

SEC Change Monthly Working Group Meeting

September 2023

Competition Act Compliance

It is everyone's responsibility to say something

The Chair will move the conversation on



Housekeeping

- Please raise your hand
- Please be clear, explain acronyms
- This session will be recorded for minuting purposes, please be courteous!
- Just a reminder that we should be able to have free discussions of ideas



■ Introductions

- When I say your name please:
 - Say hello so we can check your audio is working
 - Which company you are from
 - If you are a Supplier/Network Party/other



■ MP231: 'Firmware upgrade pathways'

Raised by Gordon Hextall on behalf of the Security Sub-Committee (SSC)

■ Objectives of the Working Group

REVIEW	The issue
REVIEW	The Proposed Solution
AGREE	The next steps

Current arrangements

- GBCS Section 11.1 contains information relating to firmware upgrades.
- Device Manufacturers can specify any special requirements to be applied to a firmware upgrade on their Device, and what controls or dependencies are included.
- Certain Device models need to have a firmware upgrade applied in a specific order.

Issue

- Not an uncommon requirement for firmware updates to be implemented in a specific order.
- Failure to follow the specific order can result in unintended consequences.
- No central location for information required to ensure each Device's firmware upgrade is applied correctly.
- No requirement in the SEC for that information to be provided.

■ Current Proposed Solution

Central Products List (CPL)

- The CPL Entry ID describes a unique Device model.
- Proposed new Fields on the CPL New Entry form:
 - Firmware upgrade pathway
 - ZigBee Chipset Vendor
 - ZigBee Stack Version
 - ZigBee Band

Firmware Information Repository (FIR)

- Inclusion of these new fields in the FIR.
- Firmware upgrade pathway contains the previous CPL Entry IDs which must be used as a base firmware version when carrying out a firmware upgrade.
 - May contain several base firmware versions when permitted.
 - Must contain “N/A” if no previous base firmware version exists.
- Firmware Upgrade Path needs to be editable by SECAS.
 - This allows updates to the be made.

Proposed Solution (2)

CPL Firmware Information Repository				
CPL Reference	Manufacturer	Contact Details	Manufacturer Firmware Description / Information	Upgrade Path CPL Reference
000462	EDMI Europe Ltd	17, Bartley Business Park, Bartley Way Hook, RG27 9XA UK 01256 830 990 https://www.edmi-meters.com/europe/ vivek.srivastava@edmi-meters.com	Electric Meter Factory and OTA release	000432
000527	EDMI Europe Ltd	17, Bartley Business Park, Bartley Way Hook, RG27 9XA UK 01256 830 990 https://www.edmi-meters.com/europe/ Suki.Nahar@edmi-meters.com	Electric Meter Factory and OTA release	000462
000528	EDMI Europe Ltd	17, Bartley Business Park, Bartley Way Hook, RG27 9XA UK 01256 830 990 https://www.edmi-meters.com/europe/ Suki.Nahar@edmi-meters.com	Electric Meter Factory and OTA release	000462 000527

000462

000462

000527

000528

000528

Feedback to date

Sub-Committees & Working Group	Refinement Consultation was supportive
	Sub-Committees supportive
Contractual issue	Solved by a technical solution?
	Is CPL appropriate to mandate Manufacturers?
Manufacturer concerns	Happy to share info upon request
	Most would require the use of an NDA
Keeping up to date	SLA needed on SECAS
	What can be mandated on Manufacturers?

■ Moving forward

Will this fix an issue?

- Should the solution be implemented regardless as a protective measure?

Will Small Suppliers use this?

- Would it be used if information required an NDA to be signed?

Do SEC Parties use the existing FIR? (~60 downloads in 2023)

Should there be an SLA placed on SECAS for updates?

