

## Änderung in gemSpec\_SST\_LD\_BD

<<Es werden in Kapitel 1 und 2 die Verweise auf die Schnittstelle I\_LogData entfernt>>

### 1.1 Zielsetzung

Dieses Dokument enthält die Anforderungen an die Schnittstelle ~~Logdaten-~~ und Betriebsdatenerfassung. Über sie werden von den Clients (z.B. Fachdienste und zentrale Dienste) versendete Betriebsdaten empfangen.

### 1.2 Zielgruppe

Das Dokument richtet sich an Hersteller und Anbieter der Schnittstelle ~~Logdaten-~~ und Betriebsdatenerfassung sowie an die Hersteller der Clients (z.B. Konnektoren und Fachdienste).

### 1.3 Abgrenzungen

Spezifiziert werden in diesem Dokument die Anforderungen und das Verhalten der Schnittstelle ~~Logdatenerfassung [I\_LogData]~~ und Betriebsdatenerfassung [I\_OpsData\_Update]. Daraus resultieren ebenfalls Abläufe in den Clients dieser Schnittstelle (z.B. den Konnektoren).

Für das Verständnis dieser Spezifikation wird die Kenntnis von [gemKPT\_Arch\_TIP] vorausgesetzt.

Dieses Dokument beschreibt für die über I\_LogData gelieferten Daten **nicht**:

- ~~die Weiterleitung der Daten zu einem Backendsystem und~~
- ~~die Verarbeitung der Daten.~~

---

## 2 Systemüberblick

---

Die Fachdienste und zentralen Dienste können ihre Betriebsdaten über die Schnittstelle Betriebsdatenerfassung I\_OpsData\_Update mit Operation [I\_OpsData\_Update]::fileUpload liefern.

<<Es wird das Kapitel 3 Schnittstelle I\_LogData inklusive der darin enthaltenen Blattanforderungen gestrichen>>

### A\_17108 - Schnittstelle Logdatenerfassung Konnektor TLS-Authentisierung durch den I\_LogData-Server

Die Schnittstelle I\_LogData MUSS bei der Absicherung der Verbindung durch TLS die serverseitige Authentisierung unter Nutzung des X.509-Komponentenzertifikats mit der TLS-Server-Identität ID.ZD.TLS\_S zur Serverauthentisierung umsetzen.[<=]

### A\_17109 - Schnittstelle Logdatenerfassung Keine Verbindungen ohne TLS

Die Schnittstelle I\_LogData MUSS ausschließlich Verbindungen mit TLS akzeptieren.[<=]

### A\_17182 - Schnittstelle Logdatenerfassung Bereitstellung DNS-Resource-Records

Der Anbieter der Schnittstelle Logdatenerfassung I\_LogData MUSS SRV- und TXT-Resource-Records im DNS bereitstellen. Die Werte der PFADx-Angaben MÜSSEN mit einem "/" beginnen.

Im DNS sind dazu folgende Einträge einzutragen:

```
Owner                      TTL Class Type Data
_logDataIf._tcp.<TOP_LEVEL_DOMAIN_TI> <TTL1> <IN> <SRV>
<Priorität1> <Gewicht1> <Port1> <FQDN1>
_logDataIf._tcp.<TOP_LEVEL_DOMAIN_TI> <TTL2> <IN> <TXT>
"txtvers=<VERSION1>" "path=<PFAD1>"
_logDataIf._tcp.<TOP_LEVEL_DOMAIN_TI> <TTL3> <IN> <SRV>
<Priorität2> <Gewicht2> <Port2> <FQDN2>
_logDataIf._tcp.<TOP_LEVEL_DOMAIN_TI> <TTL4> <IN> <TXT>
"txtvers=<VERSION2>" "path=<PFAD2>"
```

TOP\_LEVEL\_DOMAIN\_TI: in der PU = telematik.; in der RU/TU = telematik-test.[<=]

### A\_17170 - Schnittstelle Logdatenerfassung I\_LogData::getFile

Die Schnittstelle I\_LogData MUSS die Operation I\_LogData::getFile für die Übertragung von vordefinierten Dateien (siehe A\_17203 und A\_17172) an Clients entsprechend Tabelle Tab\_I\_LogData\_001 bereitstellen.

