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

C8/06

Exigences techniques générales

Système de mesure et gateway pour un point de livraison aFRR raccordé au Réseau de distribution

version 1.00

1 Journal des modifications

Version 1.0 – Version française initiale – Décembre 2023

2 Introduction

2.1 Objet de la prescription C8/06

Le design d'aFRR exige un échange des données mesurées en temps réel et la collecte des paramètres entrant dans le cadre du processus de settlement aFRR pour les points de livraison qui participent à aFRR (points de livraison pour lesquels ELIA ne reçoit pas les calendriers MW quotidiens).

Les appareils de mesure privés doivent envoyer directement les données à la plate-forme de communication (Communication Platform, CP) par le biais de gateways. Ces gateways (GW) peuvent être aussi bien locaux que centraux à condition d'être en contact direct avec la plate-forme de communication.

Pour plus d'information sur les gateways et les processus s'y rapportant, voir la note explicative C8/07.

Pour sécuriser ces données et la plate-forme, l'échange de données repose sur différents mécanismes (cryptage E2E des données mesurées entre gateway et FlexHub, authentification par certificat, etc.) nécessitant le chargement d'une documentation spécifique concernant la sécurité pour chaque type de gateway sur le portail web de la plate-forme de communication temps réel.

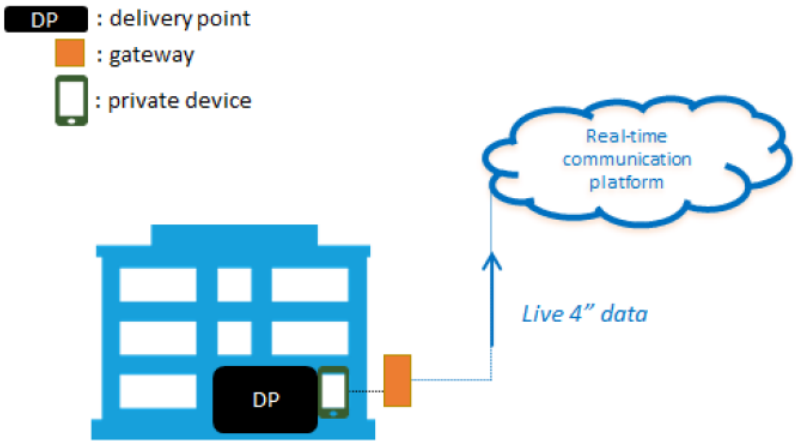


Figure 1 : vue générale

La présente prescription C8/06 :

- Concerne uniquement les points de livraison aFRR raccordés au réseau de distribution.
- Définit d'une part des exigences techniques et réglementaires minimales pour un système de mesure (= appareil de mesure et ses accessoires) en l'absence de transfert d'énergie. Si le produit de flexibilité est concerné par du transfert d'énergie, une nouvelle analyse des exigences spécifiques sera effectuée, laquelle est susceptible d'entraîner des modifications de la présente prescription.

- Décrit d'autre part le cadre technique concernant la gestion des gateways et des points de livraison (Service Delivery Points, SDP's) et leur interaction avec la plate-forme de communication en temps réel.

2.2 Configurations

Les configurations suivantes sont admissibles (voir figure 2) :

1. Un gateway unique transmet les données temps réel d'un SDP prises par un appareil de mesure.
2. Un gateway unique transmet les données temps réel de plusieurs SDPs, prises par des appareils de mesure situés dans les locaux de l'utilisateur du réseau.

Dans les deux configurations :

a. L'appareil de mesure privé se situe au niveau du SDP. Le SDP peut également se situer au niveau du Headpoint/point d'accès.

b. Il est interdit de raccorder un gateway unique à un SDP lié à plus d'un point d'accès.

c. Un gateway doit recueillir toutes les 4 secondes des valeurs instantanées de puissance en provenance d'un appareil de mesure, ainsi que d'autres paramètres nécessaires aux services aFRR, et les transmettre en temps réel à la plate-forme de communication temps réel par le biais du protocole de communication déterminé par Elia.

d. Cette communication entre gateway et plate-forme de communication doit se faire sans système de communication tiers intermédiaire.

e. Les gateways doivent toujours être situés dans les locaux de l'utilisateur du réseau délimité par le headpoint/point d'accès.