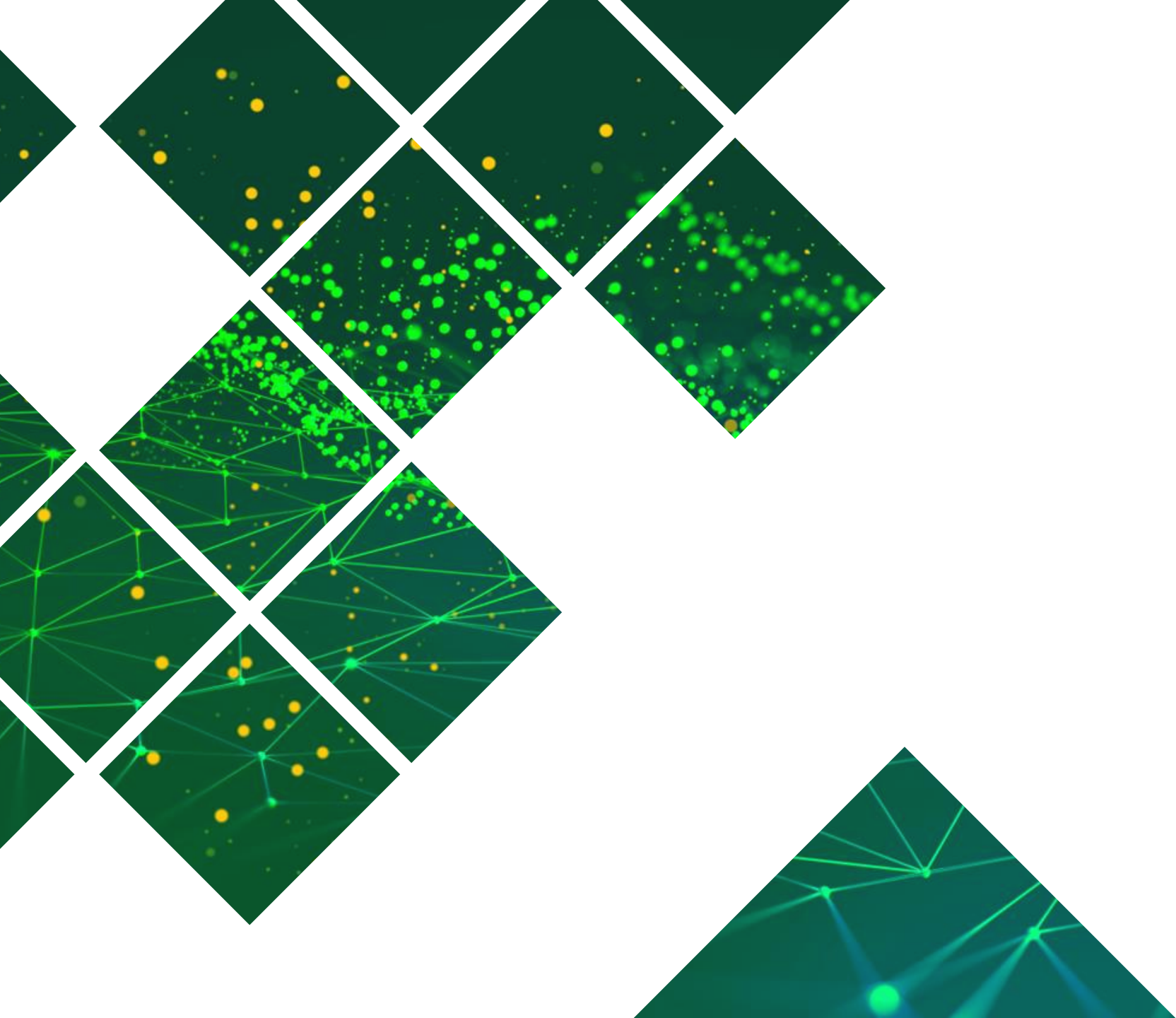
Should there be a disclaimer - Always check Release Notes and contact Manufacturer for questions

Next steps



■ Questions for the Working Group

Subject to fine tuning
from these discussions
is the Proposed
Solution suitable?



Thank you for
listening

Any questions?

■ MP223 'WAN Coverage Reporting'

Raised by Emslie Law of OVO

Objectives of the Working Group

REVIEW	DCC Preliminary Assessment
REVIEW	The Proposed Solution
AGREE	The next steps

■ MP223: Overview

Issue

- There is no obligation in the SEC for the DCC to report on WAN Coverage.

Impact

- Without reporting on WAN coverage, Suppliers may waste resources by planning installs in areas of no WAN.
- Negative impacts on the consumers view of the Smart Metering Implementation Programme (SMIP).

■ PROPOSED SOLUTION – REQ'S 1 AND 2

Business Requirements

- R1 - The DCC to produce a headline figure of WAN coverage levels for each CSP region every three months.
- R2 - The DCC to produce reporting on addresses where there is no WAN or the WAN status has changed every three months.

Proposed Solution

- Produced quarterly - will include a high-level summary of the WAN coverage in each CSP region and addresses where there is no WAN or the WAN status has changed.

■ PROPOSED SOLUTION – REQ'S 3 AND 4

Business Requirements

- R3 - The DCC to produce monthly reporting on sites where Suppliers raise WAN-related incidents in each CSP region.
- R4 - The DCC to ensure the WAN coverage checker is updated accordingly when Suppliers raise WAN-related incidents to the DCC Service Desk.

Proposed Solution

- A new template will be created to allow WAN-related incidents to be logged.
- Produced monthly – the report will detail where WAN-related incidents have been raised in each CSP region.

■ PROPOSED SOLUTION – REQ'S 5 AND 6

Business Requirements

- R5 - The DCC to produce monthly reporting on work which is ongoing to improve WAN coverage in each CSP region at sites which are currently declared to be no WAN.
- R6 - All planned WAN outages which are passed between CSPs and the DCC Service Desk to be passed to SEC Parties.