**Tabelle 1: Tab\_I\_LogData\_001 Operation I\_LogData::getFile**

Element	Beschreibung
Name	I_LogData::getFile

Beschreibung	Mit dieser Operation ruft der Client eine Datei ab. Die Dateien werden mit vordefinierten Dateinamen bereitgestellt. Der Client muss den Dateinamen kennen (der in diesem Kapitel definiert wird). Mit jedem Aufruf dieser Operation wird ein File übertragen.
Initiierender Akteur	Client von I_LogData
Weitere Akteure	keine
Auslöser	Client von I_LogData
Vorbedingungen	aufgebaute TLS-Verbindung vom Client
Nachbedingungen	Client von I_LogData hat die Datei vorliegen.
Aufruf	Aufruf von HTTP GET mit der URL "https://<host>:<port><path>/<filename>?LEI-ID=Wert (<host>:<port>" wird durch Abfrage des DNS SRV-Resource-Records ermittelt. "<path>" wird durch Abfrage des DNS TXT-Resource-Records ermittelt. "<filename>" entspricht dem Filename der Datei inklusive absolutem Pfad. Mit dem optionalen Parameter "LEI-ID" kann die Leistungsbringer-ID übergeben werden, welche dann in das bereitgestellte Dokument übernommen wird. Mindestens folgende Top-level-HTTP-Header MÜSSEN mit den angegebenen Werten unterstützt werden: <ul style="list-style-type: none"> <li>Accept-Encoding: gzip, deflate</li> </ul>
Standardablauf	Die angeforderte Datei wird dem aufrufenden Client zurückgegeben.
Fehlerfälle	Neben den Fehlercodes des aufgerufenen HTTP GET können keine weiteren Fehlercodes auftreten.

[&lt;=]

**A\_17172 - Schnittstelle Logdatenerfassung Bereitstellung****Einwilligungserklärung**

Die Schnittstelle I\_LogData MUSS über die Operation I\_LogData::getFile die Datei "LDA\_Einwilligungserklaerung.html" für alle Clients bereitstellen. Der lesende Zugriff auf diese Datei MUSS auch ohne Authentisierung auf HTTP-Ebene (ohne Authorization-Parameter) möglich sein.

[&lt;=]

**A\_17805 - Schnittstelle Logdatenerfassung Aufnahme LEI-ID in****Einwilligungserklärung**

Wenn mit Operation I\_LogData::getFile nach der URL im HTTP GET der Parameter LEI-ID übergeben wird, MUSS die Schnittstelle I\_LogData den Wert dieses Parameters in das Dokument "LDA\_Einwilligungserklaerung.html" an der vorgesehenen Stelle aufnehmen.[<=]

**A\_17203 - Schnittstelle Logdatenerfassung Bereitstellung Widerrufserklärung**

Die Schnittstelle I\_LogData MUSS über die Operation I\_LogData::getFile die Datei "LDA\_Widerrufserklaerung.html" für alle Clients bereitstellen. Der lesende Zugriff auf diese Datei MUSS auch ohne Authentisierung auf HTTP-Ebene (ohne Authorization-Parameter) möglich sein. [≤]

#### **A\_17806 - Schnittstelle Logdatenerfassung Aufnahme LEI-ID in Widerrufserklärung**

Wenn mit Operation I\_LogData::getFile nach der URL im HTTP GET der Parameter LEI-ID übergeben wird, MUSS die Schnittstelle I\_LogData den Wert dieses Parameters in das Dokument "LDA\_Widerrufserklaerung.html" an der vorgesehenen Stelle aufnehmen. [≤]

#### **A\_17340 - Schnittstelle Logdatenerfassung Willenserklärungen**

Die Schnittstelle I\_LogData MUSS die Operation I\_LogData::decIntent für die Übertragung der statischen Metadaten aus der Einwilligungserklärung und die Widerrufserklärung von Konnektoren zur Schnittstelle Logdatenerfassung entsprechend Tabelle Tab\_I\_LogData\_003 bereitstellen.

**Tabelle 2: Tab\_I\_LogData\_003 Operation I\_LogData::decIntent**

Element	Beschreibung
Name	I_LogData::decIntent
Beschreibung	Mit dieser Operation überträgt der Konnektor die statischen Metadaten aus der Einwilligungserklärung und die Widerrufserklärung zur Schnittstelle Logdatenerfassung.
Initiierender Akteur	Konnektor (Client von I_LogData)
Weitere Akteure	keine
Auslöser	Konnektor (Client von I_LogData)
Vorbedingungen	aufgebaute TLS-Verbindung vom Client
Nachbedingungen	Die Daten wurden zur Schnittstelle Logdatenerfassung übertragen.

