Proposed Change: SECMP0008 - Provision of DCC Alert (formerly Service Request Error Response) for Quarantined Service Requests

Context and Business Requirements

This section provides the context to this Modification Proposal and summarises the key business requirements for it, as currently clarified and refined by the Working Group.

Context

Sections G6.2 and G6.6 of the SEC require DCC Users and the DCC respectively to set specific ADTs. The types of the ADTs that DCC Users and the DCC are required to set are explained in Table 1.

Table 1.DCC User and DCC ADT

DCC Users ADT	DCC ADT
Total number of Critical Commands relating to each Service Reference Variant. Note that this equates to the DCC receiving Signed Pre-commands from the DCC User.	Total number of Critical Commands relating to each Service Reference Variant. Note that this equates to the DCC receiving Signed Pre-commands from DCC Users.
Total number of Service Requests relating to each Service Reference Variant where Service Responses relating to these Service Requests contain Encrypted Data.	Total number of Service Requests relating to each Service Reference Variant where Service Responses relating to these Service Requests contain Encrypted Data.
Any other ADT relating to a Service Reference Variant defined by the DCC User.	A data value within each Signed Pre-Command relating to a Service Reference Variant as agreed by the Security Sub-Committee. Note that this 'packet inspection' of data in the payload of communications is not being implemented at go-live and so is not yet reflected in the Threshold Anomaly Detection Procedures. These changes are within CR062a.
	Any other ADT relating to a Service Request Variant defined by the DCC.

The SEC then requires the DCC to put in place processes to detect whether each of the ADTs set by the DCC User or DCC has been exceeded. Except for Warning Thresholds, communications that exceed the relevant ADT have to be put in quarantine by the DCC. This means they are held in central DCC systems are not sent to Devices.

The Threshold Anomaly Detection Procedures further detail how:

a) A DCC User should notify the DCC of each of the ADT set by the DCC User;
b) The DCC should notify a DCC User if the number of Service Requests or Signed Pre-Commands have exceeded one of the User's Warning Thresholds;
c) The DCC should notify a DCC User if the number of Service Requests or Signed Pre-Command have exceeded one of the DCC ADT or User ADT;
d) The DCC should notify a DCC User if, in relation to a DCC ADT, it needs to take action in relation to quarantined Service Requests or Signed Pre-Commands; and

e) A DCC User should notify the DCC how each of the quarantined Service Requests or Signed Pre-Commands should be processed, specifically whether each should be deleted or should be sent to a Device.

In the Threshold Anomaly Detection Procedures, the DCC specifies that it would communicate with DCC Users for these purposes via an 'out of band' means. For the avoidance of doubt 'out of band' in this context means via an email notification, and not via the DCC User Interface.

SECMP0008 requests that in addition to notifying a DCC User by email of when an ADT is exceeded, the DCC also notifies the DCC User via the DCC User Interface of each Service Request or Signed Pre-Command that is quarantined as a result.

Packet Inspection

Note that the DCC will not apply the data value ADT ('packet inspection') until CR062a has been implemented, which will be after go-live. The exact implementation date is currently being discussed. As such the relevant provisions in the Threshold Anomaly Detection Procedures setting out how the DCC would manage the process of notifying each DCC User each time a Signed Pre-Command with a data value above or below the ADT has been put in quarantine have not been drafted.

However, the mechanism that is proposed as part of this Modification Proposal (to notify the DCC User via the DCC User Interface each time a Service Request or Signed Pre-Command has been quarantined) would also apply to each quarantined Signed Pre-Command containing a data value that is higher or lower than the set ADT related to packet inspection. Therefore, this Solution Document covers the amendments that would need to be made to the relevant parts of the regulatory framework (except for the Threshold Anomaly Detection Procedures) to implement this Modification Proposal for all types of ADTs, including the data value ADT.

Testing

The Working Group collectively agreed that the DCC should provide Testing Services to support the implementation of this Modification Proposal.

DCC should also be required to undertake testing of the DCC Total Systems to support the implementation of this Modification Proposal.

The Working Group also agreed that testing of SECMP0008 should be optional for Users, although it is expected that at least two large suppliers will take part in testing.

