Beim vorliegenden Dokument handelt es sich um einen Entwurf der gematik in Vorbereitung auf zukünftige normative Festlegungen als Grundlage entsprechender Zulassungs- und Bestätigungsverfahren. Die gematik veröffentlicht diesen Entwurf mit dem Ziel, dass sich Interessierte bereits frühzeitig einen Überblick über die mögliche Weiterentwicklung der Telematikinfrastruktur verschaffen können. Die gematik übernimmt keine Gewähr für die Aktualität, Richtigkeit und Vollständigkeit dieses Entwurfes und behält sich das Recht vor, ohne vorherige Ankündigung Änderungen oder Ergänzungen vorzunehmen oder von den Regelungen insgesamt bzw. teilweise Abstand zu nehmen.

Elektronische Gesundheitskarte und Telematikinfrastruktur

Spezifikation Logdaten- und Betriebsdatenerfassung

Version:	1.~~1~~2.0 CC
Revision:	~~198542~~231073
Stand:	~~02.03~~30.04.2020
Status:	zur Abstimmung freigegeben
Klassifizierung:	öffentlich_Entwurf
Referenzierung:	gemSpec_SST_LD_BD

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~~2.0 CC	~~03.02~~30.04.20		~~freigegeben~~Anpassungen gemäß Änderungsliste P22.1 und Scope-Themen aus Systemdesign R4.0.0	gematik

Inhaltsverzeichnis

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 und Fachdienste) 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

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.

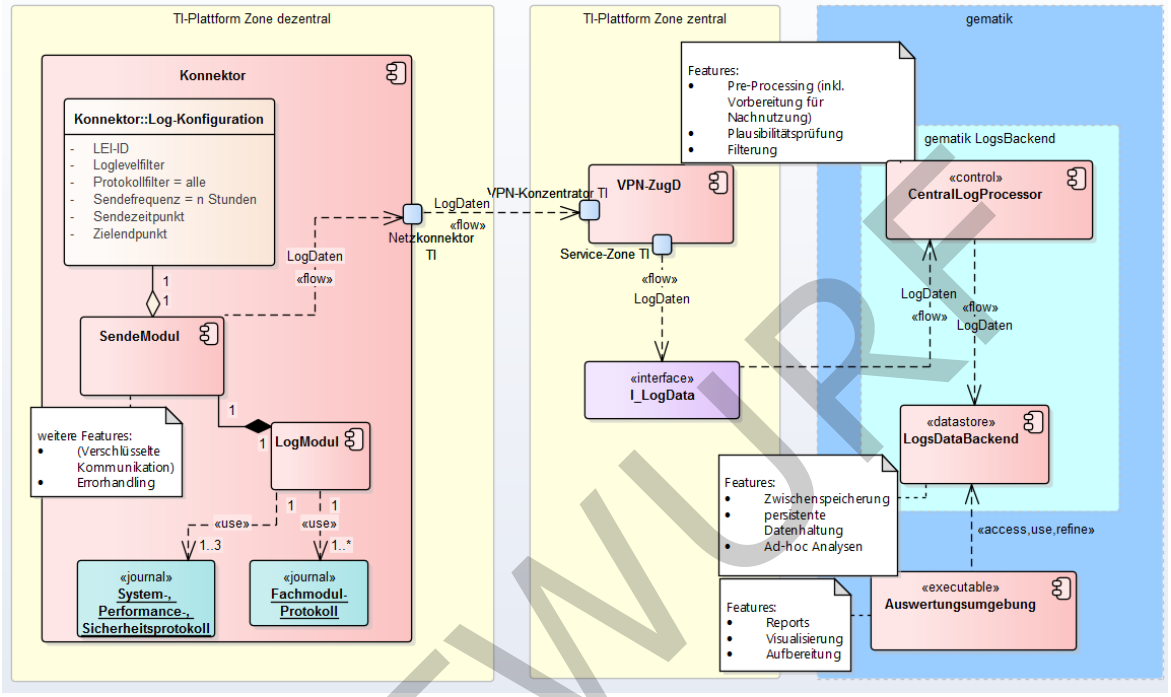

Abbildung 1: Überblick Schnittstelle Logdatenerfassung

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::decIntent (A_17340)
5. Senden von Logdaten durch Aufruf I_LogData::fileUpload (A_17112)

Die Fachdienste 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.

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.**[<=]**

3.2 DNS Resource Record

Die Schnittstelle I_LogData stellt Funktionen bereit, die über URLs aufgerufen werden können.

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.**[<=]**

Die "ldif"-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.

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: • Accept-Encoding: gzip, deflate

Standardablauf	Die angeforderte Datei wird dem aufrufenden Client zurückgegeben.
Fehlerfälle	Neben den Fehlercodes des aufgerufenen HTTP GET können keine weiteren Fehlercodes auftreten.

