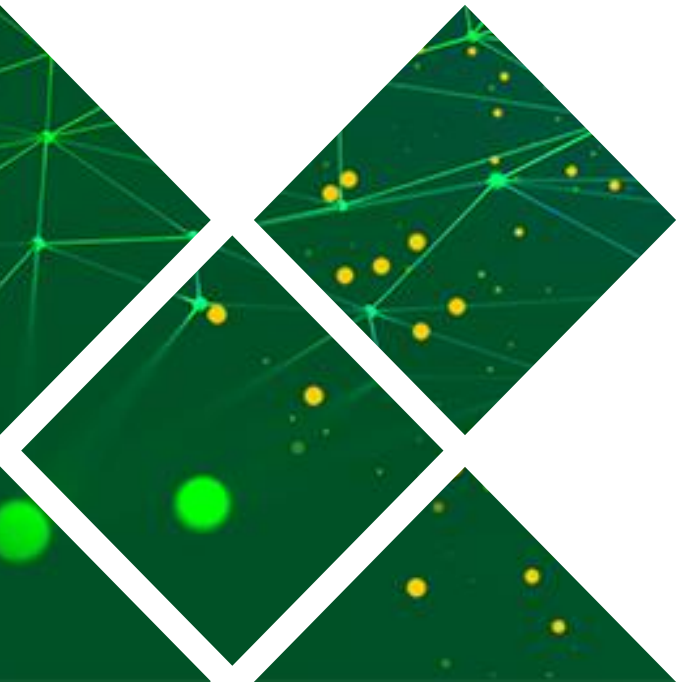


# SEC Change Monthly Working Group Meeting

August 2024



# 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



# ■ MP169: 'Managing SEC Obligations and the Consumer's right to refuse a Smart Meter'

Raised by Emslie Law of OVO

Ben Giblin

HIGH

# ■ Objectives of the Working Group

|        |                                            |
|--------|--------------------------------------------|
| NOTE   | The issue                                  |
| REVIEW | The applicability of the Proposed Solution |
| AGREE  | The next steps                             |

# Overview

## Issue

- Ombudsman are ruling that in some cases Suppliers must install Smart Meters in 'dumb' mode. Consumers are also approaching Suppliers requesting this.
- Suppliers have obligations in the SEC to ensure a Smart Metering System is installed and communicating.
- There is no concept in the SEC for a Device to be installed in 'dumb' mode.

## Impact

- Consumers right to refuse a Smart Meter cannot be met and Ombudsman rulings cannot be followed as an enduring process unless Suppliers are deliberately non-compliant with the SEC and Supply Licence Conditions.

# ■ Ofgem position

- SECAS has engaged with Ofgem throughout the modification process to determine their view on the Proposed Solution.
- Ofgem provided the following statement:  
*“Whilst Ofgem is unable to provide an opinion on an Authority Determined modification until it is sent to us for decision, our initial concerns regarding SECMP169 related to the meter’s ability to effectively communicate therefore inhibiting its smart functionality. However, on review of the Allowed SRV List we are comfortable that the meter, as proposed in the current modification, is still operational and is able to communicate with the DCC. Suppliers must take steps to ensure that all smart meters are compliant with electricity supply licence condition 48 and gas supply licence condition 43 – Operational Requirements”.*
- No controls will be introduced as part of this modification on when the Restricted Attribute can be used.

# ■ Proposed Solution

Introduction of a 'Restricted' attribute, applicable to SMETS2+ Devices

Restricted attribute will be added to the data for each Device in the SMI – each Device will be set as 'false' until changed

This will limit the SRVs and Alerts which can be delivered to/ from the Device – this is determined by a configurable list (currently this is the same SRV's which are allowed to a Device in 'Suspended')

'Restricted' will be displayed on the SSI read inventory screen and included in a response to SRV 8.2 'Read Inventory'

The Restricted Attribute can be applied and removed at any point by the Supplier

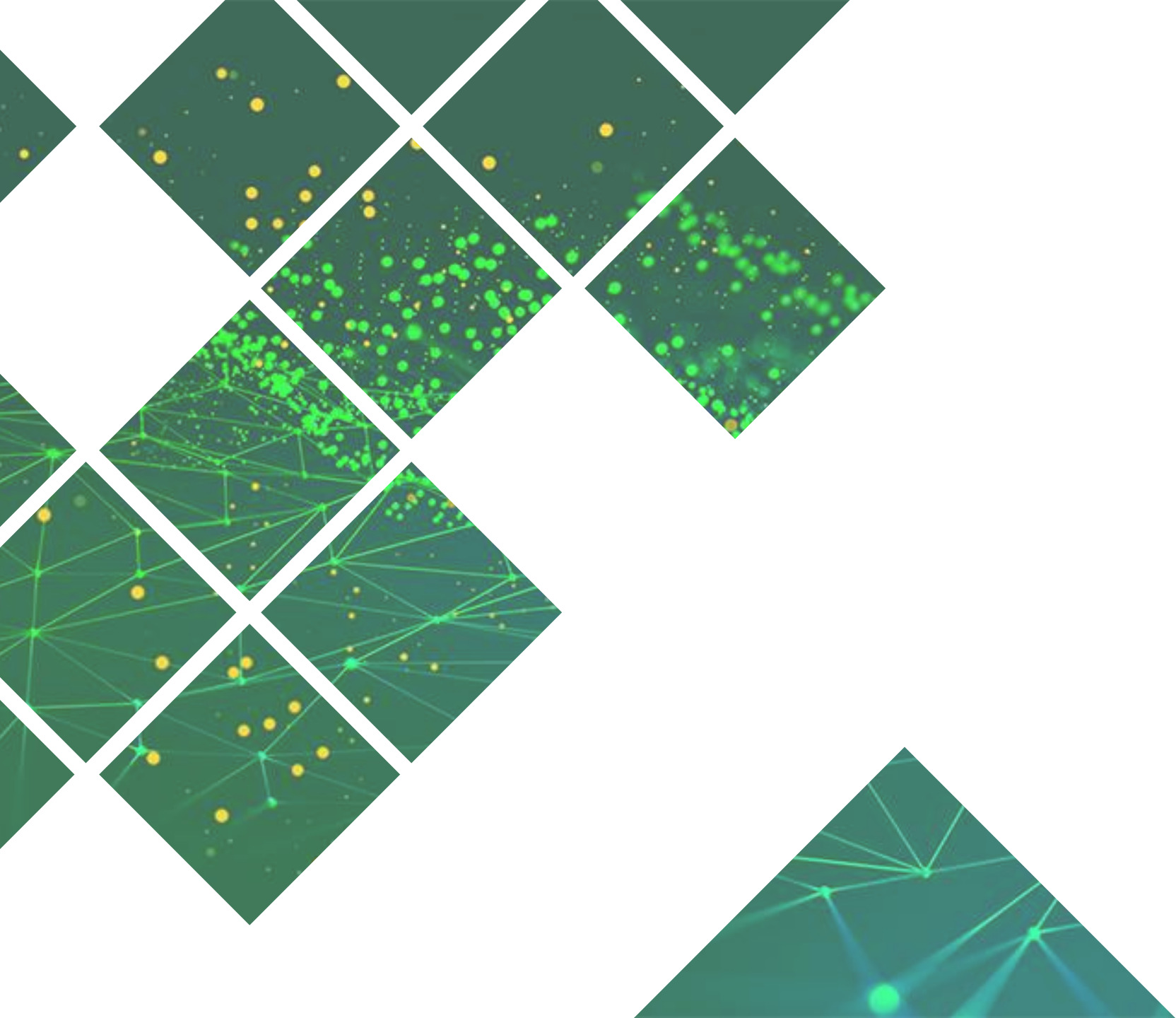
# ■ Questions for Working Group

Do you have any  
comments regarding  
the proposed  
applicability of the  
Restricted Attribute?

Any further comments?

# Next Steps





# Thank you for listening

---

Any further  
comments?

# ■ MP241 'Interoperability Checker Update'

This is a Placeholder Slide. Parties will be notified once the MP241 slides are available.