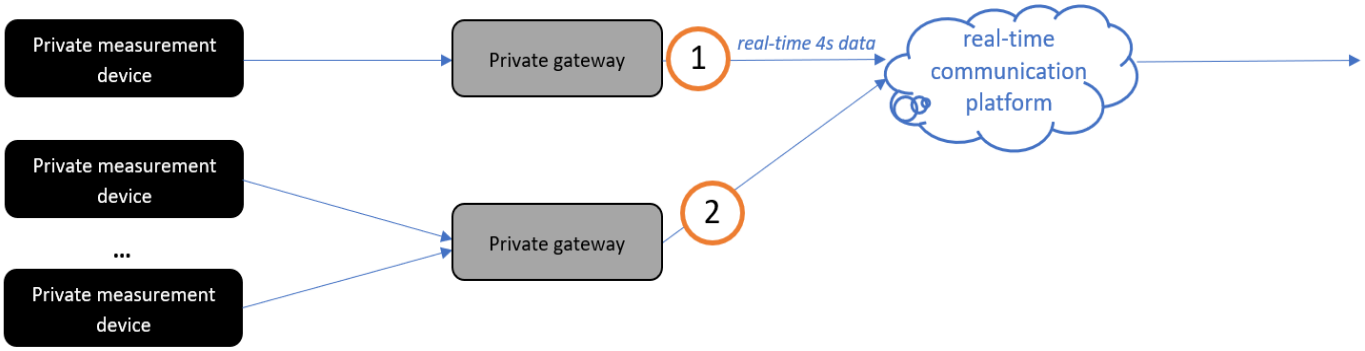


Figure 2 : vue schématique

Un local gateway directement connectée à la Real-Time Communication Platform (telle que décrite ci-dessus) est l'exigence finale. Une période transitoire est prévue jusqu'au 31 décembre 2026 au plus tard.

Cette période de transition implique qu'un écart temporaire par rapport aux exigences techniques finales énoncées ci-dessus (aux points b,d et e) est autorisé (acceptation d'un mode dégradé). Cette dérogation temporaire permet l'utilisation de la connexion à la Real-Time Communication Platform via des **virtual gateways centralisés**.

Les données sont toujours envoyées par point de livraison, où plusieurs points de livraison peuvent être liés à un virtual gateway , vers la Plateforme de Communication. Toutes les spécifications décrites dans ce document et les processus métier associés restent applicables et doivent être respectés. À la fin de la période de transition, tous les participants doivent répondre aux exigences techniques finales, avec des local gateways installés localement et connectés directement à la plateforme de communication.

3 Exigences relatives aux systèmes de mesure

Sauf indication contraire dans les Règlements Techniques relatifs au réseau de distribution des différentes régions, le système de mesure privé doit satisfaire aux exigences minimales suivantes :

- La classe de précision du noyau de mesure des transformateurs de courant (TC) doit être au minimum conforme aux exigences relatives aux transformateurs de courant pour les mesures de puissance indiquées au tableau 1 ci-dessous.

- La classe de précision du noyau de mesure des transformateurs de tension (TT) doit être au minimum conforme aux exigences relatives aux transformateurs de tension pour les mesures de puissance indiquées au tableau 1 ci-dessous.

- La classe de précision du système de mesure de puissance 4 secondes doit être conforme aux exigences relatives aux mesures de puissance figurant au tableau 1 ci-dessous.

- Le gestionnaire du réseau de distribution contrôle la précision des CT et VT, ainsi que du système de mesure.

- Le système de mesure doit avoir une fréquence d'échantillonnage lui permettant de produire une nouvelle valeur toutes les 4 secondes exactement. La fréquence d'échantillonnage doit être de $1/2^n$ fois l'intervalle de 4 secondes (n étant un entier > 0).

- Conformément aux dispositions de la prescription technique Synergrid C2/112, tout câble reliant le transformateur de courant et de tension à un appareil de mesure doit être de type LIYY et satisfaire aux exigences suivantes en matière de section et de longueur :

Longueur électrique du câble	Circuit de tension	Circuit de courant
< 8 m (minimum 3 m)	4 x 2,5 mm² Cu	6 x 2,5 mm² Cu
≥ 8 m (maximum 18 m)	4 x 2,5 mm² Cu	6 x 4 mm² Cu

La connexion des câbles entre les transformateurs et l'appareil de mesure doit être ininterrompue (sans aucun type de dérivation ou de branchement intermédiaire), et respecter les dispositions de l'article 4.4.2.2. du règlement général RGIE.
Les lignes de connexion aux transformateurs de courant et de tension ne doivent pas faire partie d'un même câble.

