigD, NCPeH_FD, funkt. Eignung: Test Produkt/FA】

[Zuweisen zu Prüfverfahren "funkt. Eignung: Test Produkt/FA" - TSL-Dienst, gematik Root-CA, TSP X.509 Komp](#)

A_26182-01 -User-Agent - Erkennung des eingesetzten Clientsystems

Der Produkttyp MUSS das vom aufrufenden Nutzer verwendete Clientsystem anhand des im HTTP-Request enthaltenen Header-Feld "TI-User-Agent" erkennen und in den Einträgen zur Betriebsdatenerfassung gemäß [gemSpec_Perf] erfassen. Findet eine VAU-Kommunikation statt, so ist vorrangig der User-Agent des inneren HTTP-Requests zu erfassen. [<=, ,]

Zuweisen zu Prüfverfahren "funkt. Eignung: Test Produkt/FA" - TSL-Dienst, gematik Root-CA, TSP X.509 Komp

A_26183-01 -User-Agent - Format

Der Produkttyp, welcher gem. [A_26182-*] das HTTP Header-Feld "TI-User-Agent" erkennt, MUSS dieses ausschließlich in folgendem Format akzeptieren:

<Client-ID>/<Version>

- <Client-ID>: Alphanumerische Zeichen a-z,A-Z,0-9, sowie dem Trennzeichen "-" mit Länge von 3 bis 20 Zeichen
- <Version>: Alphanumerische Zeichen a-z,A-Z,0-9, sowie dem Trennzeichen "." und "-" mit Länge von 3 bis 20 Zeichen

[<=, ,]

Zuweisen zu Prüfverfahren "funkt. Eignung: Test Produkt/FA" - TSL-Dienst, gematik Root-CA, TSP X.509 Komp

Von der Anforderung A_26184-01 wird eine neue Version erstellt und die Formulierung so angepasst, dass die Anfrage bei Verstößen des TI-User-Agents gegen die Regular Expression nicht abgelehnt wird. Die Anfrage soll weiterhin bearbeitet werden und lediglich der TI-User-Agent soll in den Betriebsdaten nicht sondern anstelle dessen der Wert "invalid" protokolliert werden:

A_26184-02 -User-Agent - Reporting im Fehlerfall

Der Produkttyp MUSS das HTTP Header-Feld "TI-User-Agent" auf die folgenden gültigen Zeichen überprüfen und bei Verstößen die Anfrage mit einem Error Code gem. [A_26185-*] ablehnen anstelle des HTTP Header-Feldes "TI-User-Agent" den Wert "invalid" protokollieren. Das HTTP Header-Feld "TI-User-Agent" MUSS dem folgenden regulären Ausdruck entsprechen, damit eine entsprechende Code-Injection ausgeschlossen werden kann:

[\\w-]{3,20}V[\\w.-]{3,20}

~~Wird das bemängelte HTTP Header-Feld "TI-User-Agent" aufgrund mangelnder Konformität mit den benannten regulären Ausdruck nicht protokolliert, so ist entsprechend der Regelungen zur Betriebsdatenerfassung der Wert "invalid" zu protokollieren und zu übertragen. [<=, ,]~~

Zuweisen zu Prüfverfahren "funkt. Eignung: Test Produkt/FA" - TSL-Dienst, gematik Root-CA, TSP X.509 Komp

2 Produkttypspezifische Vorgaben

2.1 Trust Service Provider X.509 nonQES - Komponentenzertifikate (PDT37)

Es wird eine neue Version der AFO A_23725-03 erstellt, damit der TI-User-Agent in den Betriebsdaten berücksichtigt wird:

A_23725-04 -Performance - Betriebsdatenlieferung v2 - Spezifika TSP X.509 nonQES - Komp - Message

Der Produkttyp TSP X.509 nonQES - Komp MUSS bei Betriebsdatenlieferungen im "message"-Feld die folgenden Daten im JSON-Format übermitteln:

```
{ "prot": "$protocol", "res": "$result", "zert": "$zertifikatstyp", "cc": $certCount, "ip": "$IP-Adresse", "rs": "$responseStatus", "cid": "$clientID", "ver": "$version" }
```

