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

C8/06

Algemene technische vereisten

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

versie 1.00

1 Logboek wijzigingen

Versie 1.0 – Oorspronkelijke Nederlandstalige versie - december 2023

2 Inleiding

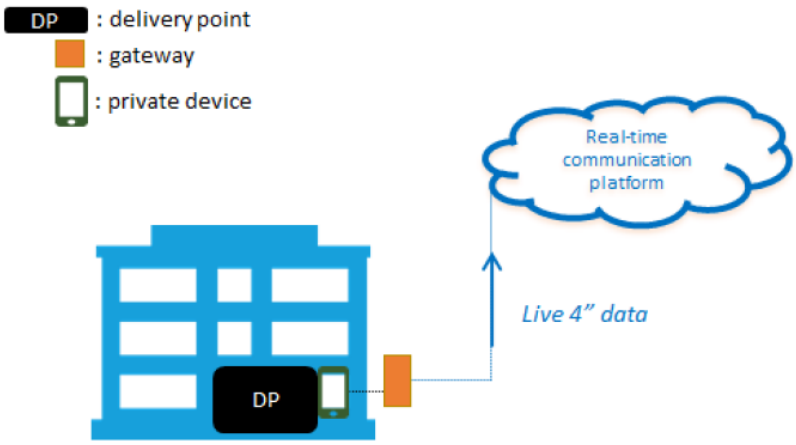
2.1 Voorwerp van voorschrift C8/06

In het ontwerp van aFRR is een realtime uitwisseling van meetgegevens en een verzameling van parameters, gebruikt voor het aFRR settlement proces, vereist voor dienstleveringspunten (d.w.z. leveringspunten waarvoor ELIA geen MW-dagschema's ontvangt) die deelnemen aan de dienst 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:

- beperkt zich tot aFRR-dienstleveringspunten aangesloten op het distributienet.
- definieert enerzijds minimale technische en regulatorische vereisten voor een meetsysteem (= meettoestel met accessoires) wanneer energieoverdracht niet van toepassing is. Wanneer energieoverdracht wel van toepassing is op het flexibiliteitsproduct, zal een nieuwe analyse van de specifieke vereisten worden uitgevoerd, wat kan resulteren in wijzigingen van het huidige voorschrift.

- beschrijft anderzijds het technisch kader met betrekking tot het beheer van de gateways en leveringspunten (Service Delivery Points, SDP's) en hun interacties met het realtime Communicatieplatform.

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.

In beide configuraties,

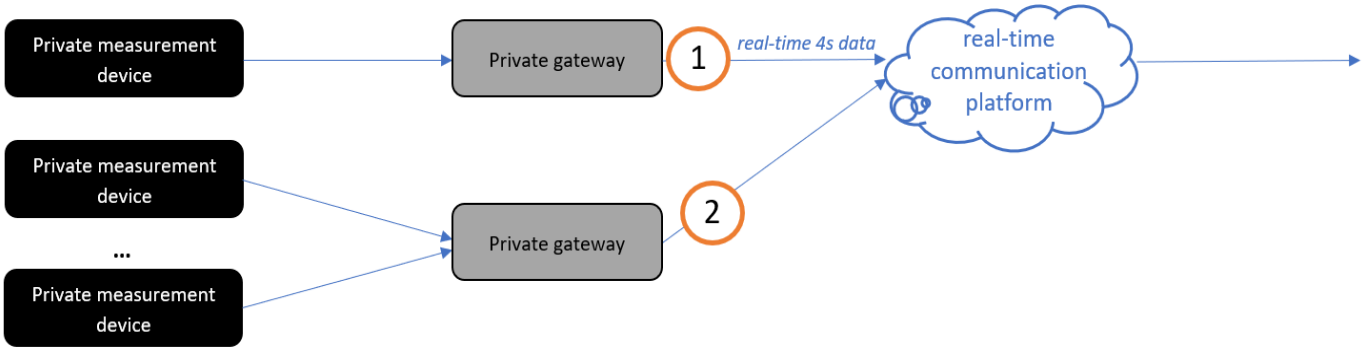
a. Bevindt het private meettoestel zich bij het SDP. Het SDP kan ook gedefinieerd worden op het niveau van het hoofdpunt/toegangspunt.

