# SEC Modification Proposal, SECMP0109

## DCC CR 1366, ADT and Exit Quarantine File Delivery Mechanism

### DCC Preliminary Impact Assessment (Updated)

| | |
|---|---|
| **Version:** | **1.42** |
| **Date:** | **21st July 2021** |
| **Author:** | **DCC** |
| **Classification:** | **DCC PUBLIC** |

# Contents

# 1 Executive Summary

The Change Board are asked to approve the following:

- Total cost to implement SECMP0109 of £0 (nil).
- The implementation of the Modification as part of the February 2022 SEC Release

**Problem Statement**

The Smart Energy Code (SEC) details that Anomaly Detection Threshold (ADT) and Exit Quarantine files can only be sent via email, which prevents alternative methods of delivery being used. The current arrangements mean that emails are the single means of sending these files.

The DCC believes there are more secure methods available to send these files. The DCC also believes that using email to provide ADT Files and subsequent updates is not secure, and that there are potential scenarios where this process could result in a breach of Security, either by malicious activity or human error. If the ADT and Exit Quarantine files are not securely delivered there is potential for unauthorised persons to be able to access private data. If these data breaches occur, it could undermine the security and commercial image of DCC's business processes.

**Solution**

The Modification proposes that Service Users send the Anomaly Detection Threshold (ADT) files and Exit Quarantine files to DCC via the DCC's preferred secure delivery method, which currently is SharePoint. Changes will be made to the Self Service Interface (SSI) to facilitate this, but no changes to SEC Party systems will be required.

The SEC Party shall submit their files via their own SEC Party SharePoint site, onto a designated named folder. This is currently the preferred secure delivery method.

# 2 Introduction

## 2.1 Document Purpose

The purpose of this DCC Preliminary Impact Assessment (PIA) is to provide the relevant Working Group with the information requested in accordance with SEC Section D6.9 and D6.10.

## 2.2 Previous Information Provided by DCC

The Business Proposer for this Modification is Christopher de Asha of the DCC.

A previous version of this PIA was requested in May 2020, and published in September 2020. However the potential solution was deemed not fit for purpose by the DCC, and a changed solution with the associated new PIA was requested in May 2021.

## 2.3 Modification Description

The Smart Energy Code (SEC) details that Anomaly Detection Threshold (ADT) and Exit Quarantine files can only be sent via email, which prevents alternative methods of delivery being used. Users are obligated to do this. For example, in SEC Appendix AA Section 3.4, 4.7, 4.13 and 6.1 it states, “Each User shall investigate and resolve the ADT exceeded event. Each User shall provide an email to the Service Desk indicating the action to be taken on each of the quarantined communications”. The current arrangements mean that emails are the single means of sending ADT and Exit Quarantine files.

The DCC believes there are more secure methods available to send these files. The ADT and Exit Quarantine files are data records that must be securely delivered, as they contain information private to both a User and the DCC. Failure to deliver this information securely would be a classed as a data breach. Additionally, ADTs provide protection to the smart metering network by specifying the maximum number of Service Requests forecasted, which in turn ensures there are no unexpected or malicious surges or reductions in power on the National Grid from an individual Service User. This aligns with the DCC’s Global ADT process.

The DCC also believes that using email to provide ADT Files and subsequent updates is not secure, and that there are potential scenarios where this process could result in a breach of Security, either by malicious activity or human error. If the ADT and Exit Quarantine files are not securely delivered there is potential for unauthorised persons to be able to access confidential data. If these data breaches occur, it could undermine the security and commercial image of DCC’s business processes.

## 2.4 Requirements

The requirements for this modification have been developed by the Working Group during the Refinement phase. The impact on DCC has been assessed against the Business Requirements, and the DCC are suggesting a change to the SEC text associated with business requirement 1 as detailed below.

Business Requirement 1

**The wording in the SEC needs to also be amended to allow for the new delivery method of the files and for any prospective moves of responsibility within the DCC of ADT and therefore should not name one specified team.**

Current:

“Each User shall investigate and resolve the ADT exceeded event. Each User shall provide an email to the Service Desk indicating the action to be taken on each of the quarantined communications."

The DCC propose:

"Each User shall investigate and resolve the ADT exceeded event. Each User shall provide a submission to the DCC via its secure delivery method of choice to the DCC indicating the action to be taken on each of the quarantined communications."

Business Requirement 2

*Replace the main delivery method of ADT and Exit Quarantine files of emails with the a more secure method.*

For this requirement, it should provide the most simple and cost-effective means of changing the email method of delivering ADT and Quarantine Communication Action Files (QCAF) with the DCC’s secure delivery method of choice.

Business Requirement 3

*Retain the email delivery method for sending ADT and Quarantine Communication Action Files as an alternative method if the primary method is unavailable or in a disaster recovery situation.*

Having reviewed the availability of the current primary secure delivery method, DCC do not believe that the additional complexity and expense of an alternative method is required.

Business Requirement 4

The DCC will communicate preferred delivery methods in the ADT User Guide, this will also be communicated via Monthly Customer Ops forum and mass business communications.

Any changes to these methods will be communicated in advance to give notice to customers and will be communicated via the above channels.

Based on the discussions at the Working Group and the Business Requirements as set out in the Business Requirements Document, DCC assume the requirements for SECMP0109 to be **STABLE**.

# 3 Impact on DCC's Systems, Processes and People

This section describes the impact of SECMP0109 on DCC's Services and Interfaces that impact Users and/or Parties.

