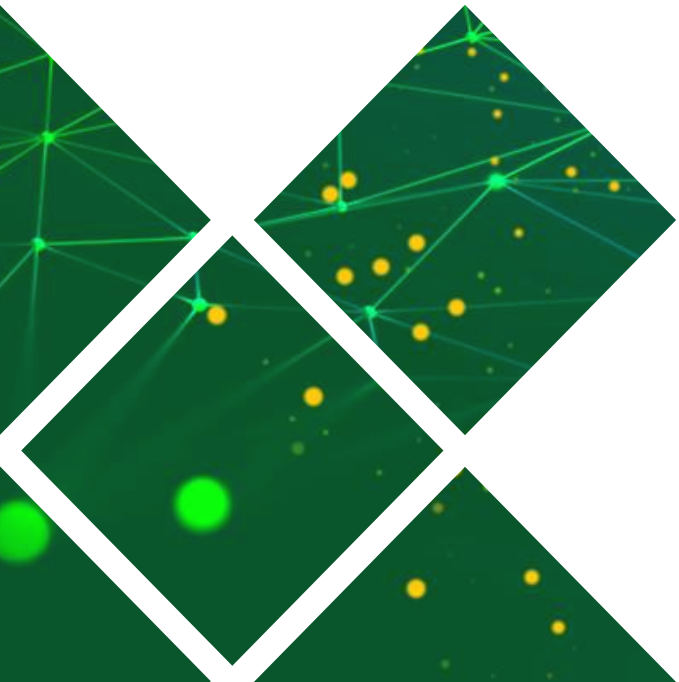


SEC CHANGE MONTHLY WORKING GROUP MEETING

MAY 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



MP235 'Enhanced Meter Data Access for Other Users'

Raised by Matt Roderick of n3rgy

■ Objectives of the Working Group

NOTE	The issue
REVIEW	The business requirements
AGREE	The next steps

■ MP235: Overview

Issue

- Other Users are limited in the Service Requests they can retrieve from Smart Metering Systems.

Impact

- Consumers are limited in the Parties which can provide them with more granular information about their usage.
- Other Users are limited in their abilities to offer innovative services to Energy Consumers.

■ MP235: Service Requests

Service Request Variant	Service Request Name
4.1.1	Read Instantaneous Import Registers
4.1.2	Read Instantaneous Import TOU Matrices
4.2	Read Instantaneous Export Registers
4.6.1	Retrieve Import Daily Read Log
4.6.2	Retrieve Export Daily Read Log
4.12.1	Read Maximum Demand Import Registers
4.12.2	Read Maximum Demand Export Registers
4.13	Read Prepayment Configuration
4.14	Read Prepayment Daily Read Log
4.16	Read Active Power Import
4.18	Read Meter Balance
6.2.1	Read Device Configuration (Voltage)
6.2.5	Read Device Configuration (Instantaneous Power Thresholds)
6.2.9	Read Device Configuration (Payment Mode)
7.4	Read Supply Status

■ MP235: Business Requirements

Requirement 1

- Includes all 15 SR's – this will have impacts on GBCS.
- ESME's, GSME's and Communications Hubs are impacted.

