

**Elektronische Gesundheitskarte und Telematikinfrastruktur**

# Spezifikation Logdaten- und Betriebsdatenerfassung

Version:	1. <del>24</del> .0
Revision:	<del>827587916462</del>
Stand:	<del>30.06</del> 03.02.2020 <del>3</del>
Status:	freigegeben
Klassifizierung:	öffentlich
Referenzierung:	gemSpec_SST_LD_B D

## Dokumentinformationen

### Änderungen zur Vorversion

Anpassungen des vorliegenden Dokumentes im Vergleich zur Vorversion können Sie der nachfolgenden Tabelle entnehmen.

### Dokumentenhistorie

Version	Stand	Kap./Seite	Grund der Änderung, besondere Hinweise	Bearbeitung
1.0.0	15.05.19		freigegeben	gematik
1.0.1	28.06.19		Begriffsklarstellung	gematik
1.1.0	03.02.20		Einarbeitung lt. Änderungsliste P21.1	gematik
1.1.1	26.06.20		Einarbeitung lt. Änderungsliste P21.3	gematik
1.2.0	30.06.20		Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik
<a href="#">1.3.0</a>	<a href="#">02.12.22</a>	<a href="#">Kap. 3</a>	<a href="#">Einarbeitung CI_Maintenance_22.5: Entfernen Schnittstelle I_Log_Data, Konkretisierung Betriebsdatenübermittlung Konnektor</a>	<a href="#">gematik</a>
<a href="#">1.4.0</a>	<a href="#">03.02.23</a>		<a href="#">Einarbeitung Betr_Maintenance_22.3</a>	<a href="#">gematik</a>

---

## Inhaltsverzeichnis

---

<b>1 Einordnung des Dokuments.....</b>	<b>4</b>
1.1 Zielsetzung.....	4
1.2 Zielgruppe.....	4
1.3 Geltungsbereich.....	4
1.4 Abgrenzungen.....	4
1.5 Methodik.....	5
<b>2 Systemüberblick.....</b>	<b>6</b>
<b>3 Schnittstelle I_LogData.....</b>	<b>7</b>
3.1 Transport Layer Security (TLS).....	7
3.2 DNS Resource Record.....	7
3.3 Willenserklärungen zur Konnektor-Logdatenerfassung.....	8
3.4 Datei Upload.....	11
<b>4 Schnittstelle I_OpsData_Update.....</b>	<b>14</b>
4.1 Transport Layer Security (TLS).....	14
4.2 DNS Resource Record.....	14
4.3 Datei Upload.....	15
<b>5 Anhang – Verzeichnisse.....</b>	<b>18</b>
5.1 Abkürzungen.....	18
5.2 Glossar.....	18
5.3 Abbildungsverzeichnis.....	18
5.4 Tabellenverzeichnis.....	18
5.5 Referenzierte Dokumente.....	19
5.5.1 Dokumente der gematik.....	19
5.5.2 Weitere Dokumente.....	19

<b>1 Einordnung des Dokuments.....</b>	<b>5</b>
1.1 Zielsetzung.....	5
1.2 Zielgruppe.....	5
1.3 Geltungsbereich.....	5
1.4 Abgrenzungen.....	5
1.5 Methodik.....	6

<b>2 Systemüberblick.....</b>	<b>7</b>
<b>n (darunter falle.....</b>	<b>15</b>
2.1 Transport Layer Security (TLS).....	15
2.2 DNS Resource Record.....	15
2.3 Datei Upload.....	16
2.4 Content Upload XML.....	18
2.5 Content Upload JSON Format.....	19
<b>3 Anhang - Verzeichnisse.....</b>	<b>21</b>
3.1 Abkürzungen.....	21
3.2 Glossar.....	21
3.3 Abbildungsverzeichnis.....	21
3.4 Tabellenverzeichnis.....	21
3.5 Referenzierte Dokumente.....	22
3.5.1 Dokumente der gematik.....	22
3.5.2 Weitere Dokumente.....	22

