Federatie van de elektriciteits- en gasnetbeheerders in België
Fédération des gestionnaires de réseaux électricité et gaz en Belgique

C8/06

General technical requirements

Measurement system and Gateway for an aFRR service delivery point connected to the Distribution Grid

version 2.2

1 Version change log

Version 1.0 – Initial version - January 2020

Version 1.1 – Minor changes – 13/03/2020

Version 2.0 – Changes – 6/04/2020

Version 2.1 – Update on Gateway technical requirements – 12/05/2020

Version 2.11 – Adding contacts – 25/05/2020

Version 2.2 – Additional changes gateway – 12/06/2020

2 Introduction

2.1 Subject of prescription C8/06

In the new aFRR design, a real-time data exchange of measured data and collection of parameters, used for the aFRR-settlement process is required for service delivery points (i.e. delivery points for which ELIA does not receive MW daily schedules) participating in the aFRR service.

Private measurement devices must send the data, via gateways, directly to Communication Platform (CP). The gateways (GW) have to be installed locally within the premise of the grid user and must have direct connection with the Communication Platform.

More information regarding the gateways and related processes can be found in the explanatory note C8/07.

To secure this data and the platform, we will deploy multiple mechanisms with respect to the data exchange (E2E encryption of the measured data between the gateway and the FlexHub, certificate-based authentication) and require the upload on the real-time Communication Platform Web Portal of specific security-related technical documentation for each gateway model.

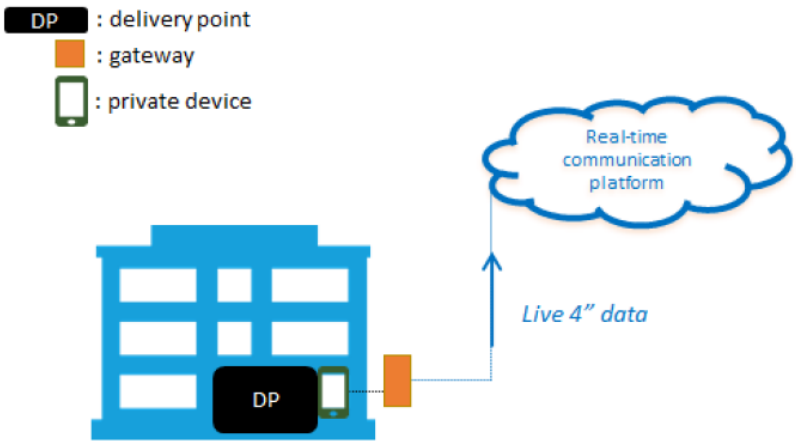


figure 1: general view

The present prescription C8/06:

- is limited to aFRR service delivery points connected to the distribution grid.
- defines on the one hand minimal technical and regulatory requirements for a measurement system (= measurement device including its accessories) when the transfer of energy is not applicable. When transfer of energy is well applicable to the flexibility product, a new analysis of the specific requirements will be performed and could lead to changes of to the present prescription.

- describes on the other hand the technical framework related to the management of the gateways and delivery points (SDPs) and their interaction with the real-time Communication Platform.

Remark:

- URL's for integration test environment and production environment will be communicated later on, before the integration testing phase.

2.2 Asset configurations

The following configurations are authorised (see figure 2):

1. A single gateway transmits real-time data from one SDP measured by a measurement device.
2. A single gateway transmits real-time data from multiple SDPs measured by measurement devices.

In both configurations,

a. The private measurement device is located at the SDP. The SDP can also be defined at the level of the headpoint/access point.

b. The connection of a single gateway to SDPs located on two or more access points is not allowed.

c. A gateway must collect every 4s, the instantaneous power measurement values of a measurement device and other necessary parameters required for the aFRR services, and communicate this in real-time to the real-time Communication Platform using the communication protocol determined by Elia.

d. The communication from gateway to Communication Platform is to be done without an intermediate third-party communication system.

e. The gateways always have to be installed locally within the premise of the grid user which is delimited by the headpoint/access point.