# ■ MP244 'Device Alerts for Smart Meter credit replenishment'

Raised by Kevin Clark on behalf of Utilita

Georgie Severin

LOW

# Objectives of the Working Group

NOTE

The updates from the last Working Group

AGREE

The next steps

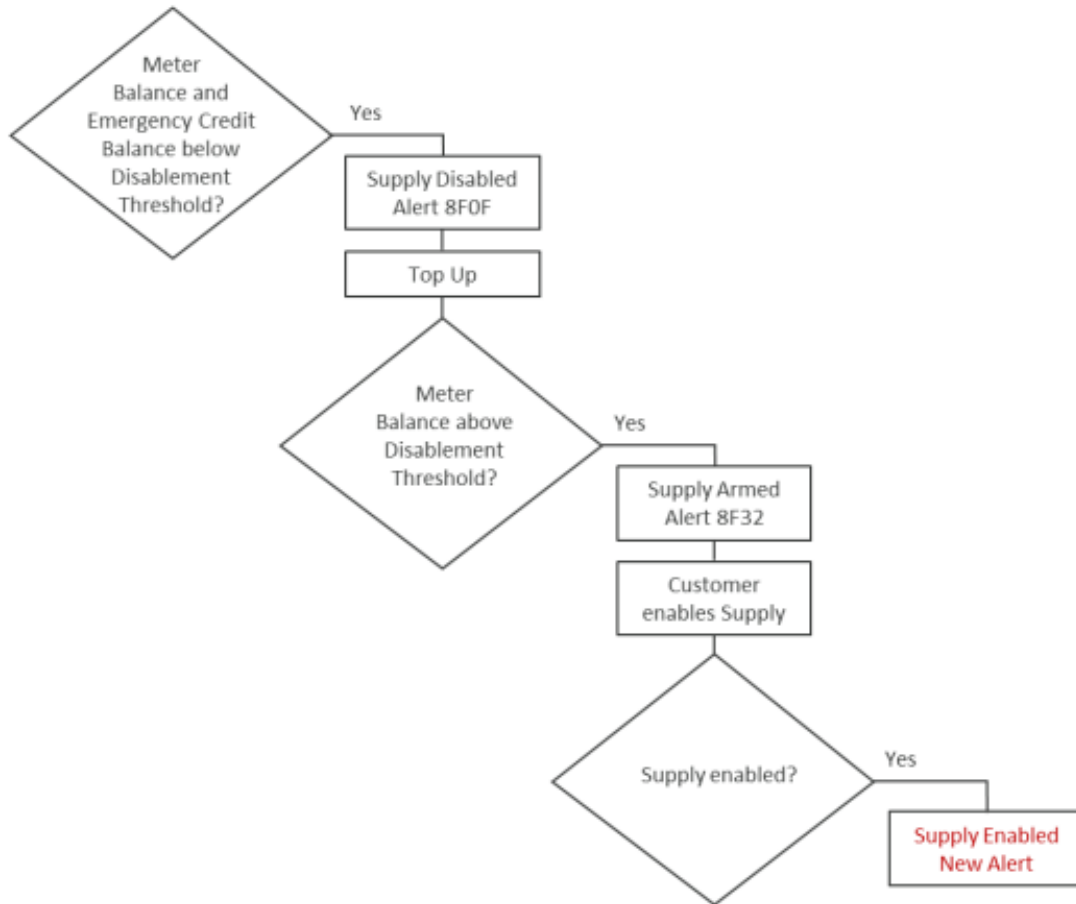
## Issue

- Multiple scenarios where a Supply could have exhausted its credit value potentially resulting in loss of power.
- There are currently no Device Alerts to notify a Supplier of issue resolution e.g., credit being topped up.
- This impacts Suppliers' ability to proactively provide support to vulnerable consumers who might be rationing or Self-Disconnecting.
- It also adds potentially avoidable traffic to the Data Communications Company (DCC), as Suppliers resort to sending SRV7.4 'Read Supply Status' multiple times to receive an update.

## Solution

- The Solution centres around adding a new configurable Device Alert that sends a notification once the supply is re-enabled.
- This would potentially lower traffic by removing the need to send multiple SRV7.4 to receive a supply update.
- It would also enable Suppliers to take proactive action in protecting vulnerable customers.

# ■ Proposed Solution Summary



Manufacturers' costs – £1.7 – £2m to introduce new Alert to Devices in line with SMETS/GBCS/DUIS changes

New Alert is configurable

Requires new version of GBCS

Requires new SMETS

Requires new version of DUIS

New version of MMC

DSP changes required to support new Alert.

# ■ Key points – July Working Group

## Non-Mandated/Non-GBCS Alert

- Favoured solution by Working Group and TABASC
- Would be a commercial agreement between Supplier & Manufacturer(s) to have this add-on
- Would only be a text-only change to DUIS

- Unable to make configurable – once Device has this added, it would not turn off. It may therefore become a nuisance Alert.
- Does not address the issue at wider level – different processes for different Devices.

# ■ Key points – July Working Group

## Impact on Devices

- It can be argued that Devices may be impacted because of the changes proposed
- Older or outdated Devices may be retired prematurely.
- Statistics should be available in relation to the number of firmware upgrades that fail to be delivered

- Hard to quantify the number of Devices that would be affected by a specific firmware upgrade.
- If a Device firmware upgrade fails to be delivered, it is likely due to a number of reasons (e.g. poor signal area).
- As long as Device is within IVP and MVP dates in the TSAT then there wouldn't be a need to carry out a firmware upgrade.

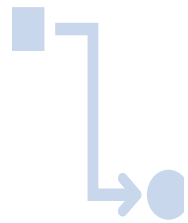
# ■ TSIRS views

Attendees highlighted the implementation of the new Alert would be expensive

One member expressed no opposition to Alert being Non-GBCS/Non-Mandated.

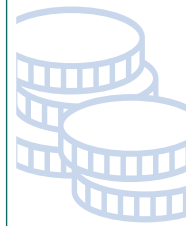
Alert would have been a good addition had it been established earlier in the program. It is now unlikely to be needed, as workarounds have been established.

# ■ Assessment of Change



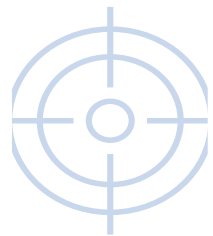
## Impacted Parties

- Suppliers
- Other SEC Parties
  - Manufacturers



## Costs

- DCC costs £60,000 - £200,000
- Consequential costs to Manufacturers £1.7 - £2m



## Target Release

- June 2026 SEC Release



## Benefits

- Better visibility of vulnerable prepayment consumers
- Enables proactive action

# ■ Questions for the Working Group

Should the Impact Assessment be requested?

