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.

MP109

'ADT and Exit Quarantine file delivery mechanism'

Modification Report

Version 0.4

16 August 2021

Corporate member of Plain English Campaign
Committed to clearer communication
592

About this document

This document is a draft Modification Report. It currently sets out the background, issue, and progression timetable for this modification, along with any relevant discussions, views and conclusions. This document will be updated as this modification progresses.

Contents

This document also has one annex:

- **Annex A** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.
- **Annex B** contains the Anomaly Detection Threshold (ADT) User Guidance document.
- **Annex C** contains the full Data Communications Company (DCC) Preliminary Assessment response.

Contact

If you have any questions on this modification, please contact:

Khaleda Hussain

020 7770 6719

Khaleda.Hussain@gemserv.com

1. Summary

This Modification Proposal was raised by Chris de Asha of the DCC.

SEC Appendix AA 'Threshold Anomaly Detection Procedures' currently requires the ADT File and Exit Quarantine files to be provided to the DCC by email. 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 classed as a data breach. It is believed the current method is insecure and poses potential security risk as email is not considered a secure delivery method. This is due to it lacking end to end encryption and being potentially susceptible to Security breaches through either deliberate malicious activity or erroneous activity.

To mitigate the potential security risk posed by email, the DCC have proposed to change the wording of SEC Appendix AA from "Email" to "DCC's preferred secure delivery method of choice". The DCC's current secure delivery method of choice would be via DCC SharePoint. There are no DCC cost associated with this change and if approved will be targeted for the February 2022 SEC Release.

This modification will affect the DCC, Suppliers, Network Parties and Other SEC Parties. There are no DCC costs associated with this change. If approved this modification will be implemented in the February 2022 SEC Release. This is a Self-Governance Modification.

2. Issue

What are the current arrangements?

The SEC explicitly states that email is the delivery method required for ADT files. The following sections in SEC Appendix AA either state email as the only delivery method, or refer to an action required prior to an email being sent:

- Section 3.1
- Section 3.4
- Section 3.4(a)
- Section 4.7
- Section 4.7(a)
- Section 4.13
- Section 4.13(a)
- Section 6.1

What is the issue?

The SEC specifically details that 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 'Threshold Anomaly Detection Procedures' Section 4.7 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". With the current arrangements, this results in emails being 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 must be securely delivered due to these being data records that contain information private to both a User and the DCC. Failure to do so would be a classed as a data breach. Additionally, ADTs provide protection to the electricity network by specifying the maximum number of Critical commands expected. This ensures there are no unexpected or malicious surges or reductions in power on the National Grid.

What is the impact this is having?

The DCC believes that using email to provide ADT Files and subsequent updates is not secure as 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 aren't securely delivered, then it allows the potential for unauthorised persons being able to access private data. If these data breaches occur, it could undermine the security and commercial image of DCC's business processes. The additional benefits suggested by the Proposer are a single system for the delivery of files, resulting in less effort for end Users and DCC.

3. Solution

Proposed Solution

The DCC initially proposed for DCC Users to send ADT and Exit Quarantine files via the Self-Service Interface (SSI). A DCC Preliminary Assessment was conducted based on this original solution proposal which was presented to Working Group. The Working Group considered the SSI solution proposal to be too expensive. As a result, SECAS and the DCC explored alternative methods.

To mitigate the potential security risk posed by email, the DCC have proposed a change of SEC Appendix AA. The Proposed Solution is to change the wording from "Email" to "DCC's preferred secure delivery method of choice. The DCC' current secure delivery method would be via DCC SharePoint which all Service Users have access to as part of the onboarding process. The wording change to the SEC would also allow future improvements to the ADT process without another SEC Modification. Changes would be communicated via the Customer Ops Forum and business wide Mass Communications. Detailed explanations on delivery method will also be added to the ADT User Guidance document available to all Service Users via DCC SharePoint and the Self-Service Interface (SSI).