- \$protocol= "ECC" | "RSA" | "WEB" | "SOAP" | "CMP", Datentyp String
- \$result= "GOOD" | "REVOKED" | "UNKNOWN", Datentyp String
- \$zertifikatstyp = Zertifikatstyp aus Tab_gemSpec_Perf_Berichtsformat_TSP X.509 nonQES - Komp, Datentyp String
- \$certCount = Anzahl der angefragten Zertifikate innerhalb eines Requests, Datentyp Integer
- \$IP-Adresse = IP-Adresse des anfragenden Dienstes, Datentyp String
- \$responseStatus = Response Status der Anfrage gem. GS-A_4686, Datentyp String
- \$clientID = <Client-ID> aus dem HTTP-Header-Feld "TI-User-Agent" gemäß [A_26183-01], Datentyp String
- \$version = <Version> aus dem HTTP-Header-Feld "TI-User-Agent" gemäß [A_26183-01], Datentyp String

Für die jeweilige Operation sind dabei nur die in der Spalte "Message" aus Tabelle Tab_gemSpec_Perf_Berichtsformat_TSP_X.509_nonQES_Komp angegebenen Daten zu übermitteln.

Gemäß der Anforderung [A_22513-02] MUSS in dem speziellen Fall, wenn für den Key "res" der Wert "UNKNOWN" geliefert wird, der Key "zert" entfernt werden.

Der Key "rs" MUSS weggelassen werden, wenn der Response Status "successful" ist.

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. [≤, TSP X.509 nonQES - gSMC, funkt. Eignung: Test Produkt/FA]

Die Tabelle "Tab_gemSpec_Perf_Berichtsformat_TSP_X.509_nonQES_Komp" wird entsprechend den Änderungen aus A_24171-04 aktualisiert:

Tabelle 2: Tab_gemSpec_Perf_Berichtsformat_TSP_X.509_nonQES_Komp

Operation /	Aufgerufene Schnittstelle::Operation	Message
-------------	--------------------------------------	---------

Usecase		
TSPK_1	I_OCSP_Status_Information::check_Revocation_Status (TI)	<pre>{ "prot": "\$protocol", "res": "\$result", "zert": "\$zertifikatstyp", "ip": "\$IP-Adresse", "rs": "\$responseStatus", "cid": "\$clientID", "ver": "\$version" }</pre> <ul style="list-style-type: none"> • \$protocol = "ECC" "RSA" • \$result = "GOOD" "REVOKED" "UNKNOWN" • \$zertifikatstyp = Liste Zertifikatstyp gemäß Mapping OID => Zerttyp (gemSpecOID) • \$IP-Adresse = IP-Adresse des anfragenden Dienstes • \$responseStatus = Response Status der Anfrage gem. [GS-A_4686] • \$clientID = <Client-ID> gem. [A_26183-*)] • \$version = <Version> gem. [A_26183-*)]
TSPK_2	I_OCSP_Status_Information::check_Revocation_Status (Internet)	<pre>{ "prot": "\$protocol", "res": "\$result", "zert": "\$zertifikatstyp", "rs": "\$responseStatus", "cid": "\$clientID", "ver": "\$version" }</pre> <ul style="list-style-type: none"> • \$protocol = "ECC" "RSA" • \$result = "GOOD" "REVOKED" "UNKNOWN" • \$zertifikatstyp = Liste Zertifikatstyp gemäß Mapping OID

		<p>=> Zerttyp (gemSpecOID)</p> <ul style="list-style-type: none"> • \$responseStatus = Response Status der Anfrage gem. [GS-A_4686] • \$clientID = <Client-ID> gem. [A_26183-*)] • \$version = <Version> gem. [A_26183-*)]
TSPK_3	I_CRL_Download::download_CRL	<p>{ "prot": "\$protocol", "cid": "\$clientID", "ver": "\$version" }</p> <ul style="list-style-type: none"> • \$protocol = "ECC" "RSA" • \$clientID = <Client-ID> gem. [A_26183-*)] • \$version = <Version> gem. [A_26183-*)]
TSPK_4	I_Cert_Provisioning::provide_Certificate (SOAP / CMP)	<p>{ "prot": "\$protocol", "cc": \$certCount }</p> <ul style="list-style-type: none"> • \$protocol = "SOAP" "CMP" • \$certCount = Anzahl der angefragten Zertifikate innerhalb eines Requests als Integer
TSPK_5	I_Cert_Provisioning::provide_Certificate (WEB Benutzerschnittstelle)	<p>{ "prot": "\$protocol", "cc": \$certCount }</p> <ul style="list-style-type: none"> • \$protocol = "WEB" • \$certCount = Anzahl der angefragten Zertifikate innerhalb eines Requests als Integer
TSPK_6	I_Cert_Revocation::revoke_Certificate (SOAP / CMP)	<p>{ "prot": "\$protocol", "cc": \$certCount }</p> <ul style="list-style-type: none"> • \$protocol = "SOAP" "CMP"

