Schnittstellenbeschreibung IF_GW_CON

CONEXA 3.0 Smart Meter Gateway

Inhaltsverzeichnis

Änderungshistorie

Datum	Version	Ersteller	Änderung
16.09.19	0.1	ths	Initiale Erstellung
23.09.19	1.1	ths	Umzug Dokument, Formatierungen
04.12.19	1.2	ths	taf-state eingefügt bei Vertragsdaten laden
08.01.20	1.2	ths	Literaturverzeichnis angepasst
26.03.20	1.3	ths	Redaktionelle Anpassungen
04.04.20	1.4	ths	Aufnahme der Kurvenform secp384r1 im HAN im Kapitel TLSv1.2

A Logische Schnittstellen

A-1 Allgemeine Beschreibung

A-1.1 Datums- und Zeitformate

Datums- und Zeitformate, welche als Parameter für Abfragen verwendet werden, können in Anlehnung an das XML-Format (XSD Date and Time Data Types) angegeben werden.

A-1.1.1 Datumsformat

Das Datumsformat muss in der Form „YYYY-MM-DD" angegeben werden, wobei

- YYYY das Jahr repräsentiert
- MM den Monat repräsentiert
- DD den Tag repräsentiert.

Alle Angaben müssen angegeben werden und sind nicht optional.

Beispiel:

```
2019-01-07
```

Zeitzonen

Um eine Zeitzone zu spezifizieren bestehen folgende Möglichkeiten:

- Eine UTC-Zeit wird mittels anhängen eines „Z" angegeben
- Ein Versatz (Offset) zur UTC-Zeit wird mittels anhängen einer positiven oder negativen Zeit angegeben. Das Format ist mit „hh:mm" definiert.

Beispiele:

```
2019-01-07Z
2019-01-07+1:00
2019-01-07-1:00
```

A-1.1.2 Zeitformat

Das Zeitformat muss in der Form „hh:mm:ss" angegeben werden, wobei

- hh die Stunde repräsentiert
- mm die Minute repräsentiert
- ss die Sekunde repräsentiert.

Beispiel:

```
15:22:45
```

Zeitzonen

Um eine Zeitzone zu spezifizieren bestehen folgende Möglichkeiten:

- Eine UTC-Zeit wird mittels anhängen eines „Z" angegeben
- Ein Versatz (Offset) zur UTC-Zeit wird mittels anhängen einer positiven oder negativen Zeit angegeben. Das Format ist mit „hh:mm" definiert.

Beispiele:

```
15:22:45Z
15:22:45+01:00
15:22:45-01:00
```

A-1.1.3 Datumzeitformat

Das Datumzeitformat muss in der Form „YYYY-MM-DDThh:mm:ss" angegeben werden, wobei

- YYYY das Jahr repräsentiert
- MM den Monat repräsentiert
- DD den Tag repräsentiert
- T den Trenner zwischen Datums- und Zeitangabe repräsentiert
- hh die Stunde repräsentiert
- mm die Minute repräsentiert
- ss die Sekunde repräsentiert.

Beispiel:

```
2019-01-07T15:22:45
```

Zeitzonen

Um eine Zeitzone zu spezifizieren bestehen folgende Möglichkeiten:

- Eine UTC-Zeit wird mittels anhängen eines „Z" angegeben
- Ein Versatz (Offset) zur UTC-Zeit wird mittels anhängen einer positiven oder negativen Zeit angegeben. Das Format ist mit „hh:mm" definiert.

Beispiele:

```
2019-01-07T15:22:45Z
2019-01-07T15:22:45+01:00
2019-01-07T15:22:45-01:00
```

A-1.2 TLSv1.2

Verwendungszweck

Alle TLS-Kanäle im Smart Meter Gateway werden gemäß TLS 1.2 [1] und den Vorgaben aus der TR umgesetzt [2]. Ein Fallback auf eine ältere TLS-Version ist nicht möglich. Die Funktion *Session-Renegotiation* ist deaktiviert und wird im TLS-Handshake nicht angeboten. Fordert ein TLS-Server für eine bestehende Verbindung die *Session-Renegotiation* an, wird diese Verbindung beendet.

Authentifizierung mittels *Mutual Authentication*

Zur Authentifizierung sowohl des Smart Meter Gateway gegenüber der Gegenstelle als auch der Gegenstelle gegenüber dem Smart Meter Gateway wird die *Mutual Authentication* mittels TLS-Zertifikaten verwendet.

Bei der Mutual Authentication authentifizieren sich der Server und der Client gegenseitig im TLS-Handshake (siehe [1]). Um einen verschlüsselten Kanal zu öffnen werden insgesamt 12 Nachrichten verwendet:

1. Der Client sendet die Nachricht **ClientHello**
2. Der Server antwortet mit dem **ServerHello**
3. Der Server schickt sein **Server Zertifikat**
4. Der Server verlangt das Zertifikat des Client in einem **CertificateRequest**, die Verbindung gegenseitig authentifiziert werden kann
5. Der Server bestätigt seine Nachricht mit einem **ServerHelloDone**
6. Der Client antwortet mit seinem **Client Zertifikat**
7. Der Client schickt die Session Key Information in einer **ClientKeyExchange** Nachricht (Verschlüsselt mit dem Public Key des Servers, welche er aus dem Server Zertifikat entnommen hat)
8. Der Client schickt eine **CertificateVerify** Nachricht um den Server wissen zu lassen, dass er der Besitzer des Zertifikats ist
9. Der Client schickt die **ChangeCipherSpec** Nachricht um die gewählte Verschlüsselungsmethode zu bestätigen
10. Der Client schickt eine **Finished** Nachricht, damit der Server die aktivierten Optionen prüfen kann
11. Der Server schickt ebenfalls eine **ChangeCipherSpecNachricht** um die gewählte Verschlüsselungsmethode zu aktivieren
12. Der Server schickt ebenfalls eine **Finished** Nachricht zum Abschluss des Handshakes