Aufruf	<p>Aufruf von POST Request entsprechend [RFC7231] mit folgenden Optionen</p> <ul style="list-style-type: none"> <li>Für die URL "https://&lt;host&gt;:&lt;port&gt;&lt;path&gt;/" MUSS im POST Request folgendes beachtet werden: <ul style="list-style-type: none"> <li>"&lt;host&gt;:&lt;port&gt;" wird durch Abfrage des DNS-SRV-Resource-Records ermittelt.</li> <li>"&lt;path&gt;" wird durch Abfrage des DNS TXT-Resource-Records ermittelt.</li> </ul> </li> <li>Der POST Request MUSS den Content-Type application/x-www-form-urlencoded nutzen.</li> <li>Mindestens folgende Top-level-HTTP-Header MÜSSEN mit den angegebenen Werten unterstützt werden: <ul style="list-style-type: none"> <li>Authorization: Basic entsprechend [RFC7617] mit Nutzernamen "Registration" und leerem Passwort (0-Byte-langem Passwort).</li> <li>Content-Type: application/x-www-form-urlencoded</li> <li>Content-Length: entsprechend [RFC7230] zu setzen</li> <li>Accept-Encoding: gzip, deflate</li> </ul> </li> <li>Die Daten (statische Metadaten aus der Einwilligungserklärung und die Widerrufserklärung) sind im POST Request Body enthalten.</li> </ul>
Standardablauf	<p>Die Daten werden vom Konnektor zur Schnittstelle Logdatenerfassung übertragen. Die Autorisierung erfolgt über den statischen Nutzernamen "Registration", welcher immer freigeschaltet ist (der Nutzer mit dem LEI-ID Nutzernamen wird erst nach Prüfung der Einwilligungserklärung eingerichtet). Bei erfolgreicher Ablage der Datei wird im POST Response der HTTP-200-OK-Status zurückgegeben.</p>
Fehlerfälle	<p>Neben den registrierten HTTP-Status-Codes des aufgerufenen HTTP POST können keine weiteren Fehlercodes auftreten. Bei allen Fehler-HTTP-Status-Codes werden keine Datei abgelegt und der POST Request MUSS wiederholbar sein.</p>

[&lt;=]

### A\_17112 - Schnittstelle Logdatenerfassung Datei-Upload

Die Schnittstelle I\_LogData MUSS die Operation I\_LogData::fileUpload für die Übertragung von Dateien von Clients zur Schnittstelle Logdatenerfassung entsprechend Tabelle Tab\_I\_LogData\_002 bereitstellen.

**Tabelle 3: Tab\_I\_LogData\_002 Operation I\_LogData::fileUpload**

Element	Beschreibung
Name	I_LogData::fileUpload

Beschreibung	Mit dieser Operation überträgt der Client eine Datei zur Schnittstelle Logdatenerfassung.
Initiierender Akteur	Client von I_LogData
Weitere Akteure	keine
Auslöser	Client von I_LogData
Vorbedingungen	aufgebaute TLS-Verbindung vom Client
Nachbedingungen	Die Datei wurde zur Schnittstelle Logdatenerfassung übertragen.
Aufruf	<p>Aufruf von POST Request entsprechend [RFC7231] mit folgenden Optionen</p> <ul style="list-style-type: none"> <li>Für die URL "https://&lt;host&gt;:&lt;port&gt;&lt;path&gt;/" MUSS im POST Request folgendes beachtet werden: <ul style="list-style-type: none"> <li>"&lt;host&gt;:&lt;port&gt;" wird durch Abfrage des DNS SRV-Resource-Records ermittelt.</li> <li>"&lt;path&gt;" wird durch Abfrage des DNS TXT-Resource-Records ermittelt.</li> </ul> </li> <li>Der POST Request Format MUSS dem multipart/related Content-Type [RFC2387] entsprechen.</li> <li>Der "filename"-Parameter im Content-Disposition-Header MUSS den Namen der übertragenen Datei enthalten.</li> <li>Mindestens folgende Top-level-HTTP-Header MÜSSEN mit den angegebenen Werten unterstützt werden: <ul style="list-style-type: none"> <li>Authorization: Basic entsprechend [RFC7617] mit Nutzernamen und leerem Passwort (0-Byte-langem Passwort).</li> <li>Content-Type: multipart/related</li> <li>Content-Length: entsprechend [RFC7230] zu setzen</li> <li>Accept-Encoding: gzip, deflate</li> </ul> </li> <li>Die Daten der Datei sind im POST Request Body enthalten</li> </ul>
Standardablauf	<p>Die Datei wird – nach Autorisierung über "Authorization"-Parameter – vom Client zur Schnittstelle Logdatenerfassung übertragen.</p> <p>Bei erfolgreicher Ablage der Datei wird im POST Response der HTTP-200-OK-Status zurückgegeben.</p>
Fehlerfälle	<p>Neben den registrierten HTTP-Status-Codes des aufgerufenen HTTP POST können keine weiteren Fehlercodes auftreten.</p> <p>Bei allen Fehler-HTTP-Status-Codes wird keine Datei abgelegt und der POST Request MUSS mit gleichem "filename" wiederholbar sein.</p> <p>Im Fall von HTTP-Status-Code "401 Unauthorized" ist der Client nicht berechtigt, Dateien an die Schnittstelle Logdatenerfassung zu</p>