---

## 1 Einordnung des Dokuments

---

### 1.1 Zielsetzung

Dieses Dokument enthält die Anforderungen an die Schnittstelle ~~Logdaten-~~  
~~und~~ Betriebsdatenerfassung. Über sie werden von den Clients (z.B.  
~~Konnektoren~~ Fachdienste und Fachzentrale 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 Geltungsbereich

Dieses Dokument enthält normative Festlegungen zur Telematikinfrastruktur des  
Deutschen Gesundheitswesens für den Online-Produktivbetrieb (Stufe 2). Der  
Gültigkeitszeitraum der vorliegenden Version und deren Anwendung in Zulassungs- oder  
Abnahmeverfahren wird durch die gematik GmbH in gesonderten Dokumenten (z.B.  
Dokumentenlandkarte, Produkttypsteckbrief, Leistungsbeschreibung) festgelegt und  
bekannt gegeben.

### Wichtiger Schutzrechts-/Patentrechtshinweis

*Die nachfolgende Spezifikation ist von der gematik allein unter technischen  
Gesichtspunkten erstellt worden. Im Einzelfall kann nicht ausgeschlossen werden, dass  
die Implementierung der Spezifikation in technische Schutzrechte Dritter eingreift. Es ist  
allein Sache des Anbieters oder Herstellers, durch geeignete Maßnahmen dafür Sorge zu  
tragen, dass von ihm aufgrund der Spezifikation angebotene Produkte und/oder  
Leistungen nicht gegen Schutzrechte Dritter verstoßen und sich ggf. die erforderlichen  
Erlaubnisse/Lizenzen von den betroffenen Schutzrechtsinhabern einzuholen. Die gematik  
GmbH übernimmt insofern keinerlei Gewährleistungen.*

### 1.4 Abgrenzungen

Spezifiziert werden in diesem Dokument die Anforderungen und das Verhalten der  
Schnittstellen 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.~~

## **1.5 Methodik**

~~An~~

## **1.6 Methodik**

Anforderungen als Ausdruck normativer Festlegungen werden durch eine eindeutige ID sowie die dem RFC 2119 [RFC2119] entsprechenden, in Großbuchstaben geschriebenen deutschen Schlüsselworte MUSS, DARF NICHT, SOLL, SOLL NICHT, KANN gekennzeichnet.

Sie werden im Dokument wie folgt dargestellt:

