Smart Energy Code

This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public and any members may publish the information, subject to copyright.

Stage 03: Modification Report

SECMP0008:

Provision of a DCC Alert for Quarantined Service Requests

SECMP0008 proposes that when an Anomaly Detection Threshold has been breached, the DCC will send a DCC Alert notifying Users that a particular Service Request or Signed Pre-Command is quarantined. This is in addition to the current email notification from the DCC to Users.

SECMP0008 impacts SEC Parties that are/will be DCC Users and who chose to use this additional functionality.

What stage is this document in the process?

01 Initial Modification Report
02 Refinement Process
03 Report Phase
04 Final Modification Report

Proposer:
Scottish Power - Graham J Smith
graham.smith@scottishPower.com
0141 614 2662

Any questions?

Contact:
Samuel Browne
secas@gemserv.com
020 7090 7755

Contents

About this document

This document is the draft Modification Report for SECMP0008. The SEC Panel will consider this report to ensure that due process has been followed and then determine whether or not to issue the Modification Proposal for the Modification Report Consultation. SEC Parties will then be asked to comment on the suitability of this Modification Proposal before the Change Board undertake a vote on whether to recommend its approval to the Authority.

This draft Modification Report has three attachments:

- **Attachment A**: Solution Design Document and Legal Text;
- **Attachment B**: Working Group detailed considerations; and
- **Attachment C**: Modification Report Consultation Response Form.

Administered by Gemserv

8 Fenchurch Place, London EC3M 4AJ

1. Summary

This section provides an overview of SECMP0008. Defined terms and acronyms used in this document are listed in the Glossary (Appendix 1) of this document.

1.1 Why Change?

When a User's Anomaly Detection Threshold (ADT) is exceeded the DCC places all Service Requests (SRs) / Signed Pre-Commands into 'quarantine' and stops them from reaching Devices. The DCC then notifies the User via email that the SRs/Signed Pre-Commands have been quarantined.

If the User does not see the DCC email notifying that SRs/Signed Pre-Commands have been quarantined they may attempt to re-send the SRs/Signed Pre-Commands. This could lead to excessive network traffic and may in turn lead to network availability problems. Equally, having a more proactive alert system will allow Parties to more quickly take action to resolve issues, better manage customer experience and to more easily see where there is a genuine attack on the system.

1.2 Solution

SECMP0008 proposes the creation of three new DCC Alerts. When a specific ADT is exceeded, and the SR/Signed Pre-Command is quarantined by the DCC, Users will be notified using these DCC Alerts via the DCC User Interface. SECMP0008 does not replace the existing DCC email notification of quarantined SRs/ Signed Pre-Commands, but introduces additional DCC Alert functionality.

1.3 Impacts and Costs

SECMP0008 is an optional functionality and Users may choose to adopt it. Testing requirements are set out in section 5 below.

The estimated DCC cost is circa £980,000. The DCC has included provisions for the potential cost of SECMP0008, should it be approved and implemented, into the DCC Charging Statement for Regulatory Year 2017/2018.

1.4 Implementation

The recommended implementation for SECMP0008 approach is 28th June 2018 if the modification is progressed as a Path 3 change. If the Panel believe that Path 2 is more approve for the modification then the implementation approach will be:

- implementation on **28th June 2018 (June 2018 Release)**, if a decision to approve is made by **1st June 2017**; or
- implementation on **1st November 2018 (November 2018 release)**, if a decision to approve is made after 1st June 2017, but before 2nd October 2017.

1.5 Working Group's Views

The Working Group unanimously agree that SECMP0008 should be approved as it better facilitates applicable objectives a) and f) since the Modification allows for increased automation which increases efficiency of dealing with alerts, avoids Users re-sending SRs if they have been previously quarantined and assists Users to detect any system compromise in a timely manner.

2. Why Change?

2.1 Background

In order to help detect anomalous activity and events, Users and the DCC set Anomaly Detection Thresholds (ADTs). These set a level for the number of Service Requests (SRs) / Signed Pre-Commands that can be issued during a certain period or a level of a particular data value within a Signed Pre-Command. Some thresholds are set by the DCC User; other thresholds are set by the DCC.

