
C_12694_Anlage

Inhaltsverzeichnis

1	Änderungsbeschreibung.....	2
2	Änderung in gemSpec_TSL.....	3
2.1	in Kapitel 6.3.1.2 Umsetzung.....	3
3	Änderung in gemSpec_Perf.....	6
3.1	in Kapitel 3.16.2 Betriebsdatenerfassung v2 Spezifika TSL-Dienst.....	6
4	Änderungen in Steckbriefen.....	11
4.1	Änderungen in gemProdT_TSL.....	11
4.2	Redaktionelle Anpassung in gemSpec_TSL.....	11

1 Änderungsbeschreibung

In verschiedenen Spezifikationen (gemSpec_TSL und gemSpec_Perf) sind die URIs der Download-Punkte (DLP) für TSL und Hash-Werte in der TI und im Internet nicht mehr aktuell. Diese werden im Zuge der RSA-ECC-Migration aktualisiert.

2 Änderung in gemSpec_TSL

2.1 in Kapitel 6.3.1.2 Umsetzung

(...)

A_17680-02 -I_TSL_Download::download_TSL: GET-Befehl (ECC-Migration)

Der TSL-Dienst MUSS die logische Operation I_TSL_Download::download_TSL so implementieren, dass die folgenden URIs realisiert werden:

Für die Produktivumgebung (PU):

TSL(RSA) und deren SHA256-Hashwert in der TI:

TSL: [http\(s\)://download.tsl.telematik/TSL.xml](http(s)://download.tsl.telematik/TSL.xml)

Hash: <https://download.tsl.telematik/TSL.sha2>

Backup TSL: [http\(s\)://download-bak.tsl.telematik/ECC/TSL.xml](http(s)://download-bak.tsl.telematik/ECC/TSL.xml)

Backup Hash: <https://download-bak.tsl.telematik/ECC/TSL.sha2>

TSL(ECC-RSA) und deren SHA256-Hashwert in der TI:

TSL: [http\(s\)://download.tsl.telematik/ECC/ECC-RSA_TSL.xml](http(s)://download.tsl.telematik/ECC/ECC-RSA_TSL.xml)

Hash: https://download.tsl.telematik/ECC/ECC-RSA_TSL.sha2

Backup TSL: [http\(s\)://download-bak.tsl.telematik/ECC/ECC-RSA_TSL.xml](http(s)://download-bak.tsl.telematik/ECC/ECC-RSA_TSL.xml)

Backup Hash: https://download-bak.tsl.telematik/ECC/ECC-RSA_TSL.sha2

TSL(RSA) ~~(der PU)~~ und deren SHA256-Hashwert im Internet:

TSL: <https://download.tsl.ti-dienste.de/TSL.xml>

Hash: <https://download.tsl.ti-dienste.de/TSL.sha2>

TSL(ECC-RSA) und deren SHA256-Hashwert im Internet:

TSL: https://download.tsl.ti-dienste.de/ECC/ECC-RSA_TSL.xml

Hash: https://download.tsl.ti-dienste.de/ECC/ECC-RSA_TSL.sha2

Für die Referenzumgebung (RU):

~~TSL(RSA) und deren SHA256-Hashwert in der TI:~~

Primär TSL: [http\(s\)://download-ref.tsl.telematik-test/TSL-ref.xml](http(s)://download-ref.tsl.telematik-test/TSL-ref.xml)

Primär Hash: <https://download-ref.tsl.telematik-test/TSL-ref.sha2>

~~Backup TSL: [http\(s\)://download-bak-ref.tsl.telematik-test/TSL-ref.xml](http(s)://download-bak-ref.tsl.telematik-test/TSL-ref.xml)~~

~~Backup Hash: <https://download-bak-ref.tsl.telematik-test/TSL-ref.sha2>~~

TSL(ECC-RSA) und deren SHA256-Hashwert in der TI:

TSL: [http\(s\)://download-ref.tsl.telematik-test/ECC/ECC-RSA_TSL-ref.xml](http(s)://download-ref.tsl.telematik-test/ECC/ECC-RSA_TSL-ref.xml)