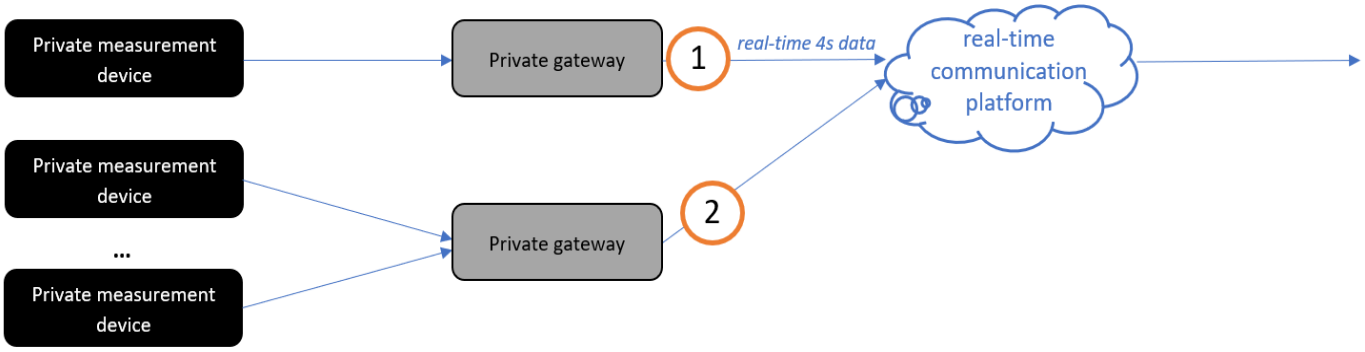


figure 2: schematic view

A local gateway being directly connected to the Real-Time Communication Platform (as described in point d & e above), is the final requirement. A transition period related to the final technical requirement is introduced for maximum one year starting on the go-live of the aFRR design foreseen on the 1st of September 2020. The transition period is foreseen until the 31st of August 2021 at the latest.

This transition period implies that a temporary deviation of the final technical requirement above (i.e. point d & e above) is permitted (acceptance of a degraded mode). This temporary deviation permits the use of a connection via **centralized virtual gateways** to the real-time Communication Platform.

The data will still be sent per delivery point, each delivery point being linked to a separate virtual gateway, to the Communication Platform. All specifications written in this document and corresponding business processes remain valid and must be complied with. At the end of the transition period, all participants need to comply with the final requirements, whereby gateways must be installed locally and connected directly to Communication Platform.

3 Requirements measurement systems

Unless specified in the Technical Regulations for the Distribution Grid according to the Region, the private measurement system shall meet the following minimum requirements:

- The accuracy class of the measurement core of the current transformers (CT) should at least be in line with the requirements of the current transformers for the energy metering as specified in the current Technical Regulations for the Distribution Grid.

- The accuracy class of the measurement core of the voltage transformers (VT) should at least be in line with the requirements of the voltage transformers for the energy metering as specified in the current Technical Regulations for the Distribution Grid.

- The distribution system operator will check the accuracy of the CTs and VTs.

- The accuracy class of the measurement system for the 4s power measurements should be in line with the requirements of the energy metering as specified in the Technical Regulations for the Distribution Grid in force.

- The measurement system must have a sampling rate which allows to give a new value exactly each 4s. Sampling rate must be $1/2^n$ times the 4s interval (with n as an integer > 0).

- As required by Synergrid technical requirement C2/112, any cable connecting the current and voltage transformer to a measurement device is of type LIYY and must comply with following requirements regarding section and length:

Electrical length of cable	**Voltage circuit**	**Current circuit**
< 8m (minimum 3m)	4 x 2,5 mm² Cu	6 x 2,5 mm² Cu

≥ 8m (maximum 18m)	4 x 2,5 mm² Cu	6 x 4 mm² Cu

The connection of the cables between the transformers and the measurement device must be continuous (without any junction, nor intermediate connection strips) and executed according to article 4.4.2.2. of the AREI/RGIE.
The connection wires to current and voltage transformers shall not be part of the same cable.