Proposed Solution

- There is no obligation for CSPs to report on planned or in progress work to improve WAN.
- No obligation for CSPs to report on planned WAN outages – therefore DCC will ask for this on an informal basis from each CSP.

■ MP223: Preliminary Assessment

Costs

- £40,000 for new reports and template to report WAN-related incidents.
- £5,000 optional cost to validate addresses and postcodes included in CSP WAN coverage data.
- £2,000 for a full Impact Assessment.

Release

- Changes are not part of SMS or technical specifications, so MP223 can be implemented separately from standard SEC Release dates.
- Six months of DCC testing before implementation.
- Targeted for November 2024 SEC Release.

■ MP223: Proposed legal text

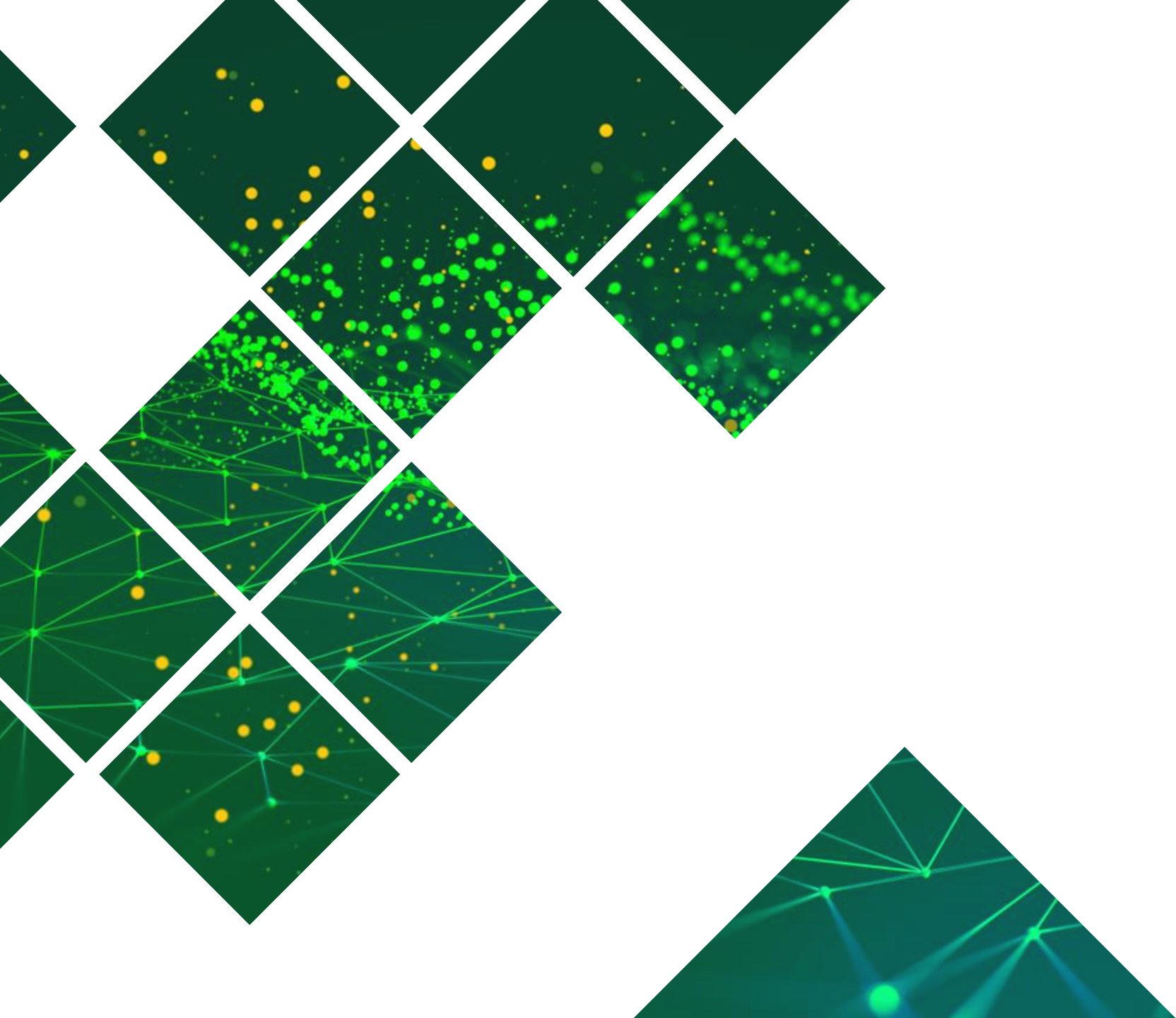
- Addition to Section H ‘DCC Services’:
 - *H13.15 The DCC shall:*
 - a) *produce quarterly reporting on WAN coverage levels for each CSP region. This figure should be calculated by the number of ‘covered’ addresses which have some level of WAN coverage against the total addresses in that CSP region.*
 - b) *produce monthly reporting where there is no WAN coverage, or the WAN coverage level has changed since the last quarterly report, this should be recorded and provided to SEC Parties.*
 - c) *produce monthly reporting when Suppliers raise WAN-related incidents to the DCC Service Desk and the address where this has been raised.*
 - d) *record all WAN incidents raised to the DCC Service Desk. A monthly report shall be produced showing all incidents in each CSP region.*
 - e) *on an informal basis, request information from CSPs about planned work and work that is ongoing to improve WAN at sites which are currently declared to have no WAN.*
 - f) *on an informal basis, request information from CSP’s about WAN outages which will then be provided to SEC Parties.*