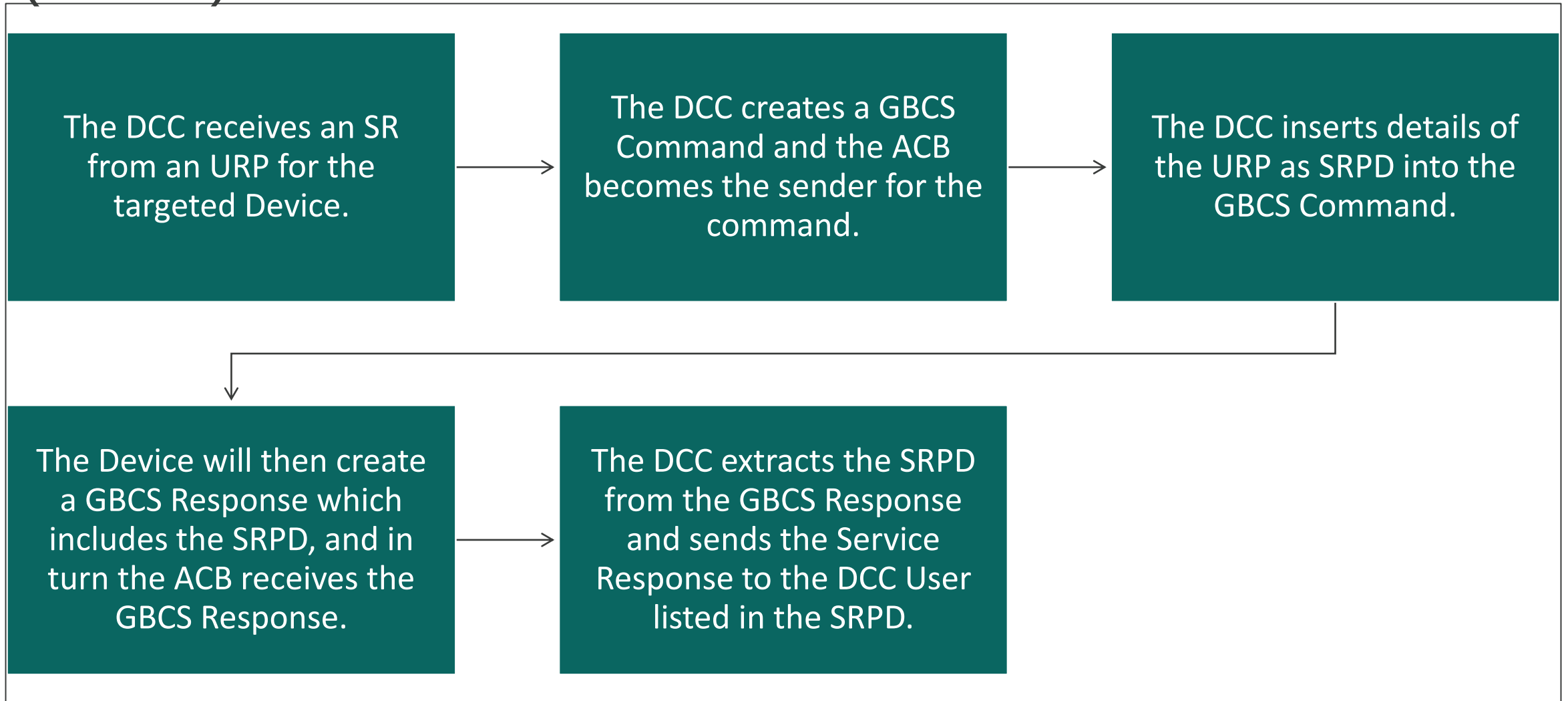
Requirement 2

- Removes the five SR's which have issues with Supplementary Remote Party Data and Encryption.

Supplementary Remote Party Data (SRPD)

- Impacted by SRVs:
 - 4.1.1, 4.1.2, 4.13, 4.18, 6.2.1.
- Other Users do not have security credentials on Devices and are considered an Unknown Remote Party (URP) when requesting GBCS Commands to be executed on Devices.
- For an URP to execute Commands it must be specified in GBCS for execution by the ACB. This is because the ACB requests the command on behalf of the URP.

Supplementary Remote Party Data (SRPD)



■ Encryption (4.1.1 + 4.1.2)

Due to sensitive information, some GBCS Commands require encryption of the data which is sent back in a GBCS response.

For URPs the receiving Device does not hold their certificate and therefore the ACB sends the UKR certificate as part of the SRPD.

The Device uses the certificate in the SRPD and sends the GBCS Response to the ACB.

The DCC will then extract the address of the URP from the SRPD and forwards the data to the DCC User.

Only the DCC User can decrypt this information as it requires the private key of the DCC User.

■ Questions for the Working Group

Do you have any comments about the business requirements?