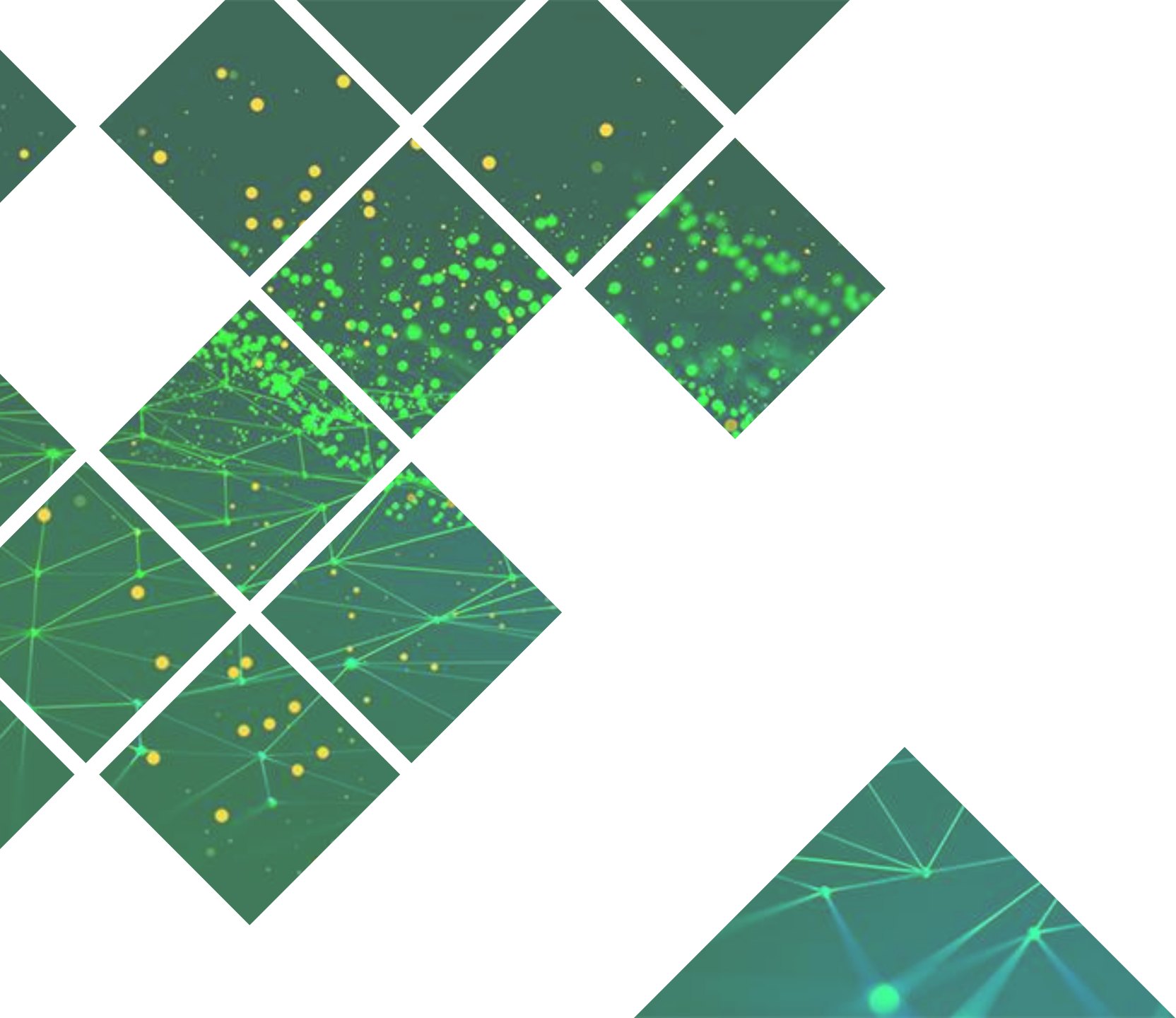


Any other comments?



# ■ Next Steps





Thank you for  
listening

---

Any questions?

# BREAK



---

PLEASE RETURN IN 10 MINUTES

# ■ MP247 'Future Dating of Service Requests for SMETS1 Devices'

Liz Woods

Raised by Rosie Davies from the DCC

**MEDIUM**

# ■ Objectives of the Working Group

|        |                            |
|--------|----------------------------|
| NOTE   | The issue                  |
| REVIEW | The reduced scope solution |
| AGREE  | The next steps             |

## Issue

- Short-term peak usage caused incidents for S1SP, e.g. during previous Price Change events
- Future dating reads allows the DCC to better manage traffic in advance of peak events
- Currently, DUIS prevents the DCC from being able to do this for SMETS1 Devices
- All Future Dated Requests for SMETS1 Devices are effectively Future Dated Response Pattern (DSP)
- DSP holds all SMETS1 Future Dated SRs, for release to SMETS1 Devices at a future date

## Solution

- Allow Users to send Future Dated Service Requests to SMETS1 Devices without being held at the DSP.
- Reduced scope Proposed Solution will only include SRV 1.1.1 'Update Import Tariff (Primary Element)' and SRV 1.2.1 'Update Price (Primary Element)'.

# Business Requirements

| Ref | Requirement                                                                                                                                       | Responsible for delivery |
|-----|---------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| 1   | DCC Users must be able to send Device Future Dated Service Request (SR) to any Smart Metering Equipment Technical Specifications (SMETS)1 Device. | DCC                      |
| 2   | DCC User systems will not require changes to support Device Future Dated SRs.                                                                     | DCC                      |
| 3   | DCC User processes to remain consistent for all different SMETS1 Device Models.                                                                   | DCC                      |
| 4   | Reporting to monitor Future Dated SRs sent to and stored on SMETS1 Devices.                                                                       | DCC                      |

- The reduced scope of the Proposed Solution targets only:
- SRV 1.1.1 'Update Import Tariff (Primary Element)'
  - SRV 1.2.1 'Update Price (Primary Element)'

## S1SP & DCO Impacts

Execution Date Time in the SR passed to Device as an Activation Date Time for the associated command(s)

Send cancellation commands to Devices where a Service User either cancels a command explicitly or there is an implicit cancellation

Send cancellation commands to SMETS1 ESME/GSME, where DCC User either cancels a command or an implicit cancellation (e.g. CoS)

# ■ Preliminary Assessment Impacts 2/2

## DSP Impacts

DSP to cancel all Future Dated (Device) Service Requests when there's a CoS

Timeout for affected SRVs to be extended

## Reporting

DCC Data Science and Analytics (DS&A) team to provide the reporting required

Details to be established at part of Full Impact Assessment

## Appendix AD - DUIS

- Changes to 1.4.4
- To be detailed in DCC Full Impact Assessment
- No changes required to DUIS schema

## DUGIDS

- corresponding changes in DUGIDS for the changes in DUIS

### **1.4.4 Future Dating of Service Requests for SMETS1 Devices**

Where, as identified in clause 3.1 (Service Request Matrix), a SMETS1 Service Request has a Future Dated Response Pattern of 'Device', the DCC, and not the Device, shall undertake the required processing to implement the future dating, in line with the requirements of the Service Request Processing Document.

# Forum views

Full Scope  
Preliminary Assessment v0.4

Reduced Scope  
Preliminary  
Assessment v1.41

**Working Group**

**TABASC**

**TABASC**

**Process & DCC  
User behaviour**

Resistance from some DCC Users to use Future Dated SRs and might not be used

**Cost-benefit**

Queries on practical difference it would make to warrant the cost

**Links to MP253**

If approved, would mandate change in DCC User behaviour to use Future Dated SRs

**Reduced scope**

If costs were reduced enough, might be worth pursuing

Does not impact on technical and business architecture

Supportive for another PA with reduced scope

**PLACEHOLDER**  
for comments from  
1 Aug 2024 meeting

# Questions for the Working Group

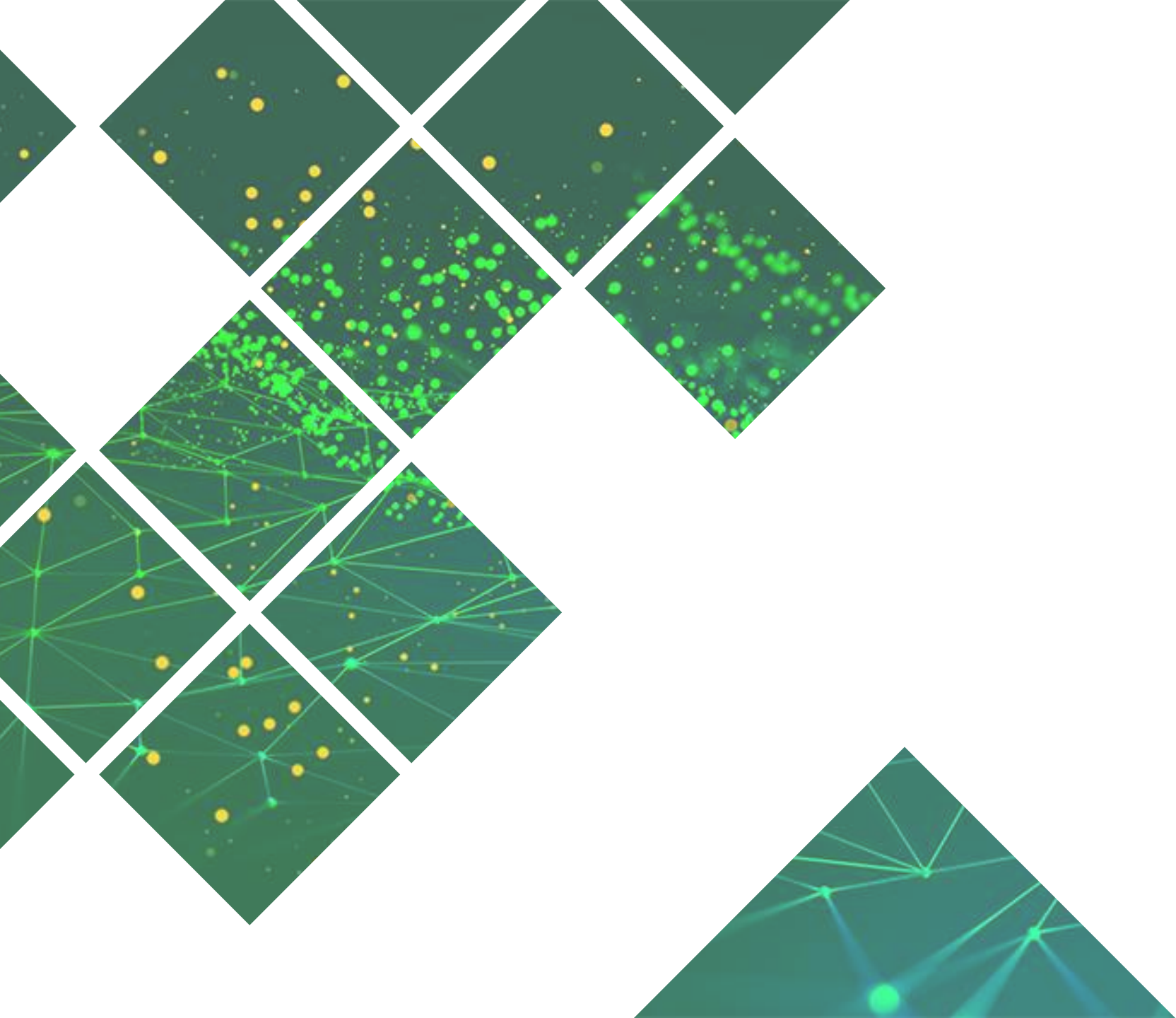
Is there a positive business case with the reduced scope Proposed Solution?