	senden (z.B. weil die Einwilligungserklärung noch nicht vorliegt und der Client freigeschaltet wurde).
--	--

[&lt;=]

**A\_17132 - Schnittstelle Logdatenerfassung Zugriff auf Dateien**

Die Schnittstelle I\_LogData MUSS

- den lesenden Zugriff auf Willenserklärungen erlauben und
- das Hochladen (HTTP POST) von Dateien durch - auf HTTP Ebene authentifizierte - Clients erlauben.

Alle anderen Zugriffe auf Dateien MÜSSEN verhindert werden.[&lt;=]

<<Zur Konkretisierung wird eine zusätzliche Blattanforderung für die Schnittstelle I\_OpsData\_Update (Kapitel 4) neben dem Upload als Datei und XML Format noch das Format JSON aufgenommen.

Die Blattanforderung wird in dem Abschnitt 4.x Content Upload JSON Format aufgenommen.>>

**4 Schnittstelle I\_OpsData\_Update****4.x Content Upload JSON Format****A\_23110 - Schnittstelle Betriebsdatenerfassung Content-Upload JSON Format**

Die Schnittstelle I\_OpsData\_Update MUSS die Operation

I\_OpsData\_Update::contentUploadJSON für die Übertragung von Content im JSON Format von Clients zur Schnittstelle Betriebsdatenerfassung entsprechend Tabelle Tab\_I\_OpsData\_Update\_004 bereitstellen.

Tabelle : Tab\_I\_OpsData\_Update\_004 Operation I\_OpsData\_Update::contentUploadJSON

Element	Beschreibung
Name	I_OpsData_Update::contentUploadJSON
Beschreibung	Mit dieser Operation überträgt der Client pro Lieferung genau einen Content im JSON Format an die Schnittstelle Betriebsdatenerfassung.
Initiierender Akteur	Client von I_OpsData_Update

Weitere Akteure	keine
Auslöser	Client von I_OpsData_Update
Vorbedingungen	aufgebaute TLS-Verbindung vom Client
Nachbedingungen	Der Content im JSON Format wurde zur Schnittstelle Betriebsdatenerfassung übertragen.
Aufruf	<p>Aufruf von POST Request entsprechend [RFC7231] mit folgenden Optionen</p> <p>Für die URL " <b>Fehler! Linkreferenz ungültig.</b>" MUSS im POST Request folgendes beachtet werden:</p> <p>"&lt;host&gt;:&lt;port&gt;" wird durch Abfrage des DNS SRV-Resource-Records ermittelt.</p> <p>"&lt;path&gt;" wird durch die gematik zur Verfügung gestellt.</p> <p>Mindestens folgende Top-level-HTTP-Header MÜSSEN mit den angegebenen Werten unterstützt werden:</p> <p>Content-Type: text/xml; charset="utf-8"</p> <p>Content-Length: entsprechend [RFC7230] zu setzen</p> <p>Accept-Encoding: gzip, deflate</p> <p>Der zu liefernde Content MUSS im POST Request Body geliefert werden.</p>
Standardablauf	<p>Der Content wird vom Client zur Schnittstelle Betriebsdatenerfassung übertragen.</p> <p>Bei erfolgreicher Übermittlung des Contents wird in der Response der HTTP-200-OK-Status zurückgegeben.</p>
Fehlerfälle	<p>Bei allen Fehler-HTTP-Status-Codes wird kein Content abgelegt und der POST Request MUSS mit gleicher CI-ID wiederholbar sein.</p> <p>Im Fall von HTTP-Status-Code "400 Bad Request" enthält der HTTP Request einen Fehler.</p>

[&lt;=]