
C_12310_Anlage - TI-User-Agent

Vorabinformation zum Änderungseintrag:

Folgende Änderungen sind Bestandteil des Änderungseintrages:

- Aktualisierung der übergreifenden Anforderungen zum User-Agent
- Hinzufügen neuer Anforderungen zum Senden eines User-Agents

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.

Inhaltsverzeichnis

| | |
|--|----------|
| 1 gemSpec_Perf - Leistungsanforderungen an die Produkttypen der TI..... | 3 |
| 1.1 User-Agent..... | 3 |
| 2 gemILF_PS - Funktionsmerkmale..... | 9 |
| 2.1 Kommunikation mit Diensten der TI..... | 9 |

gemSpec_Perf Änderungen

1 gemSpec_Perf - Leistungsanforderungen an die Produkttypen der TI

1.1 User-Agent

Dieses Kapitel hält die zusammengefassten Vorgaben rund um das http-Header Feld **TI-User-Agent** auf der Seite des eingesetzten, zugelassenen Dienstes der TI. Die Vorgaben sind notwendig, um aufrufende Softwaresysteme eindeutig mit den angegebenen Metainformationen zu klassifizieren. Dadurch wird es explizit zu keiner Zeit möglich, den einzelnen Aufrufer (z.B. Leistungserbringende) zu identifizieren.

Die Vorgaben helfen dabei, dass eine Klassifikation der eingesetzten Clientsysteme hinsichtlich des Verhaltens an den Fachdiensten der TI regelmäßig und fehlerfrei stattfinden kann. Gleichzeitig werden durch den eingeschränkten Lösungsraum weniger Freiräume für Angriffsvektoren geschaffen.

Hinweis: Gemäß RFC9110 ist im http-Header ein User-Agent einzutragen. Dieser RFC-User-Agent enthält z.B. Angaben zum Betriebssystem oder zum Browser und ist nicht zu verwechseln mit dem hier definierten TI-User-Agent. Dieser (TI-User-Agent) MUSS deshalb als zusätzlicher Parameter im http-Header eingetragen werden und NICHT im User-Agent-Parameter gem. RFC9110.

Hinzufügen einer neuen Anforderung für Produkttypen der TI, welche einen User-Agent in einem separaten HTTP-Header-Feld in ihren HTTP-Kommunikationen senden sollen:

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"

Table 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 |

[<=, ,]

Hinzufügen einer neuen Anforderung für weitere Clientsysteme (z.B. FdV, Primärsysteme), welche einen User-Agent in einem separaten HTTP-Header-Feld in ihren HTTP-Kommunikationen senden sollen:

A_27784 -User-Agent - Senden eines User-Agents (Clientsysteme)

Das Clientsystem (z.B. FdV) MUSS in allen HTTP-Requests an Dienste der TI 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>: Alphanumerische Zeichen a-z,A-Z,0-9, sowie dem Trennzeichen "." und "-" mit Länge von 3 bis 20 Zeichen → vergeben durch Clientsystem

Die Versionsnummer MUSS eindeutig sein und geändert werden, wenn es eine Änderung am Clientsystem gibt. Es ist empfohlen, dass das Format der Versionsnummer dabei dem grundlegenden Aufbau der TI-Versionsnummern gemäß [gemSpec_OM#GS-A_3695] entspricht.

Beispiel: "CLIENTID1234567890AB/2.1.12-45"

[<=, ,]

Hinweis zum Erhalt der Client-ID für Clientsysteme: Die Client-ID wird durch die gematik vergeben und übermittelt, sobald sich ein (Client-)Produkthersteller (z.B. FdV oder Primärsystem) unter idp-registrierung@gematik.de registriert hat. Dazu ist im Rahmen dieser Registrierung der Name des Herstellers und der Name des zu registrierenden Produktes zu übermitteln. Sollte im Rahmen einer TI-Anwendung bereits eine Registrierung vorgenommen worden sein, kann die Client-ID auch für andere TI-Anwendungen genutzt werden (sofern es sich um das gleiche Softwareprodukt handelt).

Hinweis für FdV-Hersteller: Bei Entwicklung eines White-Label-Clients ist der TI-User-Agent Teil des kundenspezifischen Customizings, sodass über die Client-ID im TI-User-Agent das spezifische Clientsystem erkennbar sein muss.

Die bisherigen Anforderungen werden aktualisiert, damit diese den neuen TI-User-Agent unterstützen:

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" gemäß [RFC7231] 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. [<=, ,]

A_26183-01 -User-Agent - Format

Der Produkttyp, welcher gem. [A_26182-*)] das HTTP Header-Feld "TI-User-Agent" erkennt, Format des HTTP Header-Feldes "User-Agent" gemäß [RFC7231] MUSS dieses ausschließlich in folgendem Format akzeptieren werden:

<Client-ID>/<Version>

- <Client-ID>: Alphanumerische Zeichen a-z,A-Z,0-9, sowie dem Trennzeichen "-" mit Länge von 18 bis 20 Zeichen → vergeben durch die gematik
- <Version>: Alphanumerische Zeichen a-z,A-Z,0-9, sowie dem Trennzeichen "." und "-" mit Länge von 1 bis 20 Zeichen → vergeben durch das Clientsystem
- <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

[<=, ,]

Die AFO A_26184 wird komplett überarbeitet, damit deutlicher wird, dass ein inkorrekt formatierter User-Agent, welcher nicht dem regulären Ausdruck entspricht, abgelehnt werden muss. Der reguläre Ausdruck wird entsprechend der Vorgaben aus A_26183-01 angepasst.