Hash: https://download-ref.tsl.telematik-test/ECC/ECC-RSA_TSL-ref.sha2

Backup TSL: [http\(s\)://download-bak-ref.tsl.telematik-test/ECC/ECC-RSA_TSL-ref.xml](http(s)://download-bak-ref.tsl.telematik-test/ECC/ECC-RSA_TSL-ref.xml)

Backup Hash: https://download-bak-ref.tsl.telematik-test/ECC/ECC-RSA_TSL-ref.sha2

~~TSL(RSA) im Internet: <https://download-ref.tsl.ti-dienste.de/TSL-ref.xml>~~

Hash der TSL(RSA) im Internet: <https://download-ref.tsl.ti-dienste.de/TSL-ref.sha2>
TSL(ECC-RSA) und deren SHA256-Hashwert im Internet:

TSL: https://download-ref.tsl.ti-dienste.de/ECC/ECC-RSA_TSL-ref.xml
Hash: https://download-ref.tsl.ti-dienste.de/ECC/ECC-RSA_TSL-ref.sha2

Für die Testumgebung (TU):

TSL(RSA) und deren SHA256-Hashwert in der TI:

Primär TSL: [http\(s\)://download-test.tsl.telematik-test/TSL-test.xml](http(s)://download-test.tsl.telematik-test/TSL-test.xml)
Primär Hash: <https://download-test.tsl.telematik-test/TSL-test.sha2>
Backup TSL: [http\(s\)://download-bak-test.tsl.telematik-test/TSL-test.xml](http(s)://download-bak-test.tsl.telematik-test/TSL-test.xml)
Backup Hash: <https://download-bak-test.tsl.telematik-test/TSL-test.sha2>

TSL(ECC-RSA) und deren SHA256-Hashwert in der TI:

TSL: [http\(s\)://download-test.tsl.telematik-test/ECC/ECC-RSA_TSL-test.xml](http(s)://download-test.tsl.telematik-test/ECC/ECC-RSA_TSL-test.xml)
Hash: https://download-test.tsl.telematik-test/ECC/ECC-RSA_TSL-test.sha2
Backup TSL: [http\(s\)://download-bak-test.tsl.telematik-test/ECC/ECC-RSA_TSL-test.xml](http(s)://download-bak-test.tsl.telematik-test/ECC/ECC-RSA_TSL-test.xml)
Backup Hash: https://download-bak-test.tsl.telematik-test/ECC/ECC-RSA_TSL-test.sha2

TSL(RSA) im Internet: <https://download-test.tsl.ti-dienste.de/TSL-test.xml>
Hash der TSL(RSA) im Internet: <https://download-test.tsl.ti-dienste.de/TSL-test.sha2>
TSL(ECC-RSA) und deren SHA256-Hashwert im Internet:

TSL: https://download-test.tsl.ti-dienste.de/ECC/ECC-RSA_TSL-test.xml
Hash: https://download-test.tsl.ti-dienste.de/ECC/ECC-RSA_TSL-test.sha2

【<=,TSL-Dienst,funkt. Eignung: Test Produkt/FA】

Hinweis:

Folgende DL-Punkte sind in Bezug auf RSA-ECC-Migration aktuell deaktiviert:

Referenzumgebung (RU):

TSL(RSA) und deren SHA256-Hashwert in der TI:

Primär TSL: [http\(s\)://download-ref.tsl.telematik-test/TSL-ref.xml](http(s)://download-ref.tsl.telematik-test/TSL-ref.xml)
Primär Hash: <https://download-ref.tsl.telematik-test/TSL-ref.sha2>

TSL(RSA) und deren SHA256-Hashwert im Internet:

TSL: <https://download-ref.tsl.ti-dienste.de/TSL-ref.xml>
Hash: <https://download-ref.tsl.ti-dienste.de/TSL-ref.sha2>

Testumgebung (TU):

TSL(RSA) und deren SHA256-Hashwert in der TI:

Primär TSL: [http\(s\)://download-test.tsl.telematik-test/TSL-test.xml](http(s)://download-test.tsl.telematik-test/TSL-test.xml)
Primär Hash: <https://download-test.tsl.telematik-test/TSL-test.sha2>

TSL(RSA) und deren SHA256-Hashwert im Internet:

TSL: <https://download-test.tsl.ti-dienste.de/TSL-test.xml>
Hash : <https://download-test.tsl.ti-dienste.de/TSL-test.sha2>

(...)