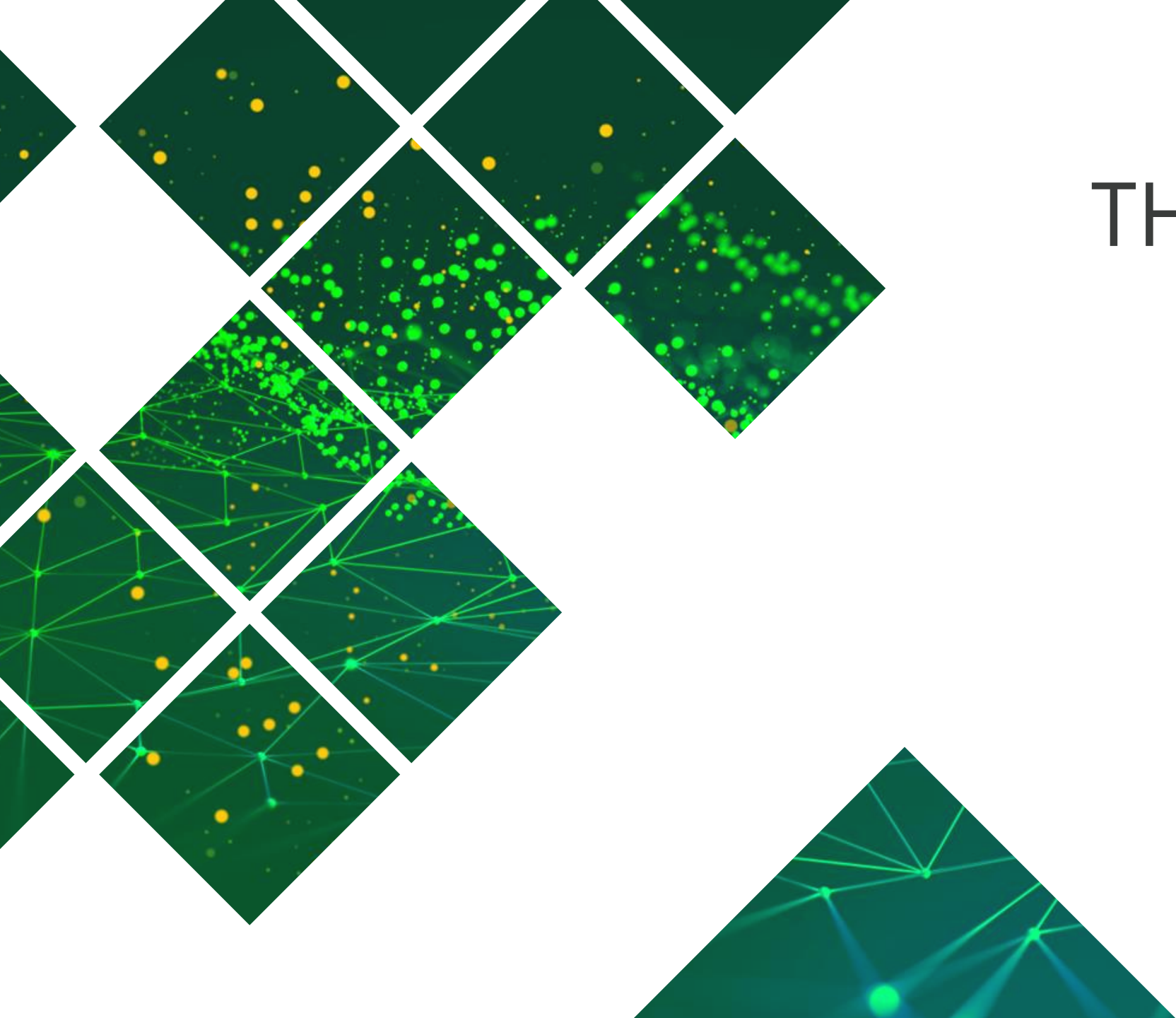


Any further comments?



Next Steps





THANK YOU FOR LISTENING

ANY FURTHER COMMENTS?

MP207: Allowing Registered Supplier Agents to Maintain Meter Firmware

Raised by Tom Woolley from SMS Plc

Objectives of the Working Group

REVIEW

SSC Feedback received

AGREE

The next steps

Issue

- MOPs and MAMs are able to become DCC Users in the User Role 'Registered Supplier Agent (RSA)'.
- Only Suppliers are currently able to deploy and activate firmware.
- RSAs are authorised to maintain the Supplier's meters but unable to maintain Device Firmware.

Potential Solution

- Allow RSAs to deploy firmware (*SRV 11.1 'Update Firmware'*).
- Suppliers will still need to activate firmware following the deployment.
- No changes to User CIO Assessment.

■ Proposed Solution Summary

Appointed RSAs

- Adds capability for RSAs to send SRV11.1s to ESME/GSME
- Receive all Alerts related to distribution & changes of firmware on Devices
- RSAs & Suppliers will receive confirmation of delivery

SSI

- RSAs and Suppliers able to see firmware tracking for Devices where the other Party has sent the SRV 11.1 using SSI

Definition change

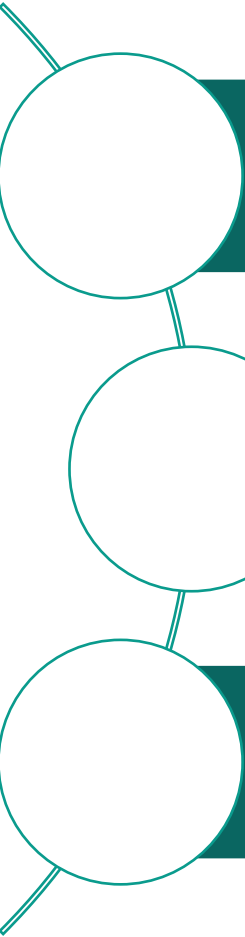
- Invalid Device check (W110101*) to include checking an RSA is appointed to the Device (ESME/GSME)

*W110101 - Used when Device does not exist or sender is not the Registered Supplier

■ Feb 2023 Working Group feedback

- Have seen Firmware variants passed testing and still resulted in faulty Firmware distributed.
- Negative effects on consumers.
- These issues only come to light when a Supplier or consumer complains about a non-functioning Device.
- Security concerns of RSAs potentially distributing faulty Firmware onto a Supplier's estate.

■ Feedback from SSC



Is the potential of an RSA distributing faulty Firmware onto a Supplier's estate a security risk?

Is the security risk the same as when a Supplier is potentially distributing faulty Firmware onto their own estate?

Any steps to be taken to mitigate this?

■ Questions for the Working Group

Are the security concerns addressed?



Should the Impact Assessment be requested?