b. De verbinding van een enkele gateway met SDP's die zich op twee of meer toegangspunten bevinden is niet toegestaan.

c. 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.

d. De communicatie van de gateway naar het Communicatieplatform dient zonder intermediair communicatiesysteem van derden te gebeuren.

e. De gateways worden altijd lokaal geïnstalleerd binnen de locatie van de netgebruiker dat wordt afgebakend door het hoofdpunt/toegangspunt.



figuur 2: schematisch overzicht

Een local gateway die rechtstreeks verbonden is met het Real-Time Communication Platform (zoals hierboven beschreven), is de finale vereiste. Een overgangsperiode is voorzien tot uiterlijk 31 december 2026.

Deze overgangsperiode impliceert dat een tijdelijke afwijking van de finale technische vereisten zoals hierboven vermeld onder punten b, d & e is toegestaan (aanvaarding van een gedegradeerde modus). Deze tijdelijke afwijking staat het gebruik van connectie naar het Real-Time Communication Platform via **gecentraliseerde virtual gateways** toe.

De gegevens worden nog steeds per leveringspunt verzonden, waarbij meerdere leveringspunten gekoppeld kunnen worden aan een virtuele gateway, naar het Communicatieplatform. Alle in dit document beschreven specificaties en de bijhorende bedrijfsprocessen blijven van toepassing en moeten worden nageleefd. Aan het einde van de overgangsperiode moeten alle deelnemers voldoen aan de definitieve technische vereisten, waarbij gateways lokaal moeten geïnstalleerd zijn en rechtstreeks verbinding maken met het Communicatieplatform.

3 Vereisten meetsystemen

Tenzij anders gespecificeerd 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.

- De distributienetbeheerder zal de nauwkeurigheid van de CT's, VT's en het meetsysteem controleren.

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

De verbinding van de kabels tussen de transformatoren en het meettoestel moet ononderbroken zijn (zonder aftakkingen, noch tussenliggende verbindingsstrips) 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.

- De installatie moet correct geaard zijn.

- Nauwkeurigheidscontrole 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[1]	2%[2][3]
≥ 11kVA en < 32kVA	NA	0,5[1]	3,5%[2][3]
≥ 4kVA en < 11kVA	NA	0,5[1]	6%[2][3]
< 4 kVA	NA	0,5[1]	10%[2][3]

[1] Indien vereist.
[2] Compliancy en gecertificeerd volgens de certificeringsprocedure beschreven in "General technical requirements for private measurement" zoals gepubliceerd op de ELIA website.
[3] Alleen van toepassing bij een minimaal biedvolume van 100kW.