- A system of 2 or 3 current/voltage transformers is allowed (two- or three-wattmeter method) but the three-wattmeter method is preferred.

- The installation must be properly grounded.

- Precision control of the measurement system is mandatory every 5 years following technical specifications of the distribution system operators. A copy of the report shall be transmitted to the distribution system operator.

- The relevant system operator has the right to perform an ad-hoc on-site audit at any time.

4 Requirements gateways

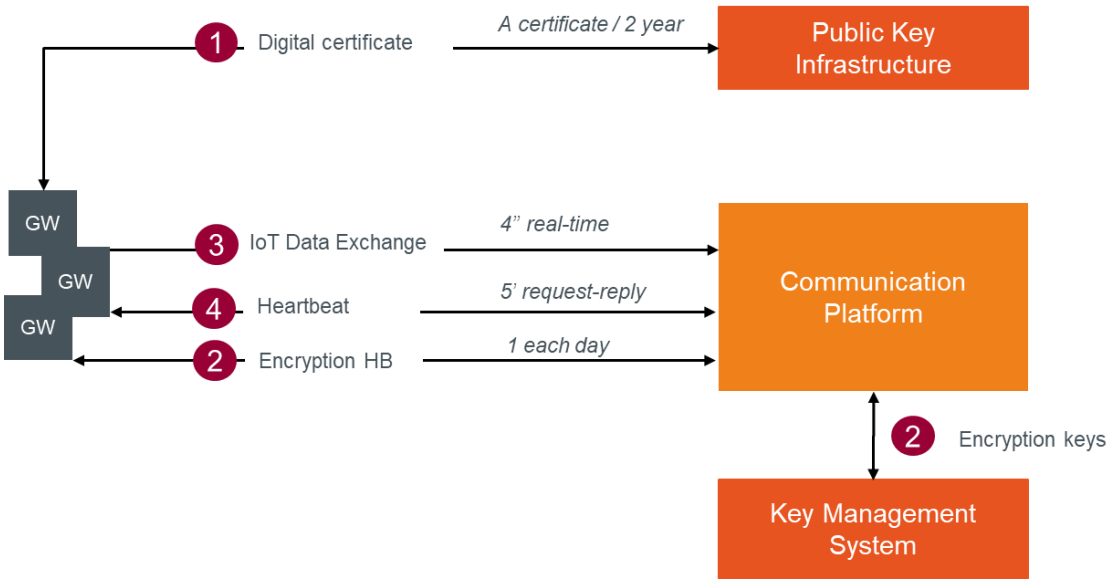
4.1 Data exchange specifications

This section describes the detailed data exchange interface specifications to exchange data between the gateways, the Communication Platform and the security components. In the first version of the platform, the exchange of aFRR data is unidirectional (except for the heartbeat) from the gateways via the aFRR Communication Platform to the Flexhub. The message flow will consist of real-time 4s aFRR messages, used for the settlement of aFRR activations. One message will be sent for each delivery point connected to a gateway.

The security mechanisms allow a reliable and secure data exchange: the Public Key Infrastructure (PKI) allows certificate-based authentication of the gateways and the Key Management System distributes encryption keys that can be used to encrypt the aFRR message body.

4.1.1 Data flows

Below a visualisation of the E2E process flow of all data exchanges the gateways must be able to support.



1. Each gateway and application that will connect to the Communication Platform will need to acquire a digital certificate from the Public Key Infrastructure (valid for 2 years). This certificate is used to authenticate the gateway for all connections to the platform and Key Management System.

2. The data (body) has to be end-to-end encrypted (from the gateway to the FlexHub). Every day, an independent Key Management System (KMS) will generate encryption keys to be used for message body encryption and will send these via the Communication Platform to the gateways.