Should a reduced scope Impact Assessment be requested, or this modification be withdrawn?

Any other considerations?

# ■ MP247: Next Steps





# Thank you for listening

---

Any further  
comments?

# ■ MP253 'Traffic Management for Price Cap Update Event - User Actions Required'

Raised by David Rollason from the DCC

**MEDIUM**

# Objectives of the Working Group

REVIEW

The second Refinement Consultation Responses

AGREE

The next steps

# ■ MP253 - Overview

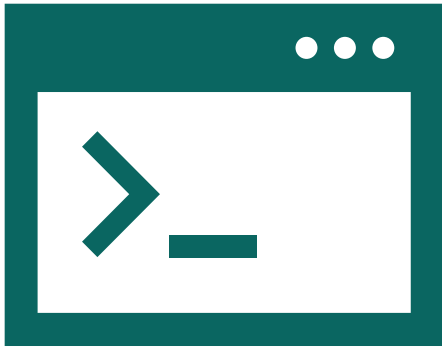
## Issue

- There are no formal rules or requirements in the SEC on how DCC Users should process high volumes of traffic on the DCC Network. Therefore, there is no standard process for the execution of such industry-wide Price Cap Update Events (PCUE's), either within the Supplier community or through DCC Systems.

## Solution

- The DCC would like to place the current 'guidance' issued during a PCUE into a Code Required Document called the Price Cap Instructions Document (PCID) and place an obligation into the SEC for DCC Users to follow.
- Should these instructions require changes in readiness for future PCUEs, any proposed amendments needs to be consulted upon by DCC, before seeking approval from the SEC Panel. If DCC Users were unable to adhere to instructions in the PCID, they must contact the DCC one month in advance of the relevant PCUE to establish alternative instructions.

# ■ MP253 - Expected Benefits



Greater control of DCC  
System traffic during  
industry-wide PCUE's



Improved confidence  
of DCC System stability  
for DCC Users



Reduced likelihood of  
potential message  
failure or timeouts

# ■ MP253 – Legal Text (1/2)

## SEC Appendix AB 'Service Request Processing Document'

Contains obligation for DCC Users to follow PCID during a PCUE

Obliges DCC Users to contact DCC if not able to follow PCID

## 'Price Cap Instructions Document'

Outline the specific actions the DCC would require DCC Users to undertake during a PCUE

The aim is to prioritise the traffic of credit consumer related traffic within the DCC System over a longer period

## ■ MP253 - Legal Text (2/2)

Only applies to  
Domestic  
Consumers

Changes to PCID  
must be approved  
by the SEC Panel

Only 3 SRVs  
impacted

# ■ MP253 - PCID Instructions (1/3)

| SMETS1 & SMETS2 DEVICES IMPACTED |                      |                                   |                        |                                   |
|----------------------------------|----------------------|-----------------------------------|------------------------|-----------------------------------|
| SRV's                            | DAY OF PCUE          |                                   | DAY AFTER PCUE         |                                   |
|                                  | Prepayment Consumers | Credit Consumers - Monthly Billed | Other Credit Consumers | Credit Consumers – Monthly Billed |
| 1.1.1                            | 00:00-05:00          | 05:00-23:59                       | 00:00-06:00            | 12:00 onwards                     |
| 1.2.1                            | 00:00-05:00          | 05:00-23:59                       | 00:00-06:00            | 12:00 onwards                     |

## Specific Points to Note

- Future Dated SRV's required
- Messages should be evenly distributed across time periods
- Try to avoid Future Dated SRV's being sent between 06:00-12:00 on the day of, and day after, a PCUE
- No On-Demand messages between 06:00-12:00 on day of a PCUE, and the day after a PCUE

# ■ MP253 - PCID Instructions (2/3)

## Other Points of Note

- SRV 4.6.1 – Utilise Future Dated SRV's instead of On Demand requests
- SRV 1.1.1 & 1.2.1 – Parties encouraged to use 1.2.1 in place of 1.1.1, as SRV 1.2.1 is relatively smaller in size, and returns fewer Alerts to SEC Parties
- DSP Overload Protection is triggered by peak demand spikes in On-Demand traffic
  - ❖ when activated, flow of all On-Demand SRV's (**not Future Dated**) will be restricted
  - ❖ if activated, HTTP 503 errors will be returned to SEC Parties
  - ❖ These messages will **not** have been received by the DCC, so re-submission after 30 minutes would be required
- SEC Parties must not user On-Demand SRV's to execute their updates

# ■ MP253 - PCID Instructions (3/3)

## Non-Essential Activity

- Non-essential activities must be suspended during PCUE's
- Examples of essential activities include:
  - ❖ Install & Commission (I&C);
  - ❖ Change of Supplier (CoS);
  - ❖ Pre-Payment Meter (PPM) actions;
  - ❖ Any other actions that are required to be completed in short timescales (same day actions).
- Parties are asked to consider their activity on the PCUE date, and where possible delay activity until a later date. This requirement should not stop or delay business activity that is required to be completed on the day of the price cap update