- Un circuit de 2 ou 3 transformateurs de courant/tension est admissible (méthode à deux ou trois wattmètres), mais la méthode à trois wattmètres est à privilégier.

- L'installation doit être correctement mise à la terre.

- Il est obligatoire de procéder tous les 5 ans à un contrôle de la précision du système de mesure, dans le respect des spécifications techniques des gestionnaires de réseaux de distribution. Un exemplaire du compte-rendu est à communiquer au gestionnaire du réseau de distribution.

Puissance mesurée	TT	TC	Wattmètre
	Classe de précision	Classe de précision	Classe de précision/exigences
≥ 10 MVA	0,2	0,2S	0,2S ou 0,25
≥ 5 MVA à < 10 MVA	0,2	0,2S	0,5S
≥ 1 MVA à < 5 MVA	0,2	0,2	0,5
≥ 100 kVA à < 1 MVA	0,5	0,5	1
≥ 32 kVA et < 100 kVA	S.O.	0,5[1]	2 %[23]
≥ 11 kVA et < 32 kVA	S.O.	0,5[1]	3,5 %[23]
≥ 4 kVA et < 11 kVA	S.O.	0,5[1]	6 %[23]
< 4 kVA	S.O.	0,5[1]	10 %[23]

4 Exigences relatives aux gateways

4.1 Échange de données – spécifications

Cette section décrit les spécifications détaillées régissant les interfaces d'échange de données entre les gateways, la plate-forme de communication et les composants de sécurité. Dans la première version de la plate-forme, on a un échange de données aFRR unidirectionnel (sauf pour le « heartbeat »), des gateways vers le FlexHub via la plate-forme de communication aFRR. Le flux de

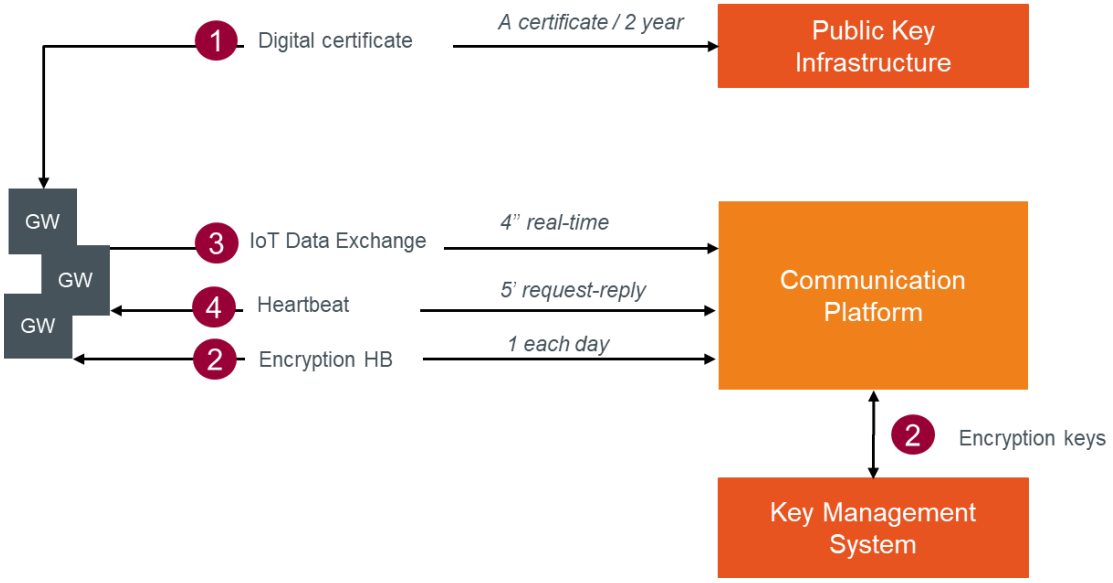
[1]Si nécessaire.
[2]Conformité et certification selon la procédure de certification décrite dans le document « General technical requirements for private measurement », à consulter via le site web d'ELIA.
[3] Uniquement dans le cas d'une offre d'au moins 100 kW.

messages consiste en des messages aFRR 4s temps réel servant au settlement des activations aFRR. Un message est envoyé pour chaque point de livraison raccordé à un gateway.

Les mécanismes de sécurité assurent un échange de données fiable et sûr : la Public Key Infrastructure (PKI) permet l'authentification des gateways par certificat, et le système de gestion des clés fournit des clés de cryptage pouvant servir à crypter le corps du message aFRR.