Im Anschluss an diesen Handshake ist Client und Server in Besitz der Zertifikate der Gegenstelle und kann weitere Prüfungen mit diesen Zertifikaten durchführen. Beispielsweise existiert im Smart Meter Gateway ein zum Client-Zertifikat passendes Benutzerprofil gilt der Benutzer als authentifiziert. Die Prüfung erfolgt durch Abgleich des im Zertifikat hinterlegten Fingerabdrucks gemäß [2].

Verwendungszweck im WAN

Alle TLS-Kanäle auf den Schnittstellen WAN-1 und WAN-A-T werden in jedem Fall vom Smart Meter Gateway aufgebaut. Die maximale Sitzungslänge beträgt 48h. Dabei nimmt das Smart Meter Gateway die Rolle des TLS-Clients ein.

Verwendungszweck im HAN

Das Smart Meter Gateway agiert im HAN als TLS-Server. Die Maximale Sitzungslänge beträgt dabei 48h. Bei den Schnittstellen IF_GW_CON und IF_GW_SRV gilt eine maximale Leerlaufzeit von 10 Minuten. Nach überschreiten dieser Leerlaufzeit wird die TLS-Sitzung getrennt.

Das Smart Meter Gateway unterstützt im HAN die Kurfenform secp384r1. Alle anderen Kurvenformen werden nicht unterstützt.

Verwendungszweck im LMN

Das Smart Meter Gateway agiert im LMN als TLS-Client. Die maximale Sitzungslänge beträgt dabei 31 Tage. Innerhalb der maximalen Sitzungslänge dürfen nicht mehr als 5 MB (5.000.000 Bytes)[1] übertragen werden. Bei Überschreiten der maximalen Sitzungslänge oder der maximalen Datenmenge wird die TLS-Sitzung getrennt und erneut aufgebaut.

Fehler- und Rückmeldungen

Folgende TLS-Fehlercodes werden vom Smart Meter Gateway als Rückmeldung auf einen TLS-Verbindungsaufbau zurückgeliefert:

Fehlercode	Beschreibung
0	close notify
10	unexpected message
20	bad recorded mac
40	handshake failure
41	no certificate
70	protocol version
86	inapropriate fallback
100	no renegotiation
112	unrecognized name
115	unknown psk identity
120	no application protocol

Tabelle 1: TLS-Fehlercodes

[1] Die Datenmenge bezieht sich auf das Gesamtvolumen der ausgetauschten Nachrichten (ohne die Nachrichten des TLS-Handshakes)

A-2 IF_GW_CON

A-2.1 Zugriff auf Root für M2M-Schnittstelle / Anmeldung

Verwendungszweck

Basis-Zugriff auf M2M-Schnittstelle des Letztverbrauchers zum Auslesen der *userid*.

Art der Verwendung

```
GET /smgw/m2m HTTP/1.1
<header>

<body>
```

Parameter

Parameter	Beschreibung
<header>	Irrelevant, bzw. sofern HTTP Digest Informationen vorliegen, dann diese Informationen nach [3]. Das Feld *Content-Type* muss *application/json* sein.
<body>	Leer

Beschreibung

Dient dazu die *userid* des Letztverbrauchers abzurufen.

Für jeden auf dem System verfügbaren Letztverbraucher wird eine separate *userid* bereitgestellt, die über die Identifizierung des Letztverbrauchers aufrufbar ist. Wird die Authentifizierung über das TLS-Zertifikat durchgeführt, oder liegen dem Befehl im HTTP-Header Digest-Authentifizierungsinformationen (nach [3]) vor, so wird die Anfrage mit dem HTTP StatusCode 307 Temporary Redirect beantwortet. Aus dieser Antwort kann die korrekte userid / POC für den angemeldeten Letztverbraucher entnommen werden.

Fehler- und Rückmeldungen

StatusCode	Beschreibung
307 Temporary Redirect	Die POC muss weitergeleitet werden auf die konkrete POC des angemeldeten Letztverbrauchers. Die konkrete POC muss aus dem *HTTP Location header field* entnommen werden.
401 Unauthorized	Es liegen keine Authentifizierungsinformationen für diesen Befehl vor. Muss sich der Letztverbraucher mittels Benutzernamen und Passwort anmelden kann nun eine neue Anfrage mit den in der Antwort zugrundeliegenden Digest-Authentifizierungsinformationen (nach [3]) durchgeführt werden.

A-2.2 Smart Meter Gateway Informationen über M2M-Schnittstelle

Verwendungszweck

Abruf von Informationen über das Smart Meter Gateway durch den Letztverbraucher.

Art der Verwendung

```
POST /smgw/m2m/<userid>/json HTTP/1.1
<header>

<body>
```

Parameter

Parameter	Beschreibung
<header>	Sofern HTTP Digest Informationen vorliegen, müssen diese Informationen nach [3] angegeben werden. Das Feld *Content-Type* muss *application/json* sein.
<body>	JSON nach [4]:
	{ "method" : "smgw-info" }

Beschreibung

Dient dazu die Daten über das Smart Meter Gateway abzurufen.

