

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.

SECMP0008 'Provision of an additional DCC Alert (formerly Error Response) for Quarantined Service Requests'

1st April 2016

Meeting 1 Minutes

Attendees:

Working Group 2 Members	Organisation
Paul Saker (SECMP0004 Proposer)	EDF Energy
Graham Smith (SECMP0008 Proposer) (teleconference)	Scottish Power Energy
Jane Franklin	Lowribeck
Sam Charlton	EON
Andy Knowles (teleconference)	Utilita Energy
Emslie Law	SSE

Representing	Other attendees
DCC	Stuart Scott
	Adam Pearce
SECAS	Jill Ashby (Chair)
	Ian Swanson (Technical Support)
	David Barber (Modifications Lead)
	Sebastian Rattansen (Meeting Secretary)
	Sam Browne (Modifications Analyst)

Apologies:

Working Group 1 Members	Organisation
James Goldsack	DECC

SECMP0008 – Provision of an additional DCC Alert (formerly Error Response) for Quarantined Service Requests

- **Overview**

The Proposer presented a brief overview of the Modification Proposal (Mod), which seeks a new mechanism to give DCC Users visibility of quarantined Service Requests (SRs) following a breach of the DCC's and/or the individual DCC Service User's Anomaly Detection Threshold (ADT).

- **Working Group consideration of Modification Proposal**

This Mod as proposed would add a DCC Alert (rather than an SR error response: a revision to the Mod agreed by the Proposer at the WG) following discussions set out below.

Where an SR becomes quarantined due to a Threshold Anomaly Detection breach, in addition to the current email response outlining this error, adding this alert would act as a second level of defence that allows the DCC User to control the level of requests that might be sent as re-tries and improve response time.

Below is a summary of the main topics discussed:

3.2.1 Clarification of the correct terminology. This requirement should be aimed at a DCC Alert rather than SR response

The Working Group agreed to this clarification and that it should be reflected as such in the Mod title and when describing the proposed modification solution going forwards. The Proposer agreed amendment to the title of Modification Proposal to more accurately reflect the proposed solution as an out of bound communication, consistent with the intent of the email notice.

3.2.2 Initial refinement of Mod scope

The DCC raised a concern regarding whether the intent of this Mod was the potential for this mechanism replacing the existing one. It was clarified that this Mod would not replace the current method but run in parallel.

The rationale for this is that a DCC Alert provides for earlier intervention by a DCC User through an automated signal that attention is required. Running this in parallel will facilitate DCC Users to define their own level of business response to the quarantine event, relevant to their business solution.

3.2.3 Transitional Security Expert Group (TSEG) change consideration of payload inspection

The WG noted that the consideration of any requirements for payload inspection anomalies may need to be considered and this should be monitored by the Mod and/or TSEG.

3.2.4 DCC concern about how much information should be provided in the DCC Alert response

The DCC highlighted a concern where they would be reluctant to re-transcribe the whole SR. The WG agreed that the response should only contain the SR ID and the code error, and that it would be issued via an alert rather than a response. The alert is intended to be supportive of the existing mechanism and to aid the effective resolution of the matter via the existing planned processes as set out in the Threshold Anomaly Detection Procedure (TADP).

It was also agreed that there should be consideration of three DCC Alert responses to cover where the User ADT, the DCC ADT and any other inspection threshold is breached, to aid investigation of what has prompted the quarantining of the SRs.

3.2.5 Processing the release of SRs requests from quarantine

The WG suggested, as noted above that the new DCC Alert would not change or replace any existing process in how the quarantined SR(s) are subsequently released.

3.2.6 The DCC suggested that the SSC may have more input

It was noted that introduction of a DCC alert would need consultation with the Security Sub-Committee (SSC) and possibly Transition Security Expert Group (TSEG). The WG were keen to ensure that the underlying intent of this Mod is communicated to these governance bodies such that the objective of the Mod (to enable DCC Users to react more efficiently to the potential issue) is not unduly diluted. The WG view was that the Mod, as clarified, does not pose any significant additional risk as the DCC Alert mechanism serves as a form of out of bound communication. However, the SSC/TSEG input will be an early critical dependency on the requirements definition.

It was agreed that the SSC would be asked to make sure that the approach agreed does not prompt concerns, and does not cause any issues relating to the Security Architecture (noting that the approach of a minimal detail DCC Alert could serve to mitigate any such concerns).

- **Business Requirements**

Below are the Business Requirements that have been agreed for this Modification Proposal discussed at the first WG2 meeting:

Business Requirement	WG Refinement
SECMP0008 'Provision of an additional DCC Alert (formerly Error Response) for Quarantined Service Requests'	
Retain existing mechanisms and augment them with more User friendly means to signal an issue	Email notice to be retained to enable routing to Sharepoint to derive details of the SRs affected
Create an additional Alert (to existing email based mechanisms) notifying Service Request sender that a SR has been quarantined. The User then uses existing planned processes as defined in the TADP to check the related incident.	- Update to DCC User Interface Specification (DUIS) DCC Alert Definition (3.6) and uplift Schema. - TADP document (to make reference to the additional DCC Alert)
DCC alerts communication	- DCC to generate DCC Alert reports via DUIS - This will be governed by an update to the TADP document - Security implications will be taken into account
Content of the DCC Alert	- The DCC Alert should contain: - Service Request ID - DCC Alert Code - This will be governed by an update to DUIS (3.6 - Device Alerts and DCC Alerts). - Security implications will be taken into account
ADT instances coverage under this Mod	The new Alert should cover all instances relating to Anomaly Detection Threshold.

Business Requirement	WG Refinement
	- This will be governed by an update to DUIS (3.6 - Device Alerts and DCC Alerts) - Security implications will be taken into account
Implications on other anomaly detection mechanisms	Payload detection techniques may be impacted, and the Alert will follow the format identified in the DCC alert content above
Handling of quarantined SRs following a DCC Alert	DCC Users will engage with the existing solution design to investigate the underlying quarantine issue. The new DCC Alert is intended only as a mechanism for 'early warning' of a quarantine event that does not supersede the 'out of bound' communication of the means for the DCC User to obtain further information as to the quarantined SRs.

Table 3: Outline Business Requirements for SECMP0008

- Decisions and next steps**

1.

The Chair proposed that SECAS would draft business requirements for SECMP0008 and that DCC could use them to develop the DCC's Preliminary Assessment (PA). These business requirements are described in section 3.3.

The business requirements developed by the WG will allow DCC to begin a PA for SECMP0008, conditional upon TSEG/SSC feedback. With all WG members agreeing on the outlined solution of SECMP0008 no optionality is being discussed for this Mod. DCC's PA for SECMP0008 will include costs for creating an additional Alert (to existing email based mechanisms) notifying the relevant DCC User that an SR has been quarantined.

The WG agreed that SSC input should be sought on the Mod (see section 3.2.6). It was also noted that any future technical drafting will need to be presented to the Technical Sub-Committee (TSC). DCC will, however, begin their PA after receiving business requirements from the WG.

The WG agreed to reconvene in a months' time.

ACTION WG2_01_04: SECAS to arrange next Working Group meeting for May 2016.