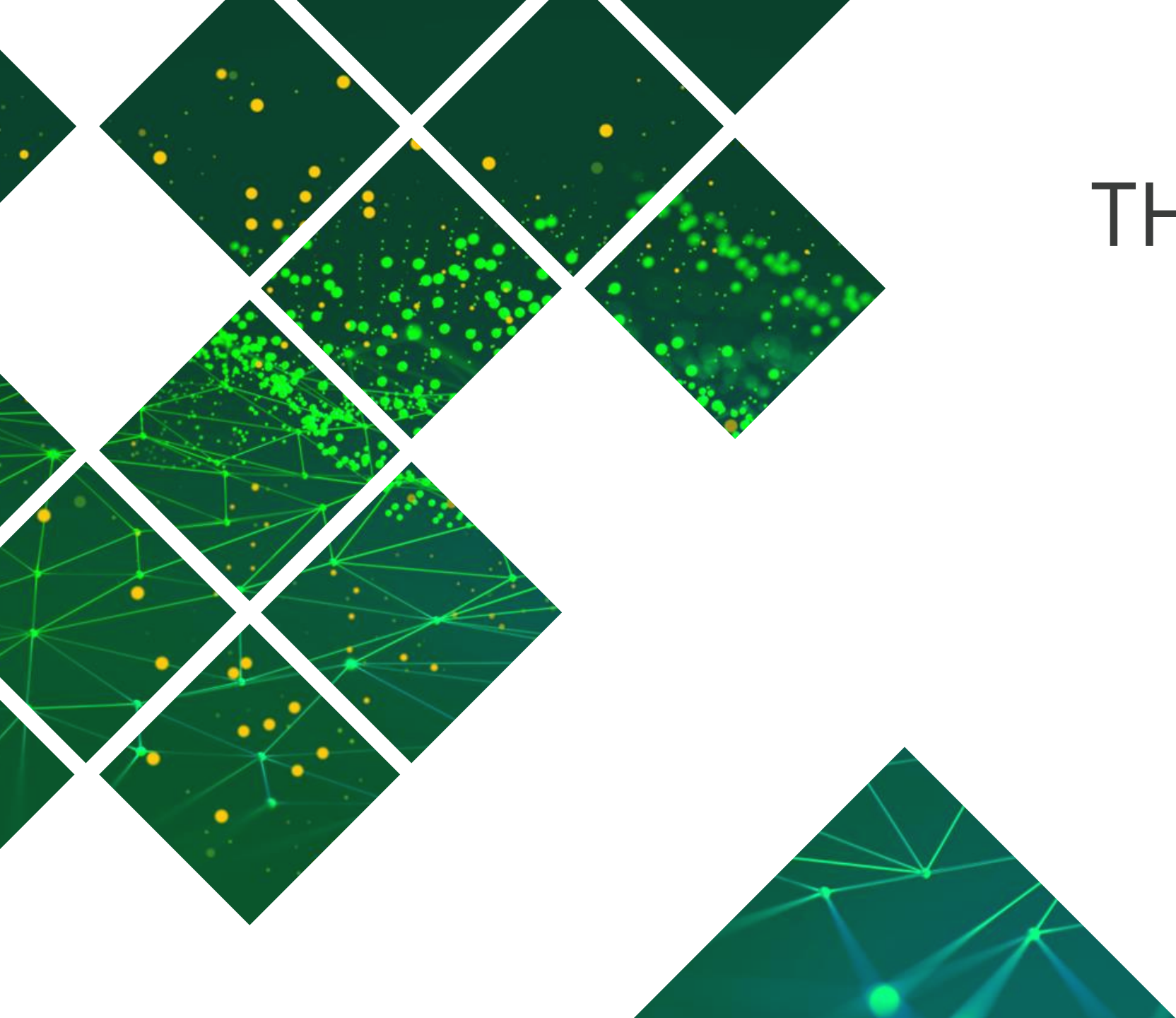


Next Steps

17 May – 9 Jun
Refinement
Consultation

Oct – Discuss DCC
IA response with
Working Group

June Change Board
– Request Impact
Assessment



THANK YOU FOR LISTENING

ANY FURTHER COMMENTS?

BREAK



PLEASE RETURN IN 10 MINUTES

■ MP202 'Enduring Solution for SMETS1 and SMETS2+ PPMIDs'

Raised by David Walsh of DCC

■ MP202: Overview

Issue

- Some models of PPMID can work as both a SMETS1 and SMETS2+ Device.
- The SEC differentiates so that a Device can be either SMETS1 or SMETS2+, but not both.
- PPMID's can't behave as both a SMETS1 or SMETS2+ PPMID, even if it can operate in such a manner.

Impact

- Suppliers need to ensure the correct version of PPMID is pre-notified and the correct SMETS version is installed.
- Should the Installer experience issues with the process, they need to contact DCC for manual SMI changes following an unsuccessful installation.

Solution

- Involves having two rows of the same firmware version for a Device Model included in the CPL.
- Allowing Devices to be pre-notified as S1/S2, with the DSP using the SMETS version from the Comms Hub to determine which version of SMETS the SMS is and update the SMI accordingly.

■ MP202: Current Arrangements

DCC Tactical Interim Solution

- The DCC's tactical interim solution involves creating distinct entries in the CPL for both the SMETS1 and SMETS2+ with a differentiating firmware version.
- The SMETS2+ PPMID CPL entry uses the real firmware version whereas the SMETS1 PPMID CPL entry uses a 'fictitious' firmware version.

