

C8/06

Exigences techniques générales

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

version 3.00

1	<i>Journal des modifications</i>	3
2	<i>Introduction</i>	4
2.1	Objet de la prescription C8/06	4
2.2	Configurations	5
3	<i>Exigences relatives aux systèmes de mesure</i>	6
4	<i>Exigences relatives aux gateways</i>	7
4.1.1	Flux de données	7
4.1.2	Interfaces	8
4.1.2.1	Authentification par certificat	8
4.1.2.2	Messages FCR et aFRR	8
4.1.2.3	Clés de cryptage	8
4.1.2.4	"Demande de clé de cryptage	8
4.1.2.5	Heartbeat	8
4.1.3	Traitement des exceptions	9
4.1.3.1	Buffering	9
4.1.3.2	Throttling	9
4.1.3.3	Regroupement des messages	9
4.1.3.4	Fichiers fallback	9
4.1.4	Conventions de service	9
5	<i>Synchronisation et horodatage (timestamp)</i>	9
6	<i>Contacts</i>	9

1 Journal des modifications

Version 1.0 – Version française initiale – Décembre 2023

Version 2.0 – Extension du champ d'application à FCR

Version 3.0 - Mise en place d'une configuration de gateway centrale comme solution permanente aux côtés de la configuration de gateway locale et suppression des descriptions de processus.

2 Introduction

2.1 Objet de la prescription C8/06

Les designs des produits FCR et aFRR exigent un échange des données mesurées en temps réel et la collecte des paramètres entrant dans le cadre du processus de settlement FCR/aFRR pour les points de livraison de services (liés aux points de livraison pour lesquels ELIA ne reçoit pas les calendriers MW quotidiens) qui participent à FCR ou à aFRR.

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 locales que centrales, à condition d'être en contact direct avec la plate-forme de communication.

Pour plus d'informations 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.

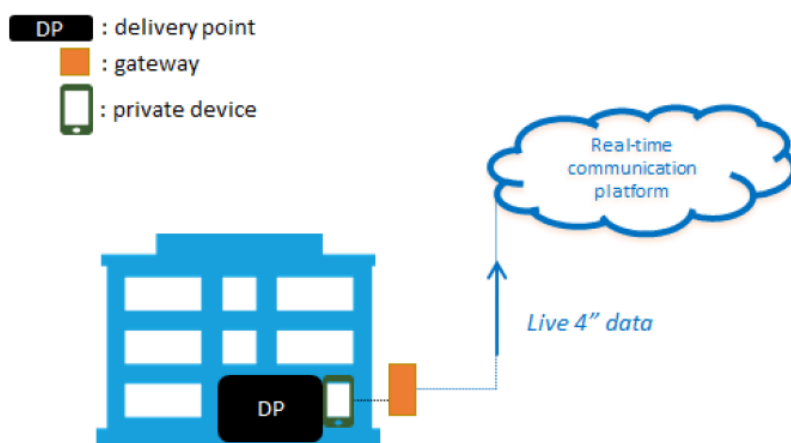


Figure 1 : vue générale

La présente prescription C8/06 décrit le cadre technique concernant l'équipement de mesure, dont la gestion des gateways et des points de livraison de services (Service Delivery Points, SDP) et leur interaction avec la plate-forme de communication en temps réel. Ceci sert à la valorisation de la flexibilité via aFRR et/ou FCR qui est fournie, installée et entretenue par un tiers. La lecture n'est pas effectuée par le GRD dans ce cas¹. Dans la mesure où aucun transfert d'énergie ne s'applique au

¹ Sous réserve de l'adaptation en cours du cadre décretaal wallon

service de flexibilité concerné, l'équipement de mesure n'est pas tenu de respecter les éventuelles exigences des règlements techniques régionaux.

Il est important de noter que, bien que les processus liés aux données FCR et aFRR soient similaires, les responsabilités liées à ces données peuvent être différentes.

2.2 Configurations

Les configurations suivantes sont admissibles (voir figure 2) :

1. Une gateway unique transmet les données temps réel d'un SDP prises par un appareil de mesure.
2. Une 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.
3. Une gateway centrale transmet les données temps réel de plusieurs SDPs, mesurés par des appareils de mesure situés dans les locaux de plusieurs utilisateurs du réseau.

Dans les configurations 1 et 2, les gateways sont toujours installées localement sur le site où se trouve l'utilisateur du réseau.

Dans toutes les configurations :

- a. L'appareil de mesure privé se situe au niveau du SDP. Le SDP est défini au niveau du point de livraison ou du point d'accès.
- b. Une 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.