The proposed redlined changes can be found in Annex A and the ADT User Guidance document can be found in Annex B.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
✓	Large Suppliers	✓	Small Suppliers
✓	Electricity Network Operators	✓	Gas Network Operators
✓	Other SEC Parties	✓	DCC

Breakdown of Other SEC Party types impacted			
✓	Shared Resource Providers	✓	Meter Installers
✓	Device Manufacturers	✓	Flexibility Providers

This Modification Proposal affects all SEC Parties who use email to submit their ADT and Exit Quarantine file to the DCC, meaning it shall impact all Suppliers, Network Operators and Other SEC Parties that submit Critical Service Requests.

DCC System

There are no impacts on the DCC systems.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Appendix AA 'Threshold Anomaly Detection Procedures'.

Consumers

No impacts of Consumers have been identified.

Other industry Codes

No other industry Codes are impacted by this proposal.

Greenhouse gas emissions

This proposal will have no effects on greenhouse gas emissions.

5. Costs

DCC costs

There are no DCC costs to implement this proposal.

SECAS costs

The estimated SECAS implementation costs to implement this modification is one day of effort, amounting to approximately £600. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.

SEC Party costs

There will be no cost to SEC Parties to implement this proposal.

6. Implementation approach

Recommended implementation approach

SECAS is recommending an implementation date of:

- **24 February 2022** (February 2022 SEC Release) if a decision to approve is received on or before 21 December 2021; or
- **30 June 2022** (June 2022 SEC Release) if a decision to approve is received after 21 December 2021 but on or before 20 April 2022.

The work required will be updates made to the SSI which will be covered outside of this Modification, the ADT User Guide, Customer Operations Forum communication and notice for the SEC Parties to use the new method. As the change will be a document-only February 2022 SEC Release is the earliest release this can be targeted for.

The DCC advised the in August 2021 Working Group the updates made to the SSI will include renaming the current method and replacing this with the DCC's preferred secure delivery method of choice. This Modification does not propose any changes to the charging arrangements set out in SEC Section K.

7. Assessment of the proposal

Observations on the issue

The views of the Panel Sub-Committees were sought during the Development Stage. Only the Security Sub-Committee (SSC) confirmed it had an interest in the progress of this Modification Proposal. It agreed that this was an issue and requested further involvement as the solution develops so that it can remain updated on its progress and ensure that it would be fit for purpose.

The Change Sub-Committee (CSC), on its initial viewing of the Modification Proposal, was supportive of the issue and agreed that it was clear in what was looking to be addressed. It requested that the Panel Sub-Committees be consulted before returning for decision, which only the SSC acknowledged as an issue. When it was returned to the CSC for decision, they only noted that it should be taken to the Refinement Process as the recommended progression before agreeing it should be taken to Panel for conversion to a Modification Proposal. SECAS and the SSC agreed that if converted to a Modification Proposal, it should proceed to a decision under Self-Governance.

Solution development

The DCC initially suggested for DCC Users to send ADT and Exit Quarantine files via the Self-Service Interface (SSI) as the secure method. A DCC Preliminary Assessment was performed which was shared with the Working Group. The Working Group raised concerns regarding the high cost associated with the SSI method which the DCC noted. The DCC then looked at alternative secure methods and proposed ADT and Exit Quarantine files are sent to the DCC via SharePoint. The proposed SharePoint solution has no DCC cost associated with the change and the Working Group members were supportive of this method.

The full DCC Preliminary Assessment response can be found in Annex C

Support for Change

The views of the Working Group have been mixed. Originally, there was a lack of support for the change in the first Working Group meeting held in April 2020. One of the main issues was that a Working Group member raised that the DCC had previously agreed with industry members that the email system would be used to send the ADT and Exit Quarantine files. Between this, concerns that changing the setup could lead to Users missing individual events among the wider notifications in the SSI and that they have no issue with the existing setup, this indicated a lack of desire for the change.