**<AFO-ID> - <Titel der Afo>**

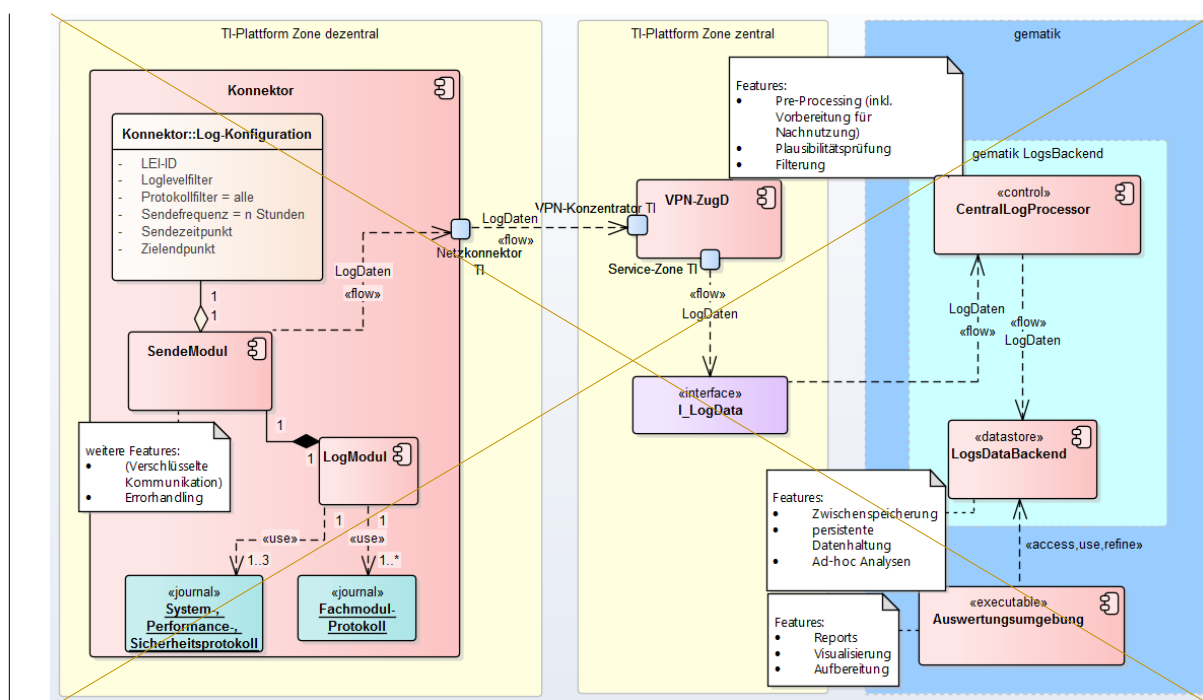
Text / Beschreibung

[<=]

Dabei umfasst die Anforderung sämtliche zwischen Afo-ID und der Textmarke [<=] angeführten Inhalte.

## 2 Systemüberblick

In folgender Abbildung ist die Einbettung der Schnittstelle Logdatenerfassung [I\_LogData] in die TI dargestellt.



**Abbildung 1: Überblick Die Fach Schnittstelle Logdatenerfassung**

Nach Einwilligung des Leistungserbringers werden alle Logdaten des Konnektors periodisch pseudonymisiert und mit einigen Metadaten angereichert an [I\_LogData] gesendet. Von dort werden sie weiter an ein Logdaten-Analyse-System gesendet. Die Einwilligungserklärung und die Widerspruchserklärung werden dem Konnektor über Operation I\_LogData::getFile bereitgestellt.

Beispielablauf für den Konnektor:

1. Lokalisierung der Schnittstelle über DNS (A\_17182)
2. Aufbau-TLS-Verbindung (A\_17108, A\_17273)
3. Einwilligungserklärung laden durch Aufruf I\_LogData::getFile mit Parameter LEI-ID (A\_17172)
4. Statische Metadaten aus der Einwilligungserklärung senden durch Aufruf I\_LogData::declIntent (A\_17340)
5. Senden von Logdaten durch Aufruf I\_LogData::fileUpload (A\_17112)

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

## 3 Schnittstelle I\_LogData

Die Konnektoren liefern ihre Logdaten über die Schnittstelle Logdatenerfassung I\_LogData.

### 3.1 Transport Layer Security (TLS)

Die Schnittstelle I\_LogData wird durch TLS abgesichert.

#### Mainline\_OPB1/ML-92644A\_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. [<=]

#### Mainline\_OPB1/ML-92645A\_17109 – Schnittstelle Logdatenerfassung Keine Verbindungen ohne TLS

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

### 3.2 DNS Resource Record

Die Schnittstelle I\_LogData stellt Funktionen bereit, die über URLs aufgerufen werden können.

#### Mainline\_OPB1/ML-92821A\_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. [<=]

Die "Idif"-DNS-Resource-Records werden von den Konnektoren zur Lokalisierung der Schnittstelle genutzt.



### 3.3 Willenserklärungen zur Konnektor-Logdatenerfassung

Der Leistungserbringer muss der Verarbeitung seiner Konnektor-Logdaten zustimmen. Zur Unterstützung dieses Prozesses wird die Einwilligungs- und Widerrufserklärung über die Schnittstelle I\_LogData bereitgestellt. Weiterhin werden die statischen Metadaten (welche keine personenbezogenen Daten enthalten) aus der Einwilligungserklärung und die Widerrufserklärung vom Konnektor an die Schnittstelle gesendet.