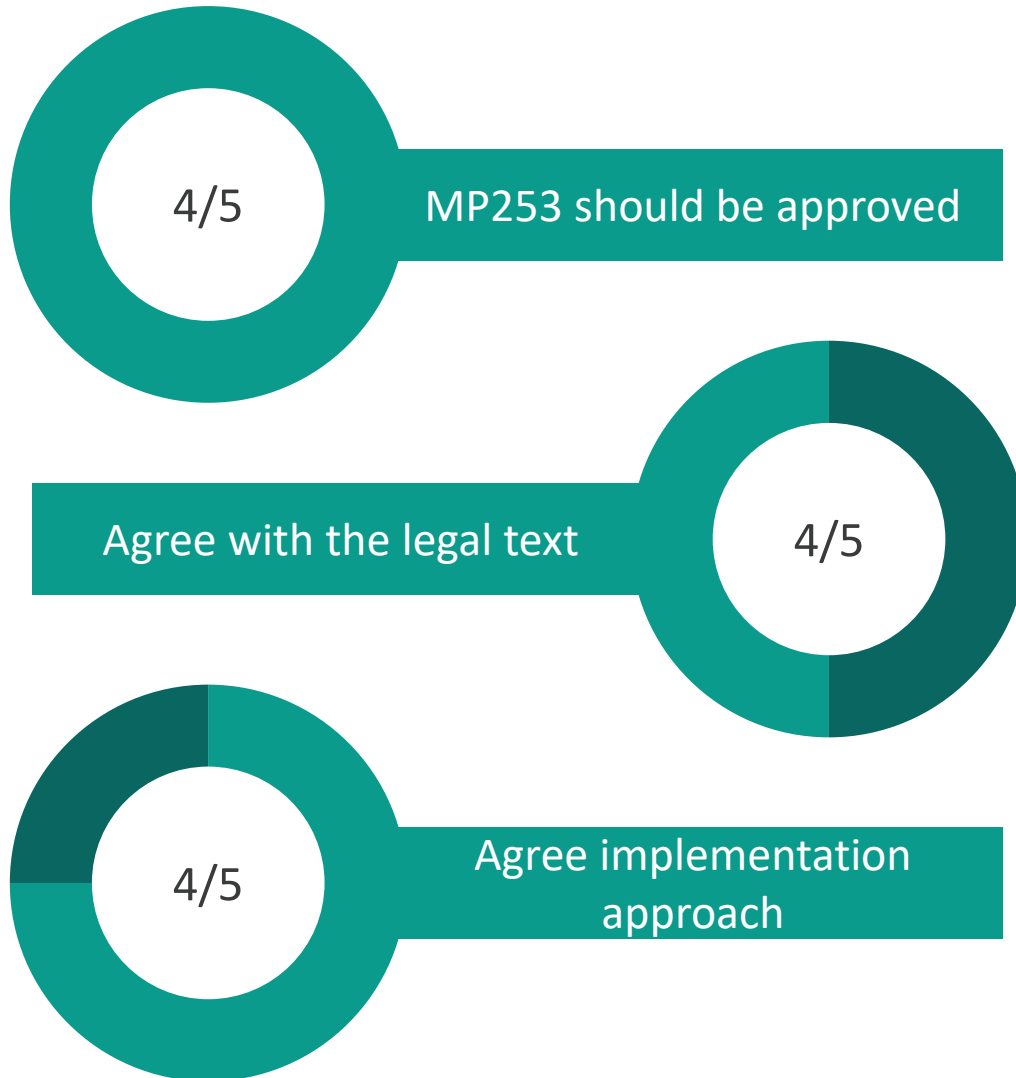
# Refinement Consultation key points



## Consumer impact

**Large Supplier – ‘From a PrePay perspective, the instructions enabled by this modification are critical to ensuring the tariff updates are delivered to PrePay customers in as timeous a manner as possible’**

**Large Supplier – ‘These measures are only required because an automated technical solution is not available’.**



# Refinement Consultation key points

## Implementation costs

In excess of £1m (Large Supplier)



| Large Suppliers<br>£1m+ | Small Suppliers<br>N/A | Network Parties<br>N/A | Other SEC Parties<br>N/A |
|-------------------------|------------------------|------------------------|--------------------------|
|-------------------------|------------------------|------------------------|--------------------------|

(a)

Facilitate the efficient provision, installation, operation and interoperability of smart metering systems at energy consumers' premises within Great Britain.

(b)

Enable the DCC to comply at all times with the objectives of the DCC licence and to discharge the other obligations imposed upon it by the DCC licence.

(c)

Facilitate energy consumers' management of their use of electricity and gas through the provision of appropriate information via smart metering systems.

**Large Supplier** – *'No lead time from the modification itself, however, depending on the instructions contained within the initial document there may be required system changes and associated lead time from those.'*



## Lead times

6-12 months (Large Supplier)



| Large Suppliers<br>6-12 months | Small Suppliers<br>N/A | Network Parties<br>N/A | Other SEC Parties<br>N/A |
|--------------------------------|------------------------|------------------------|--------------------------|
|--------------------------------|------------------------|------------------------|--------------------------|

# Refinement Consultation key points

## Respondent comment

The Price Control Instructions Document (PCID) does not outline what would happen in the event of a DCC incident or outage affecting key systems which could impact Price Cap Update Events, i.e., is everything shifted forward by 'x-hours'?

The original intent of the modification is to formalise the intent to engage with and encourage best practices in order to improve performance across the system around these critical events, not to provide additional means to penalise users, and while penalties have not been mentioned as yet, we feel it necessary to reiterate this point for enduring clarity.

## SECAS response

A verbal update will be provided by SECAS during the Working Group meeting.

The DCC & SECAS re-affirms there is no intention to implement penalties or consequences in line with this modification. The sole intention is to effectively and proactively manage DCC Total System traffic during a PCUE.



# Refinement Consultation key points

## Respondent comment

There has been no update to the outcome and performance of the Price Change Events beyond October 2023

it would seem that this solution is counter to General SEC Objective (c). Though it is not clear from the drafting of the PCID, it seems that the solution requires the overwhelming majority of credit customers to wait up to 4 days for their smart meters to accurately reflect their current price of energy. This would seem to contradict General SEC Objective (c)

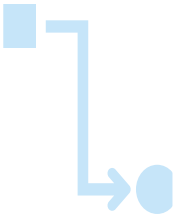
## SECAS response

SECAS note the point made, and have now procured more recent 2024 statistics which will be reflected in the next iteration of the Modification Report

A verbal update will be provided by SECAS during the Working Group meeting.