4 Vereisten gateways

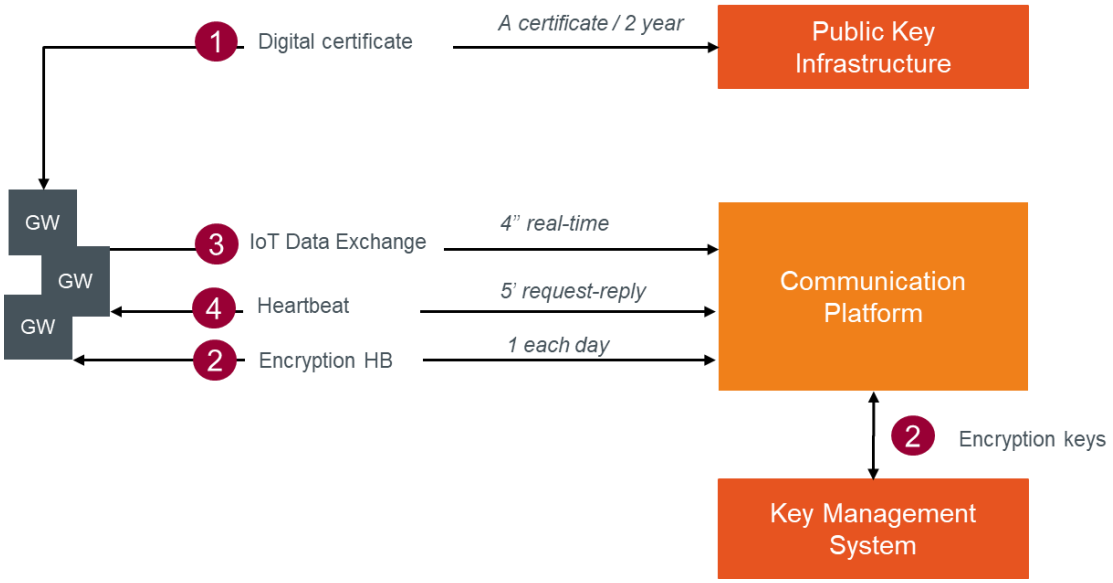
4.1 Vereisten voor Gegevensuitwisseling

Dit deel beschrijft de gedetailleerde interfacevereisten voor gegevensuitwisseling voor het uitwisselen van gegevens tussen de gateways, het Communicatieplatform en de beveiligingscomponenten. In de eerste versie van het platform is de uitwisseling van aFRR-gegevens unidirectioneel (behalve de heartbeat), van de gateways via het aFRR-communicatieplatform naar de Flexhub. De berichtenstroom zal bestaan uit realtime 4s aFRR-berichten, die worden gebruikt voor de settlement van aFRR-activaties. Er wordt één bericht verzonden voor elk leveringspunt dat verbonden is met een gateway.

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 het aFRR bericht (body) te versleutelen.

4.1.1 Gegevensstromen

Hieronder een weergave van de E2E-processtroom van alle gegevensuitwisselingen die de gateways moeten kunnen ondersteunen.



1. Elk gateway en applicatie die wil verbinden met het Communicatieplatform zal een digitaal certificaat moeten verkrijgen van de Public Key Infrastructure (2 jaar geldig). Dit certificaat wordt gebruikt om de gateway te authenticeren voor alle verbindingen met het platform en het Key Management System.

2. De gegevens (body) moeten end-to-end versleuteld zijn (van de gateway tot de FlexHub). Elke dag genereert een onafhankelijk Key Management System (KMS) encryptiesleutels voor de versleuteling van de body en stuurt deze via het Communicatieplatform naar de gateways.

3. Om de 4 seconden stuurt de gateway een aFRR-bericht met versleutelde body naar het communicatieplatform. Om een verbinding te kunnen maken en het bericht in de wachtrij te

plaatsen, moeten de gateways een digitaal certificaat hebben dat wordt verkregen van de Public Key Infrastructure (PKI).

4. Met regelmatige tussenpozen (aanvankelijk om de 5 minuten) plaatst het Communicatieplatform een heartbeatbericht over de topic waarop de gateway moet antwoorden. Het bericht bevat kernwaarden voor specifieke use cases en voor statusupdates van gatewayverbindingen.

