

C8/06

Algemene technische vereisten

Meetsysteem en Gateway voor een FCR of aFRR- dienstleveringspunt aangesloten op het Distributienet

versie 3.00

1	Logboek wijzigingen	3
2	Inleiding	4
2.1	Voorwerp van voorschrift C8/06	4
2.2	Assetconfiguraties	5
3	Vereisten meetsystemen	6
4	Vereisten gateways	7
4.1	Gegevensstromen	7
4.2	Interfaces	8
4.2.1	Verificatie op basis van certificaten	8
4.2.2	FCR en aFRR Berichten	8
4.2.3	Encryptiestleutels	8
4.2.4	Aanvraag encryptiesleutel	8
4.2.5	Heartbeat	8
4.3	Verwerking van uitzonderingen	8
4.3.1	Buffering	8
4.3.2	Throttling	9
4.3.3	Berichtengroepering	9
4.3.4	Fallbackbestanden	9
4.4	Service level agreements	9
5	Tijdsynchronisatie en tijdstempel	9
6	Contactpersonen voor gateway	9

1 Logboek wijzigingen

Versie 1.0 – Oorspronkelijke Nederlandstalige versie - december 2023

Versie 2.0 – uitbreiding toepassingsgebied naar FCR

Versie 3.0 – Verankering van de centrale gatewayconfiguratie als permanente oplossing naast de lokale gatewayconfiguratie, gecombineerd met de schrapping van procesbeschrijvingen.

2 Inleiding

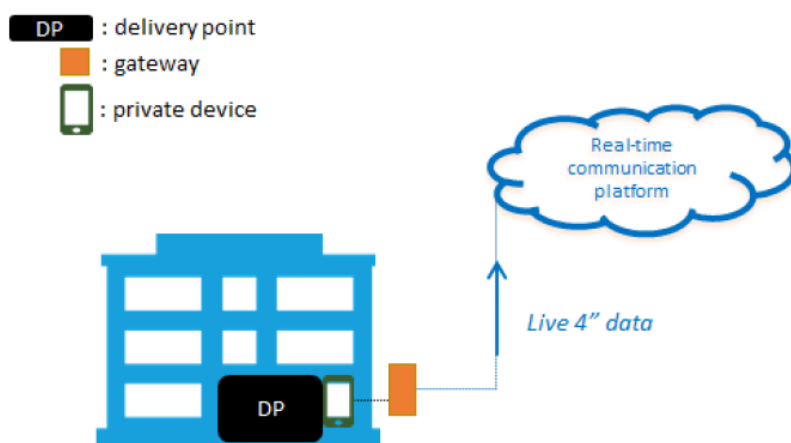
2.1 Voorwerp van voorschrift C8/06

In het ontwerp van FCR en aFRR is een realtime uitwisseling van meetgegevens en een verzameling van parameters, gebruikt voor het FCR/aFRR settlement proces, vereist voor dienstverleningspunten (gekoppeld aan leveringspunten waarvoor ELIA geen MW-dagschema's ontvangt) die deelnemen aan de dienst FCR of aFRR.

Private meettoestellen moeten de gegevens d.m.v. gateways rechtstreeks naar het Communicatieplatform (CP) versturen. Zowel lokale als gecentraliseerde gateways (GW) mogen worden gebruikt en moeten een directe verbinding hebben met het Communicatieplatform.

Meer informatie met betrekking tot de gateways en gerelateerde processen is te vinden in toelichting C8/07.

Om deze gegevens en het platform te beveiligen, wordt gebruik gemaakt van meerdere mechanismen voor gegevensuitwisseling (E2E-versleuteling van de meetgegevens tussen de gateway en de FlexHub, authenticatie op basis van certificaten) en moeten specifieke veiligheidsgerelateerde technische documenten voor elk gatewaymodel worden geüpload op het realtime Communication Platform Web Portal.



figuur 1: algemeen overzicht

Dit voorschrift C8/06 beschrijft het technisch kader met betrekking tot de meetuitrusting waaronder het beheer van de gateways en dienstverleningspunten (Service Delivery Points, SDP's) en hun interacties met het realtime Communicatieplatform. Dit dient voor de valorisatie van flexibiliteit via aFRR en/of FCR die door een derde partij geleverd, geplaatst en onderhouden wordt. De uitlezing gebeurt in dit geval niet door de DNB. In zover geen energieoverdracht van toepassing is voor de betreffende flexibilitiedienst dient de meetuitrusting niet te voldoen naar eventuele vereisten van de gewestelijke technische reglementen.