4.1.1 Flux de données

Voici une visualisation du flux de processus E2E de tous les échanges de données devant être pris en charge par les gateways.



1. Chaque gateway et application se connectant à la plate-forme de communication doit disposer d'un certificat numérique (valable 2 ans) fourni par la Public Key Infrastructure. Ce certificat sert à l'authentification du gateway à chaque connexion à la plate-forme, ainsi que dans le cadre du système de gestion des clés.

2. Les données (corps du message) doivent être cryptées de bout en bout (du gateway au FlexHub). Chaque jour, un système indépendant de gestion des clés génère des clés de cryptage destinées au chiffrement du corps du message et les envoie aux gateways via la plate-forme de communication.

3. Toutes les 4 secondes, le gateway envoie à la plate-forme de communication un message aFRR dont le corps est crypté. Pour se connecter et introduire le message dans la file d'attente, les gateways doivent disposer d'un certificat numérique obtenu auprès de la Public Key Infrastructure (PKI).

4. À intervalles réguliers (soit toutes les 5 minutes pour commencer), la plate-forme de communication publie un message Heartbeat sur le topic auquel doit répondre le gateway. Ce message comprend des valeurs clés destinées à des cas d'utilisation spécifiques ainsi qu'à l'actualisation de l'état de la connexion gateway.

Les files d'attente messages assurent une communication asynchrone, ce qui signifie que les points finaux (endpoints) qui produisent et consomment des messages interagissent avec la file

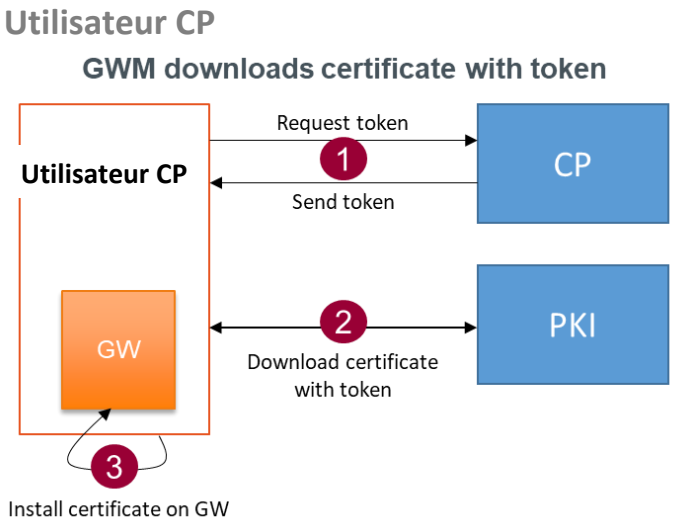
d'attente, et non entre eux. Contrairement aux files d'attente, dans lesquelles chaque message est traité par un seul consommateur, les **topics** et les abonnements assurent une communication one-to-many sur le mode publication/abonnement.
L'échange de données entre le gateway et la plate-forme de communication se fait sur la base de deux topics différents (un par direction).

4.1.2 Interfaces

4.1.2.1 Authentification par certificat

Les scénarios ci-après concernent l'acquisition de tokens et de certificats :

Scénario 1 : Acquisition d'un certificat via le portail



1. L'utilisateur CP demande un token pour un gateway par le biais de l'interface utilisateur du portail. Le portail génère et affiche un code de validation dans l'écran d'information du gateway concerné, et un email est envoyé à l'utilisateur CP avec un token.
2. L'utilisateur CP ouvre une page web sécurisée par le biais du portail web, et télécharge le certificat à l'aide du token et du code de validation.

   Après validation de la demande, l'utilisateur CP peut télécharger un fichier ZIP contenant un fichier PFX et le mot de passe permettant d'extraire le certificat (fichier CERT – certificat X.509).

Scénario 2 : Acquisition d'un certificat par un gateway à l'aide d'un token

Ce deuxième scénario sera proposé dans le cadre d'une prochaine version, la spécification détaillée étant mise à disposition dans une mise à jour ultérieure du présent document.

4.1.2.2 Messages aFRR

Les messages servant à l'échange de données se composent d'un en-tête fonctionnel et d'un corps de message.

Voir ci-après la description des champs obligatoires (et facultatifs). Dans la colonne « Élément », des abréviations permettent de réduire la taille des tags du message, et donc celle de ce dernier.

Concernant les datetimes, nous avons opté pour le format « ticks », qui correspond aux millisecondes, décomptées à partir de la date de référence : **01-01-2019 00:00:00 UTC**.