3 Änderung in gemSpec_Perf

3.1 in Kapitel 3.16.2 Betriebsdatenerfassung v2 Spezifika TSL-Dienst

(...)

A_24171-05 -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]

Tabelle 61: Tab_gemSpec_Perf_TSL-Dienst_URLs

BU	Referenz	URL	Returned Value
PU	-	https://download.bnetzavl.telematik/BNA-TSL.xml	TSL-BNA
		https://download-bak.bnetzavl.telematik/BNA-TSL.xml	TSL-BNA-Bak
	TIP1-A_6755	https://download.bnetzavl.telematik/BNA-TSL.sha2	Hash-BNA

	A_17680-02	http://download.tsl.telematik/TSL.xml	RSA-TSL
		https://download.tsl.telematik/TSL.sha2	RSA-Hash
		http://download-bak.tsl.telematik/TSL.xml	RSA-TSL-Bak
		https://download-bak.tsl.telematik/TSL.sha2	RSA-Hash-Bak
		https://download.tsl.ti-dienste.de/TSL.xml	RSA-TSL-Inet
		https://download.tsl.ti-dienste.de/TSL.sha2	RSA-Hash-Inet
	A_21182	http://download.crl.ti-dienste.de/TSL-RSA/TSL.xml	RSA-TSL-Notfall
	A_17680-02	http://download.tsl.telematik/ECC/ECC-RSA_TSL.xml	ECC-TSL
		https://download.tsl.telematik/ECC/ECC-RSA_TSL.sha2	ECC-Hash
		http://download-bak.tsl.telematik/ECC/ECC-RSA_TSL.xml	ECC-TSL-Bak
		https://download-bak.tsl.telematik/ECC/ECC-RSA_TSL.sha2	ECC-Hash-Bak
		https://download.tsl.ti-dienste.de/ECC/ECC-RSA_TSL.xml	ECC-TSL-Inet
		https://download.tsl.ti-dienste.de/ECC/ECC-RSA_TSL.sha2	ECC-Hash-Inet
	A_21182	http://download.crl.ti-dienste.de/TSL-ECC/ECC-RSA_TSL.xml	ECC-TSL-Notfall
RU	-	https://download-testref.bnetzavl.telematik-test/BNA-TSL.xml	TSL-BNA
		https://download-bak-testref.bnetzavl.telematik/BNA-TSL.xml	TSL-BNA-Bak
		https://download-testref.tsl.ti-dienste.de/P-BNetzA/Pseudo-BNetzA-VL.xml	TSL-BNA-PSE
	TIP1-A_6755	https://download-testref.bnetzavl.telematik-test/BNA-TSL.sha2	Hash-BNA

	A_17680-02	http://download-ref.tsl.telematik-test/TSL-ref.xml	RSA-TSL
		https://download-ref.tsl.telematik-test/TSL-ref.sha2	RSA-Hash
		http://download-bak-ref.tsl.telematik-test/TSL-ref.xml	RSA-TSL-Bak
		https://download-bak-ref.tsl.telematik-test/TSL-ref.sha2	RSA-Hash-Bak
		https://download-ref.tsl.ti-dienste.de/TSL-ref.xml	RSA-TSL-Inet
		https://download-ref.tsl.ti-dienste.de/TSL-ref.sha2	RSA-Hash-Inet
	A_21182	http://download-testref.crl.ti-dienste.de/TSL-RSA-ref/TSL-ref.xml	RSA-TSL-Notfall
	A_17680-02	http://download-ref.tsl.telematik-test/ECC/ECC-RSA_TSL-ref.xml	ECC-TSL
		https://download-ref.tsl.telematik-test/ECC/ECC-RSA_TSL-ref.sha2	ECC-Hash
		http://download-bak-ref.tsl.telematik-test/ECC/ECC-RSA_TSL-ref.xml	ECC-TSL-Bak
		https://download-bak-ref.tsl.telematik-test/ECC/ECC-RSA_TSL-ref.sha2	ECC-Hash-Bak
		https://download-ref.tsl.ti-dienste.de/ECC/ECC-RSA_TSL-ref.xml	ECC-TSL-Inet
		https://download-ref.tsl.ti-dienste.de/ECC/ECC-RSA_TSL-ref.sha2	ECC-Hash-Inet
	A_21182	http://download-testref.crl.ti-dienste.de/TSL-ECC-ref/ECC-RSA_TSL-ref.xml	ECC-TSL-Notfall
TU	-	https://download-testref.bnetzavl.telematik-test/BNA-TSL.xml	TSL-BNA
		https://download-bak-testref.bnetzavl.telematik-test/BNA-TSL.xml	TSL-BNA-Bak