Für jeden auf dem System verfügbaren Letztverbraucher wird eine separate *userid* (Kapitel A-2.1) bereitgestellt, die über die Identifizierung des Letztverbrauchers aufrufbar ist.

Wird die Authentifizierung über das TLS-Zertifikat durchgeführt oder liegen dem Befehl im HTTP-Header Digest-Authentifizierungsinformationen (nach [3]) vor, so wird die Anfrage mit dem HTTP StatusCode 200 OK beantwortet und der HTTP-Content enthält die Daten im JSON-Format [4].

Die zurückgelieferten Daten enthalten:

- HUID des Smart Meter Gateway
- Die Firmware-Version
- Der HASH über die Firmware
- Der aktuelle Status des Smart Meter Gateway
- Die aktuelle Systemzeit des Smart Meter Gateway
- Das HAN-Zertifikat

- Die für die Signaturerzeugung der Messwerte verwendeten Zertifikate
- Die für die Signaturerzeugung zugehörigen SubCA-Zertifikate

Die JSON-Schemas der zurückgelieferten Antwort ist in [5] beschrieben.

Fehler- und Rückmeldungen

StatusCode	Beschreibung
200 OK	Die Anfrage war gültig. Der HTTP-Content enthält die Daten im JSON-Format.
400 Bad Request	Die übermittelten Daten sind nicht interpretierbar.
	Die Anfrage kann aufgrund fehlerhafter Parameter im HTTP-Content nicht durchgeführt werden.
	Es sind ungültige HTTP-Header-Informationen übermittelt worden.
401 Unauthorized	Es liegen keine Authentifizierungsinformationen für diesen Befehl vor. Muss sich der Letztverbraucher mittels Benutzernamen und Passwort anmelden kann nun eine neue Anfrage mit den in der Antwort zugrundeliegenden Digest-Authentifizierungsinformationen (nach [3]) durchgeführt werden.
404 Not Found	Der angeforderte Pfad ist nicht vorhanden.
405 Method not allowed	Für die ausgewählte Ressource ist die Methode im Request nicht erlaubt (z.B. GET oder PUT)
500 Internal Server Error	Tritt auf, wenn ein interner Verarbeitungsfehler aufgetreten ist.

Antwort

Parameter	Bedeutung
version	Die Version der JSON-Schnittstelle. Bei späteren Erweiterungen wird die Versionsnummer hochgezählt.
elapsed-time	Wie lange hat die Generierung der JSON-Datei gedauert.
smgw-info.firmwareinfo.component	Auf welchen Bereich bezieht sich Version und Hash
smgw-info.firmware-info.version	Firmwareversion
smgw-info.firmware-info.hash	Hash der Firmware. Dieser Hash wird als SHA-256 über alle Packages gebildet und hexkodiert zurückgegeben
smgw-info.smgw-id	Herstellerübergreifende Identifikationsnummer des DKE
smgw-info.certificates[han].tls	Das auf der HAN-Schnittstelle genutzte X509-TLSZertifikat, wird hexkodiert zurückgegeben
smgw-info.certificates[wan][i].cert-index	Der interne Index des Zertifikats. Der Index 0 kennzeichnet das Gütesiegelzertifikat.
smgw-info.certificates[wan][i].sig	Ein zur Signierung von Messwerten genutztes X509-Zertifikat, wird hexkodiert zurückgegeben
smgw-info.certificates[wan][i].sig	Das zum Signaturzetrifikat gehörende Sub-CA-Zertifikat, wird hexkodiert zurückgegeben

Beispielantwort


```
{
  "elapsed-time": "52 miliseconds",
  "method": "smgw-info",
  "smgw-info": {
    "certificates": {
      "han": {
        "tls": "2d2d2d2d2d...2d2d2d2d2d0a"
      },
      "wan": [
        {
          "cert-index": "0",
          "sig": "3082024630...09d5d90799",
          "sub-ca": "3082025230...c94a13f256"
        },
        {
          "cert-index": "1",
          "sig": "3082024c30...675604f434",
          "sub-ca": "3082024230...c9918e247f"
```

```
          }
        ]
      },
      "firmware-info": {
        "component": "Firmware",
        "hash":
"b27dfcc0fbcf8939071ca5e6584e8dc3ce32b06b960316c3432018046bb2cc44",
        "version": "v3.25.2"
      },
      "smgw-id": "ethe0300004261",
      "smgw-state": "a0000000",
      "smgw-time": "2019-05-03T10:55:44"
    },
    "version": "1.2.0"
}
```

A-2.3 Vertragsdaten laden über M2M-Schnittstelle

Verwendungszweck

Abruf der Vertragsdaten des Letztverbrauchers.

Art der Verwendung

```
POST /smgw/m2m/<userid>/json HTTP/1.1
<header>

<body>
```

Parameter

Parameter	Beschreibung
<header>	Sofern HTTP Digest Informationen vorliegen, müssen diese Informationen nach [3] angegeben werden. Das Feld *Content-Type* muss *application/json* sein.
<body>	JSON nach [4]:

	`{`
	`  "method" : "user-info"`
	`}`

Beschreibung

Dient dazu die Vertragsdaten des Letztverbrauchers abzurufen.

Für jeden auf dem System verfügbaren Letztverbraucher wird eine separate *userid* (Kapitel A-2.1) bereitgestellt, die über die Identifizierung des Letztverbrauchers aufrufbar ist.