[<=]

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.
[<=]

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	Aufruf von POST Request entsprechend [RFC7231] mit folgenden Optionen
	• Für die URL "https://<host>:<port><path>/" MUSS im POST Request folgendes beachtet werden:
	  • "<host>:<port>" wird durch Abfrage des DNS-SRV-Resource-Records ermittelt.
	  • "<path>" wird durch Abfrage des DNS TXT-Resource-Records ermittelt.
	• Der POST Request MUSS den Content-Type application/x-www-form-urlencoded nutzen.
	• Mindestens folgende Top-level-HTTP-Header MÜSSEN mit den angegebenen Werten unterstützt werden:
	  • Authorization: Basic entsprechend [RFC7617] mit Nutzername "Registration" und leerem Passwort (0-Byte-langem Passwort).
	  • Content-Type: application/x-www-form-urlencoded
	  • Content-Length: entsprechend [RFC7230] zu setzen
	  • Accept-Encoding: gzip, deflate
	• Die Daten (statische Metadaten aus der Einwilligungserklärung und die Widerrufserklärung) sind im POST Request Body enthalten.

Standardablauf	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.
Fehlerfälle	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.

238 **[<=]**

3.4 Datei Upload

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	Aufruf von POST Request entsprechend [RFC7231] mit folgenden Optionen
	• Für die URL "https://<host>:<port><path>/" MUSS im POST Request folgendes beachtet werden:
	  • "<host>:<port>" wird durch Abfrage des DNS SRV-Resource-Records ermittelt.
	  • "<path>" wird durch Abfrage des DNS TXT-Resource-Records ermittelt.
	• Der POST Request Format MUSS dem multipart/related Content-Type [RFC2387] entsprechen.
	• Der "filename"-Parameter im Content-Disposition-Header MUSS den Namen der übertragenen Datei enthalten.
	• Mindestens folgende Top-level-HTTP-Header MÜSSEN mit den angegebenen Werten unterstützt werden:
	  • Authorization: Basic entsprechend [RFC7617] mit Nutzername und leerem Passwort (0-Byte-langem Passwort).
	  • Content-Type: multipart/related
	  • Content-Lenght: entsprechend [RFC7230] zu setzen
	  • Accept-Encoding: gzip, deflate
	• Die Daten der Datei sind im POST Request Body enthalten

Standardablauf	Die Datei wird – nach Autorisierung über "Authorization"-Parameter – vom Client zur Schnittstelle Logdatenerfassung übertragen. Bei erfolgreicher Ablage der Datei wird im POST Response der HTTP-200-OK-Status zurückgegeben.
Fehlerfälle	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).

[<=]

Hinweise:

- 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.

A_17132 - Schnittstelle Logdatenerfassung Zugriff auf Dateien

Die Schnittstelle I_LogData MUSS

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

Alle anderen Zugriffe auf Dateien MÜSSEN verhindert werden.**[<=]**

4 Schnittstelle 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 - 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 eine Datei zur 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	Aufruf von POST Request entsprechend [RFC7231] mit folgenden Optionen
	• Für die URL "https://<host>:<port><path>/" MUSS im POST Request folgendes beachtet werden:
	  • "<host>:<port>" wird durch Abfrage des DNS SRV-Resource-Records ermittelt.
	  • "<path>" wird durch Abfrage des DNS TXT-Resource-Records ermittelt.
	• Der POST Request Format MUSS dem multipart/related Content-Type [RFC2387] entsprechen.
	• Der "filename"-Parameter im Content-Disposition-Header MUSS den Namen der übertragenen Datei enthalten.
	• Mindestens folgende Top-level-HTTP-Header MÜSSEN mit den angegebenen Werten unterstützt werden:
	  • Content-Type: multipart/related
	  • Content-Lenght: entsprechend [RFC7230] zu setzen
	  • Accept-Encoding: gzip, deflate
	• Die Daten der Datei sind im POST Request Body enthalten

Standardablauf	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.
Fehlerfälle	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.

[<=]

Hinweise:

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

A_17734-01~~A_17734~~ - Schnittstelle Betriebsdatenerfassung Zugriff auf Dateien

Die Schnittstelle I_OpsData_Update MUSS

- das Hochladen (HTTP POST) von Dateien durch ~~- auf TLS Ebene authentisierte -~~ Clients (ohne TLS Client Authentisierung) erlauben~~.~~

~~Alle anderen Zugriffe auf Dateien MÜSSEN verhindert werden.~~**~~[<=]~~[<=]**

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

5.4 Tabellenverzeichnis

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 Telematikinfrastruktur. 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.

[Quelle]	Herausgeber: Titel
[gemGlossar]	gematik: Glossar der Telematikinfrastruktur

5.5.2 Weitere Dokumente

[Quelle]	Herausgeber (Erscheinungsdatum): Titel
[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