Questions for the Working Group

- Do you have any comments on the DCC Preliminary Assessment?
- Should the additional £5,000 for independent validation of address data be included in the solution?
- A new report on planned outages and work which is ongoing to improve WAN would require DCC contract changes and would likely have very high costs. Is this something you are interested in?
- Do you have any further considerations before the Refinement Consultation?
- Any further comments?

Next Steps



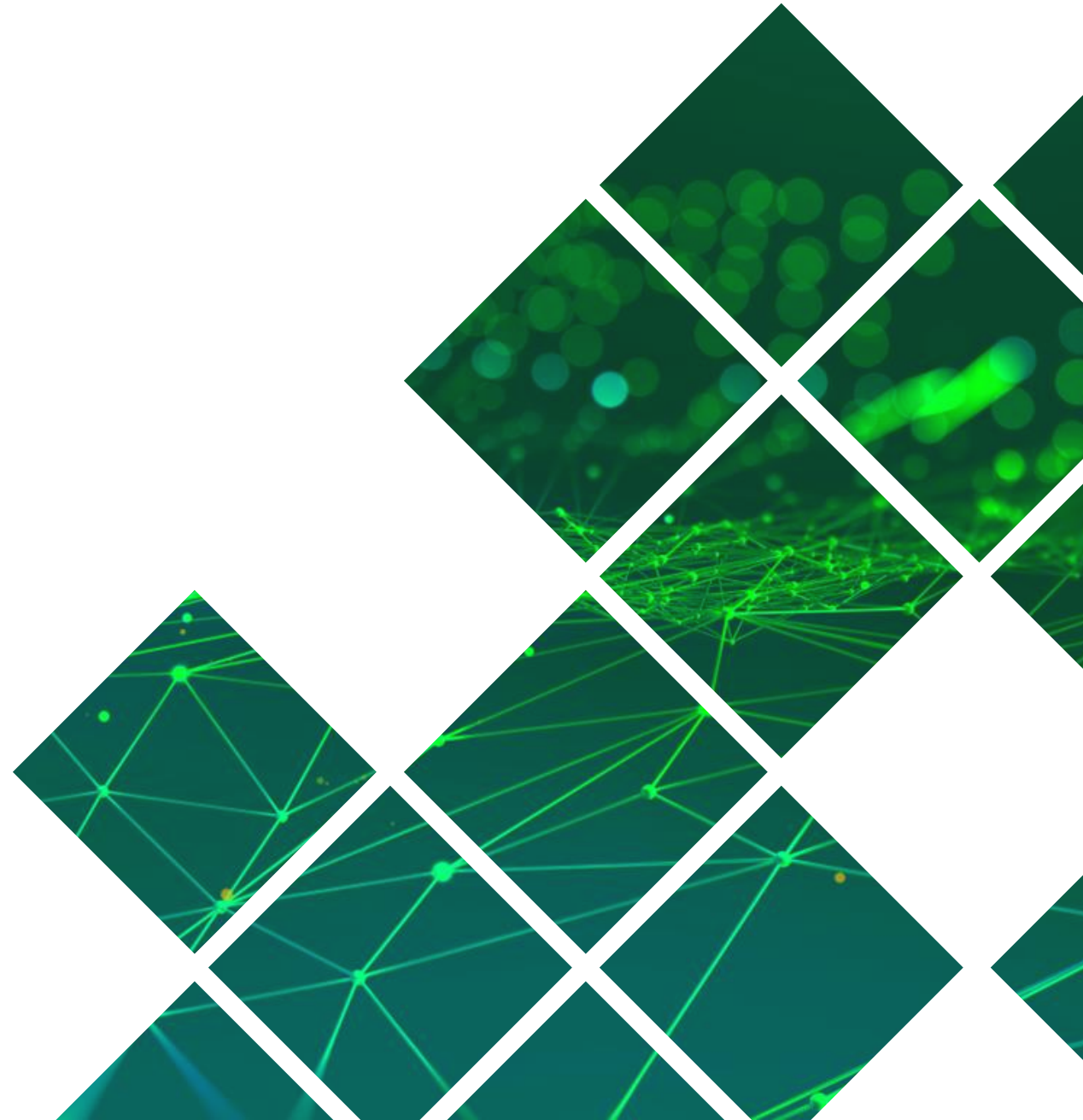


Thank you for listening

Any further
comments?