4.1.2.2.1 Corps du message (à crypter – voir sections suivantes)

Élément	Type données	Origine	Description
SDP – SDP EAN	Série	SCADA / FSP BE	Numéro EAN du point de livraison du service aFRR.
DPM – DPmeasured	Décimale (JSON)	Appareil de mesure	Puissance instantanée nette (ou brute si cette dernière n'est pas mesurable) mesurée par point de livraison (en MW).
DPB – DPbaseline	Décimale (JSON)	SCADA / FSP BE	Puissance (en MW) que le point de livraison aurait injectée/consommée sans l'activation d'un service aFRR pour l'horodatage dans le champ MTS - Measure Timestamp + 1 minute.
AS – DPaFRR	Entier (JSON)	SCADA / FSP BE	Signal logique (0 ou 1) indiquant si le point de livraison assure le service voulu pour la période concernée.
PS – DPaFRR,supplied	Décimale (JSON)	SCADA / FSP BE	ΔPsec_tot4 en nombre de MW attribué par le BSP au point de livraison en question.
MTS – Measure timestamp	Ticks (UTC)	Appareil de mesure / gateway	Datetime de prise du snapshot Pmeasured. Dans ce message, Pbaseline représente la valeur pour ce timestamp + 1 minute dans le futur.

4.1.2.2.2 En-tête

Élément	Type données	Origine	Description
MT - Message Type	String	Données source	Représente le type de message et la fréquence. Fait en sorte que chaque type de message soit unique indépendamment de la fréquence demandée.
SID – Sender Id	String	Données source	Endpoint Id enregistré sur la plate-forme de communication.

GID – Gateway Id	String	Données source	ID gateway généré par la plate-forme de communication.
EKV – Encrypted key version	Integer (optional)	Données source	Version de la clé de cryptage en utilisation (change de temps à autre) En son absence, le corps du message est considéré comme non crypté.
HV - Header version	Integer	Données source	La version d'en-tête permet de communiquer sur le même type de message mais avec des versions différentes si la structure de l'en-tête du message est mise à jour. L'expéditeur a ainsi le temps de s'adapter, et le destinataire sait comment interpréter le message.
BV - Body version	Integer	Données source	La version du corps permet de communiquer sur le même type de message mais avec des versions différentes si la structure du corps du message est mise à jour. L'expéditeur a ainsi le temps de s'adapter, et le destinataire sait interpréter le message
CTS - Creation timestamp	Ticks (UTC)	Données source	Heure et date d'envoi du message.

4.1.2.2.3 Protocole

Le protocole MQTTS est obligatoire pour une communication entre gateway et plate-forme de communication.

4.1.2.2.4 Algorithme de cryptage

Cryptage des corps de message via algorithme Advanced Encryption Standard (AES) / Rijndael (128 bits) avec des clés symétriques. De nombreuses bibliothèques d'implémentation sont disponibles : Python, JAVA, C#, etc.

L'algorithme est décrit dans la norme ISO/IEC 18033-3. Le lien ci-dessous mène à une description simple de cet algorithme :

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

Par défaut, cet algorithme fait usage des paramètres suivants :

- Taille de bloc : 128 bits
- Taille clé : 128 bits
- Cypher : CBC
- Padding : PKCS7

4.1.2.3 Clés de cryptage

Comme décrit dans les processus, un Key Management System génère des clés de cryptage et les met à la disposition de chaque gateway distinct via la plate-forme de communication.

En conséquence, un type de message spécifique sera échangé.

4.1.2.3.1 En-tête

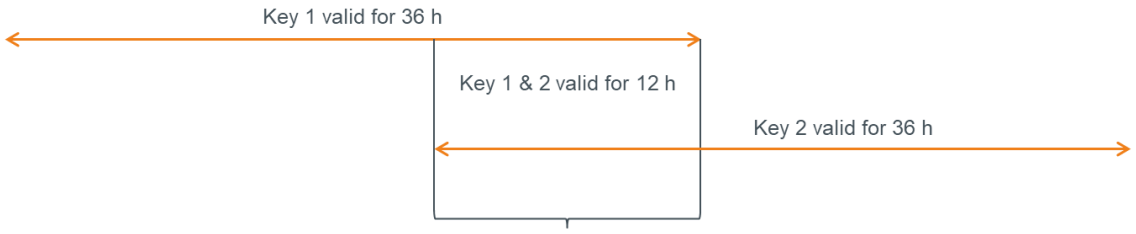
Paramètre	Valeur	Description
MT - Type de message	String (ENCRYPTION KEY)	Représente le type de message et la fréquence. Fait en sorte que chaque type de message soit unique indépendamment de la fréquence demandée.