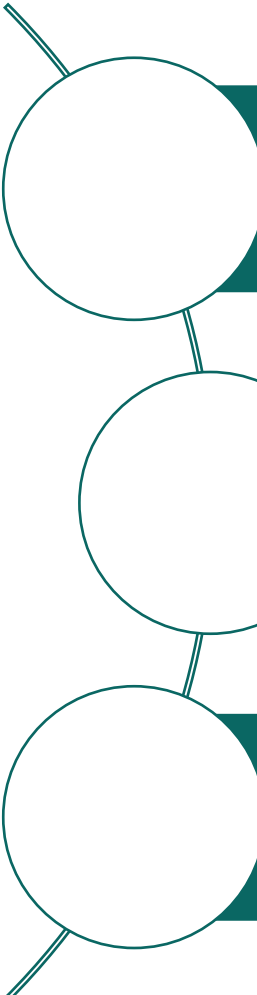
Scale of Issue

- Change Board questioned how many Parties this is impacting.
- SECAS received two responses to the Refinement Consultation which said they had issues with the current DCC tactical interim solution.

■ MP202: OTA Firmware Upgrades

- As part of the solution to MP202, OTA firmware upgrades will only be allowed for dual mode PPMIDs which are enrolled in a SMETS2+ SMS.
- **OTA firmware upgrades would no longer be available to PPMIDs enrolled in SMETS1 SMS.**
 - If OTA firmware upgrades were allowed to PPMIDs enrolled in SMETS1 SMS this requires an S1SR specific piece of information in OTA firmware payloads.
 - This would require three entries on the CPL for SMETS1 Devices, meaning there would be four different entries on the CPL, rather than the two as this modification proposes.
 - This would require a new process to be developed to enable the CPL entries to be identifiable from one another.
 - This contradicts another requirement for this modification for the DCC System to be able to distinguish between a single SMETS1 and single SMETS2 entry for the same PPMID entry.

■ Questions for Working Group



Does the issue identified under MP202 impact you?

Do you believe there is an industry benefit for this modification to be developed further?

Are you experiencing any issues with the DCC's tactical interim solution?

■ MP202: Request for Information

- Parties are invited to respond to the RFI by 22 May 2023. The link to the RFI can be found [here](#).

MP178: Removing DSP validation against the SMI join status for SR8.8.x

Raised by David Walsh from the Data Communications Company (DCC)

Issue and Solution

- Instances where the Devices are joined in the field but not reflected in the Smart Metering Inventory (SMI)
- SRV 8.8.1 and SRV 8.8.2 validate the join status of Devices on SMI and are rejected if join not found
- Proposed Solution to remove join check in the SMI for SRV 8.8.1 and SRV 8.8.2

Discussions at April 2023 Working Group

- WG agreed:
 - Solution was suitable
 - Will apply to all versions of DUIS
 - Changes to DUIS and DUGIDS needed
 - Needed to ensure Response Code is not removed from DUIS as has been there for so long

Response Code	Response Code Description
E080801	According to the DCC Systems Smart Metering Inventory the ‘Other Device’ is not joined to the BusinessTargetID Device <u>This Response Code is not used. The DCC Systems Smart Meter Inventory is no longer checked for the join status of the ‘Other Device’</u>

■ Questions for the Working Group

Is the legal text suitable?