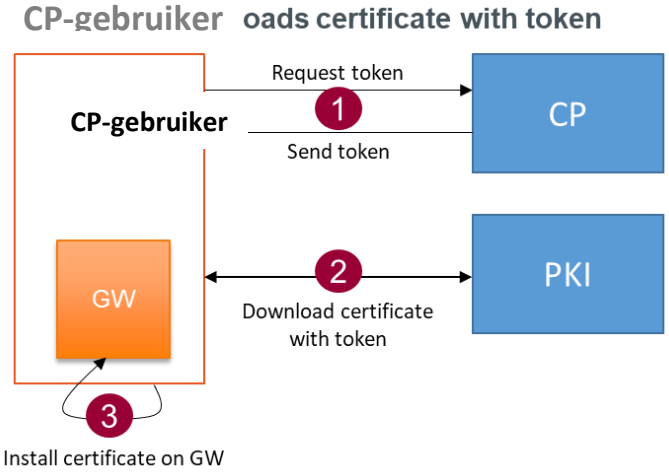
Wachtrijen voor berichten maken asynchrone communicatie mogelijk, wat betekent dat de eindpunten die berichten produceren en ontvangen interactie hebben met de wachtrij, niet met elkaar. In tegenstelling tot wachtrijen, waarin elk bericht wordt behandeld door een enkele consument, bieden **topics** en subscriptions een one-to-many vorm van communicatie, in een publish/subscribe patroon.
De gegevensuitwisseling tussen de gateway en het Comunicatieplatform gebeurt d.m.v. twee verschillende topics (1 topic per richting).

4.1.2 Interfaces

4.1.2.1 Verificatie op basis van certificaten

Voor het verkrijgen van tokens en certificaten zijn volgende scenario's voorzien:

Scenario 1: Verkrijgen van het certificaat via het portaal



1. De CP-gebruiker vraagt een token d.m.v. een actie in het gebruikersinterface van het gatewayportaal. Er wordt een validatiecode gegenereerd en weergegeven in het portaal in het betreffende gateway-informatiescherm en er vertrekt een e-mail met een token naar de CP-gebruiker.
2. De CP-gebruiker navigeert via het webportaal naar een beveiligde webpagina en gebruikt zowel het token als de validatiecode om het certificaat te downloaden.

Als de aanvraag geldig is, kan de CP-gebruiker een ZIP-bestand downloaden met een PFX-bestand en het wachtwoord om het certificaat te extraheren (CERT-bestand - X.509-certificaat).

Scenario 2: Verkrijgen van het certificaat door de gateway door middel van een token

Dit tweede scenario zal beschikbaar zijn in een volgende release en de gedetailleerde specificatie zal beschikbaar worden gesteld in een van de volgende updates van dit document.

4.1.2.2 aFRR Berichten

De berichten in de gegevensuitwisseling zullen bestaan uit een functionele header en een message body.

Alle vereiste (en optionele) velden worden beschreven in de volgende secties. In kolom Element worden afkortingen gebruikt om de tags van het bericht te beperken en zo het bericht te reduceren.

Met betrekking tot datumtijden gebruiken we het ticks-datumtijdformaat, dat zijn de milliseconden geteld vanaf de referentiedatum: **01-01-2019 00:00:00 UTC**.

4.1.2.2.1 Body (te versleutelen – zie volgende secties)

Element	Gegevens type	Oorsprong	Beschrijving
SDP – SDP EAN	String	SCADA / FSP BE	EAN van het aFRR Service Delivery Point.
DPM – DPmeasured	Decimaal (JSON)	Meettoestel	De instant nettovermogensmeting (bruto als de nettowaarde niet kan worden gemeten) (in MW) per leveringspunt.
DPB – DPbaseline	Decimaal (JSON)	SCADA / FSP BE	Het vermogen (in MW) dat het leveringspunt zou hebben geïnjecteerd/verbruikt zonder activering van een aFRR-dienst, voor de tijdstempel in het veld MTS – Measure Timestamp + 1 minuut.
AS – DPaFRR	Integer (JSON)	SCADA / FSP BE	Dit is een logisch (0 of 1) signaal dat aangeeft of het leveringspunt de dienst levert voor het betreffende tijdsbestek.
PS – DPaFRR,supplied	Decimaal (JSON)	SCADA / FSP BE	Het aantal MW van ΔPsec_tot4 dat door de BSP wordt toegewezen aan het leveringspunt in kwestie.
MTS – Measure timestamp	Ticks (UTC)	Meettoestel / gateway	De datumtijd waarop de momentopname van de Pmeasured wordt genomen. De Pbaseline in dit bericht vertegenwoordigt de waarde voor deze tijdstempel + 1 minuut in de toekomst.