Wird die Authentifizierung über das TLS-Zertifikat durchgeführt oder liegen dem Befehl im HTTP-Header Digest-Authentifizierungsinformationen (nach [3]) vor, so wird die Anfrage mit dem HTTP StatusCode 200 OK beantwortet und der HTTP-Content enthält die Daten im JSON-Format [4].

Die zurückgelieferten Daten enthalten:

- Eine Liste aller Tarife des Letztverbrauchers (*usage-point-id*) inklusive Tarifinformationen
- Die Liste der Abrechnungsperioden (*billingperiod*) für alle Tarife des Letztverbrauchers

Die JSON-Schemas der zurückgelieferten Antwort ist in [5] beschrieben.

Fehler- und Rückmeldungen

StatusCode	Beschreibung
200 OK	Die Anfrage war gültig. Der HTTP-Content enthält die Daten im JSON-Format.
400 Bad Request	Die übermittelten Daten sind nicht interpretierbar.
	Die Anfrage kann aufgrund fehlerhafter Parameter im HTTP-Content nicht durchgeführt werden.
	Es sind ungültige HTTP-Header-Informationen übermittelt worden.
401 Unauthorized	Es liegen keine Authentifizierungsinformationen für diesen Befehl vor. Muss sich der Letztverbraucher mittels Benutzernamen und Passwort anmelden kann nun eine neue Anfrage mit den in der Antwort zugrundeliegenden Digest-Authentifizierungsinformationen (nach [3]) durchgeführt werden.
404 Not Found	Der angeforderte Pfad ist nicht vorhanden.
405 Method not allowed	Für die ausgewählte Ressource ist die Methode im Request nicht erlaubt (z.B. GET oder PUT)
500 Internal Server Error	Tritt auf, wenn ein interner Verarbeitungsfehler aufgetreten ist.

Antwort

Wert	Bedeutung
version	Die Version der JSON- Schnittstelle. Bei späteren Erweiterungen wird die Versionsnummer hochgezählt.
elapsed-time	Wie lange hat die Generierung der JSON-Datei gedauert.
usage-points[n].billingPeriods[i].start-time	Start-Zeitpunkt einer Abrechnungsperiode.
usage-points[n].billingPeriods[i].end-time	End-Zeitpunkt einer Abrechnungsperiode.
usage-points[n].capture-time	Der Erfassungszeitpunkt der Auslesung
usage-points[n].delivery-id	
usage-points[n].end-time	Bis wann ist der Tarifanwendungsfall gültig, kann auch leer sein.
usage-points[n].meter[m].meter-id	Name eines mit dem Tarifanwendungsfall verbundenen Zählers.
usage-points[n].metering-point-id	Name des Messpunktes.
usage-points[n].on-demand-profileconfigured	Gibt an, ob ein On-Demand-Profil konfiguriert wurde.
usage-points[n].start-time	Ab wann ist der Tarifanwendungsfall gültig.
usage-points[n].taf-number	Welcher Tarifanwendungsfall wird hier unterstützt.
usage-points[n].taf-state	Status des Tarifanwendungsfalls. Mögliche Werte: „ready", „running", „archive"
usage-points[n].usage-point-id	Der vollständige LogicalName eines Tarifanwendungsfall.
usage-points[n].usage-point-name	Der dem Letztverbraucher bekannte Name eines Tarifanwendungsfall.

Beispielantwort


```
{
  "elapsed-time": "1471 miliseconds",
  "method": "user-info",
  "user-info": {
    "usage-points": [
      {
        "billing-Periods": [
          {
            "end-time": "2019-05-03T08:45:00Z",          "start-time": "2019-
05-03T08:30:00Z"
```

```
            },
            {
              "end-time": "2019-05-03T09:00:00Z",
              "start-time": "2019-05-03T08:45:00Z"
            }
          ],
          "capture-time": "00:00:00",
          "delivery-id": "emt1",
          "end-time": "",
          "meter": [
            {
              "meter-id": "0551010038180402"
            }
          ],
          "metering-point-id": "DE00000000000000000000000000000000",
          "on-demand-profile-configured": "true",
          "start-time": "2019-04-18T10:45:00Z",
          "taf-number": "1",
          "taf-state": "ready",
          "usage-point-id": "01005e318021.taf1-1.sm",
          "usage-point-name": "taf1"
        }
      ]
    },
    "version": "1.2.0"
}
```

A-2.4 Abruf von Informationen eines Vertrages über M2M-Schnittstelle

Verwendungszweck

Abruf von Informationen eines Vertrages durch den Letztverbraucher.

Art der Verwendung

```
POST /smgw/m2m/<userid>/json HTTP/1.1
<header>

<body>
```

Parameter

Parameter	Beschreibung
<header>	Sofern HTTP Digest Informationen vorliegen, müssen diese Informationen nach [3] angegeben werden. Das Feld *Content-Type* muss *application/json* sein.
<body>	JSON nach [4]:
	`{ "method" : "usage-point-info", "usage-point-id" : "<usage-point-id>", "database": "<database>" }`

JSON-Parameter	Beschreibung	Typ
<usage-point-id>	Ausgewählter Vertrag. Kann über A-2.3 abgerufen werden.	String
<database>	*Optional:* Die zu lesende Messwertliste. Wenn nicht angegeben werden die Werte von allen Messwertlisten zurückgeliefert. Mögliche Werte sind: origin – Die Originäre Messwertliste derived – Die Abgeleitete Messwertliste calculated – Nur bei TAF2: Tarifumschaltmesswertliste daily – Liste der Tageswerte	String

Beschreibung

Dient dazu die Daten über die Daten eines einzelnen Vertrages abzurufen.