Het is belangrijk op te merken dat, hoewel de processen met betrekking tot FCR- en aFRR-gegevens vergelijkbaar zijn, de verantwoordelijkheden met betrekking tot deze gegevens kunnen verschillen.

2.2 Assetconfiguraties

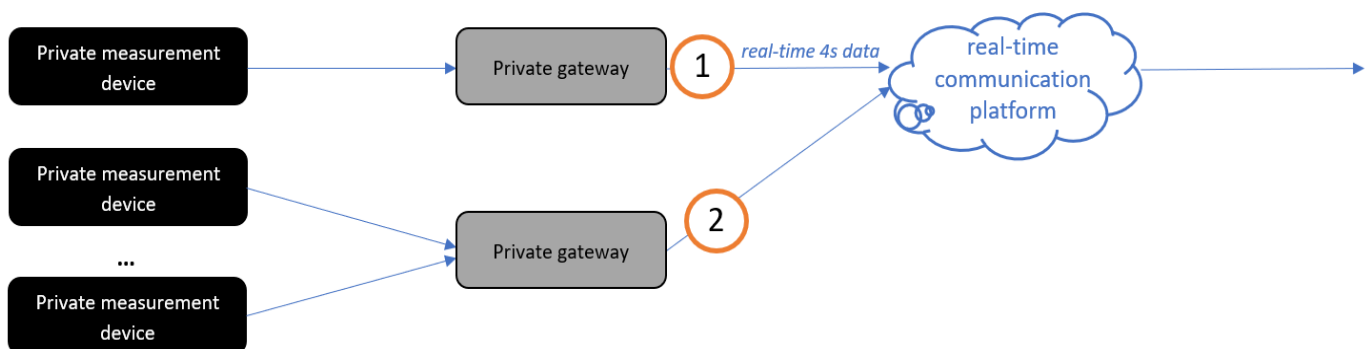
Volgende configuraties zijn toegestaan (zie figuur 2):

1. Een enkele gateway verzendt realtime gegevens van één SDP gemeten door een meettoestel.
2. Een enkele gateway verzendt realtime gegevens van meerdere SDP's gemeten door meettoestellen in de locatie van de Netgebruiker.
3. Een centrale gateway verzendt real-time gegevens van verschillende SDP's, die zijn gemeten door meetapparaten op het terrein van verschillende netwerkgebruikers.

In configuraties 1 en 2, worden de gateways altijd lokaal geïnstalleerd binnen de locatie van de netgebruiker.

In alle configuraties,

- a) Bevindt het private meettoestel zich bij het SDP. Het SDP wordt gedefinieerd op het niveau van het leveringspunt of toegangspunt.
- b) Een gateway moet om de 4s de ogenblikkelijke vermogensmeetwaarden van een meettoestel en andere noodzakelijke parameters verzamelen die nodig zijn voor de aFRR-diensten, en deze in real-time communiceren naar het realtime Communicatieplatform met behulp van een door Elia bepaald communicatieprotocol.



figuur 2: schematisch overzicht

3 Vereisten meetsystemen

Tenzij anders gespecificeerd¹ in het Technisch Reglement voor het Distributienet naargelang de Regio, moet het private meetsysteem voldoen aan volgende minimumvereisten:

