Proposed Change: SECMP0008 - Provision of an additional DCC Alert (formerly 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.

Business Requirements

1. The DCC would create three new 'Anomaly Detection Quarantine' DCC Alerts.
2. The DCC would send an 'Anomaly Detection Quarantine' 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 an 'Anomaly Detection Quarantine' 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 an 'Anomaly Detection Quarantine' 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 it sent 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 Request Variant;
    b. Quarantine Event Reference, which is the incident reference
6. The 'Anomaly Detection Threshold Quarantine Alert' would be processed in accordance with DUIS requirements for processing DCC Alerts.
7. Any testing requirements for SECMP0008 would be driven by the Panel Release Management Policy. In line with the current SEC drafting, it is anticipated that any testing requirements would be developed and approved by the Panel following SECMP0008 approval.

Legal Instructions

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.

Smart Energy Code (version published by DECC in December 2015)
Note the changes to sections A and G 6 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 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 published by the DCC in January 2016)

User and DCC Responsibilities: User Quarantine Threshold
4.4. In respect of each quarantined communication, the DCC shall also send a 'User Anomaly Detection Threshold Quarantine DCC Alert' to the User who sent the communication informing them that the communication has been quarantined.

User and DCC Responsibilities: DCC Set Quarantine Threshold
4.11 Pursuant with Section G6.6. of the Code, the DCC shall set ADTs and, were 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 actions.; and
d) in respect of each quarantined communication, send a 'DCC Anomaly Detection Threshold Quarantine DCC Alert' to the User who sent the communication informing them that the communication has been quarantined. Subsequent information

User and DCC Responsibilities: GBCS Payload Quarantine Threshold
[To be updated following the implementation of CR62a]

Appendix A Definitions
'User Anomaly Detection Threshold Quarantine DCC Alert' means a DCC Alert generated for the purpose of notifying DCC Users that a communication has been quarantined because any of the User set ADT has been exceeded

'DCC Anomaly Detection Threshold Quarantine Alert' means a DCC Alert generated for the purpose of notifying DCC Users that a communication has been quarantined because any of the DCC set ADT (except for the GBCS Payload ADT) has been exceeded

'Data Value Anomaly Detection Threshold Quarantine Alert' means a DCC Alert generated for the purpose of notifying DCC Users that a communication has been quarantined because a data value is above or below the set ADT

SEC Appendix AD - DCC User Interface Specification (version 0.8.2.1 published by the DCC on 29 March 2016)

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 exeeded	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

Table 249 and related tables will require updating. They will be updated by the DCC following the detailed design and implementation stages.

Table 249

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

3.9.13.1 Specific Data Items for this DCC Alert

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
[TBC]	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

The specific information for this DCC Alert is as follows:

<DCCAlertMessage>

```
<DCCAlertCode>N46</DCCAlertCode>
<DCCAlert>
 <QuarantinedRequest>
  <ADUserThresholdBreach>
        <RequestID>11-22-33-44-55-66-77-88:99-00-AA-BB-CC-DD-EE-FF:50</RequestID>
        <QuarantineEventRef>123</QuarantineEventRef>
  </ADUserThresholdBreach>
  </QuarantinedRequest>
 </DCCAlert>
</DCCAlertMessage>
```

Appendix – 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