Die Schnittstelle I\_LogData erlaubt den Download von vordefinierten Dateien durch den Konnektor, die in diesem Kapitel definiert werden. Dazu gehören Dateien wie die Einwilligungserklärung und die Widerspruchserklärung für die Logdatenerfassung, welche durch den Leistungserbringer ausgefüllt werden müssen.

Der Zugriff auf Dateien, die von I\_LogData-Clients mit HTTP POST bereitgestellt werden, ist nicht möglich.

#### Mainline\_OPB1/ML-92808A\_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.

**[<=]**

#### **Mainline\_OPB1/ML-92810A\_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.

**[<=]**

#### **Mainline\_OPB1/ML-94353A\_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.**[<=]**

#### **Mainline\_OPB1/ML-92894A\_17203 -- Schnittstelle Log Updatenerfassung 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.**[<=]**

#### **Mainline\_OPB1/ML-94354A\_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.**[<=]**

#### **Mainline\_OPB1/ML-93527A\_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\_LogFachdienste und zentralen Data\_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).</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 werden keine Datei abgelegt und der POST Request MUSS wiederholbar sein.</p>

[<=]

### 3.4 Datei Upload

#### ~~Mainline\_OPB1/ML-92655A\_17112--ien~~ 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-längem 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	Die Datei wird nach Autorisierung über "Authorization"-Parameter

	<del>—vom Client zur Schnittstelle Logdatenerfassung übertragen. Bei erfolgreicher Ablage der Datei wird im POST-Response der HTTP-200-OK-Status zurückgegeben.</del>
<b>Fehlerfälle</b>	<del>Neben den registrierten HTTP-Status-Codes des aufgerufenen HTTP- POST können keine weiteren Fehlercodes auftreten. Bei allen Fehler-HTTP-Status-Codes wird keine Datei abgelegt und der POST Request MUSS mit gleichem "filename" wiederholbar sein. Im Fall von HTTP-Status-Code "401 Unauthorized" ist der Client nicht berechtigt, Dateien an die Schnittstelle Logdatenerfassung zu senden (z.B. weil die Einwilligungserklärung noch nicht vorliegt und der Client freigeschaltet wurde).</del>

**[<=]**

Hinweise liefern ihre Betriebe:

- ~~• Wenn der Client testen möchte, ob er für die Lieferung von Dateien an die  
Schnittstelle Logdatenerfassung freigeschaltet wurde, kann er einen HTTP-POST-  
Request mit leerem/r Inhalt/Datei und seinem Nutzernamen im Authorization-  
Parameter senden. Erhält er als Antwort HTTP-Status-Code "401 Unauthorized", ist er  
nicht freigeschaltet.~~
- ~~• Der Client muss eindeutige Dateinamen für seine Dateien (bspw. durch Anhängen  
eines Zeitstempels, einer eindeutigen ID, o.ä.) sicherstellen.~~

**Mainline\_OPB1/ML-92724A\_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.[<=]**

## 4 Schnittsten (darunter falle I\_OpsData\_Update

Die Fachdienste und zentralen Dienste liefern ihre Betriebsdaten (darunter fallen auch die Rohdaten) über die Schnittstelle Betriebsdatenerfassung I\_OpsData\_Update.

### 4.1 Transport Layer Security (TLS)

#### A\_17272-01 - Schnittstelle Betriebsdatenerfassung TLS-Authentisierung für Fach- und zentrale Dienste durch den I\_OpsData\_Update-Server

Die Schnittstelle I\_OpsData\_Update 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\_17416-01 - Schnittstelle Betriebsdatenerfassung Prüfung des TLS-Server-Zertifikats durch Fach- und zentrale Dienste

Der Client der Schnittstelle I\_OpsData\_Update MUSS bei der Absicherung der Verbindung durch TLS die serverseitige Authentisierung durch Prüfung des I\_OpsData\_Update-X.509-Komponentenzertifikats mit der TLS-Server-Identität ID.ZD.TLS\_S zur

Serverauthentisierung entsprechend [gemSpec\_Krypt#TLS-Verbindungen] umsetzen.

