

SEC Change Monthly Working Group Meeting

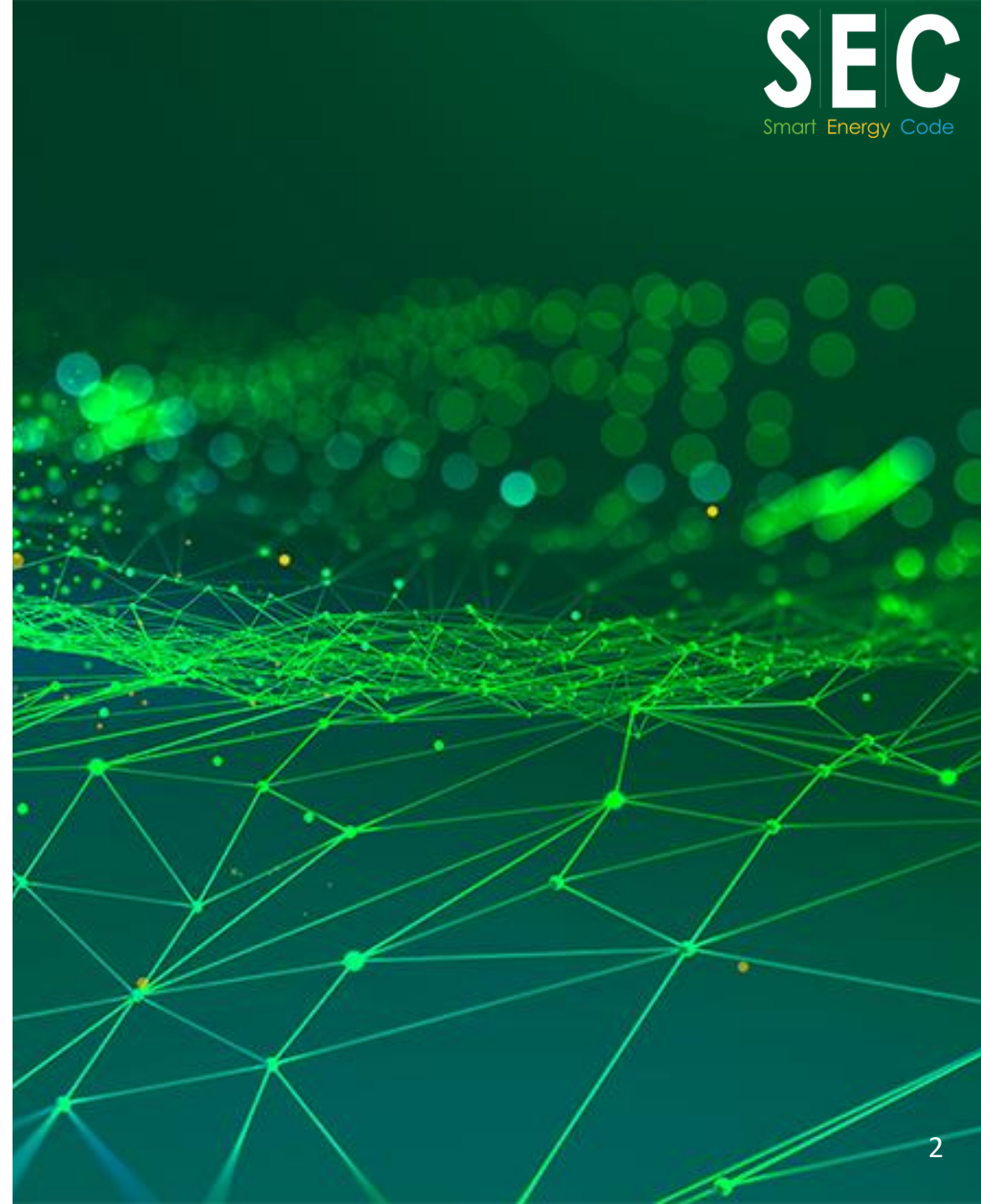
February 2025



Competition Act Compliance

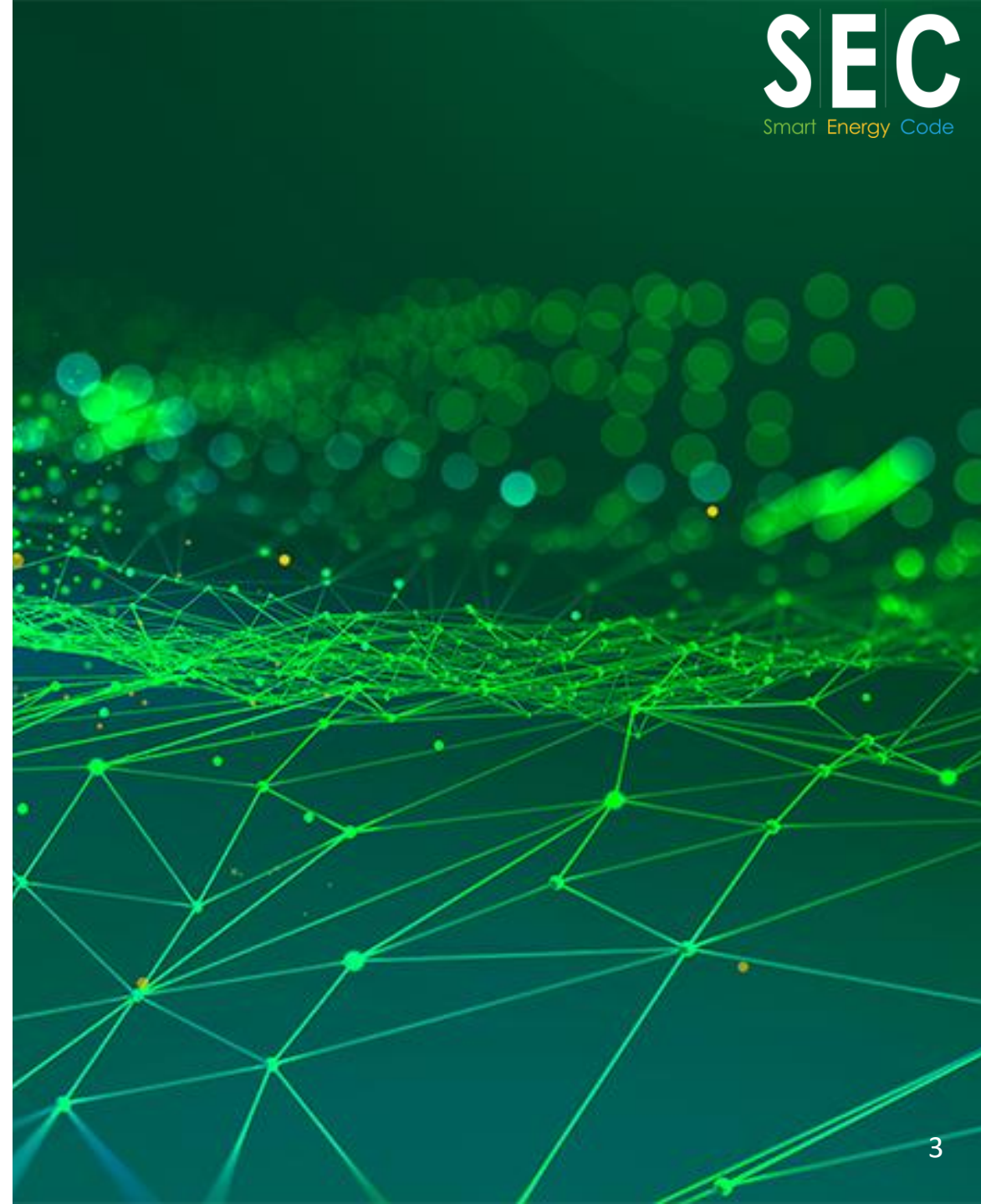
It is everyone's responsibility to say something