Für jeden auf dem System verfügbaren Letztverbraucher wird eine separate *userid* (Kapitel A-2.1) bereitgestellt, die über die Identifizierung des Letztverbrauchers aufrufbar ist.

Wird die Authentifizierung über das TLS-Zertifikat durchgeführt oder liegen dem Befehl im HTTP-Header Digest-Authentifizierungsinformationen (nach [3]) vor,

so wird die Anfrage mit dem HTTP StatusCode 200 OK beantwortet und der HTTP-Content enthält die Daten im JSON-Format [4].

Die zurückgelieferten Daten enthalten:

- Die für den Tarif vorhandenen Tarifstufeninformationen inklusive der Messkanäle (*channels*)
- Das aktuell gültige TAF-Profil

Die JSON-Schemas der zurückgelieferten Antwort ist in [5] beschrieben.

Fehler- und Rückmeldungen

StatusCode	Beschreibung
200 OK	Die Anfrage war gültig. Der HTTP-Content enthält die Daten im JSON-Format.
400 Bad Request	Die übermittelten Daten sind nicht interpretierbar.
	Die Anfrage kann aufgrund fehlerhafter Parameter im HTTP-Content nicht durchgeführt werden.
	Es sind ungültige HTTP-Header-Informationen übermittelt worden.
401 Unauthorized	Es liegen keine Authentifizierungsinformationen für diesen Befehl vor. Muss sich der Letztverbraucher mittels Benutzernamen und Passwort anmelden kann nun eine neue Anfrage mit den in der Antwort zugrundeliegenden Digest-Authentifizierungsinformationen (nach [3]) durchgeführt werden.
404 Not Found	Der angeforderte Pfad ist nicht vorhanden.
405 Method not allowed	Für die ausgewählte Ressource ist die Methode im Request nicht erlaubt (z.B. GET oder PUT)
500 Internal Server Error	Tritt auf, wenn ein interner Verarbeitungsfehler aufgetreten ist.

Antwort

Wert	Bedeutung
version	Die Version der JSON-Schnittstelle. Bei späteren Erweiterungen wird die Versionsnummer hochgezählt.
elapsed-time	Wie lange hat die Generierung der JSON-Datei gedauert.
usage-point-info.databases.channels[n].obis	Der Obiswert für diesen Kanal. Hiermit kann dieser Kanal identifiziert werden.
usage-point-info.databases.channels[n].scaler	Der Scaler für diesen Kanal gemäß DIN 62056-62.
usage-point-info.databaseinfo.channels[n].unit	Die Einheit für diesen Kanal gemäß DIN 62056-62.
usage-point-info.databases.database	Auf welche Datenbank bezieht sich die folgende Angabe von databaseinfo.records
usage-point-info.taf-profile	Das dem Tarifanwendungsfall entsprechende DKEXML-Profil wird hier in einen CMS-Container mit dem aktuellen Gütesiegelzertifikat signiert und hexkodiert übertragen. Wird von Prüfsoftware zur Verfizierung von Tarifumschaltpunkten und Abgleich der Vertragsdaten durch den Letztverbraucher benötgt.
transparency-bit	Gibt an, ob das Transparenz-Bit innerhalb des TAF gesetzt wurde.
usage-point-info.usage-point-id	Der vollständige LogicalName des Tarifanwendungsfalls.
usage-point-info.usage-point-name	Der Name des Tarifanwandungsfalls.

Beispielantwort

```
{
  "elapsed-time": "923 miliseconds",
  "method": "usage-point-info",
  "usage-point-info": {
    "databases": [
      {
        "channels": [
          {
            "obis": "0100010800ff",
            "scaler": "-1",
            "unit": "30"
          }
        ],
        "database": "origin"
      }
    ],
```

```
      "emts": [
        "emt1.sm"
      ],
      "taf-profile": "3082116b06092a86488...",
      "transparency-bit": "true",
      "usage-point-id": "01005e318021.taf1-1.sm",
      "usage-point-name": "taf1"
    },
    "version": "1.2.0"
}
```

A-2.5 Abruf von Logdaten über die M2M-Schnittstelle

Verwendungszweck

Abruf des Letztverbraucherlogbuchs des Letztverbrauchers.

Art der Verwendung

```
POST /smgw/m2m/<userid>/json HTTP/1.1
<header>

<body>
```

Parameter

Parameter	Beschreibung
<header>	Sofern HTTP Digest Informationen vorliegen, müssen diese Informationen nach [3] angegeben werden. Das Feld *Content-Type* muss *application/json* sein.

<body>	JSON nach [4]:
	`{`
	`"method" : "log",`
	`"fromtime" : "<fromtime>",`
	`"totime" : "<totime>",`
	`"fromindex" : "<fromindex>",`
	`"count" : <count>`
	`}`

JSON-Parameter	Beschreibung	Typ
<fromtime>	*Optional:* Startzeitpunkt der angeforderten Daten mit t>=fromtime. Wenn nicht angegeben, wird hier der Zeitpunkt des ältesten Logeintrags verwendet. Format gemäß A-1.1.3.	String
<totime>	*Optional:* Endzeitpunkt der angeforderten Daten mit t<totime. Wenn nicht angegeben, wird hier die aktuelle Systemzeit des Smart Meter Gateways verwendet. Format gemäß A-1.1.3.	String
<fromindex>	*Optional:* Angabe des Logeintrag-Index ab welchem abgefragt wird. Wenn nicht angegeben, wird hier der Index des ältesten Logeintrags verwendet.	integer (positive Ganzzahl)
<count>	*Optional:* Angabe der Anzahl der Log-Einträge, die abgefragt werden. Maximal erlaubt sind 1500 Einträge. Wenn nicht angegeben, werden maximal 1500 Logeinträge zurückgeliefert.	integer (positive Ganzzahl)

Beschreibung

Dient dazu das Letztverbraucherlogbuch für den Letztverbraucher abzurufen.