Break

Please return in 10 minutes



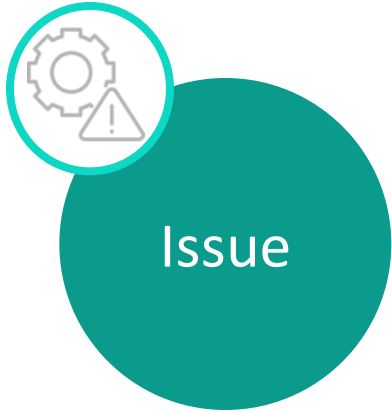
MP239 'Enduring Solution for Resolving SMETS2 Device Certificate Misalignment Issue'

Raised by Ian Turner from E.ON

■ Objectives of the Working Group

NOTE	The issue
PROVIDE	Recommendations on the business requirements
AGREE	The next steps

Overview



Device Certificate Misalignment

As part of Post Commissioning Obligations, Suppliers and WAN Providers are expected to update the Device certificate. This must be carried out within seven days following installation, via SR 6.17 'Issue Security Credentials' and Service Reference Variant (SRV) 6.15.2 'Update Security Credentials (Device)'. In some instances, the success response is not processed or not received by the DSP, resulting in a certificate misalignment between the Device and the DSP. This renders the Device incommunicable.

Approx.
120k
Devices

Common scenarios for misalignment

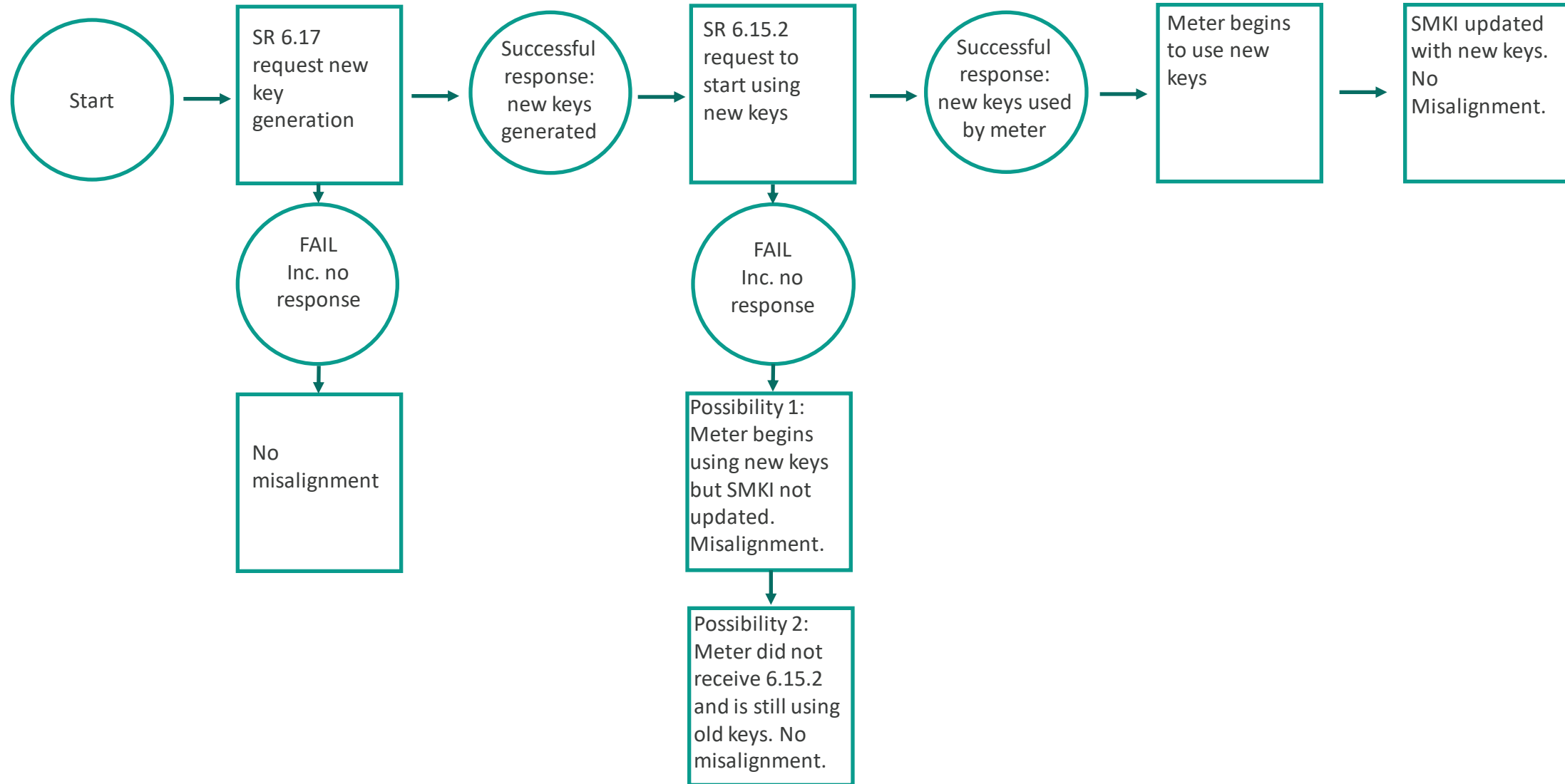
A response to SRV 6.15.2 is not processed by the DSP for reasons including:

1. the response is never generated by the Device;
2. the response is lost in transit; or
3. the response reaches the DSP after timeout.

Impact

Parties are unable to communicate with any Device that has a certificate that is misaligned with the DSP Master Key Store. Manual correction has associated costs and is prone to errors.

Current arrangements explained



Business requirements

Business Requirements		
Ref.	Requirement	Responsible for delivery
1	Device certificate misalignment issues are to be resolved to enable the Responsible Supplier to send all Service Requests (SRs) to a Device and for the Device to respond accordingly.	DCC
2	The Proposed Solution must resolve the issue for three scenarios: • Change of Supplier (CoS) when the gaining Supplier cannot rectify the issue through manual intervention. • When the previous Supplier has ceased to trade, and a Supplier of Last Resort (SoLR) has been nominated. • When the Device does not support the process of Service Reference Variant (SRV) 6.24.2 'Retrieve Device Security Credentials (Device)'.	DCC
3	Addressing Device certificate misalignment issues should not require a manual Smart Metering Inventory (SMI) update except in exceptional circumstances.	DCC
4	Device certificate reporting is to be enduring as opposed to being produced on an ad-hoc basis and made available to Smart Energy Code (SEC) Parties.	DCC
5	Device certificate reporting must not duplicate information contained with current Post-Commissioning reporting.	DCC