The Chair will move the conversation on



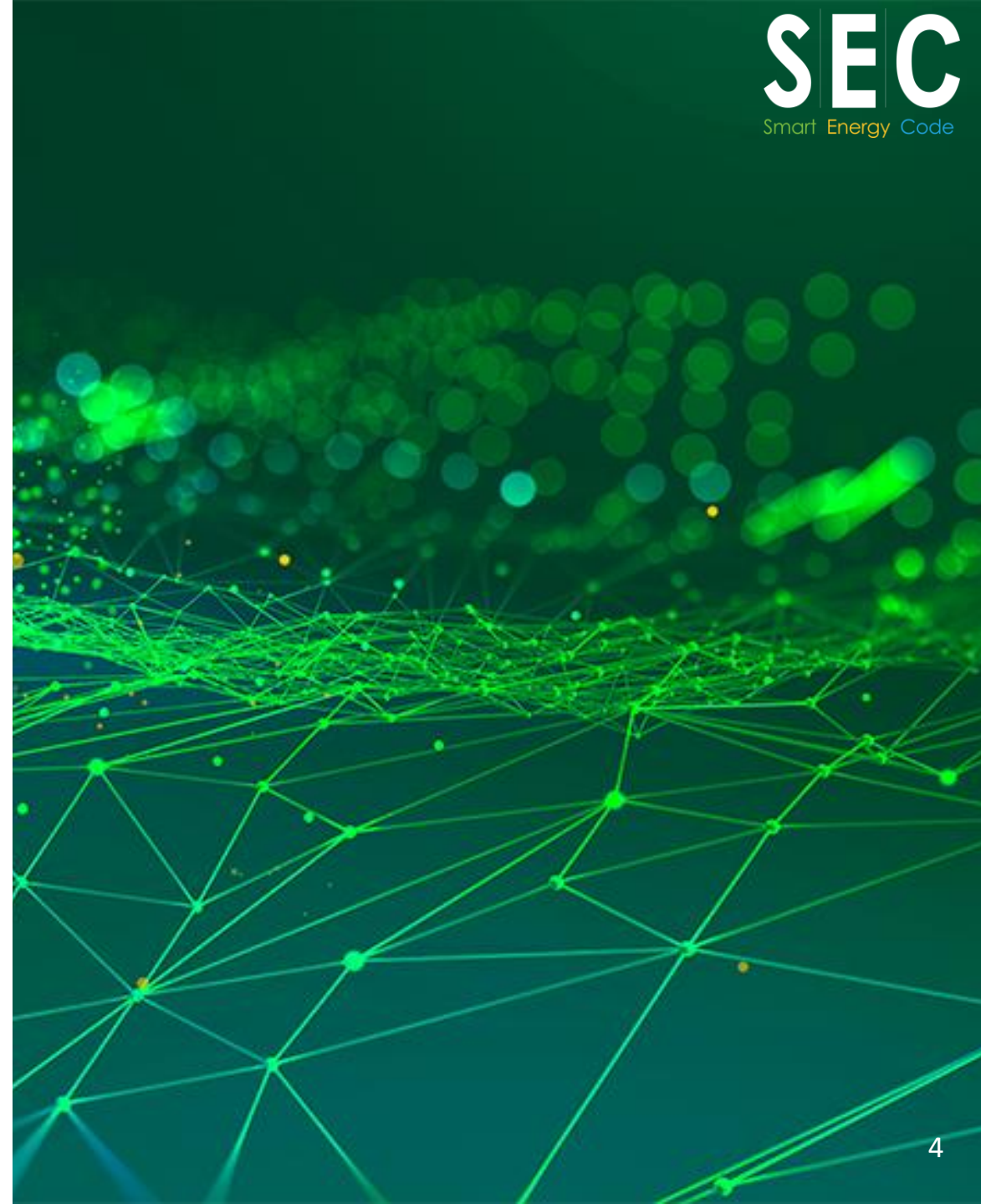
Housekeeping

- 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



■ DP257: DCC Management of Duplicate Messages

Raised by Matt Roderick from n3rgy
Georgie Severin

MEDIUM

Objectives of the Working Group

NOTE

The DCC duplicate messages data

AGREE

The Next Steps

Issue

- Issue identified relates to DCC traffic – focusing on duplicate messages;
- Large number of SRs are duplicates, according to analysis by DCC.
- Increasing number of Devices will create more traffic; increase in Parties wanting to access more data likely to increase SRs.

Impact

- Volume of duplicate messages increases strain on DCC Total System.
- High traffic times could result in DCC not meeting TRTs or cause failure of messages being delivered.
- Alternatively, the DCC could spend on additional infrastructure to meet the TRTs at these peak times. This is not deemed cost-efficient.