Per additional SEC requirements designated by the Secretary of State, which came into effect in February 2017 (issued for consultation in 2016), this document provides high level business requirements for Testing Services. This is to assist the DCC is preparation of a revised DCC Impact Assessment that includes the cost of testing of SECMP0008. In line with the new SEC requirements, we ask the DCC to prepare an analysis of any required testing of the DCC Total System, and the DCC view on the scope, phases, timetable and testing participants of testing for SECMP0008.

Business Requirements

1. The DCC would create three new 'Anomaly Detection Quarantine' DCC Alerts.
2. The DCC would send a 'Quarantined Request – Anomaly Detection User Threshold Breach' DCC Alert via the DCC User Interface to notify the sender of a Service Request each time the Service Request or Signed Pre-Command is quarantined by the DCC because any of the User's ADT has been exceeded.
3. The DCC would send a 'Quarantined Request – Anomaly Detection DCC Threshold Breach' DCC Alert via the DCC User Interface to notify the sender of a Service Request sender each time the Service Request or Signed

Pre-Command is quarantined by the DCC because any of the DCC's ADT (except for the data value ADT) has been exceeded.

4. The DCC would send a 'Quarantined Request – Anomaly Detection Attribute Limits Breach' DCC Alert via the DCC User Interface to notify the sender of a Service Request. Each time a Signed Pre-Command corresponding to the Service Request is sent it is quarantined by the DCC because a data value parameter is above or below the ADT.
5. Each of the three DCC Alerts would need to include the following data items to enable the User to cross-reference the DCC Alert with the 'out of band' communication received:
    a. RequestID of the quarantined Service Reference Variant;
    b. Quarantine Event Reference, which is the associated quarantine incident reference
6. The 'Anomaly Detection Threshold Quarantine Alert' would be processed in accordance with DUIS requirements for processing DCC Alerts.

Business Requirements relating to testing

7. The DCC will provide Testing Services to support the implementation of SECMP0008 to assess the interoperability of User Systems with DCC Systems. Examples of SECMP0008 User testing scenarios are provided in Appendix A. The Proposed changes to Section D10, will provide supporting SEC provisions for the expected testing information and documentation, subsequently provided below.
8. The DCC will provide an analysis including supporting assumptions and rationale, of any testing required to the DCC Total System.
9. The DCC will prepare a report setting out the scope, phases, timetable, testing participants, any assumptions and rationale in relation to SECMP0008 testing.
10. 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, depending on the impact of the change. The DCC must provide the costs and assumptions associated with providing this testing service, including whether the testing costs are based on a set number of users utilising the testing service, i.e. up to 10 Users, noting that at least two large Suppliers may test the functionality. This is to ensure it operates correctly before it is put into the End-to-End and Production environments.
11. The interfaces in scope of Testing Services will include the DCC User Interface.
12. The objectives of testing as part of Testing Services will be to ensure that an Anomaly Detection Threshold Breach DCC Alert is returned when a Service Request/Signed Pre-Command breaches an ADT, and the DCC Alert that is returned corresponds to the ADT.
13. The acceptance criteria for testing as part of Testing Services will be: the DCC sent the DCC Alert corresponding to the ADT that has been breached, Users receives the DCC Alerts corresponding to the ADT that has been breached.

Legal Text

This section details the required changes to the regulatory framework that are proposed to implement the requirements for this Modification Proposal. Where changes to the regulatory framework are made, they are shown by way of redlining relevant sections of the SEC and SEC Subsidiary Documents. For clarity, deletion is shown by strike through.

All the tracked SEC changes have been based against the content in Smart Energy Code (version 5.4) Note the changes to sections A and G6 are to clarify that, as per the Threshold Anomaly Detection Procedures, ADTs are set against each Service Reference Variant.

SEC Section A – Definitions

Service Reference Variant means a reference assigned to a Service Request in accordance with the DCC User Interface Specification

SEC Release means any approved Modification Proposal to be implemented in the SEC and/or SEC Subsidiary Document(s) that requires Release Management by the DCC or Users as set out in Section D10.7, and is consequently undertaken in accordance with the Panel Release Management Policy

Release Implementation Document has the mean given to that expression in Section D10.11

SEC Section D – Implementation

D10.10 To support the Panel in discharging the activities set out in Section D10.2, the Panel shall develop and publish a "Release Implementation Document" for each SEC Release in accordance with the Panel Release Management Policy. The DCC shall be required to undertake the implementation and testing activities as set out in the relevant Release Implementation Document once approved by the Panel.