After a Preliminary Assessment had been requested and returned to the Working Group in November 2020, the case for change was more positive from the Working Group members. The Working Group members were more supportive to a move to the SSI, on the condition it wouldn't create any duplication of efforts for the User. This is due to ADTs needing to be signed off by an Authorised Responsible Officer (ARO), which is fine under the current email system. Another Working Group member believed this Modification Proposal would be an improvement on the existing system but queried whether keeping the current system would be more cost effective than switching over to a primarily SSI driven delivery method. Finally, a Working Group member stated that the SSI Improvements Process (SIP) would need to be consulted upon at some point to deliver the changes given the impacts to the SSI that would result from the Proposed Solution. A SIP has been suggested to run in parallel with a Refinement Consultation for the Modification Proposal.

Since then, due to the high cost associated with the first Preliminary Assessment based on the original solution via the SSI route, the DCC investigated alternative cheaper feasible solutions. Once the Proposed Solution was refined and amended it was presented to the SSC for feedback. The SSC expressed support of the revised proposed solution of SharePoint. Once the DCC conducted a second Preliminary Assessment, SECAS presented the revised solution option of the DCC SharePoint Proposal which received full support from the Working Group. Furthermore, as there are no DCC costs associated to implement the change the DCC have confirmed an Impact Assessment will not be required. The DCC further highlighted all Users are given access to the SharePoint as part of the on-boarding process and are provided with a guidance document which explains in detail of the process in submitting ADT and Exit Quarantine files.

The full DCC Preliminary Assessment response can be found in Annex C and the ADT User Guidance document can be found in Annex B.

Views against the General SEC Objectives

Proposer's views

The Proposer believes that this Modification Proposal would help better facilitate SEC Objective (f)[1]. This is due to any solution that provides a more secure delivery method than the current email system for providing ADT and Exit Quarantine files being beneficial to the protection of data that is required in the SEC.

Views against the consumer areas

Improved safety and reliability

The change is neutral against this area.

Lower bills than would otherwise be the case

The change is neutral against this area.

Reduced environmental damage

The change is neutral against this area.

Improved quality of service

This implementation will ensure privacy is maintained when sending through data which contain information private to both Users and the Industry.

Benefits for society as a whole

The change is neutral against this area.

[1] Ensure the protection of data and the security of data and systems in the operation of the SEC.

Appendix 1: Progression timetable

A Refinement Consultation will now be issued before presenting the responses to the Working Group.

Timetable	
Action	**Date**
Business requirements agreed with the Proposer	16 Mar 2020
Working Group meeting	1 Apr 2020
Business requirements discussed at SSC	8 Apr 2020
Request Preliminary Assessment	13 May 2020
Preliminary Assessment accepted	29 May 2020
Preliminary Assessment returned	28 Sep 2020
Working Group meeting	4 Nov 2020
Presented to the SSC	24 May 2021
Updated Preliminary Assessment received	16 Jul 2021
Presented to the SSC	28 July 2021
Working Group meeting	4 Aug 2021
Refinement Consultation	16 Aug – 27 Aug 2021
Working Group meeting	6 Oct 2021
Change Sub Committee	26 Oct 2021
Modification Report Consultation	1 Nov – 19 Nov 2021
Change Board	15 Dec 2021

Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	**Full term**
ADT	Anomaly Detection Threshold
ARO	Authorised Responsible Officer
CSC	Change Sub-Committee
DCC	Data Communication Company
SEC	Smart Energy Code
SECAS	Smart Energy Code Administration and Secretariat
SIP	SSI Improvement Process
SSC	Security Sub-Committee
SSI	Self-Service Interface

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.

MP109 'ADT and Exit Quarantine file delivery mechanism'

Annex A

Legal text – version 0.3

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

Appendix AA 'Threshold Anomaly Detection Procedures'

These changes have been redlined against Appendix AA version 2.0.