Service Reference Variant – DCC Data

4.10	Read Network Data
4.14	Read Prepayment Daily Read Log
4.15	Read Load Limit Data
4.16	Read Active Power Import
4.17	Retrieve Daily Consumption Log
4.6.1	Retrieve Import Daily Read Log
4.6.2	Retrieve Export Daily Read Log
4.8.1	Read Active Import Profile Data
4.8.2	Read Reactive Import Profile Data
4.8.3	Read Export Profile Data

SMETS 2 - SPS/ Data Cache DP257

- **Problem Statement:**
“The same or different customers request multiple instances of identical messages to a unique device within a set period and the returned content has not changed, creating inefficiency through repeat and unnecessary use of capacity of the E-2-E network”
- **External validation with SEC Role as source for cacheable duplicates. (Green)**
- **Separate initiative to investigate high number of SRV's from unique customer within same day to same meter. i.e. 100 x 4.8.1**

Message Code	Comb. Supplier	EIS	GIS	ENO/ DNO	Other User	Export Supplier
4.10						
4.14						
4.15						
4.16						
4.17						
4.6.1						
4.6.2						
4.8.1						
4.8.2						
4.8.3						

Cacheable	8 Oct 2024	3 Dec 2024	Projected
Schedule Reads	1.7%	1.5%	26%
Schedule Reads & On Demand	9%	7%	29%

- When DNO's fully roll out 4.8.1 the projected cacheable SRV's increases.
- Final stage of analysis is to compare SRV request periods, e.g. is it 1 day or 2 days.
- Schedule Read SRVs have a small volume of cacheable data and is unlikely as of today to financially justify a data cache.
- We need to monitor for growth with DNO's and Other Users along with the external work on SMEDR and next step to address for investment now for the future.
- Therefore, request to move forward with this modification to continue the planning and detailed options for future network optimisation.

■ Working Group Questions

Is there any further information that would be required of the DCC before the modification can progress to the Refinement Stage?



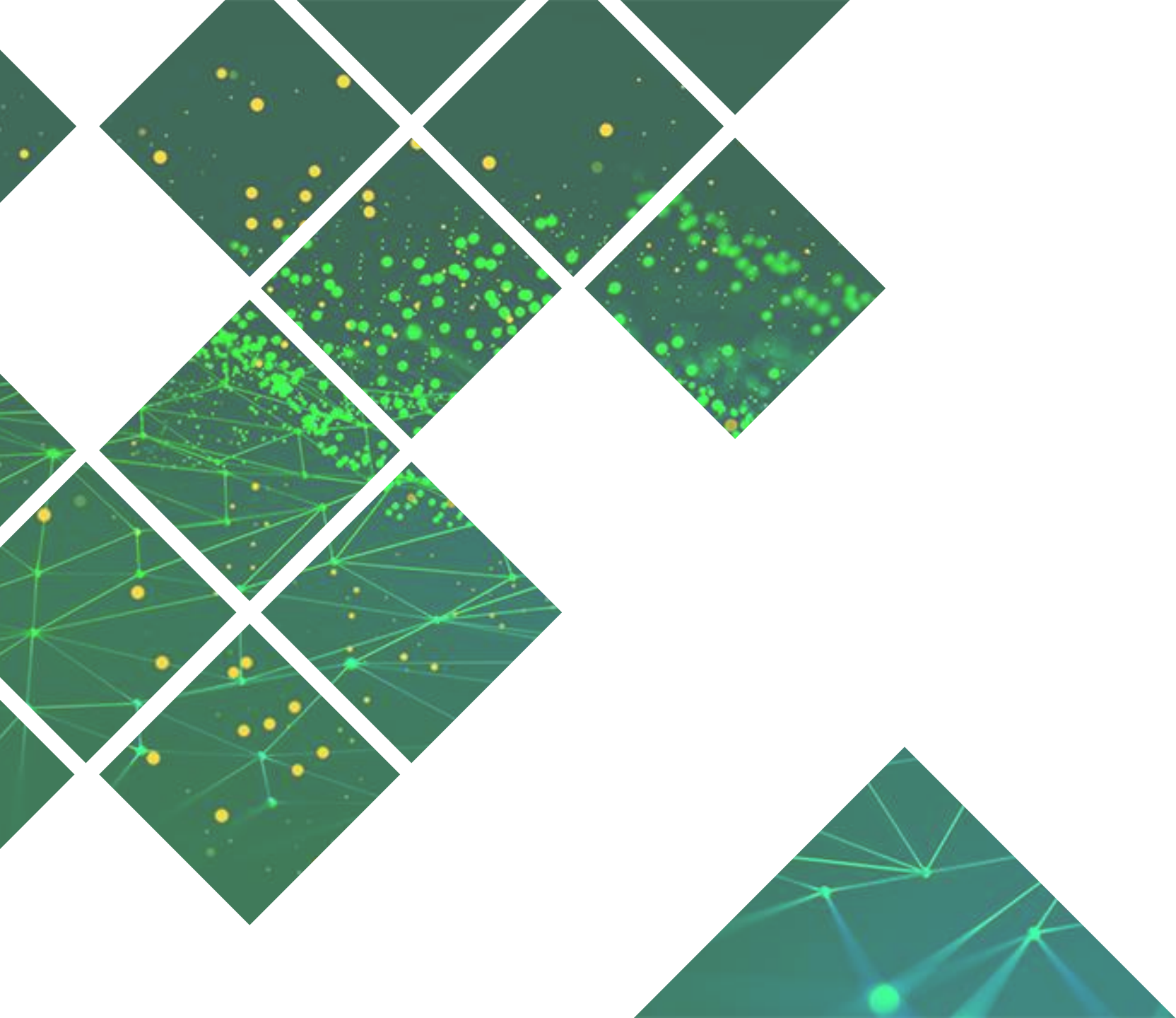
Any further comments?



■ Next Steps



DCC verbal update



Thank you for listening!

Any questions?

■ Any other business

Liz Woods

■ AOB - MP252: Amending the process for Communications Hub returns

Raised by David Lane on behalf of SMS Plc
Liz Woods & DCC

HIGH

MP252 Proposed DUIS Schema Changes

- add new error code for 8.14.3 and 8.14.4

```
<xs:enumeration value="E081401"/>
<xs:enumeration value="E081402"/>
<xs:enumeration value="E081405"/>
<xs:enumeration value="E081406"/>
<xs:enumeration value="W081401"/>
```