[<=]

#### A\_17730 - Schnittstelle Betriebsdatenerfassung Keine Verbindungen ohne TLS

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

### 4.2 DNS Resource Record

Die Schnittstelle I\_OpsData\_Update stellt Funktionen bereit, die über URLs aufgerufen werden können.

#### A\_17731 - Schnittstelle Betriebsdatenerfassung Bereitstellung DNS-Resource-Records

Der Anbieter der Schnittstelle Betriebsdatenerfassung I\_OpsData\_Update 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
_fdrdif._tcp.<TOP_LEVEL_DOMAIN_TI>	<TTL1>	<IN>	<SRV>	<Priorität1> <Gewicht1> <Port1> <FQDN1>
_fdrdif._tcp.<TOP_LEVEL_DOMAIN_TI>	<TTL2>	<IN>	<TXT>	"txtvers=<VERSION1>" "path=<PFAD1>"
_fdrdif._tcp.<TOP_LEVEL_DOMAIN_TI>	<TTL3>	<IN>	<SRV>	<Priorität2> <Gewicht2> <Port2> <FQDN2>
_fdrdif._tcp.<TOP_LEVEL_DOMAIN_TI>	<TTL4>	<IN>	<TXT>	"txtvers=<VERSION2>" "path=<PFAD2>"
_zdrdif._tcp.<TOP_LEVEL_DOMAIN_TI>	<TTL1>	<IN>	<SRV>	<Priorität1> <Gewicht1> <Port1> <FQDN1>

```
_zdrdif._tcp.<TOP_LEVEL_DOMAIN_TI> <TTL2> <IN> <TXT> "txtvers=<VERSION1>"
"path=<PFAD1>"
_zdrdif._tcp.<TOP_LEVEL_DOMAIN_TI> <TTL3> <IN> <SRV>
<Priorität2> <Gewicht2> <Port2> <FQDN2>
_zdrdif._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.【<=】

Die "fdrdif"-DNS-Resource-Records werden von den Fachdiensten und die "zdrdif"-DNS-Resource-Records von den zentralen Diensten zur Lokalisierung der Schnittstelle genutzt.

## 4.3 Datei Upload

### A\_17733-01 - Schnittstelle Betriebsdatenerfassung Datei-Upload

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

**Tabelle 4: Tab\_I\_OpsData\_Update\_002 Operation I\_OpsData\_Update::fileUpload**

Element	Beschreibung
Name	I_OpsData_Update::fileUpload
Beschreibung	Mit dieser Operation überträgt der Client pro Lieferung genau eine Datei 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	Die Datei wurde zur Schnittstelle Betriebsdatenerfassung 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>Im Top-level-HTTP-Header MUSS ein zusätzliches Feld "filename" angelegt werden. Der Wert für dieses Feld 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>Content-Type: application/octet-stream</li> <li>Content-Length: entsprechend [RFC7230] zu setzen</li> <li>Accept-Encoding: gzip, deflate</li> </ul> </li> <li>Die zu liefernde Datei MUSS im POST Request Body geliefert werden. D.h. der Request Body MUSS auf die Datei an sich in Binärform (binary data) beschränkt sein.</li> </ul>
Standardablauf	<p>Die Datei wird vom Client zur Schnittstelle Betriebsdatenerfassung übertragen. Die Datei wird auf Fehler überprüft. Bei erfolgreicher Ablage und Prüfung der Datei wird im POST Response der HTTP-200-OK-Status zurückgegeben. Der Client muss für die Prüfung der übermittelten Datei genügend Zeit berücksichtigen (Timer für das Warten auf das HTTP Response entsprechend konfigurieren). Wenn die Prüfung der Datei länger als 10 Sekunden dauert, MUSS die Schnittstelle I_OpsData_Update nach jeweils 10 Sekunden einen POST Response mit dem HTTP-102 Processing Status zurückgeben um bei dem Client ein Timeout zu verhindern.</p>