Alte AFO:

A_26184 -User-Agent - Reporting im Fehlerfall

Der Produkttyp MUSS bei inkorrekt formatiertem "UserAgent" gem. A_26183 den fehlerhaften Wert erfassen, sofern er dem regulären Ausdruck $^[\backslash w \backslash . \backslash s \backslash - \backslash (\backslash) \backslash \& \backslash \% \backslash ; \backslash [\backslash] \backslash + \backslash < \backslash > \backslash \# \backslash ? \backslash @ \backslash : \backslash , \backslash] \backslash + \backslash \$$ entspricht - also eine entsprechende Code-Injection ausgeschlossen werden kann. Der erfasste Wert soll dann entsprechend der Regelungen zum BDEv2-Messageblock als Ersatz für den Wert des eigentlichen UserAgents übertragen, mindestens jedoch protokolliert werden.

Wird der bemängelte UserAgent 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.

[<=, ,]

Neue AFO:

A_26184-01 -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. 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 Betriebsdatenlieferung der Wert "*invalid*" zu protokollieren und zu übertragen. [`<=`, ,]

A_26185-01 -User-Agent - Fehlerbehandlung

Der Produkttyp MUSS bei fehlendem oder inkorrekt formatierten Header-Feld "TI-User-Agent" den Request mit dem HTTP-Status-Code 400 beantworten.

In den Protokolleinträgen zu Betriebsdaten muss als Status der Operation/des Aufrufs jeweils einer der folgend definierten 5-stelligen Statuscodes genutzt werden:

- Statuscode 79200: fehlender User-Agent
- Statuscode 79201: inkorrekt formatierter User-Agent

[`<=`, ,]

gemILF_PS Änderungen

2 gemILF_PS - Funktionsmerkmale

2.1 Kommunikation mit Diensten der TI

Es wird eine neue Version der Anforderungen A_26171 erstellt und analog zur AFO A_27784 angepasst.

Alte AFO:

A_26171 -Clientsystem - User-Agent - Aufbau und Format bei der Kommunikation mit Diensten der TI

Das Clientsystem MUSS in alle HTTP-Requests an Dienste der TI den HTTP-Header User-Agent gemäß [RFC7231] mit <clientid>/<version> befüllen.

- <clientid> gemäß eigener Definition, Länge 18-20 Zeichen, Zeichenvorrat [0-9a-zA-Z_] → vergeben durch die gematik
- <version> gemäß Produktidentifikation, Länge 1-20 Zeichen, Zeichenvorrat [0-9a-zA-Z_\.] → vergeben durch den Hersteller des Clientsystems

Findet eine VAU-Kommunikation statt, so ist im äußeren, als auch im inneren HTTP-Request derselbe korrekte User-Agent zu setzen. [≤, PoPP_Client, funkt. Eignung: Herstellererklärung]

Neue AFO:

A_26171-01 -Clientsystem - User-Agent - Aufbau und Format bei der Kommunikation mit Diensten der TI

Das Clientsystem MUSS in allen HTTP-Requests an Dienste der TI 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>: Alphanumerische Zeichen a-z,A-Z,0-9, sowie dem Trennzeichen "." und "-" mit Länge von 3 bis 20 Zeichen → vergeben durch Clientsystem

Die Versionsnummer MUSS eindeutig sein und geändert werden, wenn es eine Änderung am Clientsystem gibt. Es ist empfohlen, dass das Format der Versionsnummer dabei dem grundlegenden Aufbau der TI-Versionsnummern gemäß [gemSpec_OM#GS-A_3695] entspricht.

Beispiel: "CLIENTID1234567890AB/2.1.12-45" [≤, PoPP_Client, funkt. Eignung: Herstellererklärung]

Hinweis: Gemäß RFC9110 ist im http-Header ein User-Agent einzutragen. Dieser RFC-User-Agent enthält z.B. Angaben zum Betriebssystem oder zum Browser und ist nicht zu verwechseln mit dem hier definierten TI-User-Agent. Dieser (TI-User-Agent) MUSS deshalb als zusätzlicher Parameter im http-Header eingetragen werden und NICHT im User-Agent-Parameter gem. RFC9110.

Hinweis zum Erhalt der Client-ID für Clientsysteme: Die Client-ID wird durch die gematik vergeben und übermittelt, sobald sich ein (Client-)Produkthersteller (z.B. FdV oder Primärsystem) unter idp-registrierung@gematik.de registriert hat. Dazu ist im Rahmen dieser Registrierung der Name des Herstellers und der Name des zu registrierenden Produktes zu übermitteln. Sollte im Rahmen einer TI-Anwendung bereits eine Registrierung vorgenommen worden sein, kann die Client-ID auch für andere TI-Anwendungen genutzt werden (sofern es sich um das gleiche Softwareprodukt handelt).