		<ul style="list-style-type: none"> • \$certCount = Gesamtzahl aller mit diesem Sperr-Request im Zusammenhang stehenden Zertifikate als Integer
TSPK_7	I_Cert_Revocation::revoke_Certificate (WEB Benutzerschnittstelle)	<pre>{ "prot": "\$protocol", "cc": \$certCount }</pre> <ul style="list-style-type: none"> • \$protocol = "WEB" • \$certCount = Gesamtzahl aller mit diesem Sperr-Request im Zusammenhang stehenden Zertifikate als Integer

2.2 TSL-Dienst (PDT04)

Es wird eine neue Version der AFO A_24171-03 erstellt, damit der TI-User-Agent in den Betriebsdaten berücksichtigt wird:

A_24171-04 -Performance - Betriebsdatenlieferung v2 - Spezifika TSL-Dienst - Message

Der Produkttyp TSL-Dienst MUSS bei Betriebsdatenlieferungen im "message"-Feld die folgenden Daten im JSON-Format übermitteln:

```
{ "prot": "$protocol", "res": "$result", "url": "$usedURL", "ip": "$IP-Adresse", "rs":  
"$responseStatus", "cid": "$clientID", "ver": "$version" }
```

- \$protocol= Genutzter Schlüsselalgorithmus des angefragten Zertifikates, Datentyp String
- \$result= Sperrstatus des angefragten Zertifikates gemäß GS-A_4690, Datentyp String
- \$usedURL = "Returned Value" aus der Tabelle Tab_gemSpec_Perf_TSL-Dienst_URLs basierend darauf, welche URL der Konnektor oder Dienst zum Download der jeweiligen Datei genutzt hat, Datentyp String
- \$IP-Adresse = IP-Adresse des anfragenden Dienstes, Datentyp String
- \$responseStatus = Response Status der Anfrage gem. GS-A_4686, Datentyp String
- \$clientID = <Client-ID> aus dem HTTP-Header-Feld "TI-User-Agent" gemäß [A_26183-01], Datentyp String
- \$version = <Version> aus dem HTTP-Header-Feld "TI-User-Agent" gemäß [A_26183-01], Datentyp String

Für die jeweilige Operation sind dabei nur die in der Spalte "Message" aus Tabelle Tab_gemSpec_Perf_Berichtsformat_TSL-Dienst angegebenen Daten zu übermitteln. Der Key "rs" MUSS weggelassen werden, wenn der Response Status "successful" ist. 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.【<=, TSL-Dienst, funkt. Eignung: Test Produkt/FA】

Die Tabelle "Tab_gemSpec_Perf_Berichtsformat_TSL-Dienst" wird entsprechend den Änderungen aus A_24171-04 aktualisiert:

Tabelle 3: Tab_gemSpec_Perf_Berichtsformat_TSL-Dienst

Operation / Usecase	Aufgerufene Schnittstelle::Operation	Duration	Message
TSL_1	I_OCSP_Status_Information::check_Revocation_Status (TI)	Die Messung der Bearbeitungszeit beginnt mit der Annahme der Nachricht durch den OCSP Responder des TSL-Dienstes und endet mit dem Versand der Antwort an den Client.	<pre>{ "prot": "\$protocol", "res": "\$result", "ip": "\$IP-Adresse", "rs": "\$responseStatus", "cid": "\$clientId", "ver": "\$version" }</pre> <ul style="list-style-type: none"> • \$protocol= "ECC" "RSA" • \$result= "GOOD" "REVOKED" "UNKNOWN" • \$IP-Adresse = IP-Adresse des anfragenden Dienstes • \$responseStatus = Response Status der Anfrage gem. [GS-A_4686] • \$clientId = <Client-ID> gem. [A_26183-*] • \$version = <Version> gem. [A_26183-*]
TSL_2	I_OCSP_Status_Information::check_Revocation_Status (Internet)		<pre>{ "prot": "\$protocol", "res": "\$result", "rs": "\$responseStatus", "cid": "\$clientId", "ver": "\$version" }</pre> <ul style="list-style-type: none"> • \$protocol=