3. Every 4 seconds, an aFRR message with encrypted body is send by the gateway to the Communication Platform. To be able to connect and publish the message on the queue, the gateways must have a digital certificate retrieved from the Public Key Infrastructure (PKI).

4. At regular interval (initially every 5 minutes), the Communication Platform will put a heartbeat message on the topic to which the gateway must reply. The message includes key values for specific use cases and for gateway connection status updates.

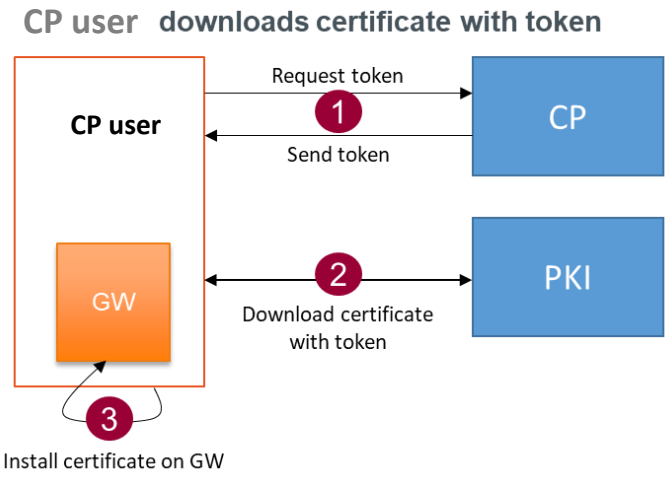
Message queues enable asynchronous communication, which means that the endpoints that are producing and consuming messages interact with the queue, not each other. In contrast to queues, in which each message is processed by a single consumer, **topics** and subscriptions provide a one-to-many form of communication, in a publish/ subscribe pattern.
The data exchange between the gateway and the Communication Platform will be done using two different topics (1 topic for each direction).

4.1.2 Interfaces

4.1.2.1 Certificate-based authentication

The following scenarios will be provided for acquisition of tokens and certificates:

Scenario 1: Acquisition of the Certificate through the portal



1. The CP user requests a token via an action in the user interface of the portal for a gateway. A validation code will be generated and shown in the portal in the concerned gateway information screen, and a mail will be sent to the CP user with a token.
2. The CP user navigates to a secure webpage via the web portal and uses the token as well as the validation code to download the certificate.

   When the request is valid, the CP user can download a ZIP file with a PFX file and the password to extract the certificate (CERT file – X.509 Certificate).

Scenario 2: Acquisition of the Certificate by the Gateway using a token

This second scenario will be available in a subsequent release and the detailed specification will be made available in one of the following updates of this document.

4.1.2.2 aFRR Messages

The messages in the data exchange will be composed of a functional header and a message body.

All required (and optional) fields are described in the following sections. In the element column, abbreviations are used to make the message tags smaller to reduce the message size.

With respect to datetimes, we use the ticks datetime format, which are the milliseconds, counted from the reference date: **01-01-2019 00:00:00 UTC**.

4.1.2.2.1 Body (to be encrypted – see next sections)

Element	Data Type	Origin	Description
SDP – SDP EAN	String	SCADA / FSP BE	The aFRR service delivery point EAN number.
DPM – DPmeasured	Decimal (JSON)	Measurement device	The instantaneous net (gross if the net value cannot be measured) power

			measurement (in MW) per delivery point.
DPB – DPbaseline	Decimal (JSON)	SCADA / FSP BE	The power (in MW) that the delivery point would have injected/consumed without the activation of aFRR service. The baseline is sent 60 seconds in advance.
AS – DPaFRR	Integer (JSON)	SCADA / FSP BE	This is a logical (0 or 1) signal that indicates whether the delivery point is delivering the service for the concerned timeframe.
PS – DPaFRR,supplied	Decimal (JSON)	SCADA / FSP BE	The number of MW of ΔPsec_tot4 that is attributed by the BSP to the delivery point in question.
MTS – Measure timestamp	Ticks (UTC)	Measurement device / gateway	The datetime on which the snapshot of the Pmeasured is taken. The Pbaseline in this message represents its value for this timestamp + 1 minute in the future.