4.1.2.2.2 Header

Element	Gegevenstype	Oorsprong	Beschrijving
MT - Message Type	String	Afkomstig van gegevensbron	Geeft het berichttype & de frequentie weer. Dit zorgt ervoor dat elk berichttype uniek is, ongeacht de gevraagde frequentie.
SID – Sender Id	String	Afkomstig van gegevensbron	Het Endpoint Id zoals geregistreerd in het Communicatieplatform.
GID – Gateway Id	String	Afkomstig van gegevensbron	De gateway-ID van de gateway zoals aangemaakt door het Communicatieplatform.
EKV – Encrypted key version	Integer (optioneel)	Afkomstig van gegevensbron	De versie van de gebruikte encryptiesleutel (verandert op geregelde tijdstippen). Indien niet verzonden wordt de body beschouwd als: niet versleuteld.
HV - Header version	Integer	Afkomstig van gegevensbron	De Header version maakt communicatie mogelijk over hetzelfde berichttype maar met verschillende versies als de headerstructuur van het bericht wordt bijgewerkt. Op deze manier hebben de verzenders de tijd om zich aan te passen en weet de ontvanger hoe hij het bericht moet interpreteren.
BV - Body version	Integer	Afkomstig van gegevensbron	De body version maakt communicatie mogelijk over hetzelfde berichttype maar met verschillende versies als de bodystructuur van het bericht wordt bijgewerkt. Op deze manier hebben de verzenders de tijd om zich aan te passen en weet de ontvanger hoe hij het bericht moet interpreteren.
CTS - Creation timestamp	Ticks (UTC)	Afkomstig van gegevensbron	De tijdstempel wanneer het bericht verzonden werd.

4.1.2.2.3 Protocol

Het MQTTS protocol moet gebruikt worden tussen de gateway en het Communicatieplatform.

4.1.2.2.4 Encryptiealgoritme

Om de berichten te versleutelen, wordt het algoritme Advanced Encryption Standard (AES) / Rijndael (128 bits) met symmetrische sleutels gebruikt. Verschillende implementatiebibliotheken zijn te vinden in Python, JAVA, C#, ...

Het algoritme wordt beschreven in de norm ISO/IEC 18033-3. Hier kan men een eenvoudige beschrijving van het algoritme vinden:

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

Dit algoritme wordt standaard gebruikt met de volgende parameters:

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

4.1.2.3 Encryptiestleutels

Zoals beschreven in de processtromen, zal een Key Management System encryptiesleutels genereren en deze beschikbaar stellen aan elke afzonderlijke gateway via het Communicatieplatform.

Daartoe wordt een specifiek berichttype uitgewisseld.

4.1.2.3.1 Header

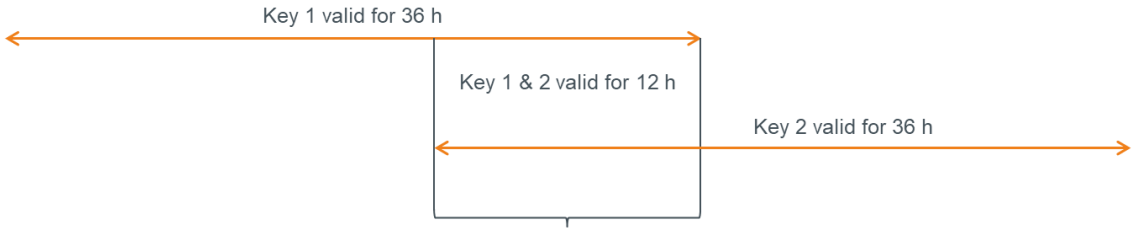
Parameter	Waarde	Beschrijving
MT - Message Type	String (ENCRYPTION KEY)	Geeft het berichttype & de frequentie weer. Dit zorgt ervoor dat elk berichttype uniek is, ongeacht de gevraagde frequentie.