Fehlerfälle	<p>Neben den registrierten HTTP-Status-Codes des aufgerufenen HTTP POST können keine weiteren Fehlercodes auftreten. Bei allen Fehler-HTTP-Status-Codes wird keine Datei abgelegt und der POST Request MUSS mit gleichem "filename" wiederholbar sein. Im Fall von HTTP-Status-Code "400 Bad Request" enthält der HTTP POST bzw. die Datei einen Fehler. Dieser Fehler kann sich in der enthaltenen Datei befinden.</p>

**[<=]**

Hinweise:

- Der Client muss eindeutige Dateinamen für seine Dateien (bspw. durch Anhängen eines Zeitstempels, einer eindeutigen ID, o.ä.) sicherstellen.

#### **A\_17734-01 - Schnittstelle Betriebsdatenerfassung Zugriff auf Dateien**

Die Schnittstelle I\_OpsData\_Update MUSS



- das Hochladen (HTTP POST) von Dateien durch Clients (ohne TLS Client Authentisierung) erlauben

[<=]

## 4.4 Anhang Content Upload XML

### **A\_23107 - Schnittstelle Betriebsdatenerfassung Content-Upload XML Format**

Die Schnittstelle I\_OpsData\_Update MUSS die Operation I\_OpsData\_Update::contentUploadXML für die Übertragung von Content im XML Format von Clients zur Schnittstelle Betriebsdatenerfassung entsprechend Tabelle Tab\_I\_OpsData\_Update\_003 bereitstellen.

Tabelle : Tab\_I\_OpsData\_Update\_003 Operation I\_OpsData\_Update::contentUploadXML

<u>Element</u>	<u>Beschreibung</u>
<u>Name</u>	<u>I_OpsData_Update::contentUploadXML</u>
<u>Beschreibung</u>	<u>Mit dieser Operation überträgt der Client pro Lieferung genau einen Content im XML Format an die Schnittstelle Betriebsdatenerfassung.</u>
<u>Initiierender Akteur</u>	<u>Client von I_OpsData_Update</u>
<u>Weitere Akteure</u>	<u>keine</u>
<u>Auslöser</u>	<u>Client von I_OpsData_Update</u>
<u>Vorbedingungen</u>	<u>aufgebaute TLS-Verbindung vom Client</u>
<u>Nachbedingungen</u>	<u>Der Content im XML Format wurde zur Schnittstelle Betriebsdatenerfassung übertragen.</u>
<u>Aufruf</u>	<p><u>Aufruf von POST Request entsprechend [RFC7231] mit folgenden Optionen</u></p> <p><u>Für die URL " https://&lt;host&gt;:&lt;port&gt;&lt;path&gt;/" MUSS im POST Request folgendes beachtet werden:</u></p> <p><u>"&lt;host&gt;:&lt;port&gt;" wird durch Abfrage des DNS SRV-Resource-Records ermittelt.</u></p> <p><u>"&lt;path&gt;" wird durch die gematik zur Verfügung gestellt.</u></p> <p><u>Im Top-level-HTTP-Header MUSS ein zusätzliches Feld "CI" angelegt werden. Der Wert für dieses Feld MUSS die CI-ID der logischen Produktinstanz des liefernden Client enthalten (in der Form "CI-nnnnnnn").</u></p> <p><u>Mindestens folgende Top-level-HTTP-Header MÜSSEN mit den angegebenen Werten unterstützt werden:</u></p> <p><u>Content-Type: text/xml; charset="utf-8"</u></p>

	<u>Content-Length: entsprechend [RFC7230] zu setzen</u> <u>Accept-Encoding: gzip, deflate</u> <u>Der zu liefernde Content MUSS im POST Request Body geliefert werden.</u>
<u>Standardablauf</u>	<u>Der Content wird vom Client zur Schnittstelle Betriebsdatenerfassung übertragen.</u> <u>Bei erfolgreicher Übermittlung des Contents wird in der Response der HTTP-200-OK-Status zurückgegeben.</u>
<u>Fehlerfälle</u>	<u>Bei allen Fehler-HTTP-Status-Codes wird kein Content abgelegt und der POST Request MUSS mit gleicher CI-ID wiederholbar sein.</u> <u>Im Fall von HTTP-Status-Code "400 Bad Request" enthält der HTTP Request einen Fehler.</u>