Folgende Kombinationen von fromtime, totime, fromindex und count sind erlaubt:

- fromtime
- totime
- fromtime und totime
- fromindex
- count
- fromindex und count
- fromtime und count
- fromtime, totime und count

Wird keiner der optionalen Parameter fromtime, totime, fromindex und count angegeben werden ab dem ältesten Logeintrag maximal 1500 Einträge zurückgegeben.

Es können pro Anfrage maximal 1500 Einträge ausgelesen werden. Wird der Parameter *count* nicht angegeben liefert das Smart Meter Gateway alle Einträge maximal jedoch 1500 Einträge zurück.

Für jeden auf dem System verfügbaren Letztverbraucher wird eine separate *userid* (Kapitel A-2.1) bereitgestellt, die über die Identifizierung des Letztverbrauchers aufrufbar ist.

Wird die Authentifizierung über das TLS-Zertifikat durchgeführt oder liegen dem Befehl im HTTP-Header Digest-Authentifizierungsinformationen (nach [3]) vor, so wird die Anfrage mit dem HTTP StatusCode 200 OK beantwortet und der HTTP-Content enthält die Daten im JSON-Format [4].

Die zurückgelieferten Daten enthalten:

- Alle angefragten Logeinträge

Die JSON-Schemas der zurückgelieferten Antwort ist in [5] beschrieben.

Fehler- und Rückmeldungen

StatusCode	Beschreibung
200 OK	Die Anfrage war gültig. Der HTTP-Content enthält die Daten im JSON-Format.
400 Bad Request	Die übermittelten Daten sind nicht interpretierbar.
	Die Anfrage kann aufgrund fehlerhafter Parameter im HTTP-Content nicht durchgeführt werden.
	Es sind ungültige HTTP-Header-Informationen übermittelt worden.
401 Unauthorized	Es liegen keine Authentifizierungsinformationen für diesen Befehl vor. Muss sich der Letztverbraucher mittels Benutzernamen und Passwort anmelden kann nun eine neue Anfrage mit den in der Antwort zugrundeliegenden Digest-Authentifizierungsinformationen (nach [3]) durchgeführt werden.
404 Not Found	Der angeforderte Pfad ist nicht vorhanden.
405 Method not allowed	Für die ausgewählte Ressource ist die Methode im Request nicht erlaubt (z.B. GET oder PUT)
500 Internal Server Error	Tritt auf, wenn ein interner Verarbeitungsfehler aufgetreten ist.

Antwort

Wert	Bedeutung
version	Die Version der JSON- Schnittstelle. Bei späteren Erweiterungen wird die Versionsnummer hochgezählt.
elapsed-time	Wie lange hat die Generierung der JSON-Datei gedauert.
log.entries[n].record-number	Eindeutige Nummer des Logeintrags
log.entries[n].event-id	Ereignisnummer des Events
log.entries[n].event-sub-id	Ereignisunternummer des Events
log.entries[n].level	Schweregrad des Events
log.entries[n].outcome	Auslöser des Events
log.entries[n].vendor-id	Organisation, welche den Logeintrag definiert hat
log.entries[n].subject-identity	Auslöser der Lognachricht
log.entries[n].user-identity	Der dem Ereignis zugeordnete Letztverbraucher
log.entries[n].level	Loglevel für diesen Eintrag. Der Level wird aufgrund des Schweregrades des auslösenden Ereignisses in folgende Werte aufgeteilt: Alert = 4 Error = 3 Warning = 2 Informational = 1
Log.entries[n].time	Zeitstempel, zu dem der Logeintrag angelegt wurde
Log.records	Anzahl der übertragenen Logeinträge

Beispielantwort


```
{
  "elapsed-time": "220 miliseconds",
  "log": {
    "entries": [
      {
        "event-id": "16001",
        "event-sub-id": "0",
```

```
            "index": "1830",
            "level": "6",
            "message": "Es wurden 359 Messwerte an den Marktteilnehmer für den Zeitraum
2019-08-23T12:09:10+02:00 (Id=18335) bis 2019-08-23T13:09:00+02:00 (Id=18693)
übertragen.",
            "outcome": "0",
            "subject-identity": "01005e318027.taf7-60.sm",
            "time": "2019-08-23T11:09:48Z",
            "user-identity": "01005e318011.consumer1.sm",
            "vendor-id": "BSI",
            "version": "1"
          }
       ],
       "records": "1"
    },
    "method": "log",     "version": "1.2.0"
}
```

A-2.6 Abruf von Messwerten über die M2M-Schnittstelle

Verwendungszweck

Abruf von Messwerten durch den Letztverbraucher.

Art der Verwendung

```
POST /smgw/m2m/<userid>/json HTTP/1.1
<header>

<body>
```

Parameter

Parameter	Beschreibung
<header>	Sofern HTTP Digest Informationen vorliegen, müssen diese Informationen nach [3] angegeben werden. Das Feld *Content-Type* muss *application/json* sein.