4.1.2.3.2 Corps de message

Paramètre	Valeur	Description
MT – Message Type (type de message)		Type du message pour lequel une clé est demandée.
CLÉ	string	Il s'agit de la clé de cryptage proprement dite. Le cryptage est assuré par le KMS sécurisé par le biais du certificat GW.
KV – Key Version (version de la clé)	integer	Version de la clé demandée
KT – Key Type (type de clé)	string	Algorithme pris en charge pour le cryptage
VF - Valide à partir de (Start Validity)	Ticks	Datetime de début de validité de la clé de cryptage
VT - Valide jusqu'à (Stop Validity)	Ticks	Datetime de fin de validité de la clé de cryptage

Gateways

Une clé de cryptage est valide **36 heures**, et une nouvelle clé sera récupérée chaque jour. En d'autres termes, pour deux clés de cryptage, il y a une période de chevauchement de 12 heures, soit la période pendant laquelle la nouvelle clé doit être récupérée et utilisée :



4.1.2.3.3 Information technique

La plate-forme de communication échangera ce type de message selon les mêmes principes que les messages aFRR, mais dans lle sens inverse. Un topic spécifique sera prévu pour cet échange de message.

À noter qu'à l'heure actuelle, la plate-forme ne prend en charge que l'algorithme AES / Rijndael. D'autres algorithmes sont susceptibles de venir s'ajouter ultérieurement.

Pour garantir la confidentialité de la clé, la clé présente dans le message est cryptée à l'aide de la clé publique du certificat gateway. Pour décrypter la clé et envoyer des messages à l'aide de celle-ci, le gateway doit faire usage de sa propre clé privée.

Exemple de message :

{

"MT": "ENCRYPTIONKEY",

"Body":
"hj7EFc+S5giTCk41loj21ILGOT4aZkafhXzSbmt/gy4ANB4as1MZsnyAwixU76vm4AEmniUw29+8g
NLEg9Yq0LeR8Hc3zEqGXFaplqNv+6TrSQy+VvZG2NR4xaK1EvAUF8GeP6U9FMVz4eB8MWB94R
W44n3QOYfCQz7CTEJXvbwbwclGHJN4wsfGPMMxdZUeUiLAuhHvGG7KeLPefTl2DoHS4N8B2m
ol7lXFZcSD1vnCy4kcF3Jyd6KPEzKfhkFJc2FZaidIjSWuo/Z5HQb74hAmg2m/REQnw7yXfaHjJ3E8Z
zoFZhw+sR7TsBnZvDInni74zuv0R7UFTg2eHmKHnA==" }

4.1.2.4 Demande de clé de cryptage

Comme décrit dans les processus, un Système de Gestion des Clés génère des clés de cryptage et les met à la disposition de chaque gateway par le biais de la plate-forme de communication. Si le gateway doit être remplacé ou redémarré avec une configuration vide, la (les) dernière(s) clé(s) de cryptage doit (doivent) être demandée(s) pour pouvoir envoyer de nouveaux messages.

En conséquence, un type de message spécifique sera échangé.

À noter qu'un message est reçu (voir description au point 4.1.2.3) pour chaque type et version de message gérés par le gateway ayant un service aFRR actif (en principe un seul puisqu'il n'existe actuellement qu'un type de message, en une seule et unique version).

4.1.2.4.1 En-tête

Paramètre	Valeur	Description
MT - Message Type	String (ENCRYPTION KEYREQUEST)	Représente le type de message et la fréquence. Cela fait en sorte que chaque type de message soit unique indépendamment de la fréquence demandée.

4.1.2.4.2 Corps de message

Le corps de message est vide.

4.1.2.4.3 Information technique

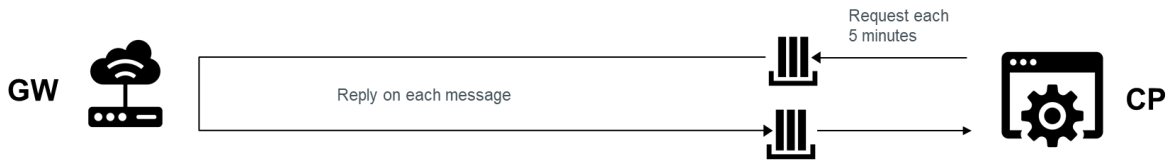
La plate-forme de communication échangera ce type de message selon les mêmes principes que les messages aFRR, mais dans le sens inverse. Un topic spécifique sera prévu pour cet échange de messages.