When a User's ADT is breached the DCC places all SRs/Signed Pre-Commands into 'quarantine' by holding the SRs/Signed Pre-Commands centrally and stopping them reaching Devices (this includes subsequent SRs/Signed Pre-Commands of the same Service Reference Variant sent after the ADT is exceeded). The DCC then notifies the User via email that the SRs/Signed Pre-Commands have been quarantined.

2.2 What is the issue?

Currently, the only way for a User to know the ADT threshold has been breached, and that information has subsequently been quarantined by the DCC, is via a process involving email notifications. If the User does not see or action the DCC's email immediately it is likely the User will attempt to re-send such SRs / Signed Pre-Commands. This could lead to excess network traffic and to network availability problems.

The quarantine process also assumes that DCC Service Users will extract a file of quarantined SRs (from the DCC's SharePoint website) to review. Each DCC User will then assign a specific action per SR before returning the file to the DCC to perform said action(s). In order to properly monitor and manage the DCC emails Users would need a dedicated internal service management function. This likely to increase overheads and complexity within individual businesses.

The DCC emails are a passive mechanism, having a more proactive mechanism will allow Parties to more quickly resolve issues, better manage customer experience and to more easily see where there is a genuine attack on the system.

3. Solution

3.1 Proposed solution

Scottish Power raised SECMP0008 in February 2016. It proposes creating three new DCC Alerts to notify the sender when an ADT (both User and DCC set) is exceeded and the SR/Signed Pre-Command is quarantined by the DCC.

The alerts will also cover those Signed Pre-Commands quarantined as a result of data value ADT (packet inspection). Packet inspection is to be introduced post-DCC live and involves checking values within a Signed Pre-Command payload (the message). If the data value in a particular Signed Pre-Command is outside the permitted range (as agreed by the DCC, DCC Users and the SSC), the Signed Pre-Command will be quarantined.

As with other DCC Alerts, Users will receive these DCC Alerts via the DCC User Interface.

The following three new DCC Alerts are proposed:

- a **'Quarantined Request – Anomaly Detection User Threshold Breach' DCC Alert**, which would be sent when a SR / Signed Pre-Command is quarantined due to a User set threshold;
- a **'Quarantined Request – Anomaly Detection DCC Threshold Breach' DCC Alert**, which would be sent when a SR / Signed Pre-Command is quarantined due to a DCC set threshold; and
- a **'Quarantined Request – Anomaly Detection User Threshold Breach' DCC Alert**, which would be sent when a Signed Pre-Command is quarantined due to failing packet inspection.

Each of the three new DCC Alerts would include the ID of the quarantined SR / Signed Pre-Command as well as an incidence reference. This will enable the User to cross-reference the DCC Alert with the 'out of band' communication received.

For the avoidance of doubt, the existing DCC email notification of quarantined SRs and Signed Pre-Commands, as outlined in the Threshold Anomaly Detection Procedures, will remain unchanged.

The more detailed business requirements and Legal text supporting the SECMP0008 solution can be found in Attachment A – Solution Design Document.

4. Impacts and Costs

The following section sets out the impacts arising from SECMP0008 as identified by the Working Group and SEC Parties.

4.1 Party Impacts

Users who implement SECMP0008 will be required to update their DCC User interface in order to receive the three new DCC Alerts. Whether Users choose to upgrade their systems or not, Users will continue to receive emails if they breach ADTs.

Users (primarily supplier Users) will need to test SECMP0008 as part of a Release. The user testing requirements can be found in section 5.2 and in Attachment A.

Parties have indicated costs of circa £0 - £50K in order to update back end systems to deal with the new alerts.

4.2 Central Costs

4.2.1 DCC

The table below details the cost of delivering the changes and Services required to implement this Modification Proposal:

Implementation costs (excluding VAT)							
Implementation Phase:	Design	Build	Pre-Integration Testing	System Integration Testing	User Testing	Implementation to Live	Total
SECMP0008	*£126,000*	*£252,000*	*£252,000*	*£280,000*	*£20,000*	*£50,000*	**£980,000**

The DCC noted that implementing SECMP0008 at the same time as SECMP0004 and SECMP0011 would result in the following savings:

- a reduction of circa 20% in costs can be assumed for System Integration Testing and User Testing; and
- a reduction of circa 33% in costs can be assumed for Implementation to Live.