4.1.2.2.2 Header

Element	Data Type	Origin	Description
MT - Message Type	String	Data source originated	Represents the message type & frequency. This makes sure that every message type is unique no matter what frequency is requested.
SID – Sender Id	String	Data source originated	The Endpoint Id as registered in the Communication Platform
GID – Gateway Id	String	Date source originated	The Gateway ID of the gateway as generated by the Communication Platform.
EKV – Encrypted key version	Integer (optional)	Data source originated	The version of the encryption key used (changes at certain periods). If not sent, then the message body is to be considered: not encrypted.
HV – Header version	Integer	Data source originated	The header version allows communication on the same message type but with different versions in case the message header structure is updated. This way, senders have time to adapt and a receiver knows how to interpret the message.
BV – Body version	Integer	Data source originated	The body version allows communication on the same message type but with different versions in case the message body structure is updated. This way, senders have time to adapt and a receiver knows how to interpret the message.

CTS - Creation timestamp	Ticks (UTC)	Date source originated	The timestamp when the message has been sent by the sender.

4.1.2.2.3 Protocol

MQTTS protocol has to be used between the gateway and the Communication Platform.

4.1.2.2.4 Encryption Algorithm

In order to encrypt the message bodies, the Advanced Encryption Standard (AES) / Rijndael algorithm (128 bits) using symmetric keys is used. A lot of implementation libraries are available in Python, JAVA, C#, …

The algorithm is described in the ISO/IEC 18033-3 standard. A simple description of this algorithm can be found here:

https://en.wikipedia.org/wiki/Advanced_Encryption_Standard

This algorithm is used with, as default, the following parameters:

- Block size: 128 bits
- Key size: 128 bits
- Cypher: CBC
- Padding: PKCS7

4.1.2.3 Encryption keys

As described in the process flows, a Key Management System will generate encryption keys and put them available to each separate gateway through the Communication Platform.

Therefore, a specific message type will be exchanged.

4.1.2.3.1 Header

Parameter	Value	Description
MT - Message Type	String (ENCRYPTION KEY)	Represents the message type & frequency. This makes sure that every message type is unique no matter what frequency is requested.

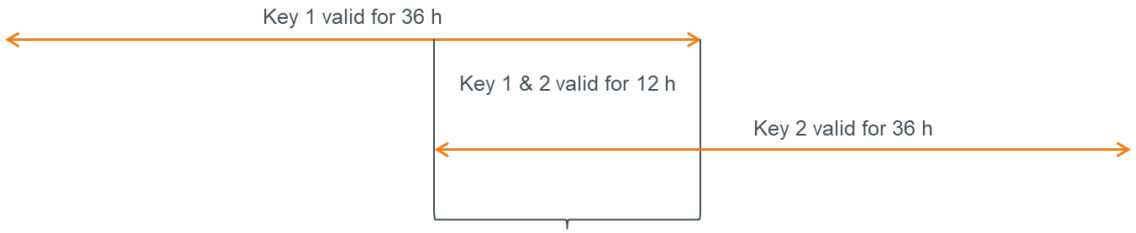
4.1.2.3.2 Body

Parameter	Value	Description
MT – Message Type		The message type for which the key is requested
KEY	string	The encryption key itself. This key is encrypted from the secure KMS using the GW certificate.
KV - Key version	integer	The key version of the requested key
KT – Key Type	string	The algorithm supported for encryption

VF - Valid From (Start Validity)	Ticks	Validity start datetime of the encryption key
VT - Valid To (Stop Validity)	Ticks	Validity end datetime of the encryption key

Gateways

An encryption key is valid for **36 hours** and a new key will be retrieved daily. This means we will have an encryption key overlap of 12 hours within which period the new key must be received and used:



4.1.2.3.3 Technical information

The Communication Platform will exchange this message type with the same principles as the aFRR messages but in the other direction. A specific topic for this message exchange will be foreseen.