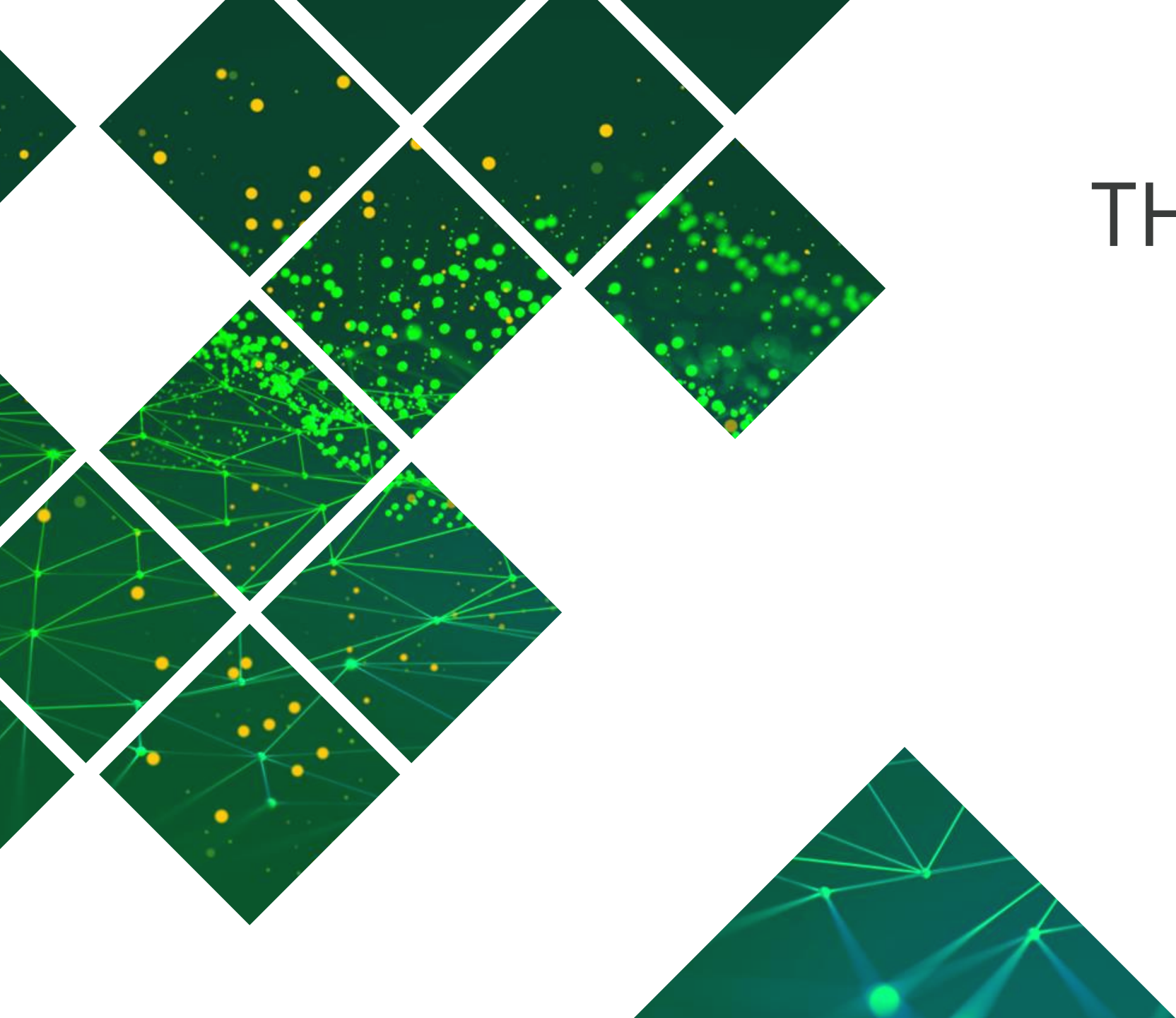


Is the modification complete?



■ Next Steps





THANK YOU FOR LISTENING

ANY QUESTIONS?

■ DP224 'Performance Assurance Framework'

Raised by Emslie Law from OVO Energy

Objectives of the Working Group

REVIEW	The request for information (RFI) responses
AGREE	The issue is defined
AGREE	The next steps

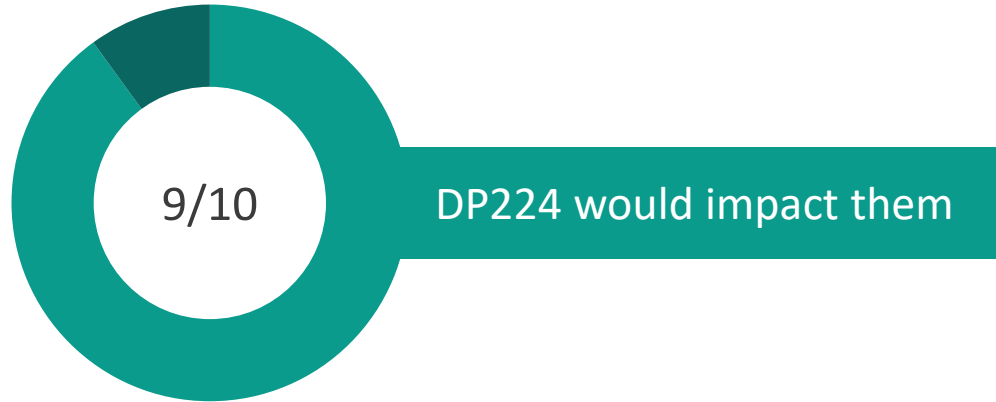
Issue

- SEC does not explicitly define a Performance Assurance Framework (PAF)
- Panel is expected to manage any performance-related matters as they arise
- Panel's scope is broad and managing matters case-by-case is challenging
- A 2022 project concluded that a risk-based PAF would give Parties confidence obligations were being met
- Project identified some issues and instances that may have fallen under scope of a PAF

Purpose of the RFI

- Further work needed to fully define the scale of the issue to support case for change
- Project defined a potential solution – this will need to be further refined and the scope of any PAF defined as part of this modification

RFI Key points



Focus of a PAF

- Focus on consumer/high impacts
- Drive performance improvements
- Not just Supplier obligations



Requirements of a PAF

- Low resource for Parties to engage with
- Built around existing SEC framework
- Provide guidance on how to correct non-compliances
- Avoid duplication (other Codes, existing reporting or financial incentives)



■ Potential scope

Alt HAN Arrangements

- One respondent noted Section Z 'Alt HAN Arrangements' does not currently sit under Panel jurisdiction
- It is governed by the Alt HAN Forum with escalations direct to Ofgem
- Could introduce similar provisions into the Alt HAN Forum if required?

Security & Charges

- Panel Paper and subsequently agreed recommendation that the following areas be out of scope:
 - Section G 'Security'
 - Section J 'Charges'
- One respondent felt Section G should not be excluded, but should be reviewed. Noted that Annual User Assessments for all Parties may not be suitable anymore.

DCC

- DCC should not be excluded.
- Concern of DCC impact to settlement if performance poor (MHHS). Currently won't be managed as not party to BSC – PAF/PAB could cover this.

■ What issues could fall under a PAF?