Exemple de message :

{
"MT": "ENCRYPTIONKEYREQUEST"
}

4.1.2.5 Heartbeat

Le mécanisme Heartbeat permet d'échanger entre les gateways et la plate-forme de communication des valeurs clés sans rapport avec l'échange de données de marché en provenance d'endpoints



La plate-forme de communication indique la fréquence d'envoi des messages Heartbeat, initialement fixée à cinq minutes.

Le message Heartbeat a deux modes de fonctionnement :

- Ad hoc : sur le portail de gestion, un bouton d'action permettra d'adresser un message Heartbeat unique au gateway. Si le gateway répond à ce message, son état de communication devient « Connected ». Cela permet à l'utilisateur de tester la connexion et l'authentification d'un gateway.

- Récurrent : après activation d'un service sur cet endpoint, la CP émet un message Heartbeat selon l'intervalle voulu (5 minutes dans un premier temps). L'état de communication du gateway est par ailleurs mis à jour sur le portail, au cas où le message Heartbeat resterait sans réponse. Le Time to Live du message Heartbeat est égal à la fréquence d'envoi (5 minutes dans un premier temps).

4.1.2.5.1 CP vers GW

En-tête

Paramètre	Valeur	Description
MID - MessageId	Entier	Compteur réinitialisable
MT - Message Type	String (HEARTBEAT)	Représente le type de message et la fréquence. Cela fait en sorte que chaque type de message soit unique indépendamment de la fréquence d'envoi.

Corps du message

Paramètre	Valeur	Description
TS - Time Sync	1	Présent uniquement quand un gateway doit synchroniser son horloge interne avec un serveur NTP.
GWV - GW Version	1	Présent uniquement quand un gateway doit donner sa version de micrologiciel/logiciel. Fait l'objet d'une demande journalière.

Les paramètres TimeSync et GWV sont 2 clés pouvant être jointes au message sous forme de liste de paramètres. On peut ajouter ultérieurement d'autres paramètres dans le corps du message.

Exemple de message sans synchronisation, avec demande de version de GW :

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

Exemple de message avec synchronisation, sans demande de version de GW :

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

Exemple de message sans synchronisation, avec demande de version de GW :

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

Exemple de message avec synchronisation et demande de version de GW :

```
{
```

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

4.1.2.5.2 GW vers CP

En-tête

Paramètre	Valeur	Description
MID - MessageId	Integer	L'ID du message du message Heartbeat demandé.
MT - Message Type	String (HEARTBEAT)	Représente le type de message et la fréquence. Fait en sorte que chaque type de message soit unique indépendamment de la fréquence demandée.
GID – Gateway Id	String	Gateway ID du gateway enregistré sur la plate-forme de communication.
CTS - Creation timestamp	Ticks (UTC)	Heure et date d'envoi du message.

Corps de message

Paramètre	Valeur	Description
SV - Software version	String	Version du logiciel sous lequel tourne le gateway. À n'envoyer que si le champ GW Version de la demande est envoyé.
FWV - Firmwareversion	String	Version du micrologiciel sous lequel tourne le gateway. À n'envoyer que si le champ GW Version de la demande est envoyé.

Exemple de message sans demande de version logiciel/micrologiciel :

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

Exemple de message avec demande de version logiciel/micrologiciel :

```
{
  "MID": 36,
```

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


4.1.2.5.3 Information technique

Le Heartbeat sera envoyé régulièrement sous le topic du GW destinataire. La réponse est envoyée sous le même topic que les messages aFRR.

4.1.3 Traitement des exceptions

4.1.3.1 Buffering

Un buffering local d'au moins 5 jours doit être assuré localement. Il a son utilité en cas d'interruption de communication entre le GW et la plate-forme de communication aFRR. Les données doivent être horodatées au moment même de leur production.

Une fois la communication rétablie, les messages qui n'ont pas été envoyés doivent être envoyés.

4.1.3.2 Throttling

Pour éviter toute congestion, un maximum de **1** message peut être envoyé par seconde et par gateway.