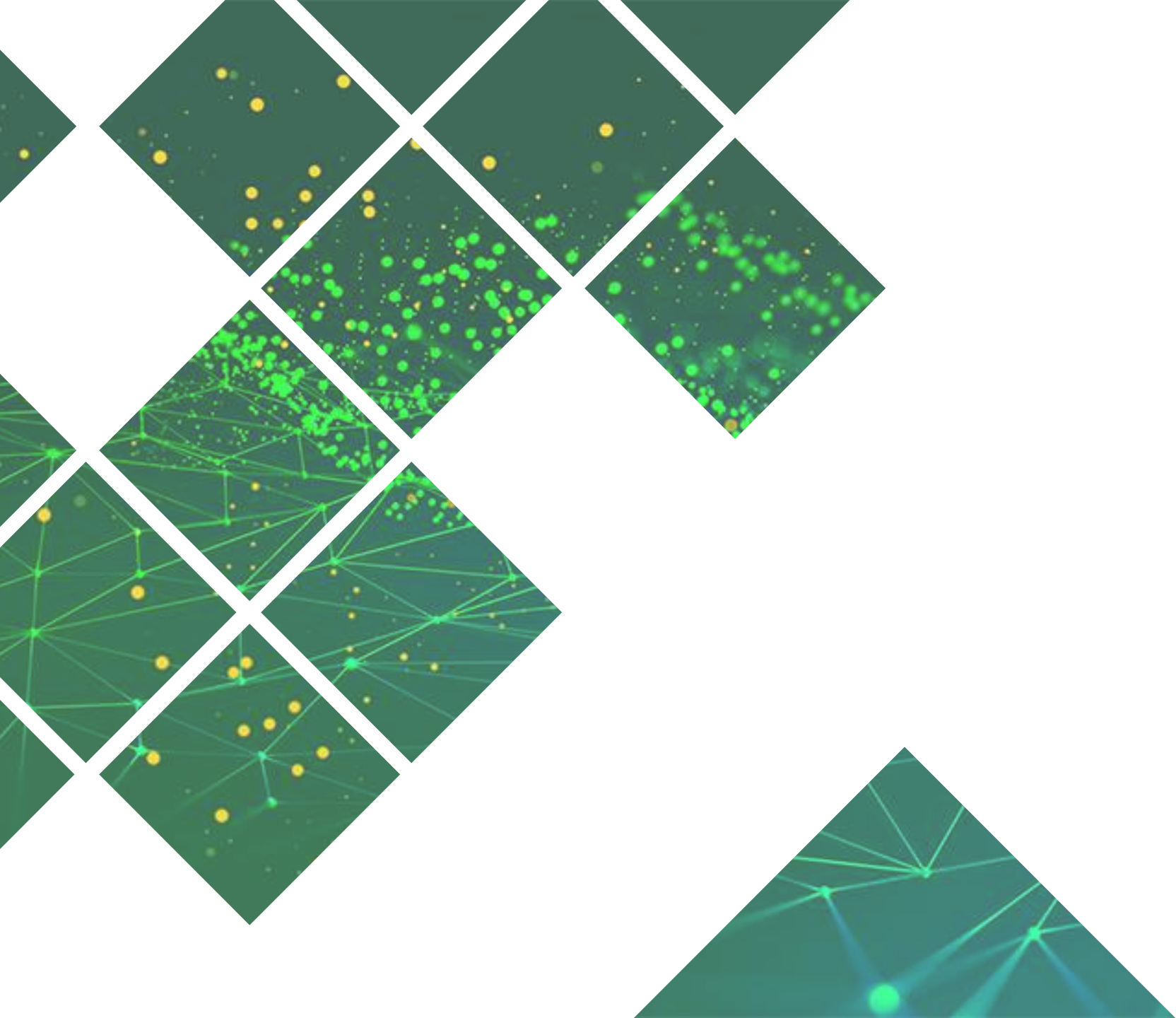
Response Code	Response Code Description
E5	The User Role is RSA and the CHF Device Status is not Pending
E081401	The Device Type of the Device being notified is not CHF
E081405	The user reference date & time supplied is a future date
E081406	The CHF Device status is not 'Decommissioned' and the CHF has associated Devices which are still communicating
W081401	The CHF Device status is not 'Decommissioned'.

- note on processing of valid CHF

3.8.120.4 Additional DCC System Processing

Where the CHF Device status is not 'Decommissioned' and response code W081401 is returned, the DCC shall update the CHF Device status to 'Decommissioned'. If the GPF Device status is also not 'Decommissioned' the DCC shall update the GPF Device status to 'Decommissioned'.

- Users on previous DUIS versions will receive E5 not E081406 if the CHF has associated Devices still communicating
 - As response code E081406 is not supported in prior DUIS, reuses a pre-existing error code as part of the synchronous response



Thank you for listening!

Any questions?

SEC Issues Group

February 2025



■ Issues Group – Data breach reporting

Raised by Sharon Armitage from E.ON (Privacy Sub-Committee member)
Georgie Severin

TBC

Objectives of the Issues Group

REVIEW

The issue

AGREE

The next steps

Issue

- Privacy Sub-Committee currently has no visibility of data breaches which may occur.
- No obligation on Users to report data breaches to the Privacy Sub-Committee.

Impact

- Data loss or compromise has a negative impact on the energy consumer.
- Can lead to reduced confidence in Smart Metering and the governance in place to protect energy consumers and their data.

Solution

- Amendments to SEC Section I 'Data Privacy'
- Include requirement for Users to report data breach to the Privacy Sub-Committee.

■ Questions for the Issues Group

Do Issues Group members believe there would be any unintended impacts caused by this issue?