## 3.1 Business Requirement 1

For Business Requirement 1, this will require the amendment to the SEC text in Appendix AA Sections 2.2, 3.4, 4.7, 4.13 & 6.1, removing email for the delivery method, thus allowing business requirements 2, 3 and 4.

## 3.2 Business Requirement 2

For Business Requirement 2, the remaining sections of this PIA cover the DCC System impacts and any costs of the proposed secure file mechanism.

## 3.3 Business Requirement 3

DCC propose to remove all forms of the current methods and processes used in support of any email file delivery mechanism.

## 3.4 Business Requirement 4

DCC propose to detail the secure delivery method into the current ADT User Guide and will communicate this to all stakeholders via business comms and monthly Ops forums. This would require a change to Appendix AA section 2.2. There are no DCC System Impacts or implementation costs associated with this.

## 3.5 Description of Solution

In order to provide an email-free mechanism to share the ADT and Quarantine Communication Action Files for the Service Users, DCC proposes the following changes.

### 3.5.1 Updates to ADT Files Processing

Currently the Service Users send the Anomaly Detection Threshold (ADT) files to DCC via email. Prior to sending the ADT files, they are required to create a Service Management Service Request (SMSR) using the Service Catalogue Interface of SSI and obtain a reference number for use in submission of the ADT files. The reference number is included as the subject of the email is used to send the ADT files to DCC.

The DCC propose that the above stays the same except for text in red, which will be replaced by the DCC's secure delivery method.

The SEC Party shall submit their files via their own SEC Party SharePoint site, onto a designated named folder. This is currently the preferred delivery method.

### 3.5.2 Updates to Quarantine Exit Files Processing

In situations where a number of Service Requests from a Service User are quarantined by the DCC Data Systems, DCC will raise a Service Management Incident and notify the Service Users. The Service Users download the Quarantined Communications Reports (QCR) file from the SSI and review it. After their review, the Service Users send a Quarantine Communications Action File (QCAF), which

specifies the required actions needed for each quarantined Service Requests. The QCAF helps a Service User to release quarantined SRVs. It is a signed CSV file containing SRV identifiers and an action to either release or delete.

Currently, the QCAF files are sent to DCC via email. The existing process requires the Service Users to also update the corresponding Service Management Incident in SSI using the Update Service Management Incident interface. The Service Centre then take the file and upload to SSI to action the SRVs.

The DCC propose that the above stays the same except for text in red, which will be replaced by the DCC's secure delivery method.

Currently the SSI does not have a Service Catalogue Request for submitting a QCAF and this would have to be implemented by an internal DCC change outside of this Modification. The SEC Party shall submit their files via their own SEC Party SharePoint site, onto a designated named folder. This is currently the preferred delivery method.

### 3.5.3 Information Security Considerations

In the case of both the ADT and QCAF files, the files received from the SEC Parties will be subject to the same method as other secure data which is stored and delivered via SEC Party SharePoint sites.

### 3.5.4 Affected Components

#### DSMS

Remedy will be updated to include a new field for the name of the files in the ADT specific SRD (Service Request Definition), and in the QCAF specific Service Management Incident template.

#### Service Impact

This change introduces a more secure method to what is currently an insecure method, and some changes to DCC Service Design will be required.

### 3.5.5 Legal Text

For the legal text associated with this solutuon, the above sections when 'email' is mentioned in regard to delivery of files, should read 'the DCC's secure delivery method of choice'.

Where "the Service Desk" is mentioned within any part of Appendix AA, Sections 3.3, 3.4, 4.3, 4.7 and 4.8, DCC propose that this be amended to read "the DCC". This will cover any prospective changes of responsibility for ADT within the DCC. This is covered within Business requirement 1.

# 4 Impact on Security

There is no security impact caused by the proposed method. The SSC has been consulted throughout the life of this Modification, and has approved the required changes.

# 5 Testing Considerations

There is no testing consideration due to the proposed method already being used for other secure data.

# 6 Implementation Timescales and Releases

## 6.1 Change Lead Times

The work included as detailed above would require updates to the SSI which is covered outside of this Modification, the ADT User Guide, Customer Ops Forum communication and notice for the SEC Parties to use the new method.

Legal text will be agreed for this Modification, and will be released by SECAS as part of the document-only February 2022 SEC Release. The new methods will apply from that date.

# 7 DCC Costs and Charges

## 7.1 Cost Impact

The implementation will be carried out by DCC with no associated charges in this Modification.

## 7.2 Impact on Charges

This section describes the potential impact on Charges levied by DCC in accordance with the SEC.

DCC notes that SECMP0109 does not propose any changes to the charging arrangements set out in SEC Section K. There will be no implementation costs for SECMP0109.

# Appendix: Glossary

| Acronym | Definition |
|---|---|
| ADT | Anomaly Detection Threshold |
| CR | DCC Change Request |
| CSV | Comma Separated Values |
| DCC | Data Communications Company |
| DSMS | DCC Service Management System |
| DSP | Data Service Provider |
| PIA | Preliminary Impact Assessment |
| QCAF | Quarantine Communication Action Files |
| QCR | Quarantined Communications Reports |
| SEC | Smart Energy Code |
| SECAS | Smart Energy Code Administrator and Secretariat |
| SMSR | Service Management Service Request |
| SRV | Service Request Variant |
| SSC | Security Sub Committee |
| SSI | Self Service Interface |