
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 "TSP X.509 QES", "TSP X.509 nonQES - HBA", "TSP X.509 nonQES - SMC-B" und "TSP X.509 nonQES - eGK"
- TSP - Erweitern der Message-Block Anforderung, 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 "TSP X.509 QES", "TSP X.509 nonQES - HBA", "TSP X.509 nonQES - SMC-B" und "TSP X.509 nonQES - eGK" 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" - TSP X.509 QES, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - eGK

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. [\leq ,,]

Zuweisen zu Prüfverfahren "funkt. Eignung: Test Produkt/FA" - TSP X.509 QES, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - eGK

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

[\leq ,,]

Zuweisen zu Prüfverfahren "funkt. Eignung: Test Produkt/FA" - TSP X.509 QES, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - eGK

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:

$[\backslash w\backslash-]\{3,20\}\backslash[\backslash w\backslash.\backslash-]\{3,20\}$

~~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 Betriebsdatenlieferung der Wert "invalid" zu protokollieren und zu übertragen. [\leq ,,]~~

Zuweisen zu Prüfverfahren "funkt. Eignung: Test Produkt/FA" -TSP X.509 QES, TSP X.509 nonQES - HBA, TSP X.509 nonQES - SMC-B, TSP X.509 nonQES - eGK

2 Produkttypspezifische Vorgaben

2.1 Trust Service Provider X.509 - Kartenherausgeber

2.1.1 Betriebsdatenerfassung v2 Spezifika TSP X.509

Es wird eine neue Version der AFO A_22492-01 erstellt, damit der TI-User-Agent in den Betriebsdaten berücksichtigt wird:

A_22492-02 -Performance - Betriebsdatenlieferung v2 - Spezifika TSP X.509 - Message

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

```
{ "prot": "$protocol", "res": "$result", "zert": "$zertifikatstyp", "rs":  
"$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
- \$zertifikatstyp = Name des Zertifikatstyp gemäß [GS-A_4445-*], 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-*] 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 - HBA, TSP X.509 nonQES - eGK, TSP X.509 QES, TSP X.509 nonQES - SMC-B,funkt. Eignung: Test Produkt/FA]