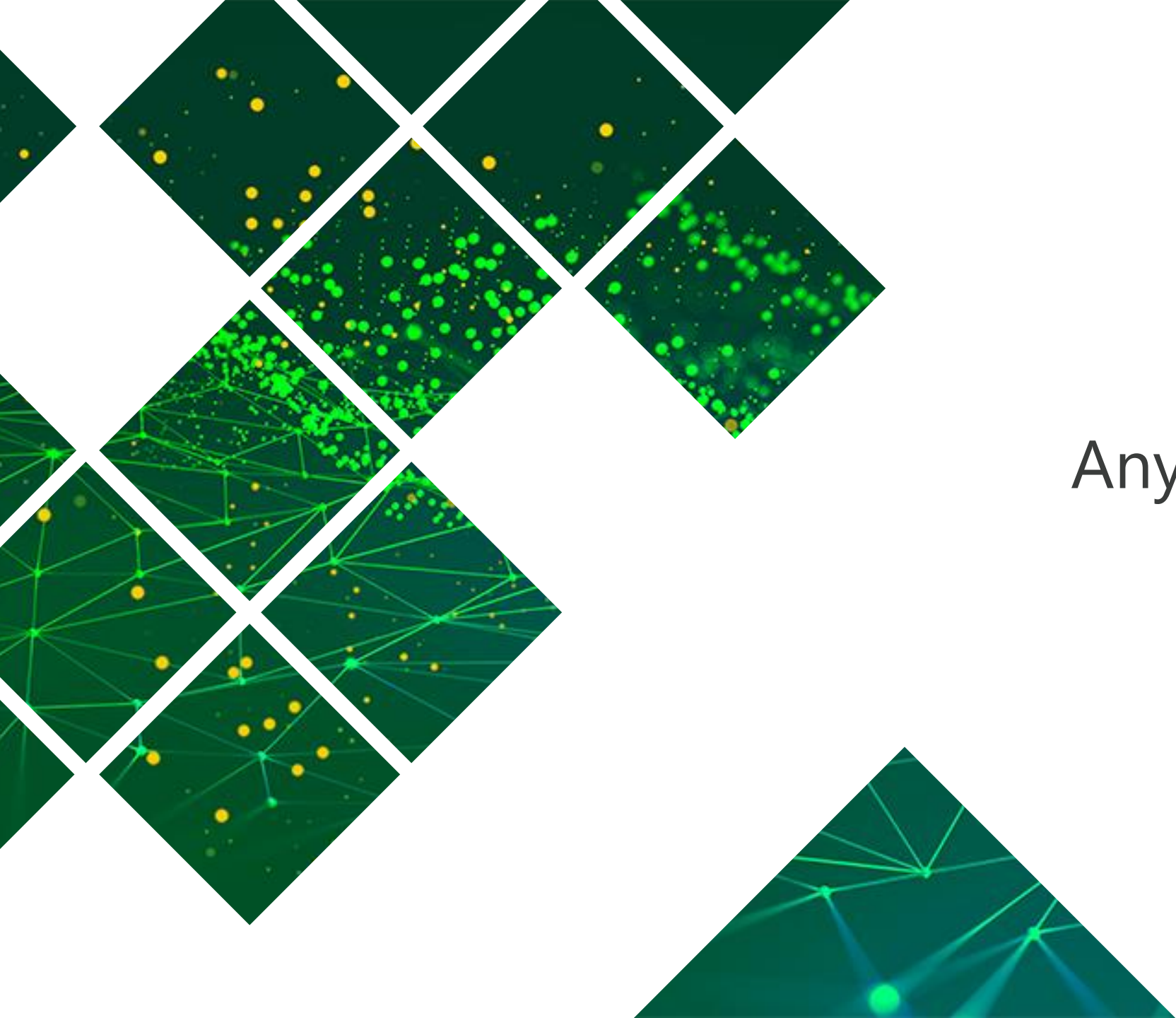
A row of seven teal parallelogram shapes, each slanted to the right, intended for input or marking.

Anything else that needs to be considered?

A row of seven teal parallelogram shapes, each slanted to the right, intended for input or marking.

Next Steps





Thank you for listening

Any further comments?

■ Issue Group - Erroneous Section J Default Notices

Submitted by Catherine Duggan from ENWL
Simon Grimwood

TBC

Objectives of the Issues Group

REVIEW

The Issue

AGREE

The next steps

Current Arrangements

- Section J2.1 'Payment Default and Disputes' enables the DCC to issue a default notice where a Party fails to pay an amount set out in an DCC charges invoice due date.
- The default notice issued by the DCC will amongst other things refer to other sections of Section J2.2 'default interest', J2.4 and J2.5 'resolution of payment disputes', J3.16 'credit assessment report' and M8.1 (c) 'events of default'.

Issue

- ENWL have identified instances where as the DCC have issued a notice due to the late collection of a Direct Debit.
- There is no provision within SEC Section J for the prevention (or exclusion) of the DCC issuing default notices to a Party due to DCC's late collection of the payment by the due date on the Party invoice.

■ Impacts & Proposed Solution

Impacts

- A Party can receive an erroneous default notice which can be resource intensive to resolve for both a Party and the DCC.
- Potential for an Event of Default against a Party being escalated to the BSC Panel.
- Could lead to unnecessary additional administrative burden on SECAS and BSC Panel members and increases the potential of reputational damage on the Party in question.

Proposed Solution

- The Proposer would like to place an obligation within the SEC preventing the DCC from raising default notices against a SEC Party on the grounds of a late Direct Debit collection.