- De nauwkeurigheidsklasse van de meetkern van de stroomtransformatoren (current transformers, CT) moet ten minste overeenstemmen met de vereisten van de stroomtransformatoren voor vermogensmetingen zoals gespecificeerd in de onderstaande tabel 1.
- De nauwkeurigheidsklasse van de meetkern van de spanningstransformatoren (voltage transformers, VT) moet ten minste overeenstemmen met de vereisten van de spanningstransformatoren voor vermogensmetingen zoals gespecificeerd in de onderstaande tabel 1.
- De nauwkeurigheidsklasse van het meetsysteem voor de 4s vermogensmetingen moet overeenstemmen met de vereisten van de vermogensmetingen, zoals gespecificeerd in de onderstaande tabel 1.
- Het meetsysteem moet een steekproefsnelheid hebben die het mogelijk maakt om precies elke 4 seconden een nieuwe waarde te geven. De steekproefsnelheid moet $1/2^n$ maal het interval van 4s zijn (met n als geheel getal > 0).
- Zoals vereist door het technisch voorschrift C2/112 van Synergrid, is elke kabel die de stroom- en spanningstransformator verbindt met een meettoestel van het type LIYY en moet het voldoen aan de volgende vereisten wat betreft doorsnede en lengte:

Elektrische kabellengte	Spanningscircuit	Vermogenscircuit
< 8 m (minimum 3m)	4 x 2,5 mm ² Cu	6 x 2,5 mm ² Cu
≥ 8m (maximum 18m)	4 x 2,5 mm ² Cu	6 x 4 mm ² Cu

De verbinding van de kabels tussen de transformatoren en het meettoestel moet ononderbroken zijn (zonder aftakkingen, noch tussenliggende verbindingstrips) en uitgevoerd worden overeenkomstig artikel 4.4.2.2. van het AREI.

De aansluitkabels naar stroom- en spanningstransformatoren mogen geen deel uitmaken van dezelfde kabel.

- Een systeem met 2 of 3 stroom-/spanningstransformatoren mag (twee- of drie-wattmetermethode), maar de drie-wattmetermethode krijgt de voorkeur.

¹ Onderstaande afwijkingen zijn enkel van toepassingen in het kader van aFRR zonder energieoverdracht

- De installatie moet correct geaard zijn.
- Nauwkeurighedscontrole van het meetsysteem is om de 5 jaar verplicht volgens de technische specificaties van de distributienetbeheerders. Een kopie van het rapport wordt aan de distributienetbeheerder bezorgd.

Vermogen van gemeten proces	VT	CT	Vermogensmeter
	Nauwkeurigheidsklasse	Nauwkeurigheidsklasse	Nauwkeurigheidsklasse /vereisten
≥ 10MVA	0,2	0,2S	0,2S of 0,25
≥ 5MVA à < 10MVA	0,2	0,2S	0,5S
≥ 1 MVA à < 5MVA	0,2	0,2	0,5
≥ 100 kVA à < 1MVA	0,5	0,5	1
≥ 32kVA en < 100kVA	NA	0,5 ²	2% ³⁴
≥ 11kVA en < 32kVA	NA	0,5 ¹	3,5% ²³
≥ 4kVA en < 11kVA	NA	0,5 ¹	6% ²³
< 4 kVA	NA	0,5 ¹	10% ²³

Tabel 1 – Tabel met nauwkeurigheidsklasse

4 Vereisten gateways

Dit deel beschrijft de gedetailleerde interfacevereisten voor gegevensuitwisseling voor het uitwisselen van gegevens tussen de gateways, het Communicatieplatform en de beveiligingscomponenten.

De beveiligingsmechanismen maken een betrouwbare en veilige gegevensuitwisseling mogelijk: de Public Key Infrastructure (PKI) maakt authenticatie van de gateways op basis van certificaten mogelijk en het Key Management System verstrekt encryptiesleutels die gebruikt kunnen worden om berichten (body) te versleutelen.

4.1 Gegevensstromen

De gateway moet een digitaal certificaat van een Public Key Infrastructure (PKI) kunnen aanvragen, ontvangen en gebruiken voor authenticatie (geldigheid: 2 jaar). De gateway moet end-to-end versleutelde berichten kunnen versturen op basis van dagelijks door een Key Management System (KMS) verstrekte encryptiesleutels.

² Indien vereist.

³ Compliancy en gecertificeerd volgens de certificeringsprocedure beschreven in "General technical requirements for private measurement" zoals gepubliceerd op de ELIA website.

⁴ Alleen van toepassing bij een minimaal biedvolume van 100kW.