DCC management of outages/ maintenance/ incidents

Identifying material risks surrounding central delivery system

Failure to meet security obligations (such as the post-commissioning obligations or SMKI obligations)

Timeliness of firmware upgrades

Traffic/demand on DCC services by specific Users which results in performance issues that impact other DCC users

Failure to maintain the DCC's Smart Metering Inventory and apply updates on a timely basis

Suppliers not responding to requests for install keys for non-commissioned Devices that have changed supplier

Other considerations

Risk Based approach

- Should consider Organisation size/portfolio.
- Metrics should use “% against industry” rather than by portfolio size as could disproportionately highlight Small Supplier issues.

Should be low impact to Parties

- Administrative burden to be borne by SEC & Service Providers (particularly around reporting data).

Consider timing and phasing of introduction

- Consider wider industry view, particularly with Code Reform
- Allow suitable time to transition to new arrangements.

Reporting changes

- DCC reports on 80 measures to OPSG. Rationalise and consolidate DCC reporting and metrics to re-focus on what matters most.
- Changes to DCC Reporting will require Impact Assessments

Questions for the Working Group

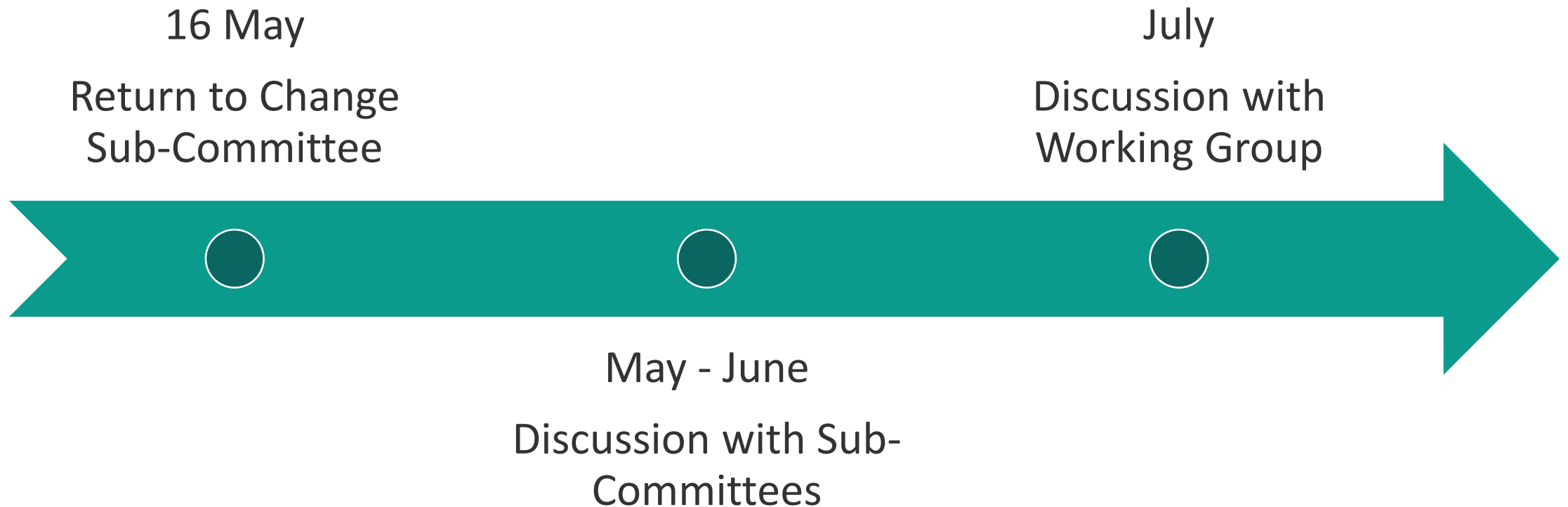
Is the issue defined?