Please note that currently, only the AES / Rijndael algorithm is supported by the platform. Others can be added later on.

To guarantee the confidentiality on the key, the key present in the message will be encrypted with the gateway certificate public key. The gateway will need to use its own certificate private key to decrypt the key and after use it to send messages.

Message example:


```
{
   "MT": "ENCRYPTIONKEY",
       "Body":
       "hj7EFc+S5giTCk41loj21ILGOT4aZkafhXzSbmt/gy4ANB4as1MZsnyAwixU76vm4AEmniUw29+8g
       NLEg9Yq0LeR8Hc3zEqGXFaplqNv+6TrSQy+VvZG2NR4xaK1EvAUF8GeP6U9FMVz4eB8MWB94R
       W44n3QOYfCQz7CTEJXvbwbwclGHJN4wsfGPMMxdZUeUiLAuhHvGG7KeLPefTl2DoHS4N8B2m
       ol7lXFZcSD1vnCy4kcF3Jyd6KPEzKfhkFJc2FZaidljSWuo/Z5HQb74hAmg2m/REQnw7yXfaHjJ3E8Z
       zoFZhw+sR7TsBnZvDInni74zuv0R7UFTg2eHmKHnA==" }
```


4.1.2.4 Encryption key Request

As described in the process flows, a Key Management System will generate encryption keys and put them available through to each separate gateway through the Communication Platform. When the

gateway has to be replaced or restarted with an empty configuration, the latest encryption key(s) has(ve) to be requested to be able to send new messages again.

Therefore, a specific message type will be exchanged.

Note that one message will be received (as described in section 4.1.2.3) for each message type and version managed by the gateway with an active aFRR service (normally only one because there is currently only one message type with only one version).

4.1.2.4.1 Header

Parameter	Value	Description
MT - Message Type	String (ENCRYPTION KEYREQUEST)	Represents the message type & frequency. This makes sure that every message type is unique no matter what frequency is requested.

4.1.2.4.2 Body

Body is empty

4.1.2.4.3 Technical information

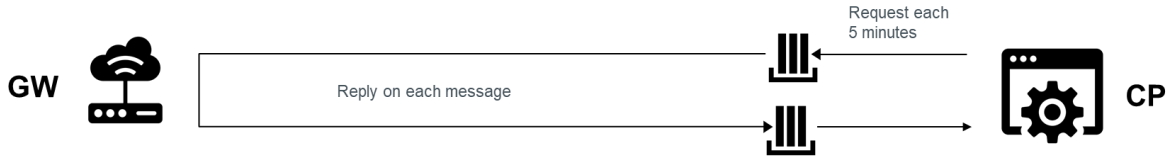
The Communication Platform will exchange this message type with the same principles as the aFRR messages but in the other direction. A specific topic for this message exchange will be foreseen.

Message example:

```
{
"MT": "ENCRYPTIONKEYREQUEST"
}
```

4.1.2.5 Heartbeat

The heartbeat mechanism allows to exchange key values between the gateways and the Communication Platform that are not related to the exchange of market data from endpoints.



The Communication Platform indicates the pace of the heartbeat messages and will be initially set to every five minutes.

The heartbeat message has two functioning methods:

- Ad hoc: an action button in the management portal will be provided in order to initiate a one-time heartbeat message sent to the gateway. If this message is successfully replied to by the gateway, its communication status will be set to 'Connected'. This allows the user to test the connection and authentication of a gateway.

- Recurrent: once a service is activated on this endpoint, the CP will initiate a heartbeat at the interval it choses (5 minutes initially). Also here, the communication status of the gateway will be updated in the portal in case a heartbeat is not replied to. The time to live of the heartbeat message will equal the heartbeat frequency (5 minutes initially).