		https://download-testref.tsl.ti-dienste.de/P-BNetzA/Pseudo-BNetzA-VL.xml	TSL-BNA-PSE
	TIP1-A_6755	https://download-testref.bnetzavl.telematik-test/BNA-TSL.sha2	Hash-BNA
	A_17680-02	http://download-test.tsl.telematik-test/TSL-test.xml	RSA-TSL
		https://download-test.tsl.telematik-test/TSL-test.sha2	RSA-Hash
		http://download-bak-test.tsl.telematik-test/TSL-test.xml	RSA-TSL-Bak
		https://download-bak-test.tsl.telematik-test/TSL-test.sha2	RSA-Hash-Bak
		https://download-test.tsl.ti-dienste.de/TSL-test.xml	RSA-TSL-Inet
		https://download-test.tsl.ti-dienste.de/TSL-test.sha2	RSA-Hash-Inet
	A_21182	http://download-testref.crl.ti-dienste.de/TSL-RSA-test/TSL-test.xml	RSA-TSL-Notfall
	A_17680-02	http://download-test.tsl.telematik-test/ECC/ECC-RSA_TSL-test.xml	ECC-TSL
		https://download-test.tsl.telematik-test/ECC/ECC-RSA_TSL-test.sha2	ECC-Hash
		http://download-bak-test.tsl.telematik-test/ECC/ECC-RSA_TSL-test.xml	ECC-TSL-Bak
		https://download-bak-test.tsl.telematik-test/ECC/ECC-RSA_TSL-test.sha2	ECC-Hash-Bak
		https://download-test.tsl.ti-dienste.de/ECC/ECC-RSA_TSL-test.xml	ECC-TSL-Inet
		https://download-test.tsl.ti-dienste.de/ECC/ECC-RSA_TSL-test.sha2	ECC-Hash-Inet
	A_21182	http://download-testref.crl.ti-dienste.de/TSL-ECC-test/ECC-	ECC-TSL-

		RSA_TSL-test.xml	Notfall
--	--	----------------------------------	---------

135

136

137

138

4 Änderungen in Steckbriefen

4.1 Änderungen in gemProdT_TSL

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

Tabelle 1: Anforderungen zur funktionalen Eignung "Produkttest/Produktübergreifender Test"

Afo-ID	Afo-Bezeichnung	Quelle (Referenz)
A_24171-05	Performance - Betriebsdatenlieferung v2 - Spezifika TSL-Dienst - Message	gemSpec_Perf
A_17680-02	I_TSL_Download::download_TSL: GET-Befehl (ECC-Migration)	gemSpec_TSL
A_17931-01 ¹⁾	TSL Unspecified ServiceTypeldentifier	gemSpec_TSL

¹⁾Gemäß dem Änderungseintrag [C_12253](#) handelt es sich zusätzlich um eine redaktionelle Anpassung des Anforderungs-Suffixes A_17931 zu A_17931-01, welcher nicht korrekt in gemSpec_TSL dargestellt wird.

4.2 Redaktionelle Anpassung in gemSpec_TSL

Änderung:

Die beiden weggefallenen Anforderungen A_17931 und A_17931-02 werden aus gemSpec_TSL#7.9 entfernt.