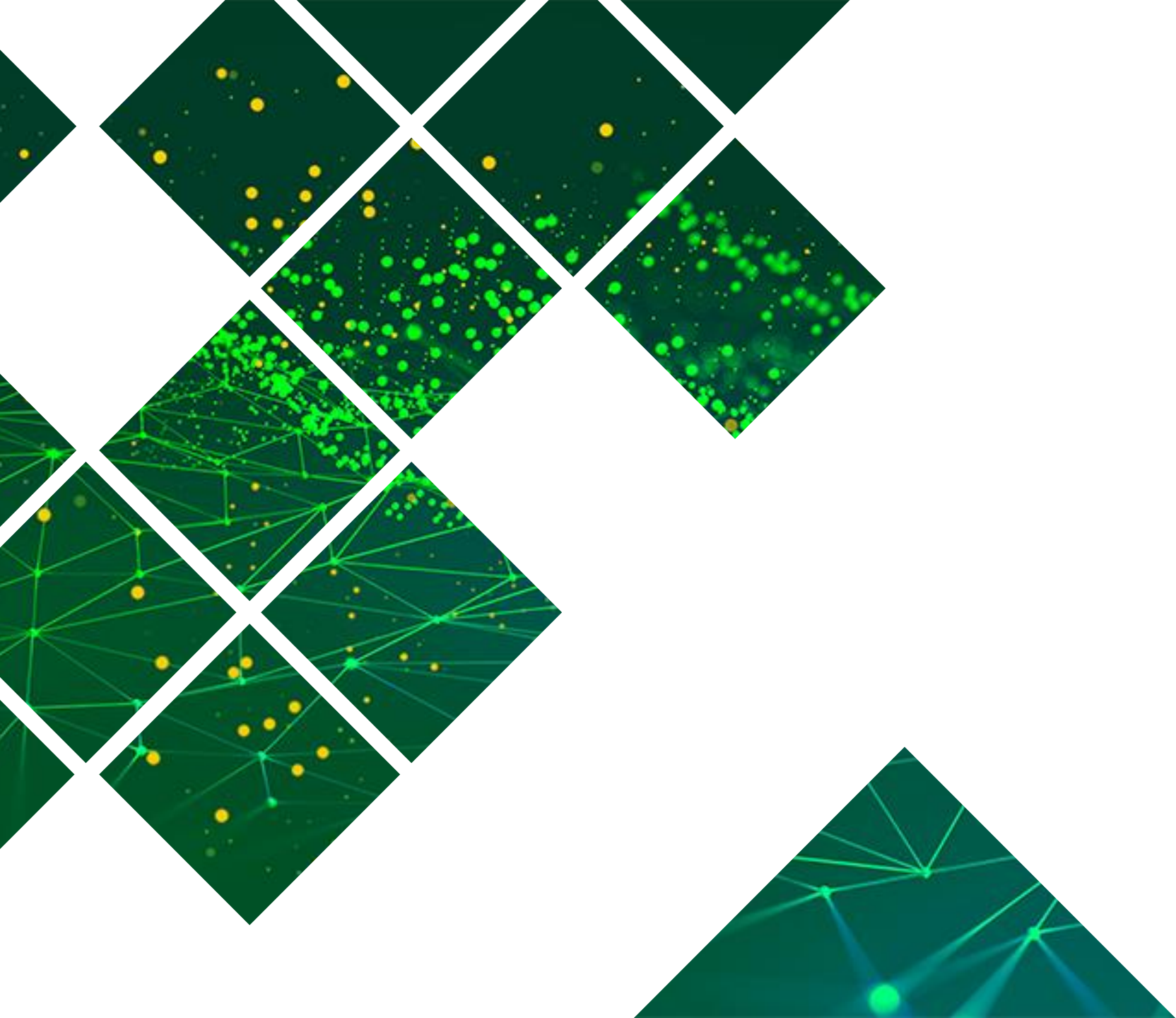
■ Questions for the Issues Group

Does the Issues Group agree with these concerns?



Does the Issues Group believe this issue should become a SEC Modification?





Thank you for listening

Any questions?

■ Issues Group - Removal Of Registration Check For Suppliers Using SR8.9 Targeting SMETS2+ CHF

Raised by Chun Chen from the Data Communications Company (DCC)
Georgie Severin

TBC

Objectives of the Issues Group

REVIEW

The Issue

AGREE

The next steps

Issue

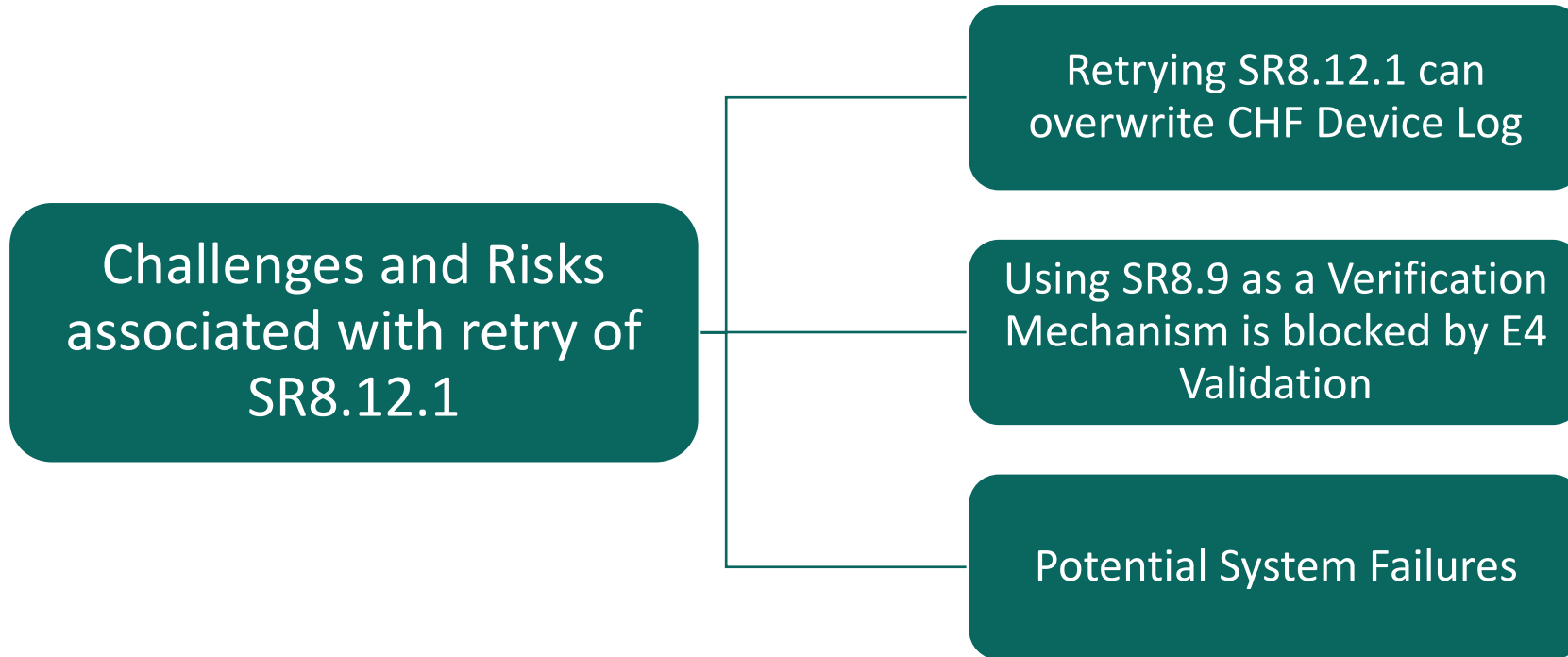
- The CHF Device Log is populated by either SR8.11 during I&C or SR8.12.1 during CH Replacement. If either results in a time out, the copy of the Device Log will be empty. Supplier will attempt SR8.9. This results in an E4 validation failure.
- Currently, the Registration Check (E4 validation) is applied to most non-critical SRs, except for those explicitly excluded in the SRPD and detailed in clause 3.8 of DUIS. SR8.9 is not exempt from E4 validation.
- Issue was discussed at TSIRS, TIRG and DRF