Amend Section 2.2 as follows:

2. DCC Anomaly Detection Threshold Guidance

2.2 DCC shall:

(a) provide guidance to support Users in setting appropriate ADT and Warning Thresholds;

(b) provide a template for the User to provide its ADT and Warning Thresholds in the format set out in clause 6.3 of this document; ~~and~~

(c) provide guidance to support Users in submitting ADT submissions to the DCC via the DCC's secure delivery method of choice; and

(d) provide the guidance and template referred to above via the Self Service Interface (SSI).

Amend Section 3.1 as follows:

3. Notification of Anomaly Detection Thresholds

User and DCC Responsibilities: ADT submissions

3.1 Prior to sending the DCC any Anomaly Detection Thresholds File, the User shall raise a DCC Service Management Service Request (SMSR) via the SSI to obtain a reference number for use in its submission to DCC, where such reference number will be generated by the SSI automatically.

Amend Section 3.4 as follows:

3.4 A User shall, in each User Role in relation to which it is required (or elects) to set ADTs, provide an Anomaly Detection Thresholds File to the DCC via the DCC's secure delivery method of choice~~an email to the Service Desk.~~ The submission via the DCC's secure delivery method of choice~~email~~ shall include:

(a) the SMSR reference number in the subject line of the submission~~email~~; and

(b) the Anomaly Detection Thresholds File (of the form set out in clause 6.3 of this document), Digitally Signed by a Private Key associated with a File Signing Certificate and provided to an Authorised Responsible Officer (ARO) in accordance with the SMKI RAPP.

Amend Section 4.7 as follows:

4.7 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~~n email~~ to the ~~Service Desk~~DCC indicating the action to be taken on each of the quarantined communications. The submission~~email~~ shall include:

(a) the Incident reference number in the ~~subject line~~title of the submission~~email~~; and

(b) a valid CSV file, updated with the required action for each communication ("Release" or "Delete"), Digitally Signed with a Private Key issued to the ARO for the purposes of CSV file signing, as set out in clause 6.5 of this document.

Amend Section 4.13 as follows:

4.13 Upon being advised of the action to be taken, but prior to sending the DCC any Quarantine Communications Actions File, the User shall raise a DCC Service Management Service Request (SMSR) via the SSI to obtain a reference number for use in its submission to DCC, where such reference number will be generated by the SSI automatically.

Users shall then send a ~~submission to the DCC via its secure delivery method of choicet an email and~~ Quarantined Communications Action File which specifies actions in respect of each quarantined communication and shall, where relevant, correspond with the actions as advised by the DCC. Such a submission~~email~~ shall be sent to the DCC ~~Service Desk~~ via ~~its~~the DCC's secure delivery method of choice~~submitted to the Service Desk~~ and shall include:

(a)the DSMS Incident reference number notified in the ~~subject line~~title of the submission~~email~~; and

(b)a valid CSV file, updated with the required action for each communication ("Release" or "Delete"), Digitally Signed with a Private Key issued to the ARO for the purposes of CSV file signing, as set out in clause 6.5 of this document.

Amend Section 6.1 as follows:

6. Communication Formats

6.1 All data sent as a submission to the DCC via its secure delivery method of choice~~email~~ for use in the DCC Systems for the purposes of these Threshold Anomaly Detection Procedures shall be in the form of a Digitally Signed CSV file. The field separator shall be a comma "," and the record separator shall be a line feed character 0x0A. In the file descriptions set out in clause 6.3 to 6.5 of this document, the character "▲" indicates the record separator. Users may include, within such CSV files, consecutive comma separators to

the left of a record separator to specify that a field has a null value. DCC shall interpret consecutive commas within a record to identify a null value.

Data Communications Company

SECMP0109

ADT User Guidance Drafted Section

Version: 1
Date: 19.07.21
Author: Adam Rawling
Classification: DCC Controlled

Background of SECMP0109

This document shows a drafted version of what the ADT User Guidance would look like when agreed with all stakeholders. This details how to use the 'DCC's secure delivery method of choice' as is a DCC responsibility specified in the SEC.

Sections will be renumbered to fit into the existing document.