<body>	JSON nach [4]:
	`{`
	`"method" : "readings",`
	`"usage-point-id": "<usage-point-id>",`
	`"database": "<database>",`
	`"channels": <channels>,`
	`"last-reading": <last-reading>,`
	`"fromtime": "<fromtime>",`
	`"totime": "<totime>"`
	`}`

JSON-Parameter	Beschreibung	Typ
<usage-point-id>	Ausgewählter Vertrag. Kann über A-2.3 abgerufen werden.	String
<database>	Die zu lesende Messwertliste. Mögliche Werte sind: origin: Die Originäre Messwertliste derived: Die Abgeleitete Messwertliste calculated: Nur bei TAF2: Tarifumschaltmesswertliste daily: Liste der Tageswerte	String
<channels>	*Optional:* Eine Liste von Objekten über die gewünschten Messkanäle (aus A-2.4) des ausgewählten Vertrags. Das Objekt hat den Namen *channel*. Der Wert des gewünschten Messkanal als String. Wenn nicht angegeben, werden alle vorhandenen Werte zurückgeliefert. Beispiel: `"channel" : "0100010800ff"`	Array

JSON-Parameter	Beschreibung	Typ
<last-reading>	Wenn *true* wird nur der letzte Werte aus der Datenbank entnommen. Hier werden die Parameter <fromtime> und <totime> ignoriert.	Bool
<fromtime>	Startzeitpunkt der angeforderten Daten mit t>fromtime. Format gemäß A-1.1.3.	String
<totime>	Endzeitpunkt der angeforderten Daten mit t<=totime Format gemäß A-1.1.3.	String

Beschreibung

Dient dazu die angefragten Messdaten für den Letztverbraucher zu übertragen.

Für jeden auf dem System verfügbaren Letztverbraucher wird eine separate *userid* (Kapitel A-2.1) bereitgestellt, die über die Identifizierung des Letztverbrauchers aufrufbar ist.

Der maximal anzufragende Zeitraum zwischen Startzeitpunkt (<fromtime>) und Endzeitpunkt (<totime>) ist auf 31 Tage pro Anfrage begrenzt.

Wird die Authentifizierung über das TLS-Zertifikat durchgeführt oder liegen dem Befehl im HTTP-Header Digest-Authentifizierungsinformationen (nach [3]) vor, so wird die Anfrage mit dem HTTP StatusCode 200 OK beantwortet und der HTTP-Content enthält die Daten im JSON-Format [4].

Die zurückgelieferten Daten enthalten:

- Die angeforderten Messwerte inklusive gebildeter Signatur des angefragten Zeitraums innerhalb <fromtime> bis <totime> bei <last-reading> = false
- Der letzte Wert der Messwert inklusive gebildeter Signatur bei <last-reading> = true

Die JSON-Schemas der zurückgelieferten Antwort ist in [5] beschrieben.

Fehler- und Rückmeldungen

StatusCode	Beschreibung
200 OK	Die Anfrage war gültig. Der HTTP-Content enthält die Daten im JSON-Format.
400 Bad Request	Die übermittelten Daten sind nicht interpretierbar.
	Die Anfrage kann aufgrund fehlerhafter Parameter im HTTP-Content nicht durchgeführt werden.
	Der Zeitraum der Anfrage von <fromtime> bis <totime> überschreitet den maximal gültigen Zeitraum.
	Es sind ungültige HTTP-Header-Informationen übermittelt worden.
401 Unauthorized	Es liegen keine Authentifizierungsinformationen für diesen Befehl vor. Muss sich der Letztverbraucher mittels Benutzernamen und Passwort anmelden kann nun eine neue Anfrage mit den in der Antwort zugrundeliegenden Digest-Authentifizierungsinformationen (nach [3]) durchgeführt werden.
404 Not Found	Der angeforderte Pfad ist nicht vorhanden.
405 Method not allowed	Für die ausgewählte Ressource ist die Methode im Request nicht erlaubt (z.B. GET oder PUT)
500 Internal Server Error	Tritt auf, wenn ein interner Verarbeitungsfehler aufgetreten ist.

Antwort

Wert	Bedeutung
version	Die Version der JSON-Schnittstelle. Bei späteren Erweiterungen wird die Versionsnummer hochgezählt.
elapsed-time	Wie lange hat die Generierung der JSON-Datei gedauert.
readings.channnels[n].obis	Der Obiswert für diesen Kanal
readings.channnels[n].readings[m].captu reTime	Der Zeitpunkt zu dem dieser Messwert im Smart Meter Gateway aufgenommen wurde
readings.channnels[n].readings[m].cose m-status	Das Kombinierte Statuswort des SMGW
readings.channnels[n].readings[m].meter -status	Das Statuswort des Zählers
readings.channnels[n].readings[m].owne rNumber	Von wem wurde dieser Werte gebildet. Bei Werten aus dem Zähler ist hier die ZählerId vermerkt, bei berechneten Werte der Tarifanwendungsfall
readings.channnels[n].readings[m].signa ture	Signatur des Messwertes gemäß Bildungsvorschrift
readings.channnels[n].readings[m].SMG wStatus	Status des Smart Meter Gateway gemäß Bildungsvorschrif
readings.channnels[n].readings[m].target Time	Der Endpunkt der Messeperiode des Tarifanwendungsfall zu dem ein Messwert gebildet werden soll
readings.channnels[n].readings[m].value	Zählwerkstand, ergibt mit Unit und Scaler den absoluten Wert
readings.records	Anzahl der übertragenden Messwerte