SR8.9 – Read Device Log

SR8.11 – Update Han Device Log

SR8.12.1 - Restore HAN Device Log

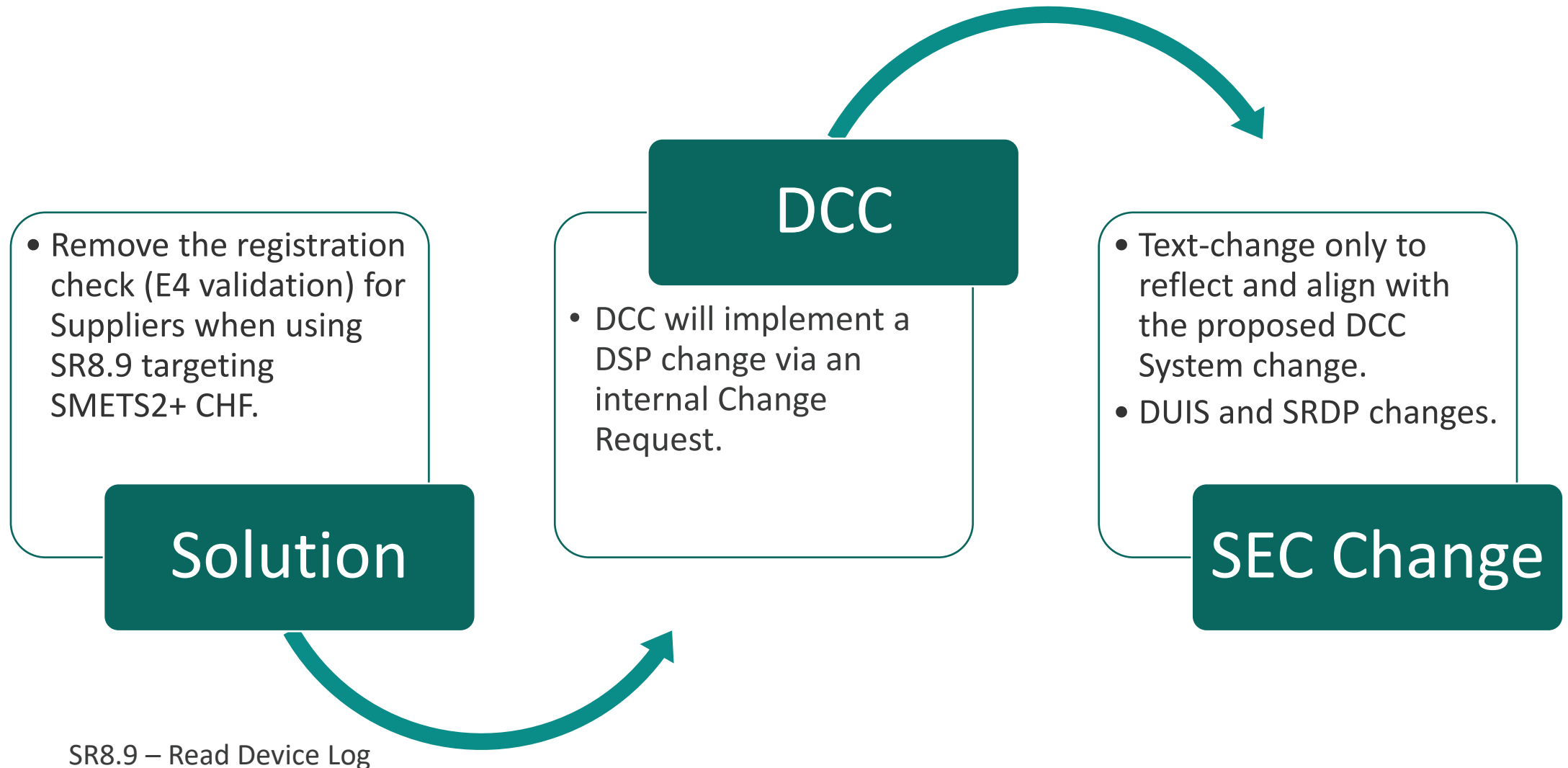
Overview (2/2)



SR8.12.1 - Restore HAN Device Log

SR8.9 – Read Device Log

■ Proposed Solution Summary



■ Questions for the Issues Group

Is the modification complete?



Anything else that needs to be considered?