4.1.2.3.2 Body

Parameter	Waarde	Beschrijving
MT – Message Type		De Message Type waarvoor de sleutel wordt aangevraagd.
KEY	string	De encryptiesleutel zelf. Deze sleutel wordt versleuteld vanuit het beveiligde KMS aan de hand van het GW-certificaat.
KV - Key version	integer	De key version van de aangevraagde sleutel.
KT – Key Type	string	Het algoritme ondersteund voor versleuteling.
VF - Geldig van (Start geldigheid)	Ticks	Datumtijd begin geldigheid van de encryptiesleutel.
VT - Geldig Tot (Einde geldigheid)	Ticks	Datumtijd einde geldigheid van de encryptiesleutel.

Gateways

Een encryptiesleutel blijft **36 uur** geldig en er wordt dagelijks een nieuwe sleutel opgehaald. Dat betekent dat er een overlapping van 12 uur is waarbinnen de nieuwe sleutel ontvangen en gebruikt moet worden:



4.1.2.3.3 Technische informatie

Het Communicatieplatform zal dit berichttype uitwisselen volgens dezelfde principes als de aFRR-berichten, maar in de andere richting. Er zal een specifiek topic voor deze berichtenuitwisseling worden voorzien.

Merk op dat momenteel alleen het AES / Rijndael algoritme ondersteund wordt door het platform. Andere kunnen later worden toegevoegd.

Om de vertrouwelijkheid van de sleutel te garanderen, wordt de sleutel in het bericht versleuteld met de publieke sleutel van het gatewaycertificaat. De gateway zal de eigen private sleutel van het certificaat nodig hebben om de sleutel te ontcijferen en vervolgens om berichten te versturen.

Voorbeeld van een bericht:

{

"MT": "ENCRYPTIONKEY",

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

4.1.2.4 Aanvraag encryptiesleutel

Zoals beschreven in de processtromen, zal een Key Management System encryptiesleutels genereren en deze beschikbaar stellen aan elke afzonderlijke gateway via het Communicatieplatform. Als de gateway moet vervangen worden of heropgestart met een lege configuratie, moet(en) de laatste encryptiesleutel(s) opgevraagd worden om nieuwe berichten te kunnen versturen.

Daartoe wordt een specifiek berichttype uitgewisseld.

Merk op dat één bericht zal ontvangen worden (zoals beschreven in sectie 4.1.2.3) voor elk berichttype en versie beheerd door de gateway met een actieve aFRR-dienst (normaal gesproken slechts één omdat er momenteel slechts één berichttype met slechts één versie is).

4.1.2.4.1 Header

Parameter	Waarde	Beschrijving
MT - Message Type	String (ENCRYPTIONKEYREQUEST)	Geeft het berichttype & de frequentie weer. Dit zorgt ervoor dat elk berichttype uniek is, ongeacht de gevraagde frequentie.

4.1.2.4.2 Body

Body is leeg.

4.1.2.4.3 Technische informatie

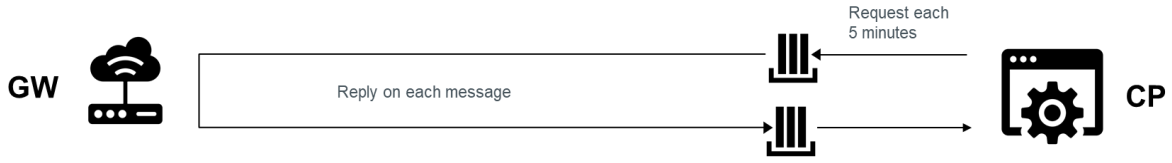
Het Communicatieplatform zal dit berichttype uitwisselen volgens dezelfde principes als de aFRR-berichten, maar in de andere richting. Er zal een specifiek topic voor deze berichtenuitwisseling worden voorzien.

Voorbeeld van een bericht:

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

4.1.2.5 Heartbeat

Het heartbeatmechanisme maakt het mogelijk om sleutelwaarden uit te wisselen tussen de gateways en het Communicatieplatform die geen verband houden met de uitwisseling van marktgegevens van eindpunten.