The combination of these savings would reduce the overall cost of SECMP0008 to circa **£907,500.**

The DCC has included provisions for the potential cost of SECMP0008, should it be approved and implemented, into the DCC Charging Statement for Regulatory Year 2017/2018.

The complete DCC Impact Assessment undertaken on SECMP0008 is available on the SEC Website via the following link: SECMP0008 DCC Impact Assessment v3.1.

4.2.2 SECAS

The costs to implement this change will be limited to the Code Administrator's time and effort to making the necessary amendments to the SEC, release a new version to SEC Parties, and the publication of it on the SEC Website. This is estimated at approximately 2 Man Days effort, which will be approximately £1200[1].

4.3 Other Potential Impacts

There are no impacts on consumers, greenhouse gas emissions and/or other industry codes.

5. Implementation

5.1 Recommended Implementation approach

When SECMP0008 was first raised was initially thought that the change may have a material impact on the security of systems, and therefore the Panel considered it a Path 2 (Authority-determined) modification. This meant that, following the Change Board vote, the Authority would determine whether SECMP0008 should be implemented.

However, the feedback from the SSC, Working Group and the majority of consultation responses, suggests that SECMP0008 does not have a material impact on the security of systems. In light of this feedback, it is recommended that SECMP0008 should be progressed to a Path 3 modification. This would mean that only the Change Board would determine whether SECMP0008 should be implemented.

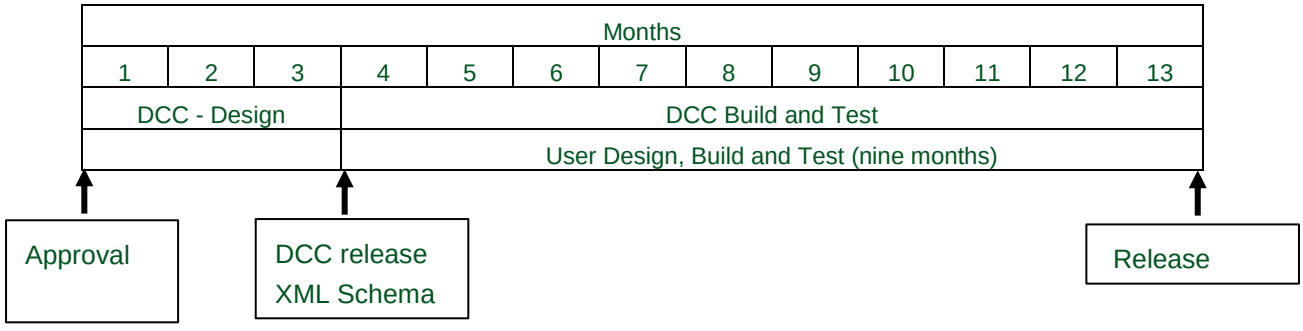
The Working Group noted that SECMP0008 should be implemented as soon as possible following approval.

The Workgroup therefore recommends that if the Modification is progressed as a Path 3 change an implementation date of 28th June 2018.

If the Panel believe that Path 2 is more approve for the Modification, then the implementation approach will be:

- SECMP0008 to be implemented in the **June 2018 Release**, if a decision to approve is made by **1st June 2017**; or
- SECMP0008 to be implemented in the **November 2018 Release,** if a decision to approve is made after 1st June 2017 but before **2rd October 2017**

The DCC have indicated they require 13 months to implement SECMP0008, and that they would need three months from the approval date to build the XML Schema.



[1] Based on a blended rate of £600 per day.

5.2 Testing

5.2.1 DCC Testing

As described in the DCC's Impact Assessment (available on the SEC Website[2]), DCC will carry out Pre-Integration Testing (PIT) and System Integration Testing (SIT) for SECMP0008.

PIT comprises the tests that each Service Provider performs on its respective System changes, prior to the integration of all Service Provider Systems.

Suggested PIT scope would include:

- Production, review and agreement of a design to enable development;
- Low level design production, development, unit test and any rework to achieve PIT complete status;
- Data generation and loading into the Test environment;
- Execution of System Tests through sufficient iterations to enable PIT complete;
- Design, implementation and execution of FAT scripts in accordance with assurance procedures used for Release 1.2; and
- Achieving PIT complete status and subsequent reporting.