4.1.2.5.1 CP to GW

Header

Parameter	Value	Description
MID - MessageId	Integer	A counter that can be reinitialized
MT - Message Type	String (HEARTBEAT)	Represents the message type & frequency. This makes sure that every message type is unique no matter the frequency with which the message heartbeat is posted.

Body

Parameter	Value	Description
TS - Time Sync	1	Only present when a gateway must synchronize its internal clock with an NTP server
GWV - GW Version	1	Only present when a gateway must send its firmware and software version. This will be requested daily.

TimeSync et GW version parameters are 2 keys that can be added as list of parameters in the message. Other parameter(s) can be added later on in body.

Message example without time synchronization and GW version needed:

```
{
   "MID": 36,
   "MT": "HEARTBEAT",
 },
```

Message example with time synchronization and without GW version needed:

```
{
   "MID": 36,
   "MT": "HEARTBEAT",
   "Body": "{"TS":1}"
 },
```

Message example without time synchronization and with GW version needed:

```
{
   "MID": 36,
   "MT": "HEARTBEAT",
   "Body": "{"GWV":1}"
 },
```

Message example with time synchronization and GW version needed:

```
{
   "MID": 36,
   "MT": "HEARTBEAT",
   "Body": "{"TS":1, "GWV”:1}"
 },
```

4.1.2.5.2 GW to CP

Header

Parameter	Value	Description
MID - MessageId	Integer	The message ID of the Heartbeat request message.
MT - Message Type	String (HEARTBEAT)	Represents the message type & frequency. This makes sure that every message type is unique no matter what frequency is requested.
GID – Gateway Id	String	The Gateway ID of the gateway as registered in the Communication Platform.
CTS - Creation timestamp	Ticks (UTC)	The timestamp when the message has been sent by the sender

Body

Parameter	Value	Description
SV - Software version	String	The model software version on which the gateway is running. Only to be sent when the GW Version field in the request is sent.
FWV - Firmware version	String	The model firmware version on which the gateway is running. Only to be sent when the GW Version field in the request is sent.

Message example without software and firmware version needed:

```
{
   "MID": 36,
   "MT": "HEARTBEAT ",
   "GID": "123-ABCD",
   "CTS": 29666589696
  },
```

Message example with software and firmware version needed:

```
{
   "MID": 36,
   "MT": "HEARTBEAT ",
   "GID": "123-ABCD",
   "CTS": 29666589696,
   "Body": "{"SV":"1.2", "FWV":"1.74"}"
  },
```

4.1.2.5.3 Technical information

The Heartbeat will be pushed regularly on the GW receiver topic. The response is sent to the same topic as the aFRR messages.

4.1.3 Exception handling

4.1.3.1 Buffering

A local buffering of at least 5 days has to be done locally. This will be used when the communication between the GW and the aFRR Communication Platform is interrupted. The data has to be timestamped at the moment they are produced.

Once the communication is back up, the messages not sent during the interruption have to be sent.

4.1.3.2 Throttling

To avoid congestion, a maximum of **1** message can be sent per second per gateway.

4.1.3.3 Message grouping

- Message grouping can be done for a period of **1** minute (15 data of 4s). Pay attention that it is only valid during exception handling (communication failure, …).
- When grouping, the header is sent only once and the bodies of the specific time series will be grouped in one body.
- The body will be encrypted only once.

4.1.3.4 Fallback files

In the event that Elia does not receive the data through real time communication for bigger gaps, the following is put in place:

- The FSP must, on the request of Elia, be able to provide a fallback file with time series containing the same parameters requested in the aFRR message.

- Elia can only request fallback files in a period covering maximum 90 days before the day of request.
- The delivery of the fallback file must be fulfilled within five working days.

4.1.4 Service level agreements

To assure correct, complete and real-time data exchange, a monitoring is foreseen on predefined KPIs.