Het Communicatieplatform geeft de frequentie van de heartbeatberichten aan en wordt in eerste instantie ingesteld op elke vijf minuten.

Het heartbeatbericht kan op twee manieren werken:

- Ad hoc: er zal een actieknop in het beheerportaal worden voorzien om een eenmalig heartbeatbericht naar de gateway te sturen. Als dit bericht succesvol werd beantwoord door de gateway, wordt de communicatiestatus op 'Verbonden' gezet. Zo kan de gebruiker de connectie en de authenticatie van een gateway testen.

- Weerkerend: zodra een dienst geactiveerd is op dit eindpunt, zal het CP een heartbeat initiëren met een interval naar keuze (aanvankelijk 5 minuten). Ook hier wordt de communicatiestatus van de gateway bijgewerkt in het portaal als een heartbeat niet beantwoord wordt. De time to live van het heartbeatbericht is gelijk aan de heartbeatfrequentie (aanvankelijk 5 minuten).

4.1.2.5.1 CP naar GW

Header

Parameter	Waarde	Beschrijving
MID - MessageId	Integer	Een teller die gereïnitialiseerd kan worden.
MT - Message Type	String (HEARTBEAT)	Geeft het berichttype & de frequentie weer. Dit zorgt ervoor dat elk berichttype uniek is, ongeacht de frequentie waarmee het heartbeatbericht gepost wordt.

Body

Parameter	Waarde	Beschrijving
TS - Time Sync	1	Alleen aanwezig wanneer een gateway zijn interne klok moet synchroniseren met een NTP-server.
GWV - GW Version	1	Alleen aanwezig wanneer een gateway zijn firmware- en softwareversie moet doorgeven. Dit zal dagelijks worden opgevraagd.

TimeSync en GW version parameters zijn 2 sleutels die als lijst met parameters in het bericht kunnen worden toegevoegd. Andere parameter(s) kunnen later worden toegevoegd in de body.

Voorbeeld van bericht zonder tijdsynchronisatie en GW-versie vereist:

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

Voorbeeld van bericht met tijdsynchronisatie en zonder GW-versie vereist:

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

Berichtvoorbeeld zonder tijdsynchronisatie en met GW-versie vereist:

```
{
   "MID": 36.
```

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

Voorbeeld van bericht met tijdsynchronisatie en GW-versie vereist:

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

4.1.2.5.2 GW to CP

Header

Parameter	Waarde	Beschrijving
MID - MessageId	Integer	ID van het Heartbeat aanvraagbericht.
MT - Message Type	String (HEARTBEAT)	Geeft het berichttype & de frequentie weer. Dit zorgt ervoor dat elk berichttype uniek is, ongeacht de gevraagde frequentie.
GID – Gateway Id	String	De gateway-ID van de gateway zoals geregistreerd in het Communicatieplatform.
CTS - Creation timestamp	Ticks (UTC)	De tijdstempel wanneer het bericht verzonden werd.

Body

Parameter	Waarde	Beschrijving
SV - Software version	String	De softwareversie waarop de gateway draait. Alleen te verzenden wanneer het veld GW Version in de aanvraag is verzonden.
FWV - Firmwareversion	String	De softwareversie waarop de gateway draait. Alleen te verzenden wanneer het veld GW Version in de aanvraag is verzonden.

Voorbeeld van een bericht waarbij geen software- en firmwareversie nodig zijn:

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

},

Voorbeeld van een bericht waarbij software- en firmwareversie nodig zijn:

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

4.1.2.5.3 Technische informatie

De Heartbeat wordt regelmatig naar het GW-ontvangertopic gestuurd. Het antwoord wordt op dezelfde topic gestuurd als de aFRR-berichten.

4.1.3 Verwerking van uitzonderingen

4.1.3.1 Buffering

Een lokale buffering van minstens 5 dagen moet lokaal gebeuren. Dit zal gebruikt worden wanneer de communicatie tussen de GW en het aFRR-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.