# ■ MP253 - Assessment of Change



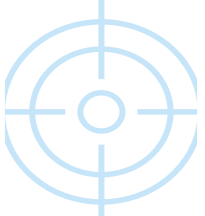
**Impacted Parties**

- Suppliers
- Network Operators
- Other SEC Parties
- DCC



**Costs**

- SECAS implementation costs



**Target Release**

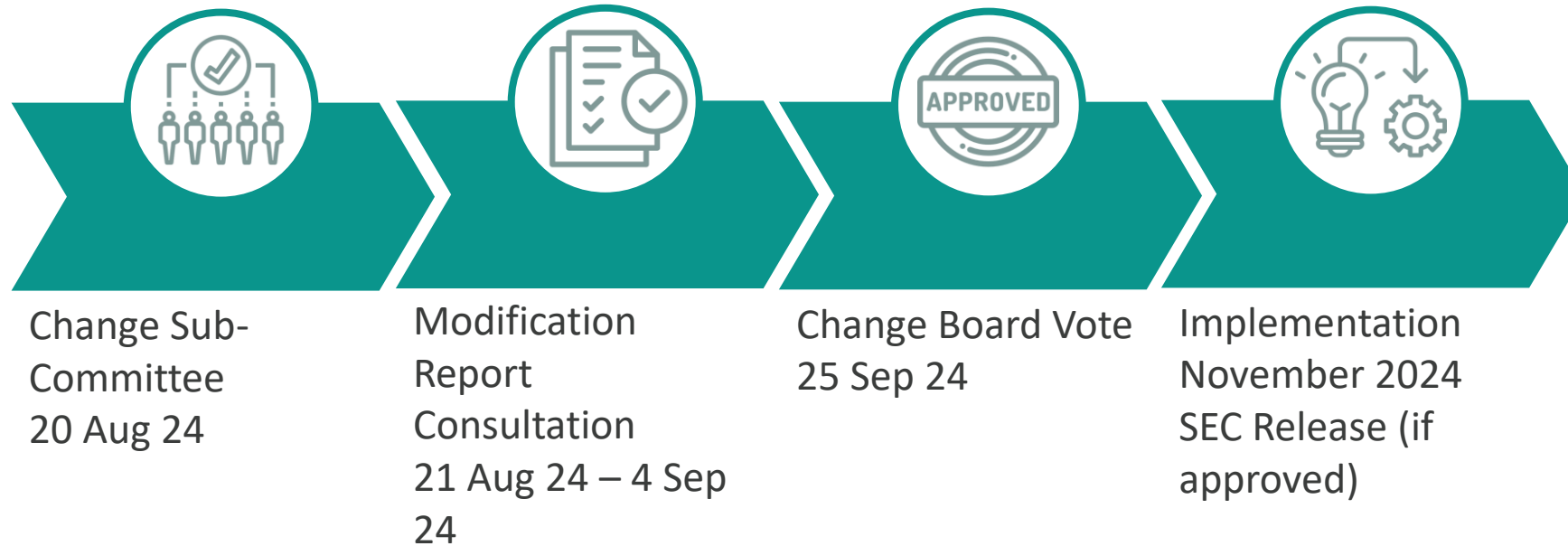
- November 2024 SEC Release

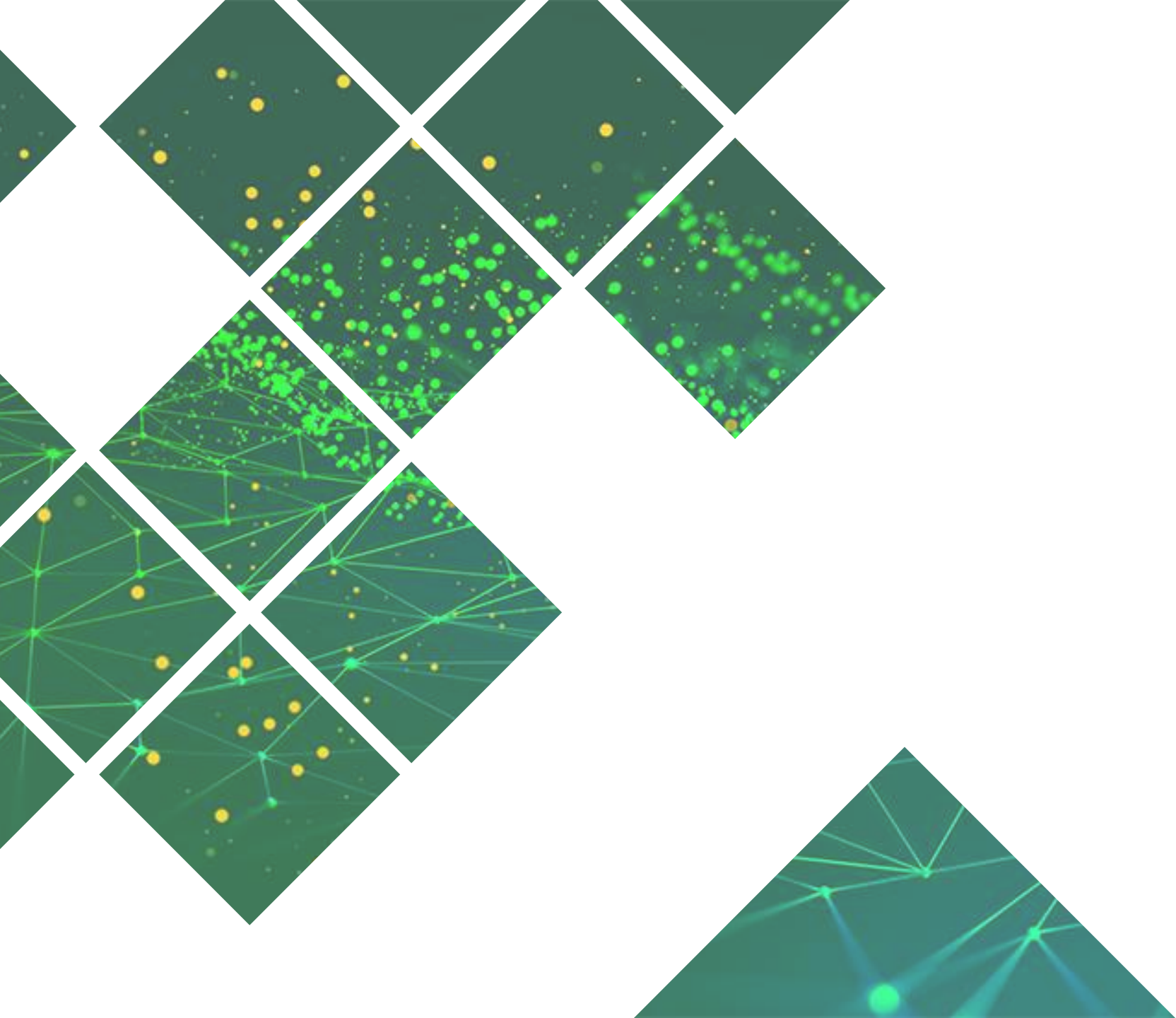


**Benefits**

- Greater DCC System control
- Increased User confidence
- Higher change of message success

# Next Steps



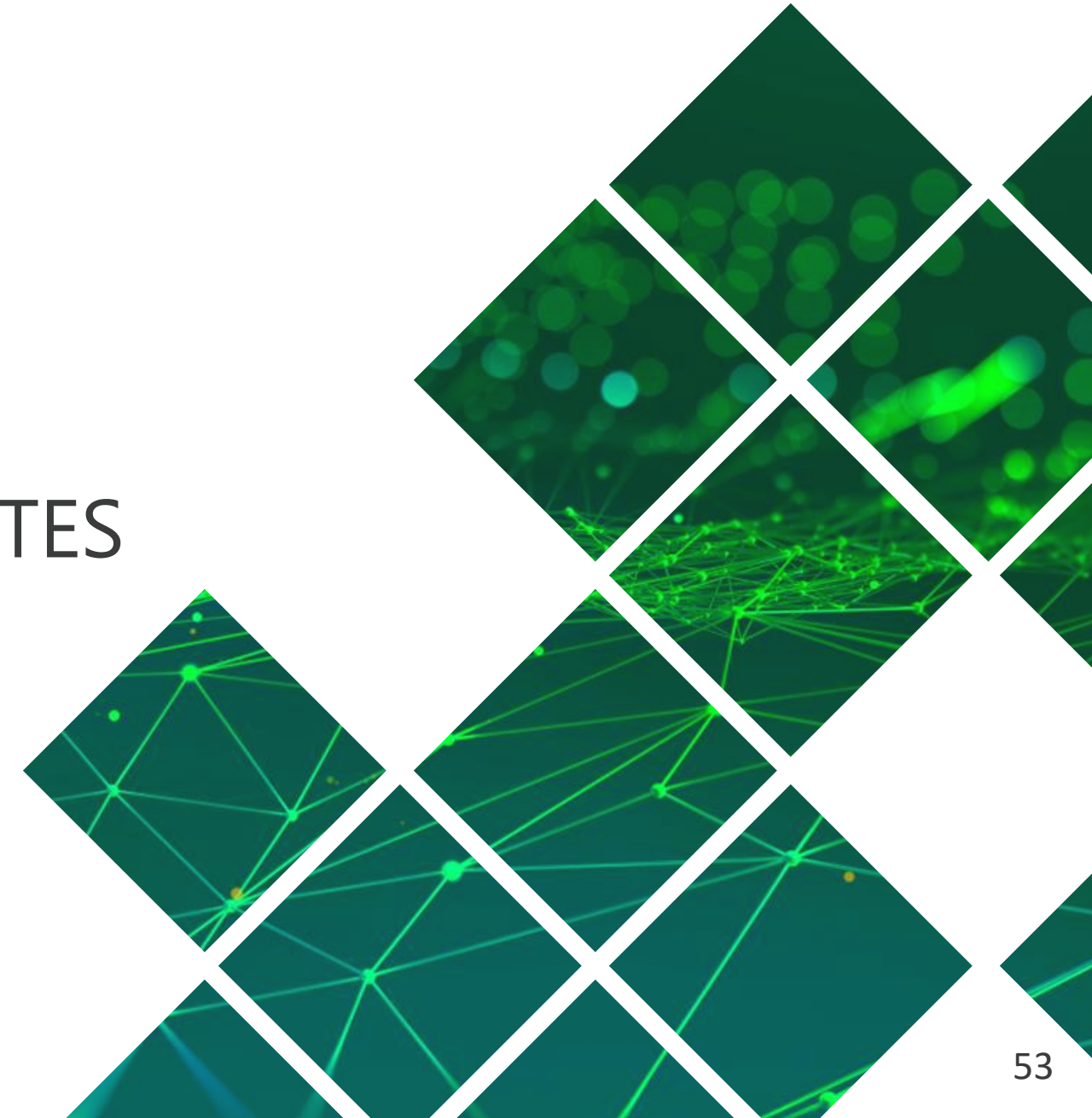


# Thank you for listening

---

Any further  
comments?