SIT is the testing of DCC's Total System, which brings together the component parts of DCC's System (e.g. DSP and CSP Systems) to allow testing of the end-to-end solution by DCC. The SIT activity is done for every DCC System release and incorporates the test and integration of multiple changes.

Additional SIT is recommended by DCC for a modification of this type. It should however be noted that the scope of SIT is likely to be more focused on regression testing to confirm that the changes applied as part of this modification have not had an impact on the wider DCC Total Systems.

Suggested SIT scope would at a high level typically include:

- System Test script and data design;
- Data generation and loading into a co-ordinated System Test environment;
- Execution of System Tests through sufficient iterations to enable SIT complete.

5.2.2 User Testing

The Working Group agreed the following high level requirements for SECMP0008 User Testing:

- Testing should be optional for Users, although a minimum of two Parties should undertake and pass User testing of the SECMP0008 functionality before the new functionality goes live;
- The testing environment that the DCC provides as part of Testing Services will be open to all User Roles and multiple Users within each User Role to ensure that any User wishing to test SECMP0008 is able to do so. This environment should be made available for a minimum of 15 working days.

It is anticipated that the DCC will drive the development of the testing services and documentation that will set out how it will complete the testing of the new functionality within its systems. This may be a form of focus Integration Testing and/or User Entry Process Testing. The testing approach documentation, will form a wider Release implementation document, that will cover SECMP0008 (if approved) and any other approved Modification Proposals that are included alongside or in addition to it.

Attachment A contains supporting legal text covering the requirements for the development of Release implementation documentation and testing approach documentation.

[2] https://www.smartenergycodecompany.co.uk/docs/default-source/modificationfiles/secmp0004_dcc_-impact-assessment-v2-0.pdf?sfvrsn=0

6. Case for Change

This section contains the views of the Proposer and Working Group regarding the modification's benefits and drawbacks against the SEC Objectives.

6.1 Proposers views

The DCC design for its Anomaly Detection Threshold process details that when a SR is quarantined due to an ADT breach, DCC Service Users will be notified of quarantined SRs via an email notification. The process then assumes that DCC Service Users will extract a file of quarantined SRs (from the DCC's SharePoint website) to review. Each DCC User will then assign a specific action per SR before returning the file to the DCC to perform said action(s).

The email notification approach means there will be no SR error response from the DCC to that impacted DCC Service User. There are a number of issues with this approach, including:

- Having to develop and manage additional internal processes to monitor and respond to DCC emails, both in and out of hours, that will also require manual analysis. User' staff monitoring notification emails will need to have the capability to identify quarantined SRs that might be critical and therefore react in a timely and efficient manner. This increased manual activity will require an uplift in resourcing / skills, knowledge and DCC awareness across Users' internal service management functions which will incur additional costs on DCC Service Users.

- The potential for DCC Service User Systems to continue to resend SRs to the DCC whilst complex analysis is being undertaken up to the point at which either:
    - the DCC User System sending the requests times out;
    - the anomaly is identified and mitigations are implemented; or
    - the anomaly is released within the DCC.

  Based on the current anomaly detection solution scenario ''a'' is most likely to occur. This will result in a significant increase in the number of anomalous events which occur within the DCC process, potentially requiring additional complex analysis to associate all events to a common incident.

- Users' service desk agents and out of hours staff will need to be Authorised Responsible Officers. This extends the scope of the security clearance controls and the number of personnel requiring security clearance.

The Proposer believes that SECMP008 will better facilitate applicable objective a) "to facilitate the efficient provision, installation, and operation, as well as interoperability, of Smart Metering Systems at Energy Consumers' premises within Great Britain" and objective f) "to ensure the protection of Data and the security of Data and Systems in the operation of this Code".