(Hinweis: Für weitere Informationen zum CI, siehe [gemRL\_Betr\_TI] Kapitel "Configuration Management".) [ $\leq$ ]

## **4.5 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

<u>Element</u>	<u>Beschreibung</u>
<u>Name</u>	<u>I_OpsData_Update::contentUploadJSON</u>
<u>Beschreibung</u>	<u>Mit dieser Operation überträgt der Client pro Lieferung genau einen Content im JSON Format an die Schnittstelle Betriebsdatenerfassung.</u>
<u>Initiierender Akteur</u>	<u>Client von I_OpsData_Update</u>
<u>Weitere Akteure</u>	<u>keine</u>
<u>Auslöser</u>	<u>Client von I_OpsData_Update</u>
<u>Vorbedingungen</u>	<u>aufgebaute TLS-Verbindung vom Client</u>
<u>Nachbedingungen</u>	<u>Der Content im JSON Format wurde zur Schnittstelle Betriebsdatenerfassung übertragen.</u>
<u>Aufruf</u>	<u>Aufruf von POST Request entsprechend [RFC7231] mit folgenden Optionen</u>

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

(Hinweis: Für weitere Informationen zum CI, siehe [gemRL\_Betr\_TI] Kapitel "Configuration Management".) [**<=**]

## 5 Anhang - Verzeichnisse

### 5.1 Abkürzungen

Kürzel	Erläuterung
DNS	Domain Name Service
TLS	Transport Layer Security
LEI	Leistungserbringerinstitution
LDA	Logdaten-Analyse

### 5.2 Glossar

Begriff	Erläuterung
Funktionsmerkmal	Der Begriff beschreibt eine Funktion oder auch einzelne, eine logische Einheit bildende Teilfunktionen der TI im Rahmen der funktionalen Zerlegung des Systems.

Das Glossar wird als eigenständiges Dokument (vgl. [gemGlossar]) zur Verfügung gestellt.

### 5.3 Abbildungsverzeichnis

Abbildung 1: Überblick Schnittstelle Logdatenerfassung.....6

No table of figures entries found.

### 5.4 Tabellenverzeichnis

Tabelle 1: Tab\_I\_LogData\_001-Operation I\_LogData::getFile.....8

Tabelle 2: Tab\_I\_LogData\_003-Operation I\_LogData::decIntent.....9

Tabelle 3: Tab\_I\_LogData\_002-Operation I\_LogData::fileUpload.....11

Tabelle 4: Tab\_I\_OpsData\_Update\_002-Operation I\_OpsData\_Update::fileUpload.....15

Tabelle 1: Tab\_I\_OpsData\_Update\_002 Operation I\_OpsData\_Update::fileUpload.....16

## **5.5 Referenzierte Dokumente**

### **5.5.1 Dokumente der gematik**

Die nachfolgende Tabelle enthält die Bezeichnung der in dem vorliegenden Dokument referenzierten Dokumente der gematik zur Telematikinfrastuktur. Der mit der vorliegenden Version korrelierende Entwicklungsstand dieser Konzepte und Spezifikationen wird pro Release in einer Dokumentenlandkarte definiert. Version und Stand der referenzierten Dokumente sind daher in der nachfolgenden Tabelle nicht aufgeführt. Deren zu diesem Dokument jeweils gültige Versionsnummer ist in der aktuellen, von der gematik veröffentlichten Dokumentenlandkarte enthalten, in der die vorliegende Version aufgeführt wird.

<b>[Quelle]</b>	<b>Herausgeber: Titel</b>
[gemGlossar]	gematik: Glossar der Telematikinfrastuktur

### **5.5.2 Weitere Dokumente**

<b>[Quelle]</b>	<b>Herausgeber (Erscheinungsdatum): Titel</b>
[RFC7230]	Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing
[RFC7231]	Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content
[RFC7617]	The 'Basic' HTTP Authentication Scheme