4.2 Interfaces

4.2.1 Verificatie op basis van certificaten

De gateway moet certificaat-gebaseerde authenticatie ondersteunen op basis van X.509-certificaten (PFX/CERT).

4.2.2 FCR en aFRR Berichten

De berichten in de gegevensuitwisseling zullen bestaan uit een functionele header en een message body. De gateway moet JSON-berichten (RFC 8259) kunnen genereren en verzenden. De gateway moet tijdstempels in ticks-formaat (UTC, referentie 01-01-2019) ondersteunen.

4.2.2.1.1 Protocol

De gateway moet het MQTTS-protocol of Azure Event Hubs ondersteunen voor communicatie naar het Communicatieplatform.

4.2.2.1.2 Encryptiealgoritme

De gateway moet AES/Rijndael (128-bit, CBC, PKCS7-padding) symmetrische versleuteling ondersteunen conform ISO/IEC 18033-3.

4.2.3 Encryptiestleutels

De gateway moet encryptiesleutels kunnen ontvangen van het Key Management System via het Communicatieplatform, en meerdere sleutelversies parallel kunnen beheren (overlappingsperiode van 12 uur, geldigheid 36 uur, dagelijkse rotatie).

4.2.4 Aanvraag encryptiesleutel

Bij vervanging of herstart met lege configuratie moet de gateway de laatste geldige encryptiesleutel(s) kunnen opvragen bij het KMS.

4.2.5 Heartbeat

De gateway moet een heartbeat-mechanisme ondersteunen (initieel elke 5 minuten), zowel ad-hoc als weerkerend, om connectie en authenticatie te kunnen verifiëren.

4.3 Verwerking van uitzonderingen

4.3.1 Buffering

Een lokale buffering van minstens 5 dagen moet lokaal gebeuren. Dit zal gebruikt worden wanneer de communicatie tussen de GW en het real-time communicatieplatform onderbroken is. De gegevens moeten worden voorzien van een tijdstempel op het moment dat ze worden aangemaakt.

Eens de communicatie hersteld is, moeten de berichten die tijdens de onderbreking niet verstuurd werden, alsnog verstuurd worden.

4.3.2 Throttling

Om overbelasting te voorkomen kan er maximaal **1** bericht per seconde per gateway verzonden worden.

4.3.3 Berichtengroepering

Berichtengroepering kan gebeuren voor een periode van 1 minuut (15 gegevens van 4s). Merk op dat dit alleen geldig is tijdens het verwerken van uitzonderingen (communicatiestoring, ...).

4.3.4 Fallbackbestanden

De FSP moet, op verzoek van Elia, in staat zijn om een fallbackbestand voor een periode van minimum 90 dagen te leveren met tijdreeksen die dezelfde parameters bevatten als die welke worden gevraagd in de FCR of aFRR-berichten.

4.4 Service level agreements

Om een correcte, volledige en realtime gegevensuitwisseling te verzekeren, is een controle voorzien op basis van KPI's die zijn gedefinieerd in de documenten beschikbaar op Elia website (bvb: "aFRR - Communication Requirements"). Niet-naleving van deze KPI's kan leiden tot diskwalificatie van de FSP.

5 Tijdsynchronisatie en tijdstempel

Omdat elke meting moet voorzien zijn van een tijdstempel, zijn er twee opties:

- (1) De tijdreferentie en -stempel worden gegeven in de gateway;
- (2) De tijdreferentie en -stempel worden gegeven in het meettoestel.

De gegevens moeten elke 4 seconden een tijdstempel krijgen.

Wat betreft tijdsynchronisatie moet het toestel dat verantwoordelijk is voor de tijdstempel te allen tijde gesynchroniseerd zijn met een NTP-server of een gelijkaardig systeem. De nauwkeurigheid van de tijdstempel moet minstens 20ms bedragen. Bij een aanhoudend tijdsverschil vraagt het CPO via een heartbeatbericht om synchronisatie met een NTP-server.

6 Contactpersonen voor gateway

Neem voor vragen contact op met de personen die worden vermeld in de "Technical Guide for Gateway Management" beschikbaar op de Elia-website [via deze link](#).