Next Steps



Change Sub-Committee

18 Feb 2025



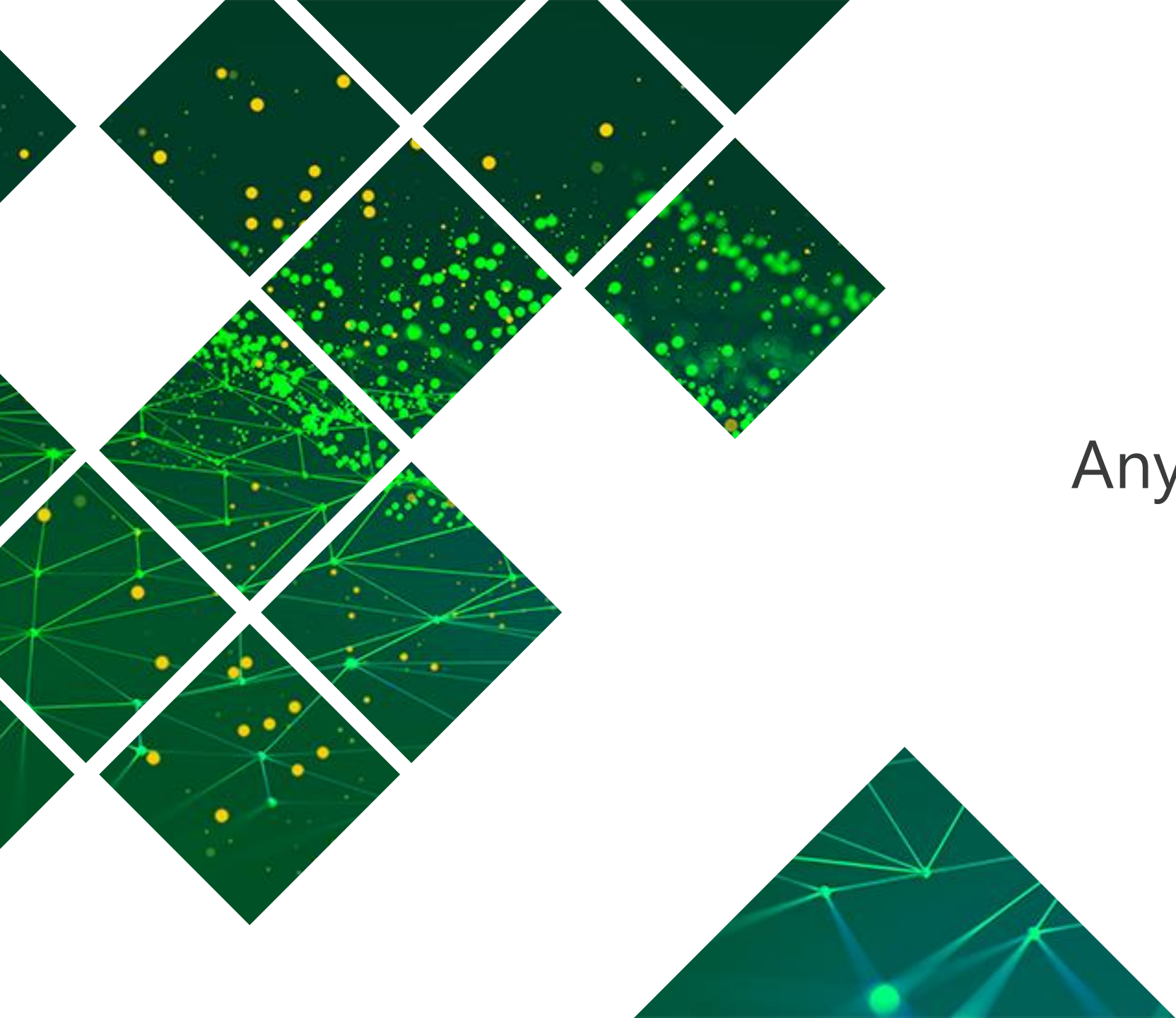
Modification Report Consultation

19 Feb – 12 Mar 2025



Change Board

26 Mar 2025



Thank you for
listening

Any further comments?

■ Issues Group - Extension of life to FOC S1SPKI End Entity Certificates

Raised by Brad Baker from the Data Communications Company (DCC)
Liz Woods

TBC

Objectives of the Issues Group

REVIEW

The Issue

AGREE

The next steps

Overview

Issue

- Final Operating Capacity (FOC) SMETS1 Service Provider Public Key Infrastructure (S1SPPKI) policy and FOC S1SPPKI itself have a number of end entity Certificates that have lifetime of 5 years from the point of generation.
- These Certificates are essential to maintain Device operation.
- There is a high cost associated with Certificate renewal every four years for the remaining lifetime of SMETS1 Devices on the wall.

Potential Solution

- The potential solution is to extend the Certificates to a date that aligns to the lifetime of the Root Certificate and therefore creating a cost saving to industry.
- SMKI PMA agreed there are no objections to DCC's proposal to align the end validity date of all SMETS1 FOC Certificates to align with the 25-year life of the Root Certificate.
- SSC agreed there are no objections from a security perspective.

Questions for the Issues Group

Does the Issues Group agree with these concerns?

Does the Issues Group believe this issue should become a SEC Modification?

Anything else that needs to be considered?

■ Next Steps



Change Sub-Committee

18 Feb 2025



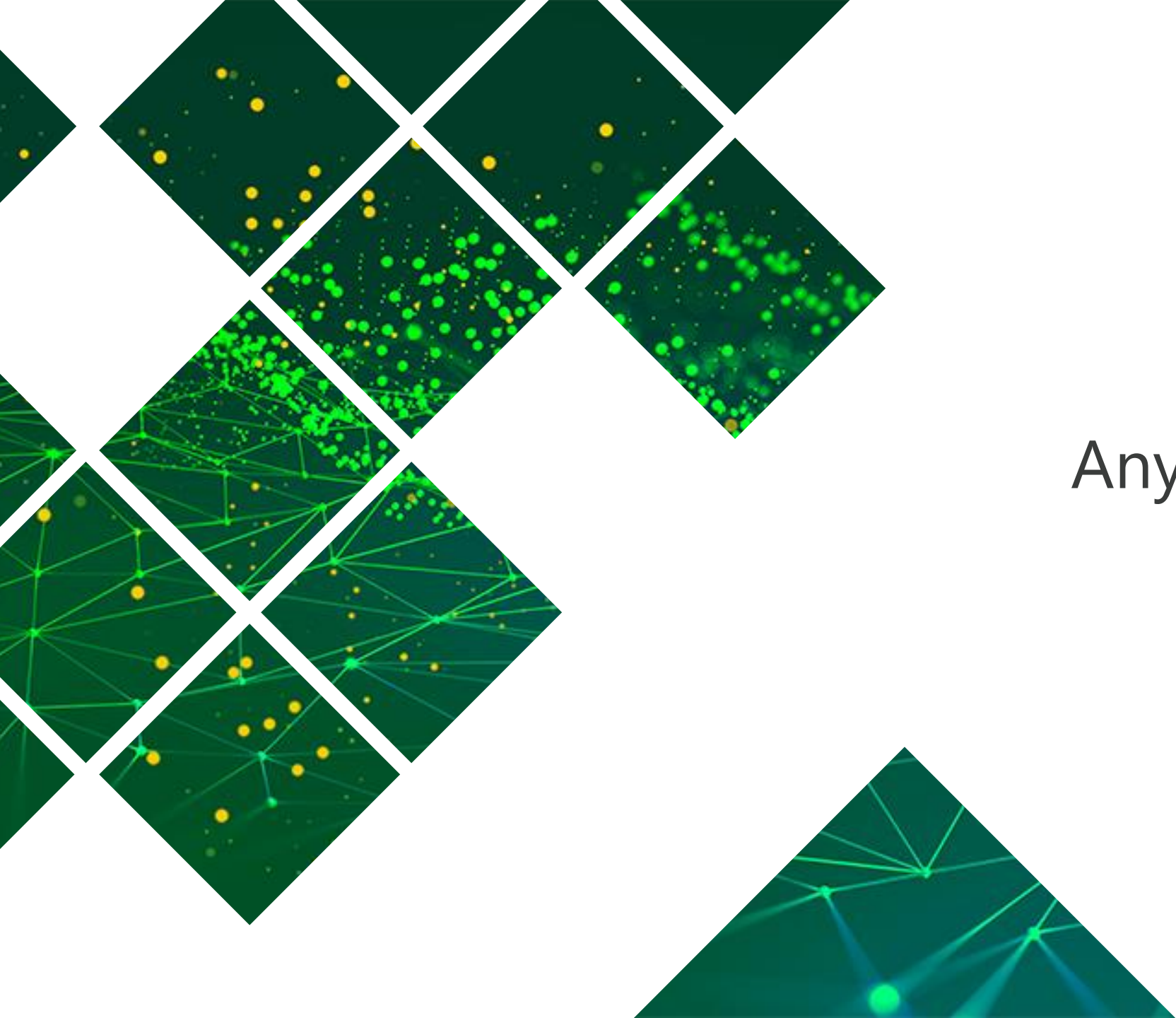
Modification Report Consultation

19 Feb – 12 Mar 2025



Change Board

26 Mar 2025



Thank you for
listening

Any further comments?

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](#)

Thank you for attending

The next meeting will be on
Wednesday 5 March 2025