# BREAK



---

PLEASE RETURN IN 10 MINUTES

# ■ MP268: Certificate rotation and expired Certificates

Mo Sumro

Raised by Bradley Baker from the DCC

**HIGH**

# Objectives of the Working Group

|        |                                                     |
|--------|-----------------------------------------------------|
| REVIEW | The DCC Preliminary Assessment Response             |
| AGREE  | The draft legal text delivers the Proposed Solution |
| AGREE  | The next steps                                      |

# Overview

## Issue

- The new manufacturing Certificates will have a 17-year Validity Period to align with the existing Organisation Certificate Authority Certificate which expires in 2041
- SMKI PMA deems that Certificates with a Validity Period longer than ten years are an increased security risk
- There are implicit requirements for the DCC, Suppliers and Network Parties to replace revoked and expired Organisation Certificates

## Impact

- Devices using current manufacturing pack certificates will need replacement post-2026 due to expiry but no explicit requirement in the SEC to do so

## Solution

- DCC to replace longer Validity Period Certificates on Devices following successful I&C with ten year Validity Period Certificates to mitigate security risk
- Make the currently implicit requirement to exchange expired or revoked Certificates explicit

# Feedback to date

## SSC/SMKI PMA

Remained neutral

Certificates should be updated no sooner than 48 hours and not later than 23 days after I&C

Reporting requirement is captured within current PCO reporting

## Working Group

Modification is supported

Agreed there is a lack of explicit instruction to replace Certificates

Should not impact I&C  
– Highlighted Certificate replacement should take place after 7 Working Days

## Requirements Workshop

Scope extended from any Certificate that has a Validity Period longer than ten years to all Certificates

Assists in better Certificate management

## TABASC

Believe Certificate replacement should take place after 48 hours but before 7 days

Most Suppliers have completed I&C after 48 hours and before 7 days to better align to PCO

# ■ Business requirements (1/2)

| Ref | Requirement                                                                                                                                                                                                                                                           |
|-----|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1   | Following Installation and Commission (I&C) completion (after 48 hours but before seven days have elapsed), the Change of Supplier (CoS) extended life Organisation Certificate (Transitional or Enduring) on that Device will under all reasonable steps be replaced |
| 2   | Following I&C completion (after seven days but before 23 days have elapsed), the “accessControlBroker” extended life Organisation Certificates on that Device will under all reasonable steps be replaced                                                             |
| 3   | Under all reasonable steps, the Relevant Subscriber will replace a Certificate before it expires, or has expired                                                                                                                                                      |
| 4   | Under all reasonable steps, the Relevant Subscriber will replace a revoked Certificate                                                                                                                                                                                |

# ■ Business requirements (2/2)

| Ref | Requirement                                                                                                                                                                                              |
|-----|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 5   | Provide reporting capabilities to confirm Relevant Subscriber compliance with SEC Section G 'Security' and SEC Appendix AC 'Inventory, Enrolment and Decommissioning Procedures'                         |
| 6   | The Relevant Subscriber's User Independent Security Assurance Service Provider will provide security assurance services according to SEC Section G8.3(f) in relation to expired and revoked Certificates |

# ■ Proposed Solution Summary

## Automatic Organisation Certificate replacement

- Daily automatic initiation of ACB Certificate replacement
- Criteria – Devices which hold manufacturing Certificates where 48 hours have passed since their commissioning
- Replacement takes place
- If replacement fails, the system retries every 7 days for up to three attempts (21 days total)

## Prioritisation and backlog management

- Newly commissioned Devices (within the last 23 days) are prioritised for ACB Certificate replacement
- This allows newer Devices to be updated promptly while the system manages the backlog

## Exclusion

- Large proportion of PPMID Devices are excluded from ACB replacement due to known issues in supporting the command

# ■ Proposed Solution Summary - Reporting

## Reporting detail

- Validity Period exceeding ten years
- Are revoked or expired
- Expiring within 18 months
- Are incorrectly assigned in Trust Anchor Cells

## Data Points

- GUID
- Device ID
- Device type
- Operational status
- Key location
- Certificate details
- Expiration dates

This additional reporting will be part of the existing monthly Post Commissioning Obligations

Service Users and CSP Service Provider receives a weekly report detailing all their Devices which are currently failing the PCO checks as introduced under MP183 'Post Commissioning Obligations Reporting'

# ■ Preliminary Assessment Summary

## Cost (Design, Build & PIT)

- £10,000 - £160,000 depending on final scope and integration testing requirements
- PIT – Creates list of Devices with recently installed Devices prioritised
- PIT regression testing is included
- Factory Acceptance Testing is included to ensure Devices are working correctly after Certificate replacement
- SIT and UIT costs are not included

## Implementation

- Expected to take approximately **3 months** up to the end of PIT after contract amendment note is signed

## Full Impact Assessment

- Based on the existing requirements, the total fixed price cost for a Full Impact Assessment is **£17,636** and would be expected to be completed in **40 Working Days**.

# ■ Preliminary Assessment Impacts

## ECoS Service Provider (Accenture) Impacts

- Minor configuration changes required, which have already been tested under the ECoS programme
- Requires updates to data management components
- Complete within 12 weeks post private key transfer

## DSP Impacts

- Automatic ACB Certificate replacement
- Prioritising newly commissioned Devices
- Retry of replacement if necessary
- Requires updates to the key management system
- Requires updates to data management components

## DCC Data Science & Analytics

- Responsible for reporting
- Responsible for overseeing the implementation

## Section G

- Two new clauses
- Reference for Appendix AC

## Appendix AC

- 4 new clauses
- New clause to introduce obligation on Certificate replacement
- Revoked and Expired Certificate obligations

# ■ SEC Section G ‘Security’

## New Clause 8.3(f) Scope of Security Assurance Service

- To reference SEC Appendix AC 5.23
- Ensures DCC User compliance with the SEC

## New Clause 9.2(e) Scope of Security Assessment Services

- To reference SEC Appendix AC 5.20
- To reference SEC Appendix AC Section 5.21
- Ensures DCC compliance with the SEC

# SEC Appendix AC 'Inventory Enrolment and Decommissioning Procedures'

New Clause – 5.20 specifies

After 48 hours but before seven Days Change of Supplier (CoS) Organisation Certificates with a Validity Period of more than 10 years is exchanged Organisation Certificate which has a 10 year Validity Period

New Clause – 5.21 specifies

After 48 hours but before 23 days following the Commissioning of any Device an ACB Certificate that has a Validity Period of more than 10 years is replaced with one that has a 10 year Validity Period

New Clause – 5.22 specifies

The Subscriber for the relevant Certificate shall take all reasonable steps to replace the Certificate for one that has not been revoked

New Clause – 5.23

The Subscriber for the relevant Certificate shall take all reasonable steps to replace the Certificate for one does not have an expired Validity Period

# ■ Questions for the Working Group

Does the Proposed Solution deliver the business requirements?



Does the draft legal text deliver the Proposed Solution?