4.2 Technical features

4.2.1 URL's and config

The platform will be available at the following URL's:

ACC: https://rtcp-acc.synergrid.be/

DEMO: https://rtcp-pre.synergrid.be/

PROD: https://rtcp.synergrid.be/

Please note that the first tests starting from May 18th have to be done with the Pre-Prod environment. The acceptance environment will be used when updates of the platform will be release. The production environment (to use for the pre-qualifications tests) will be released in the coming weeks.

The Device Provisioning System URL is the following without using the Microsoft SDK:

https://global.azure-devices-provisioning.net/{connectionScope}/registrations/{GatewayBusinessId}/register?api-version=2019-03-31

The GatewayBusinessId is generated by the platform when a new Gateway is created.

Connection scope :
ACC: 0ne000F2E25
DEMO: 0ne000F7DB8
PROD: 0ne000FEA0A

With the Microsoft SDK, the connection string is the following:

global.azure-devices-provisioning.net

Note that these URL's & configurations will not change in case of DRP.

The name of the 2 topics:
Cloud to Device: $"devices/{GatewayBusinessId}/messages/devicebound/#"
Device to Cloud: $"devices/{GatewayBusinessId}/messages/events/"

4.2.2 *Message format testing*

Testing of the validity of JSON (RFC 8259 format) messages in the communication portal interface will be foreseen.

4.2.3 *Examples*

Below, some examples of messages are given. It will also be possible to test the message format (JSON Validation) in the test platform.
To receive more detail on how to connect to the platform and a detailed example (in C#) of the code to connect to our platform, please use the technical reference as defined in point 2 of this document.
Other examples (in different programming languages) can be found here: https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-sdks.

The section to use is '**IoT Hub Device SDKs**'

4.2.3.1 Data exchange

Messages have to be sent with encrypted body. In this section, on overview is given of unencrypted and encrypted data to allow to generate the correct JSON before encryption. As previously described, the body can contain multiple 4 seconds data to cover some exception flows. Both cases are detailed below.

- aFRR data – Unencrypted JSON with one 4s data:


```
{
  "MT": "AFRR",
  "HV": 1,
  "BV": 1,
  "GID": "SN4589674",
  "CTS": 33496996088,
  "EKV": 1,
  "SID": "84V-UOU-40P",
  "Body":
"[{"DPM":0.123,"DPB":0.987,"AS":1,"PS":0.0,"MTS":0,"SDP":"541122334455667788"}]",
}
```


- aFRR data – Encrypted JSON with one 4s data :

The encryption key to use for this message has the following properties:

Encryption type: RijndaelManaged -> KeySize: 128, Padding: PKCS7, Mode: CBC
Encryption key: 9xu0DqrgaFYgrPhudq9s6A==
Encryption IV: 9xu0DqrgaFYgrPhudq9s6A==


```
{
  "MT": "AFRR",
```

```
    "HV": 1,
    "BV": 1,
    "GID": "SN4589674",
    "CTS": 33496996088,
    "EKV": 1,
"SID": "84V-UOU-40P",
    "Body":
"9pMzn4mX5b/+y5SSPVzi6vgebzyLDQJ5bog4c3mg+8cIXS1eVw5ELNlbBUqllhYznMt872Nu7dwUyBTb
Ykl7IPcC9NK8XFy9wnFtVLLmFjM="
  }
```


5 Time synchronization and time stamp

As each measurement needs to be provided with a time stamp, there are two options:

(1) The time reference and stamp are given in the gateway;
(2) The time reference and stamp are given in the measurement device.

The data must be timestamped each 4 seconds.

Regarding time synchronization, the device that is responsible for the time stamping must be synchronized with an NTP-server or an equivalent system at all times. The precision of the timestamp should be at least 20ms. In case of consistent time difference, the CPO will request, via a heartbeat message, to synchronise to an NTP-server.

6 Contacts for gateway

For any question, please contact the persons as mentioned in the 'Technical Guide for Gateway Management V2.3' available on the Elia-website via this link.