			"ECC" "RSA" <ul style="list-style-type: none"> • \$result= "GOOD" "REVOKED" "UNKNOWN" • \$responseStatus = Response Status der Anfrage gem. [GS-A_4686] • \$clientID = <Client-ID> gem. [A_26183-*] • \$version = <Version> gem. [A_26183-*]
TSL_3	I_TSL_Download::get_Hash (TI)	Die Messung der Bearbeitungszeit beginnt mit der Annahme der Nachricht durch den TSL-Dienst und endet mit dem Versand des letzten Bytes der Antwortnachricht.	{ "url": "\$usedURL", "ip": "\$IP-Adresse", "cid": "\$clientID", "ver": "\$version" } } <ul style="list-style-type: none"> • \$usedURL = "Returned Value" aus der Tabelle Tab_gemSpec_Perf_TSL-Dienst_URLs • \$IP-Adresse = IP-Adresse des anfragenden Dienstes • \$clientID = <Client-ID> gem. [A_26183-*] • \$version = <Version> gem. [A_26183-*]
TSL_4	I_TSL_Download::download_TSL (TI)		
TSL_5	I_BNetzA_VL_Download::get_Hash		{ "url": "\$usedURL", "cid": "\$clientID", "ver": "\$version" } } <ul style="list-style-type: none"> • \$usedURL = "Returned Value" aus der Tabelle Tab_gemSpec_Perf_TSL-Dienst_URLs
TSL_6	I_BNetzA_VL_Download::download_VL		
TSL_7	I_TSL_Download::get_Hash (Internet)		
TSL_8	I_TSL_Download::download_TSL (Internet)		
TSL_9	I_TSL_Download::download_TSL (Notfall)		

			rf_TSL- Dienst_URLs <ul style="list-style-type: none"> • \$clientID = <Client-ID> gem. [A_26183- *] • \$version = <Version> gem. [A_26183-*]
--	--	--	---

2.3 gematik Root-CA (PDT22)

Es wird eine neue Version der AFO A_24167-02 erstellt, damit der TI-User-Agent in den Betriebsdaten berücksichtigt wird:

A_24167-03 -Performance - Betriebsdatenlieferung v2 - Spezifika gematik Root-CA - Message

Der Produkttyp gematik Root-CA MUSS bei Betriebsdatenlieferungen im "message"-Feld die folgenden Daten im JSON-Format übermitteln:

```
{ "prot": "$protocol", "res": "$result", "cn": "$commonName", "rs":  
"$responseStatus", "cid": "$clientID", "ver": "$version" } }
```

- \$protocol= Genutzter Schlüsselalgorithmus des angefragten Zertifikates: "ECC" | "RSA", Datentyp String
- \$result= Sperrstatus des angefragten Zertifikates gemäß GS-A_4690: "GOOD" | "REVOKED" | "UNKNOWN", Datentyp String
- \$commonName = commonName des Zertifikats gem. GS-A_4737, Datentyp String
- \$responseStatus = Response Status der Anfrage gem. GS-A_4686. Datentyp String
- \$clientID = <Client-ID> aus dem HTTP-Header-Feld "TI-User-Agent" gemäß [A_26183-01], Datentyp String
- \$version = <Version> aus dem HTTP-Header-Feld "TI-User-Agent" gemäß [A_26183-01], Datentyp String

Gemäß der Anforderung [A_22513-02] MUSS in dem speziellen Fall, wenn für den Key "res" der Wert "UNKNOWN" geliefert wird, der Key "cn" entfernt werden.

Der Key "rs" MUSS weggelassen werden, wenn der Response Status "successful" ist. 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. [≤, gematik Root-CA, funkt. Eignung: Test Produkt/FA]