The views are summarised in the table below:

Summary of Proposer's view against the SEC Objectives	
SEC Objective	Benefits
a)	• It would allow Users to develop much more intuitive systems that have the ability to monitor and alert at a granular SR level. It would provide for a proactive approach to throttling SR demand where necessary from internal systems – therefore minimising needless threshold breaches, overhead in manual resolution and general system / process inefficiencies. It would allow DCC Users to manage SR forecasts and processes around the ADT effectively. • It reduces the dependency on the use of email, mailboxes, auto-forwarding rules and the need for specific / detailed DCC service knowledge for both in and out of hours support staff. This is essential for DCC Service Users as there is a huge risk that DCC Service Users' internal systems will assume messages have been dropped and thus a DCC Service User will keep resending the original SR to the DCC. There would be no specific need for a significant number of in and out of hours staff to become Authorised Responsible Officers. However, a DCC Service User may develop an "on-call" process for the limited occasions when SRs go into quarantine. Thus only a small number of Authorised Responsible Officers may be required within Users' internal service management teams. • This Modification Proposal would allow DCC Service Users to better deliver their obligations by having a fit for purpose, efficient, and effective process in place for managing quarantined SRs. Provision of a SR error response for quarantined SRs gives DCC Service Users a more responsive level of notification compared to email notifications (which is a significant overhead for DCC Service Users' internal service management functions). It removes the requirement for manual intervention in systems that fall within the scope of DCC Service User systems and necessitate minimal manual intervention.
f)	• The solution is more secure in terms of meeting the SEC security obligations including those specified around the deployment and control of systems within the scope of 'User Systems'. It would allow DCC Users to react to breaches of the ADT in a timely and efficient manner. This Modification Proposal will have a positive impact on the management of quarantined SRs – specifically relevant to the SMIP security requirements. • It is also worth noting that the Transitional Security Expert Group (TSEG) under Transitional Governance has previously agreed with the approach proposed in this Modification Proposal

6.2 Working Group discussions

In general, the Working Group agreed with the views of the proposer (as outlined above) and those provided by Working Group consultation respondents. When considering the benefits and drawbacks of SECMP0008, the Working Group discussed the following:

Automation

The Working Group noted that there is already a process for the DCC notifying Parties of an ADT breach through via email. However, the automation of this process would provide significant benefits in line with SEC Objective (a). They believed that it would increase the speed of dealing with potentially critical issues by decreasing the time necessary to pick up the alert and automate the correlation with other events (e.g. Internal ADT warnings). They also supported the view that automation would allow reduction of costs and overheads of specialised on duty staff who would be expected to deal with the current ADT alert email. Equally there would be a reduction in human error, which is significant given the possible criticality of not dealing correctly with an ADT Alert and the potential impact this could have on customers.

Necessary or backstop?

The Working Group noted that if SR forecasts were accurate enough, Users should never have to receive these DCC Alerts. However, SR forecasting is a complex process made even more difficult by the new Smart Metering environment. Therefore, the additional back-up provided by the proposed DCC Alerts would add benefit. WG members noted that forecasting accurately would be virtually impossible in the case of customer initiated commands, in particular for pre-payment devices. This could potentially lead to quarantined service requests resulting in delays for customers.

The Working Group noted that SECMP0008 benefits SEC Objectives (a) and (f). It was agreed that SECMP0008 is an improvement to the status quo.

Security improvement

In terms of the security improvements, in line with Objective (f), the Working Group all agreed that the automation and quicker response time for SECMP0008 would allow Users to detect potential malicious breaches more quickly and therefore take action to contain these more efficiently. Time could be potentially reduced from days to minutes. They also noted that detecting critical compromises would be more efficient without the added risk of human input/error.

Costs

The Working Group noted the DCC cost for the implementation of the change and, as noted in section 5 of this report, requested the DCC to provide a breakdown of those costs to the Change Board. However, even noting the central implementation costs the group believed there was benefit in implementing this Modification Proposal in the next available release.

6.3 Working Group Consultation responses

There were six responses to the Working Group Consultation (four Large Suppliers and two Networks). All supported the approval of SECMP0008 and agreed with the Group's views on the applicable objectives as noted in section 6.5 (one party did not believe that objective f) was applicable, but agreed with support for objective a)).

Parties noted that changes would be required to interface systems in order to receive and process the new DCC Alerts and that the costs for these changes would range from £0 - £500K depending on size and nature of the organisation. However, all Parties noted that there would be a benefit to their organisation of making these changes which would outweigh the cost of their systems development.

Benefits were highlighted in relation to quicker response times and increased security. The most common suggested benefit was the increase in the response speed and the possible automation, as a result of this modification. These benefits could lead to new ways of using the proposed DCC Alerts that would facilitate the wider Smart Meter Implementation Program (SMIP). However, respondents were unable to quantify these benefits.