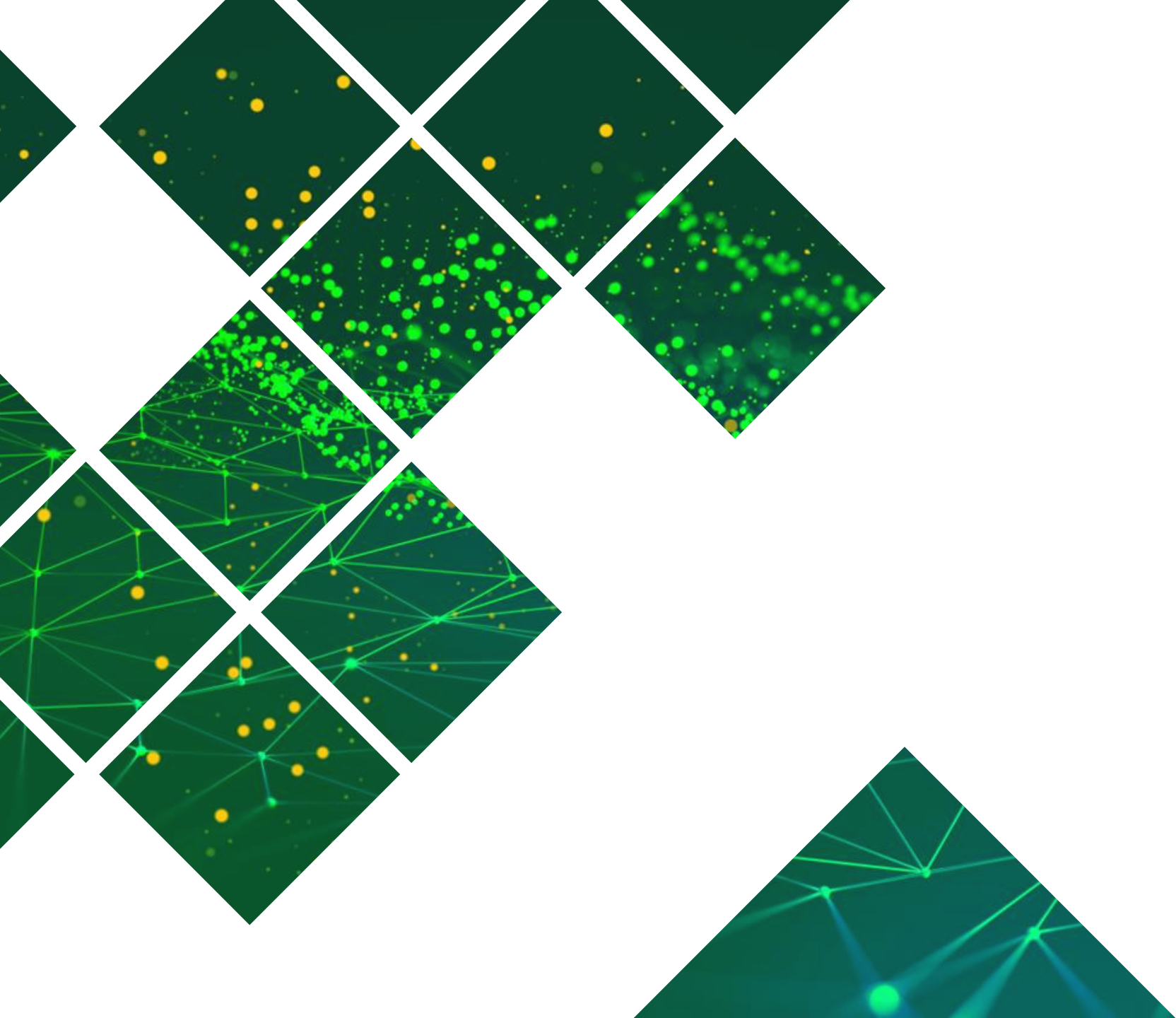
■ Question for the Working Group

Does the Working Group have any feedback on the business requirements?

Does the Working Group have any further recommendations?

Next Steps





Thank you for listening

Any further
comments?

■ MP165 'ESME Voltage Accuracy'

Raised by Alan Creighton from Northern Powergrid

Overview

Issue

- Electricity Network Parties have a statutory obligation to ensure that the voltage supplied to consumers' premises from Low Voltage electricity networks is always between defined limits.
- The Technical Specifications are silent on the voltage accuracy from ESME.

Impact

- Electricity Network Parties must make conservative planning assumptions when designing and analysing performance of Low Voltage networks. This prevents them from fully realising network-based benefits from the smart meter rollout.

Note

DNOs do not want to add further complexity to ESME, they just want to know how accurate current models are. The SEC Panel has requested that this modification is progressed to decision.

■ What we know

BEAMA

Initial investigations with BEAMA provided an indicative voltage accuracy of +/- 1% which is a voltage swing of 4.8 volts

RFI

4 respondents stating an accuracy of between +/-0.3% and +/-1%

“...The voltage is calibrated for each meter during manufacturing...”

“...samples taken from the production line and continually quality assessed...”

“...not capable of measuring to an accuracy greater than 0.2%...”

■ Proposed Solution



Codifying an agreed level of accuracy in the SEC

- An agreed level of accuracy (following consultation) to allow SEC Parties to know approximately how accurate ESME Devices are.



Testing obligations to prove compliance

- If we codify a level of accuracy – how will this be monitored and enforced?

What does ESMETS currently state?

ESMETS currently states:

5.4 Physical Requirements

ESME shall as a minimum include the following components:

- i. a Clock;*
- ii. a Data Store;*
- iii. an Electricity Meter containing one measuring element;*
- iv. a HAN Interface;*
- v. a Load Switch;*
- vi. a Random Number Generator;*
- vii. a User Interface; and*
- viii. where installed with a Communications Hub provided by the Data and Communications Company, a Communications Hub Physical Interface (this may comprise a Communications Hub Physical Interface forming part of GSME where present at the time of installation in the Premises)."*

If the Proposed Solution is implemented an Electricity Meter would need to contain two measuring elements in order to measure voltage (unless it is a Twin Element ESME which will require an additional measuring element).

■ SEC Party feedback

SECAS has presented the modification to the Working Group (2022), TABASC and BEAMA