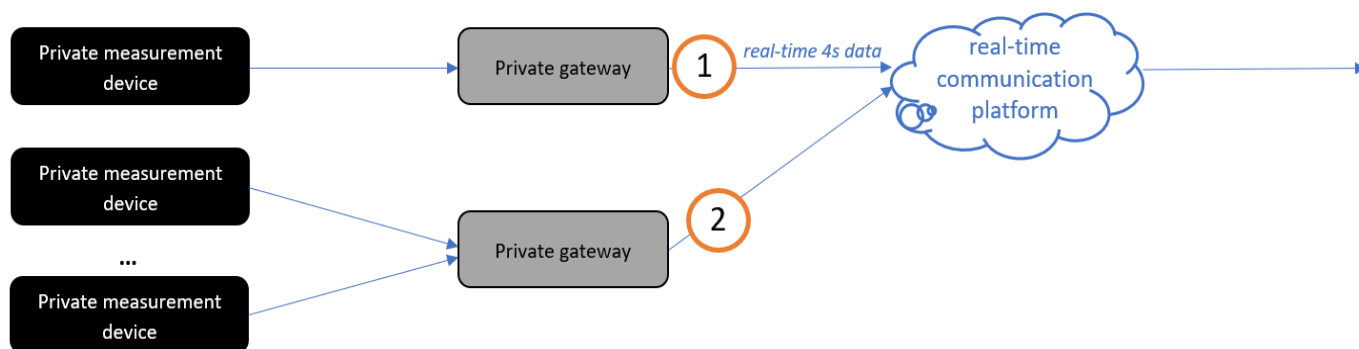


Figure 2 : vue schématique

3 Exigences relatives aux systèmes de mesure

Sauf indication contraire² 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 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 mm ² Cu	6 x 2,5 mm ² Cu
≥ 8 m (maximum 18 m)	4 x 2,5 mm ² Cu	6 x 4 mm ² 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.

² Les dérogations ci-dessous ne s'appliquent que dans le contexte de la aFRR sans transfert d'énergie.

- 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.

1	Puissance mesurée	TT	TC	Wattmètre	Tableau – Classes de précision
		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 ³	2 % ⁴⁵	
	≥ 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

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.

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 des messages.

4.1.1 Flux de données

La gateway doit pouvoir demander, recevoir et utiliser un certificat numérique émis par une Public Key Infrastructure (PKI) à des fins d'authentification (durée de validité : 2 ans). La gateway doit être capable d'envoyer des messages chiffrés de bout en bout à l'aide de clés de cryptage générées quotidiennement par un Key Management System (KMS).

³Si nécessaire.

⁴Conformité 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.

⁵ Uniquement dans le cas d'une offre d'au moins 100 kW.

4.1.2 Interfaces

4.1.2.1 Authentification par certificat

La gateway doit prendre en charge l'authentification par certificat basée sur des certificats X.509 (PFX/CERT).

Utilisateur CP

4.1.2.2 Messages FCR et aFRR

Les messages servant à l'échange de données se composent d'un en-tête fonctionnel et d'un corps de message. La gateway doit être capable de générer et d'envoyer des messages JSON (RFC 8259). Elle doit prendre en charge les horodatages au format « ticks » (UTC, référence 01/01/2019).

4.1.2.2.1 Protocole

La gateway doit être compatible avec le protocole MQTTS ou Azure Event Hubs pour communiquer avec la Plate-forme de communication.

4.1.2.2.2 Algorithme de cryptage

La gateway doit être compatible avec le cryptage symétrique AES/Rijndael (128 bits, CBC, remplissage PKCS7) conformément à la norme ISO/IEC 18033-3

4.1.2.3 Clés de cryptage

La gateway doit pouvoir recevoir des clés de cryptage du Key Management System via la Plateforme de communication, et être capable de gérer plusieurs versions de clés en parallèle (période de chevauchement de 12 heures, validité de 36 heures, rotation journalière).

4.1.2.4 "Demande de clé de cryptage"

En cas de remplacement ou de redémarrage avec une configuration vide, la gateway doit pouvoir récupérer la ou les dernières clés de cryptage valides auprès du KMS.

4.1.2.5 Heartbeat

La gateway doit être compatible avec un mécanisme heartbeat (initialement toutes les 5 minutes), aussi bien ad hoc que périodique, afin de pouvoir vérifier la connexion et l'authentification.

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 temps réel. 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.).

4.1.3.4 Fichiers fallback

- Le FSP doit, sur demande d'Elia, pouvoir fournir un fichier fallback pour une période minimale de 90 jours, dont les séries temporelles comprennent les paramètres demandés dans les messages FCR ou aFRR.

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 définis dans les documents disponibles sur le site d'Elia (p. ex. "aFRR – Communication Requirements"). Le non-respect de ces KPIs pourra mener jusqu'à la disqualification du FSP.

5 Synchronisation et horodatage (timestamp)

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

- (1) référence temporelle et horodatage attribués au niveau de la 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 [\(lien\)](#).