D10.11 The Panel shall ensure that each Release Implementation Document:

(a) Defines the content of a SEC Release;

(b) Defines the timescales associated with implementing the content of a SEC Release, including timescales for the commencement and completion of DCC and User testing phases;

(c) Defines the testing that will be undertaken by the DCC for the SEC Release;

(i) To help define the DCC testing, the DCC, on request of the Panel, shall produce a document setting out the testing approach to meet requirements of each approved Modification Proposal within each SEC Release;

(d) Defines the required level of User testing and how the DCC shall support Users to test the changes that make up each SEC Release; and

(e) Defines the SEC Release acceptance criteria that shall be agreed by the Panel in accordance with the Release Management Policy.

D10.12 The Panel shall approve the Release Implementation Document and any subsequent amendments. The Release Implementation Document cannot be further updated after the periods of notice defined in the Panel Release Management Policy (in accordance with Section D10.8(d)).

D10.13 Any Party that wishes to appeal the Panel approval of the Release Implementation Document, may do so within 10 Working Days following the publication of the decision to approve. Any appeal referred to the Authority, must specify the reasons for the appeal. The Authority shall determine what action to take with the

appeal (which determination shall, without prejudice to section 173 of the Energy Act 2004, be final and binding for the purposes of this Code).

SEC Section G6 – Anomaly Detection Thresholds: Obligations on the DCC and Users

G6.3 Each User which is an Eligible User in relation to any one or more individual Services listed in the DCC User Interface Services Schedule:

(a) shall set Anomaly Detection Thresholds in respect of:

(i) the total number of Critical Commands relating to each such Service Reference Variant; and

(ii) the total number of Service Requests relating to each such Service Reference Variant in respect of which there are Service Responses containing Data of a type which is Encrypted in accordance with the GB Companion Specification; and

(iii) may, at its discretion, set other Anomaly Detection Thresholds.

G6.6 The DCC:

(a) shall, for each individual Service Reference Variant listed in the DCC User Interface Services Schedule, set an Anomaly Detection Threshold in respect of:

(i) the total number of Critical Commands relating to that Service Reference Variant; and

(ii) the total number of Service Requests relating to that Service Reference Variant in respect of which there are Service Responses containing Data of a type which is Encrypted in accordance with the GB Companion Specification;

(b) shall set an Anomaly Detection Threshold in respect of a data value that has been agreed with the Security Sub-Committee within each ~~type of~~ Signed Pre-Command relating to that Service Reference Variant; and

(c) may, at its discretion, set other Anomaly Detection Thresholds.

SEC Appendix AA - Threshold Anomaly Detection Procedures (Version AA 1.0 (draft))

User and DCC Responsibilities: User Set Anomaly Detection Threshold

4.4A In respect of each quarantined communication, the DCC shall also send a DCC Alert to the User who sent the communication to inform them that the communication has been quarantined.

User and DCC Responsibilities: DCC Set Anomaly Detection Threshold

4.11 Pursuant to Section G6.6. of the Code, the DCC shall set ADTs. Where a DCC set ADT has been exceeded, the DCC shall:

a) quarantine the communication(s) that have exceeded the ADT;

b) raise and Incident in accordance with the Incident Management Policy; ~~and~~

c) determine the reasons for the Incident and take appropriate remedial action~~.~~; and

d) in respect of each quarantined communication, send a DCC Alert to the User who sent the communication to inform them that the communication has been quarantined.