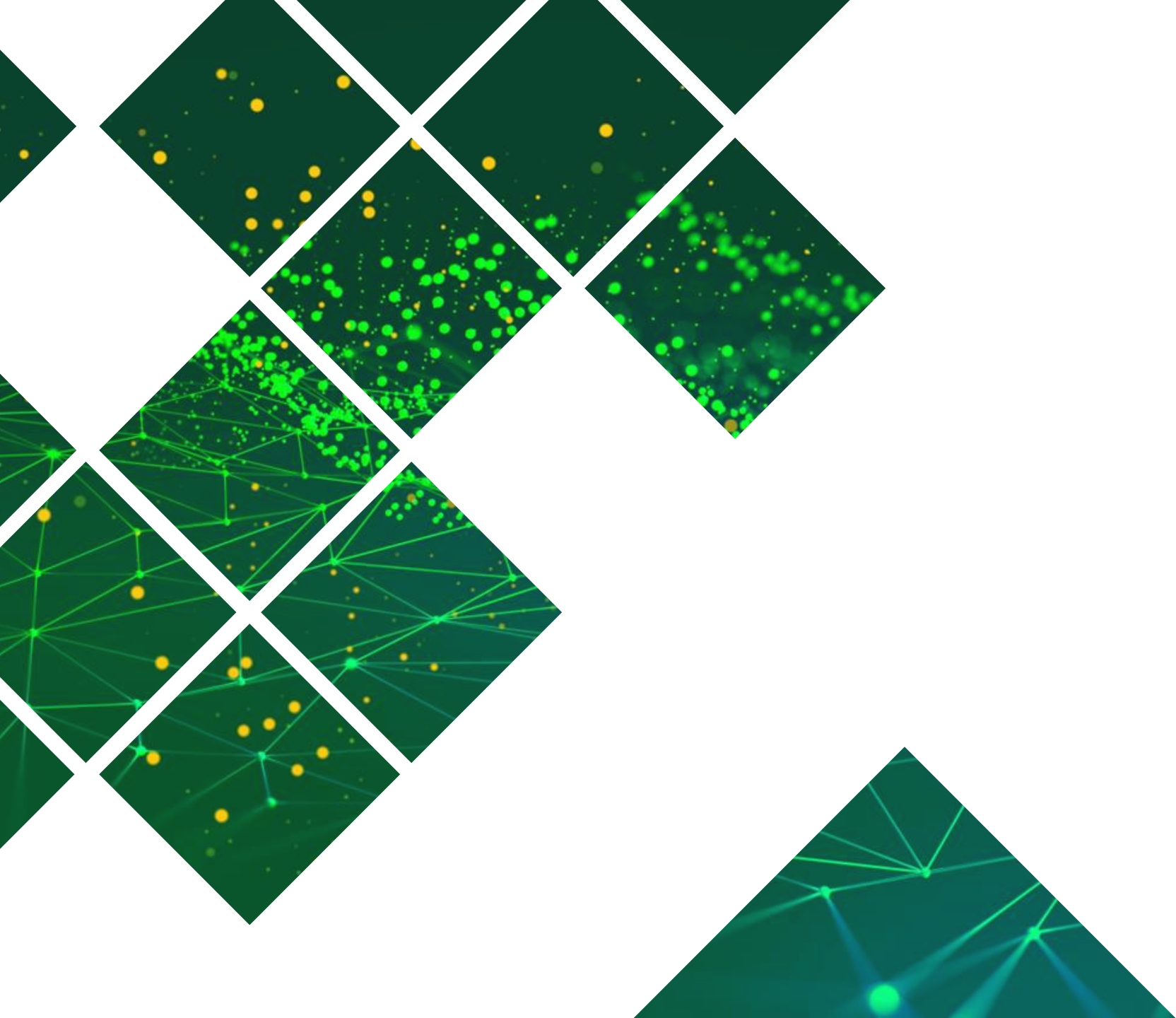
None of these have supported the inclusion of a minimum ESME voltage accuracy into the SEC, instead stating the MID and/or MIR is more suited

The TABASC did not believe this should be in the SEC, it commented that if it was to progress, it should be in its own subsidiary document

Does the Working Group have any further comments ahead of the Refinement Consultation?

Next Steps





Thank you for listening

Any further
comments?

■ Any other business

Kev Duddy

■ AOB – Panel Information Policy v6.0

A new version of the Panel Information Policy has been published – v6.0

Now in a transition phase and moving to v6.0 by early September. All live documents (policies/ guidance documents/ reports) will be updated on SEC website but not historic papers and minutes)

Please refer to the description at the top of each document to guide how the information can be shared

Key changes are:

- **RED** wording is now more explicit that information is for eyes and ears of the recipients only
- **AMBER-STRICT** is a new classification and description is equivalent to previous AMBER. This will be the default classification for DCC material marked DCC Controlled, however, we will challenge downgrading to AMBER or GREEN on case-by-case basis and become standard examples over time
- **AMBER** is a broader categorisation than previously to allow information to be shared on a need-to-know basis within SEC Party category, to their contracted third-parties as well as Trade Associations
- **GREEN** minor wording change but no impact – information can be shared with SEC Parties and SMIP stakeholders
- **CLEAR** has replaced white and can be shared publicly

YOUR FEEDBACK MATTERS

GET IN TOUCH WITH YOUR THOUGHTS AND COMMENTS

SEC.Change@gemserv.com

Want know more about SEC Change and Modifications?
Why not listen to our Modcasts?!

Available for download on our [website](#) or listen on [LinkedIn](#)

Thank you for listening

The next meeting will be on
Wednesday 4 October 2023