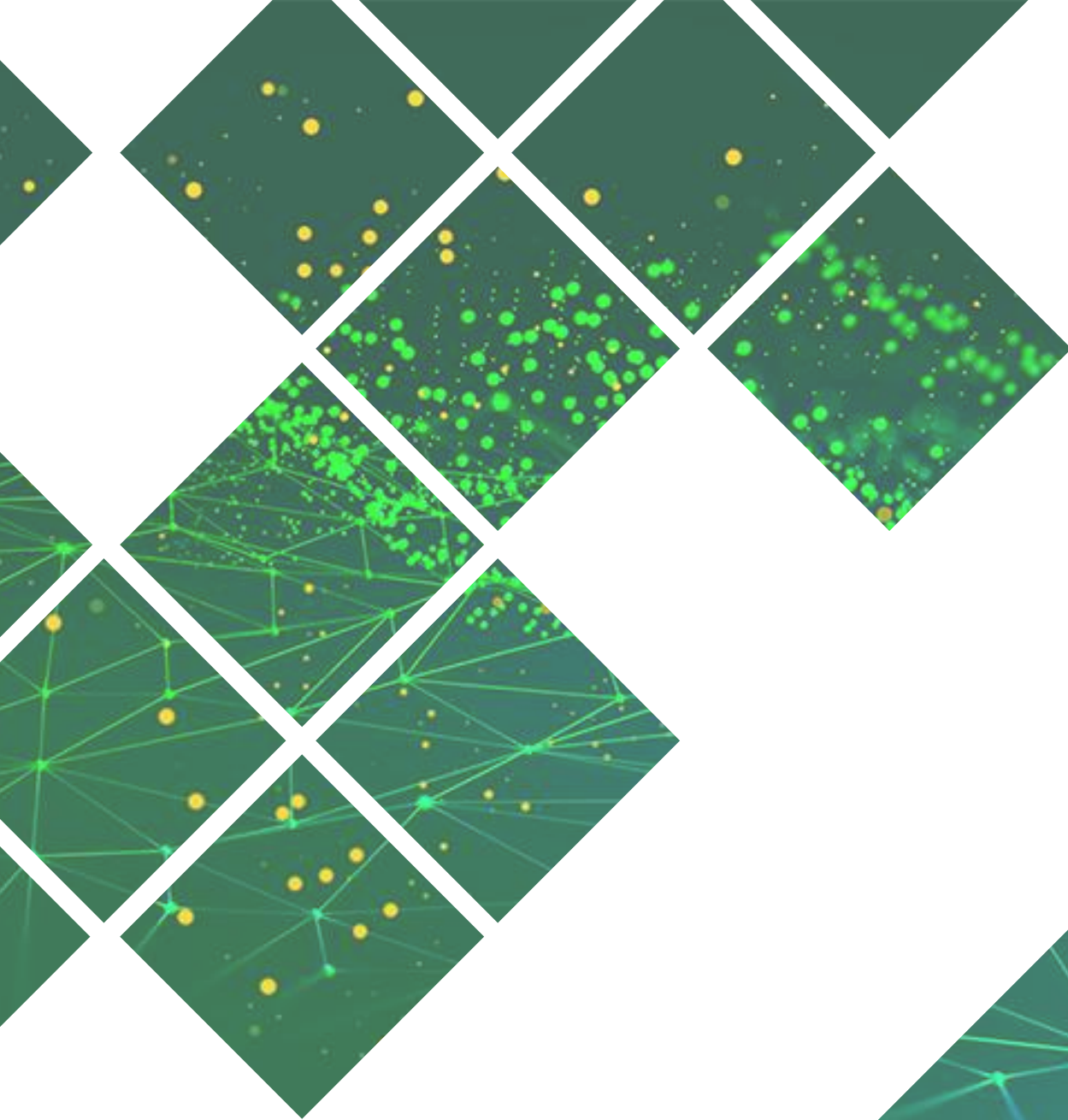


Should the Impact Assessment be requested?



# Next Steps



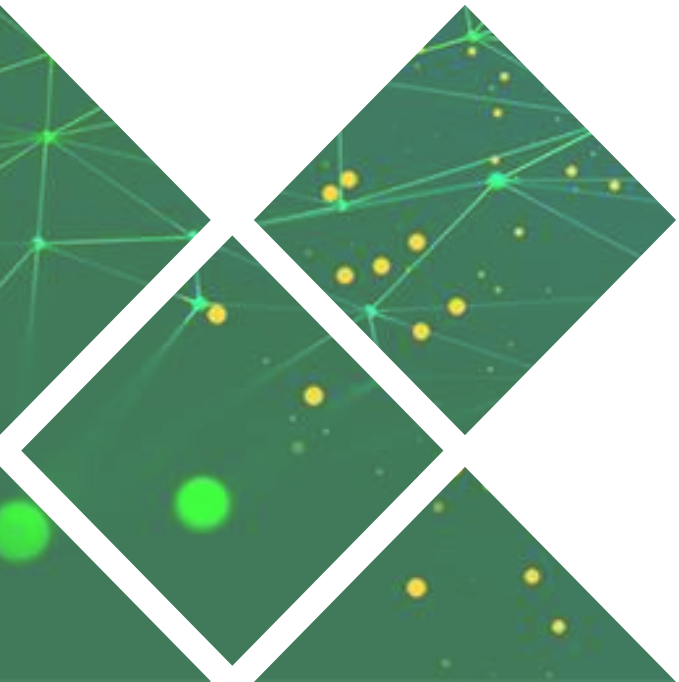


# ■ Any other business

Kev Duddy

# SEC Issues Group

August 2024



# OSP Party Categories

## Issue

- The OSP Party category is very broad and comprises different types of organisation with conflicting priorities, issues and concerns, making it difficult for anyone to fully represent all Parties.

## Impact

- Other Users, Meter Data Retrievers and Registered Supplier Agents may not receive the correct representation, leading to a lack of insight on solutions and potential costs.

# ■ Proposed Solutions

## Solution 1 – Reallocating existing OSP seats

- The Proposer would re-allocate one of the existing OSP seats at TABASC, OPSG, Change Board and Change Sub-Committee to a Party in the role of OU, MDR or RSA.
- No changes to voting - OSP voting share would remain the same.
- Changes to TABASC and Change Board would change the SEC.
- Changes to CSC and OPSG take place via Terms of Reference (Panel approval needed).

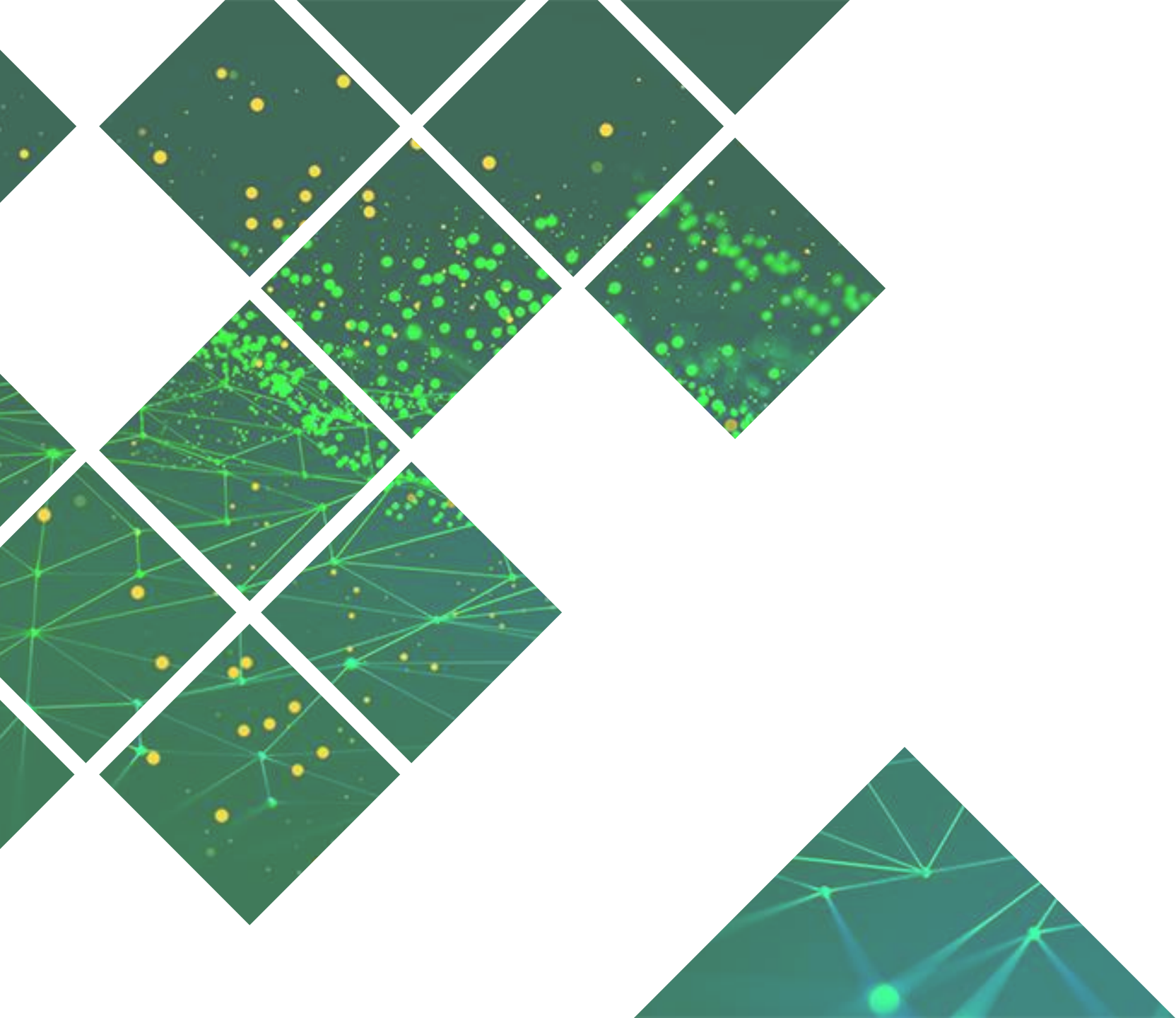
## Solution 2 – Creation of new seats for OU, MDR and RSA

- Creation of new Party category for OU, RSA and MDR 'OSP 2'.
- New seats would be created for representative in the OSP 2 category at TABASC, OPSG, Change Board and Change Sub-Committee.
- This would change voting composition of Change Board.
- Changes to TABASC and Change Board would change the SEC.
- Changes to CSC and OPSG would take place via Terms of Reference (Panel approval needed).

# ■ Issues Group questions

Do you have any  
comments on the  
Proposed Solutions?

Any other  
comments/questions?



Thank you for  
listening

---

Any questions?

# 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 to listen on our [website](#) or [LinkedIn](#)

A solid green vertical bar.

# Thank you for listening

The next meeting will be on  
Wednesday 4 September 2024