Respondents were split on the best governance to progress the modification. Half of the respondents believed that the Modification should continue as a Path 2 Modification as it had an impact on the end to end security model. The other half of respondents believed that this modification is not impacting any existing security controls and has no material impact on security, so should be progressed as a Path 3 Modification.

The full consultation responses, and the Working Groups consideration of them can be found in Attachment B.

6.4 Sub-Committee views

The SSC has been kept informed throughout the refinement of SECMP0008. The SSC re-confirmed at their 31st August 2016 meeting that the benefit of the change outweighed any potential risks, associated with the introduction of the new Alerts. This echoed discussion held at the Transitional Security Expert Group (TSEG). There were no major concerns in relation to SECMP0008 introducing a separate DCC Alerts for each ADT.

The Technical Architecture and Business Architecture Sub-Committee (TABASC) noted that it has no concerns regarding the impacts of SECMP0008 on the Technical and Business Architecture.

6.5 Working Group's views against SEC Objectives

The Working Group (including the Proposer) unanimously agree that SECMP008 better facilities the following General SEC Objectives:

- **(a)** to facilitate the efficient provision, installation, and operation, as well as interoperability, of Smart Metering Systems at Energy Consumers' premises within Great Britain; and
- **(f)** to ensure the protection of Data and the security of Data and Systems in the operation of this Code.

The below table provides the Working Group's rationale:

Summary of Working Group's view against the SEC Objectives		
SEC Objective	Benefits	Drawback
a)	• Allows for increased automation which increases efficiency of dealing with alerts. • The faster response times will help Users avoid re-sending SRs if they have been previously quarantined. This should help reduce network traffic.	None
f)	• Helps detect compromise that could be critical without relying on human input/error. • Allows Users to detect any system compromise in a timely manner, reducing the response time from potentially days to minutes.	None

7. SEC Panel Decisions

The SEC Panel is requested to:

- **AGREE** the modification progression Path;
- **AGREE** to allow the Modification Report to proceed to the Modification Report Consultation;
- **AGREE** the Party Categories that are likely to be affected by the Modification Proposal; and
- **AGREE** that the Modification Report Phase will follow the timetable as set out below:

Modification Progression Timetable	
Activity	Date
Modification Report Consultation	15th March - 5th April 2017 (15 Working Days)
Change Board Vote	19th April 2017
Issued SECMP0004 for Authority Determination	20th April 2017
Implementation (if approved by the Authority)	June 2018 Release (28th June 2018) if approved by the 1st June 2017, or November 2018 Release (1st November 2018) if approved after 1st June 2018, but before 2nd October 2017.

Appendix 1 – Glossary and References

Glossary	
Description	Term
ADT	Anomaly Detection Threshold
BEIS	Department for Business Energy and Industrial Strategy
DCC	Data and Communications Company
SSC	Security Sub-Committee
SR	Service Request

References

The following table contains any useful links relevant to this change or referenced in this document.

Links and References	
Description	Link
SECMP0008 – Modification Proposal Form v1.0	https://www.smartenergycodecompany.co.uk/docs/default-source/modificationfiles/secmp0008/secmp0008---modification-proposal-form.pdf?sfvrsn=0
SECMP0008 – Initial Modification Report v1.0	https://www.smartenergycodecompany.co.uk/docs/default-source/modificationfiles/secmp0008/secmp0008---initial-modification-report-1-0.pdf?sfvrsn=0
SECMP0008 – WG Consultation v1.0	https://www.smartenergycodecompany.co.uk/docs/default-source/modificationfiles/secmp0008---working-group-consultation.zip?sfvrsn=0
SECMP0008 – DCC Impact Assessment v3.1	https://www.smartenergycodecompany.co.uk/docs/default-source/modificationfiles/secmp0008_dcc_-impact-assessment-v3-1.docx?sfvrsn=0
SECMP0004 – SECAS Modification Register	https://www.smartenergycodecompany.co.uk/modifications/modification/SECMP-4
SECMP0011 – SECAS Modification Register	https://www.smartenergycodecompany.co.uk/modifications/modification/SECMP-11