4.1.3.2 Throttling

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

4.1.3.3 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, ...).
- Bij groepering wordt de header slechts eenmaal verzonden en worden de body's van de specifieke tijdreeksen gegroepeerd in een enkele body.
- De body wordt slechts eenmaal versleuteld.

4.1.3.4 Fallbackbestanden

In het geval dat Elia de gegevens niet ontvangt in realtime communicatie voor grotere onderbrekingen, worden de volgende maatregelen genomen:

- De FSP moet, op verzoek van Elia, in staat zijn om een fallbackbestand te leveren met tijdreeksen die dezelfde parameters bevatten als die welke worden gevraagd in het aFRR-bericht.
- Elia kan enkel fallbackbestanden opvragen voor een periode van maximum 90 dagen vóór de dag van de aanvraag.
- De aanlevering van het fallbackbestand dient binnen vijf werkdagen te gebeuren.

4.1.4 *Service level agreements*

Om een correcte, volledige en realtime gegevensuitwisseling te verzekeren, is een controle voorzien op vooraf bepaalde KPI's.

4.2 Technische kenmerken

4.2.1 *URL's en config*

Het platform zal toegankelijk zijn via volgende URL's:

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

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

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

Hou er rekening mee dat de eerste tests met de Pre-Prod-omgeving uitgevoerd zullen worden vanaf 18 mei. De acceptatieomgeving zal worden gebruikt wanneer updates van het platform worden uitgebracht. De productieomgeving (die gebruikt zal worden voor de prekwalificatietests) wordt in de komende weken beschikbaar gesteld.

Dit is de URL van het Device Provisioning System zonder gebruik te maken van de Microsoft SDK:

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

Het GatewayBusinessId wordt gegenereerd door het platform wanneer een nieuwe Gateway wordt aangemaakt.

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

Met de Microsoft SDK is de connectiestring als volgt:

global.azure-devices-provisioning.net

Merk op dat deze URL's & configuraties niet wijzigen in geval van DRP.

De naam van de 2 topics:
Cloud to Device: $"devices/{GatewayBusinessId}/messages/devicebound/#"
Device to Cloud: $"devices/{GatewayBusinessId}/messages/events/"

4.2.2 *Testen berichtenformaat*

De waarde van JSON-berichten (RFC 8259-formaat) in het communicatieportaalinterface zal worden getest.

4.2.3 ***Voorbeelden***

Hieronder worden enkele voorbeelden van berichten gegeven. Het zal ook mogelijk zijn om het berichtformaat (JSON Validation) te testen in het testplatform.
Voor meer details over hoe verbinding te maken met het platform en een gedetailleerd voorbeeld (in C#) van de code om verbinding te maken met ons platform, verwijzen we naar de technische referentie zoals omschreven in punt 2 van dit document.
Andere voorbeelden (in diverse programmeertalen) zijn hier te vinden: https://docs.microsoft.com/en-us/azure/iot-hub/iot-hub-devguide-sdks.

De betreffende sectie is '**IoT Hub Device SDKs**'

4.2.3.1 Gegevensuitwisseling

Berichten moeten worden verzonden met een versleutelde body. In dit gedeelte wordt een overzicht gegeven van niet-versleutelde en versleutelde gegevens, zodat de juiste JSON kan worden gegenereerd voor de versleuteling. Zoals eerder beschreven kan de body meerdere gegevens van 4 seconden bevatten voor het ondervangen van bepaalde uitzonderingsstromen. Beide gevallen worden hieronder omschreven.

- aFRR gegevens – Onversleuteld JSON met 4s gegevens:


```
{
  "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 gegevens – Versleuteld JSON met 4s gegevens:

De encryptiestleutel voor deze boodschap heeft volgende eigenschappen:

Encryptietype: RijndaelManaged -> KeySize: 128, Padding: PKCS7, Mode: CBC
Encryptiesleutel: 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 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.