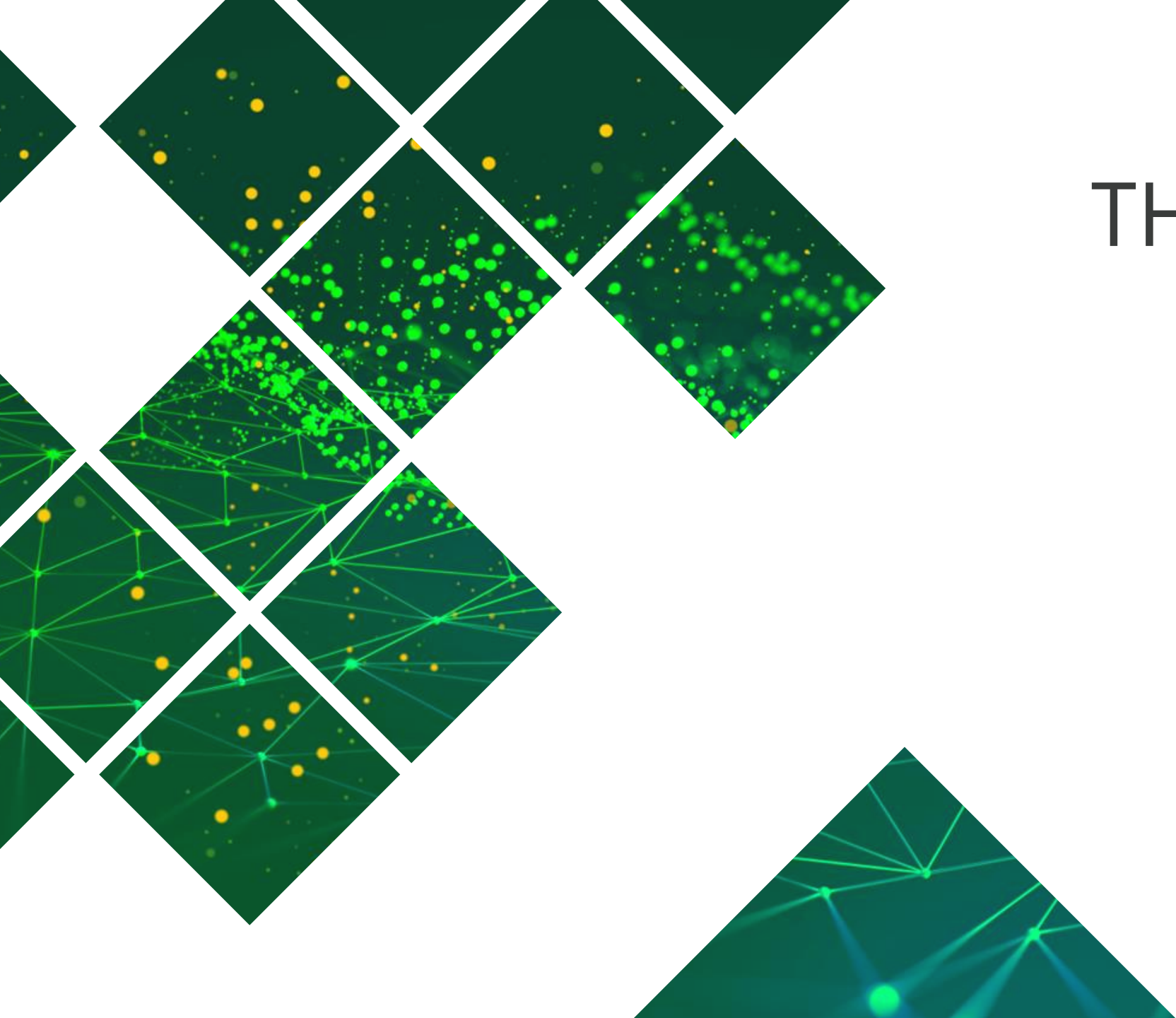
Should this modification continue to progress the introduction of a PAF?

If progressed, should DCC be required to provide Data into the PAB to assist with issue and impact analysis?

Should Sections G, J and Z remain out of scope?

Next Steps





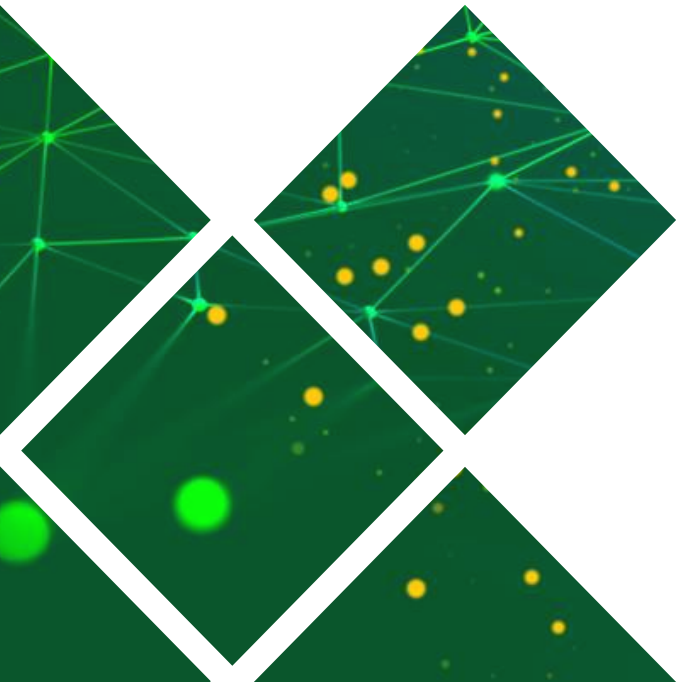
THANK YOU FOR LISTENING

ANY FURTHER COMMENTS?

■ ANY OTHER BUSINESS

Kev Duddy

SECAS ANNUAL CUSTOMER SATISFACTION SURVEY



SECAS ANNUAL CUSTOMER SATISFACTION SURVEY

- The SECAS annual Customer Satisfaction Survey is due to be held and SEC Parties are invited to provide consent to take part.
- The deadline to provide consent has been extended to **Close of Business Friday 5 May 2023**.
- To provide consent please fill in the required details of the [online Consent Form](#) using Google Chrome, Firefox or Microsoft Edge.
- SECAS commissioned DJS Research, an independent market research company to carry out the survey.
- Parties who provide consent to participate in the survey, will be contacted by DJS **by telephone** to carry out the survey.
- SECAS and the SEC Panel welcome your thoughts, feedback, and participation; and urge Parties to take part as your views will directly influence our services and how we support you.
- The SEC Panel will consider the responses and act accordingly.

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 7 JUNE 2023