Beispielantwort


```
{
  "elapsed-time": "229 miliseconds",
  "method": "readings",
  "readings": {
    "channels": [
      {
        "obis": "0100010800ff.0551010038180402.sm",
        "readings": [
          {
            "capture-time": "2019-04-18T14:25:44Z",
```

```
                "cosem-status": "e002000000000000",
                "meter-status": "00000000",
                "owner-number": "taf1-1.sm",
                "signature": null,
                "smgw-status": "e0020000",
                "target-time": "2019-05-03T07:30:00Z",
                "value": "1555597539"
              }
            ]
          }
      ],
      "records": "1"
    },
    "version": "1.2.0"
}
```

A-2.7 Selbsttest auslösen

Verwendungszweck

Auslösen eines Selbsttest.

Art der Verwendung

```
POST /smgw/m2m/<userid>/json HTTP/1.1
<header>

<body>
```

Parameter

Parameter	Beschreibung
<header>	Sofern HTTP Digest Informationen vorliegen, müssen diese Informationen nach [3] angegeben werden. Das Feld *Content-Type* muss *application/json* sein.
<body>	JSON nach [4]:

	`{`
	`  "method" : "self-test"`
	`}`

Beschreibung

Löst den Selbsttest auf dem Smart Meter Gateway aus. Das Ergebnis des Selbsttests wird im Letztverbraucherlogbuch eingetragen und muss dort abgefragt werden. Der Selbsttest kann nur mindestens 10 Minuten nach der Ausführung des letzten Selbsttests erneut ausgelöst werden.

Die JSON-Schemas der zurückgelieferten Antwort ist in [5] beschrieben.

Fehler- und Rückmeldungen

StatusCode	Beschreibung
200 OK	Der Selbsttest konnte ausgelöst werden.
400 Bad Request	Die übermittelten Daten sind nicht interpretierbar.
	Die Anfrage kann aufgrund fehlerhafter Parameter im HTTP-Content nicht durchgeführt werden.
	Es sind ungültige HTTP-Header-Informationen übermittelt worden.
401 Unauthorized	Es liegen keine Authentifizierungsinformationen für diesen Befehl vor. Muss sich der Letztverbraucher mittels Benutzernamen und Passwort anmelden kann nun eine neue Anfrage mit den in der Antwort zugrundeliegenden Digest-Authentifizierungsinformationen (nach [3]) durchgeführt werden.
403 Forbidden	Selbsttest wird bereits ausgeführt
	Die letzte Ausführung liegt nicht länger als 10 Minuten zurück.

StatusCode	Beschreibung
404 Not Found	Der angeforderte Pfad ist nicht vorhanden.
405 Method not allowed	Für die ausgewählte Ressource ist die Methode im Request nicht erlaubt (z.B. GET oder PUT)
500 Internal Server Error	Tritt auf, wenn ein interner Verarbeitungsfehler aufgetreten ist.

I. Abkürzungsverzeichnis

Abkürzung	Beschreibung
BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
CLS	Controllable Local System
COSEM	Companion Specification for Energy Metering
CRMF	Certificate Request Message Format
CSR	Certificate Signing Request
DLMS	Device Language Message Specification
DNS	Domain Name System
EMT	Externer Marktteilnehmer
ETSI	European Telecommunications Standard Institute
GWA	Gateway Administrator
HTML	Hypertext Markup Language
HTTP	Hypertext Transfer Protocol
HUID	Herstellerübergreifende Eigentumsnummer
IP	Internet Protocol
ICMP	Internet Control Message Protocol
JSON	JavaScript Object Notation
IKD	Initiale Konfigurationsdatei
LKD	Lieferkonfigurationsdatei
LV	Letztverbraucher
MAC	Message Authentication Code
NTP	Network Time Protocol
OID	Object Identifier
OMS	Object Identification System
PLMN	public land mobile network
PPP	Point-to-Point Protocol
PTB	Physikalisch Technische Bundesanstalt
POC	Point of Contact
RR	Ressource Record
SFR	Security Function Requirement
SML	Smart Message Language
SRV	Service Techniker
SYM	SYM ist ein feststehender Begriff eines Protokolls, welches an der IF_GW_MTR/HDLC zum Einsatz kommt
TCP	Transmission Control Protocol
TOE	Target of Evaluation
TR	Technische Richtlinie
TRuDI	Transparenz- und Displaysoftware
TSFI	TOE Security Functionality Interface
UART	Universal Asynchronous Receiver Transmitter
UDP	User Datagram Protocol

Abkürzung	Beschreibung
XML	Extensible Markup Language
XSD	XML Schema Definition

II. Literaturverzeichnis

[1] **Dierks, T. und Rescorla, E.** *RFC 5246: The Transport Layer Security (TLS) Protocol Version 1.2.* 2008.

[2] **BSI.** *TR-03116-3: Kryptographische Vorgaben für Projekte der Bundesregierung - Teil 3: Intelligente Messsysteme.* 2018.

[3] **Franks, J., et al., et al.** *RFC 2617: HTTP Authentication: Basic and Digest Access Authentication.* 1999.

[4] **IETF Trust.** *RFC 8259: The JavaScript Object Notation (JSON) Data Interchange Format.* 2017.

[5] **Theben AG.** *Smart Meter Gateway - CONEXA 3.0, TOE Design Specification (ADV_TDS.3).*