SEC Appendix AD - DCC User Interface Specification (Version AD 1.0)

3.6.3.4 DCC Alert Codes

To Table 35 add:

DCC Alert Code	Alert Name	Event	Trigger	DCC Alert Recipient

N46	Quarantined Request – Anomaly Detection User Threshold Breach	An Anomaly Detection User-specific volume threshold has been exceeded	Request quarantined, because an Anomaly Detection User-specific volume threshold has been exceeded	Service Request / Signed Pre-Command sender
N47	Quarantined Request – Anomaly Detection DCC Threshold Breach	An Anomaly Detection DCC system-wide volume threshold has been exceeded	Request quarantined, because an Anomaly Detection DCC system-wide volume threshold has been exceeded	Service Request / Signed Pre-Command sender
N48	Quarantined Request – Anomaly Detection Attribute Limits Breach	An Anomaly Detection Attribute Limit has been breached	Request quarantined, because an Anomaly Detection Attribute Limit has been breached	Service Request / Signed Pre-Command sender

3.6.4 Relationship between DCC Alert Codes and Response Codes

To Table 36 add:

DCC Alert Code	Response Code
N46	I0
N47	I0
N48	I0

3.9.1 Specific Data Items in the DCC Alert Message

To Table 249 add:

DCC Alert Format / Data Item	Description / Allowable values	Type	Mandatory for Alert Codes	Default	Units
ADUserThresholdBreach	Request quarantined, because an Anomaly Detection Userspecific volume threshold has been exceeded	sr:ADBreach (see ADBreach Data Items Definition	N46: Yes Otherwise: N/A	None	N/A
ADDCCThresholdBreach	Request quarantined, because an Anomaly Detection DCC system-wide volume threshold has been exceeded	sr:ADBreach (see ADBreach Data Items Definition)	N47: Yes Otherwise: N/A	None	N/A
ADAttributeLimitsBreach	Request quarantined, because an Anomaly Detection Attribute Limit has been breached	sr:ADBreach (see ADBreach Data Items Definition)	N48: Yes Otherwise: N/A	None	N/A

3.9.13 AD Breach

3.9.13.1 Specific Data Items for this DCC Alert

ADBreach Data Items Definition

DCC Alert Format / Data Item	Description / Allowable values	Type	Mandatory	Default	Units
RequestID	Request ID of the quarantined Service Reference Variant	sr:RequestIDType (see Annex 17)	Yes	None	N/A
QuarantineEventRef	Quarantine event reference generated by the DCC Data Systems for a particular instance of an Anomaly Detection quarantine threshold / attribute limit being exceeded. Note this is not an Incident reference.	Restriction of xs:integer (totalDigits = 20)	Yes	None	N/A

Table 270 : ADBreach (sr:ADBreach) data items

Appendix A - Examples of SECMP0008 - Inclusion of Device Serial Number data item in the Smart Metering Inventory - User Testing scenarios.

These test scenarios will form part of the Release Implementation Document per the proposed revisions to SEC Section D10 as set out above.
The format of the test scenarios provided below are based on the format contained within SEC Appendix R; Common Test Scenarios Document.

Steps	Description	Objective	Actions	Acceptance Criteria
DCC User Interface Testing				
1	N46 Quarantine	• Users receive DCC Alert N46 when breaching User Threshold • Ascertain no impact otherwise	• DCC set User ADT to (n) for SR[X] • Users send (n+1) SR[X]	• Users receive DCC Alert N46 for any SR[X] ≥ User Threshold (n) • Users do not receive DCC Alert N46 for SR[X] < User Threshold (n)
2	N47 Quarantine	• Users receive DCC Alert N47 when breaching DCC Threshold • Ascertain no impact otherwise	• DCC set DCC ADT to (n) for SR[X] • Users send (n+1) SR[X]	• Users receive DCC Alert N47 for any SR[X] ≥ DCC threshold (n) • Users do not receive DCC Alert N47 for SR[X] < DCC Threshold (n)
3	N48 Quarantine	• Users receive DCC Alert N48 when breaching Anomaly Detection Attribute Limits (packet inspection) • Ascertain no impact otherwise	• DCC set DCC Anomaly Detection Attribute Limits for SR[X] • Users send SR[X] where content exceeds DCC defined values	• Users receive DCC Alert N48 for any SR[X] exceeding Anomaly Detection Attribute Limits • Users DCC Alert N48 for any SR[X] within Anomaly Detection Attribute Limits

Appendix B – Acronyms

This section explains the acronyms used throughout this document. Definitions used in this document are consistent with those in the SEC and SEC Subsidiary Documents.

Acronym	Definition
ADT	Anomaly Detection Threshold
DCC	Data and Communications Company
DUIS	DCC User Interface Specification
SEC	Smart Energy Code
SSI	Self-Service Interface