4.1.3.3 Regroupement des messages

- Un regroupement des messages est possible pour une durée de **1** minute (15 données 4s). Attention : ce regroupement n'est valable que dans le cadre de la gestion d'exceptions (échec de la communication, etc.).
- Dans le cas d'un regroupement de messages, l'en-tête n'est envoyé qu'une seule fois et les corps de message sont regroupés en un seul.
- Le corps n'est crypté qu'une seule fois.

4.1.3.4 Fichiers fallback

Si Elia ne reçoit pas les données du fait d'un problème de communication temps réel plus long, la marche à suivre est la suivante :

- Le FSP doit, sur demande d'Elia, pouvoir fournir un fichier fallback dont les séries temporelles comprennent les paramètres demandés dans le message aFRR.
- Elia ne peut demander des fichiers de secours que pour les 90 jours précédant le jour de la demande.
- L'envoi du fichier de remplacement doit intervenir dans les cinq jours ouvrables.

4.1.4 Conventions de service

Pour garantir un échange de données correct, complet et en temps réel, un suivi est prévu sur la base de KPIs prédéfinis.

4.2 Caractéristiques techniques

4.2.1 URL et config

La plate-forme est accessible via les url suivantes :

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

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

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

À noter que les premiers tests doivent se faire dans l'environnement de préproduction (à partir du 18 mai). L'environnement d'acceptance servira après publication de mises à jour de la plate-forme. L'environnement de production (dans lequel doivent se dérouler les tests de préqualification) sera publié dans les semaines qui viennent.

L'url du Device Provisioning System est la suivante (pas d'utilisation du SDK de Microsoft) :

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

L'identifiant GatewayBusinessId est généré par la plate-forme à la création d'un gateway.

Paramètres de connexion :
ACC : 0ne000F2E25
DEMO : 0ne000F7DB8
PROD : 0ne000FEA0A

Avec utilisation du SDK de Microsoft, la chaîne de connexion est la suivante :

global.azure-devices-provisioning.net

Attention : ces url et paramètres ne changent pas en cas de DRP.

Intitulé des 2 topics :
Cloud to Device : $"devices/{GatewayBusinessId}/messages/devicebound/#"
Device to Cloud : $"devices/{GatewayBusinessId}/messages/events/”

4.2.2 Test de format de messages

Des tests de validité des messages JSON (format RFC 8259) seront prévus dans l'interface du portail de communication.

4.2.3 Exemples

Voici quelques exemples de messages. La plate-forme de test permettra aussi de tester le format des messages (validation JSON).
Pour en savoir plus sur le mode de connexion à la plate-forme et consulter un exemple détaillé (en C#) du code la rendant possible, voir la référence technique définie au point 2 du présent document.

Le lien suivant donne accès à d'autres exemples (en différents langages de programmation) : https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-sdks.

Choisir la section « **IoT Hub Device SDKs** ».

4.2.3.1 Échange de données

Tout message envoyé doit avoir un corps crypté. La présente rubrique donne une vue d'ensemble des données non cryptées et des données cryptées, pour une génération correcte du message JSON avant cryptage. Comme on l'a vu, le corps du message peut contenir plusieurs données 4 secondes pour parer à certains flux d'exception. Les deux cas sont détaillés ci-dessous.

- Donnée aFRR – JSON non crypté avec données 4s :


```
{
  "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"}]",
}
```


- Donnée aFRR –JSON crypté avec données 4s :

La clé de cryptage à appliquer à ce message a les propriétés suivantes :

Type de cryptage : RijndaelManaged -> KeySize : 128, padding : PKCS7, Mode : CBC
Clé de cryptage : 9xu0DqrgaFYgrPhudq9s6A==
Cryptage IV : 9xu0DqrgaFYgrPhudq9s6A==


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

5 Synchronisation et horodatage (timestamp)

Chaque mesure devant être horodatée, il y a deux possibilités :

(1) référence temporelle et horodatage attribués au niveau du gateway ;
(2) référence temporelle et horodatage attribués au niveau de l'appareil de mesure.

Les données doivent être horodatées toutes les 4 secondes.

Concernant la synchronisation, le dispositif chargé de l'horodatage doit être synchronisé en permanence avec un serveur NTP ou système équivalent. La précision de l'horodatage doit être d'au moins 20 ms. En cas de différence temporelle importante, le CPO demande via message heartbeat une synchronisation avec un serveur NTP.

6 Contacts

Toute question relative aux gateways est à adresser aux personnes dont les coordonnées figurent dans le « Technical Guide for Gateway Management », consultable via le site Internet Elia (lien).