1 How to Submit an ADT File

1.1 Quick Rules

The Anomaly Detection Threshold (ADT) files submissions process has been designed using relatively simple files and design assumptions to keep population and submission as easy as possible for Users. Four stages are described in the Threshold Anomaly Detection Procedures (TADP) document.

1. Determine the number and values to set for Anomaly Detection Thresholds
2. Export ADTs to a Comma Separated Values (CSV) file
3. Sign the ADT File
4. Send the signed ADT file to DCC (see below)

When updating rules, the ADT submission file must contain **all** rules that a User expects to be applied and counted by the DCC Systems.

Any rules not contained within the ADT submission file (i.e., from a previous submission) will be removed and will not be counted by the DCC Systems.

Any rules where the threshold values change but the time period remains the same will be considered as updates to that rule.

SEC Appendix AA states the Service User must submit an ADT File and Quarantine Communication Action File (QCAF) via the DCC's secure delivery method of choice.

Currently the DCC's secure delivery method of choice is file transfer via **DCC SharePoint**.

An ADT file must be submitted for each EUI64 User ID.

1.2 Raising a Service Catalogue Request for ADT File and QCAF Submission

The initial steps of creating a Service Catalogue Request must be completed before uploading an ADT file or a QCAF to DCC SharePoint.

To raise a Service Request, log into the Self-Service Interface (SSI) as follows:

Step 1: Select the "Tickets" tab on the SSI.

Step 2: Select "Raise a New Service Catalogue Request" from displayed content.

Step 3: Using the search field select "ADT File Submission" or "QCAF Submission" depending on the action being undertaken. For a fast track ADT File request select "FastTrack ADT File Submission".

Step 4: Fill out details within the Service Request and follow through to Service Request submission.

Step 5: Once submitted, you will be presented with a Request Id. Save this reference as it will be required for the naming of the submissions file.

Step 6: Service Request completed; you can now proceed to uploading the ADT file or QCAF submission.

Explanations of the processes and area structure to upload Anomaly Detection files is detailed in section 1.3 for ADT submission files and section 1.4 for QCAF submissions.

1.3 Submitting an ADT File

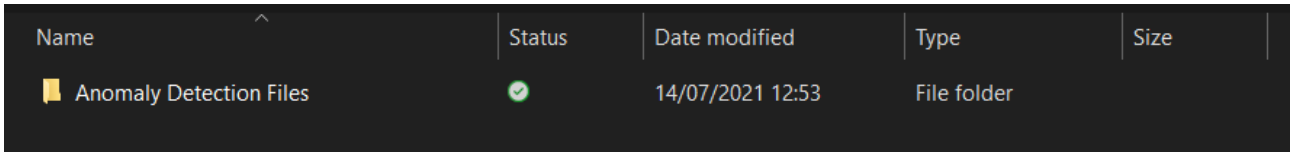
Before uploading the ADT File, the submission filename should be formatted as:

SEC Party EUI64 – RequestId – ADT

For Example: **70-00-00-00-00-00-00-01–REQ000000000001-ADT**

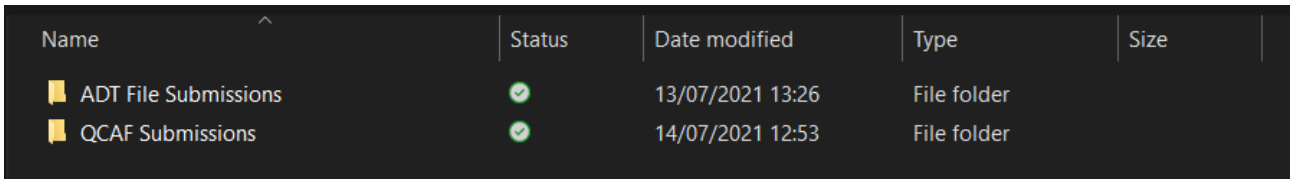
The images following illustrate the folder structure for each EUI64s ADT file submission.

Step 1: Initially access your SEC Party SharePoint page, where you will find the 'Anomaly Detection Files' folder as below:



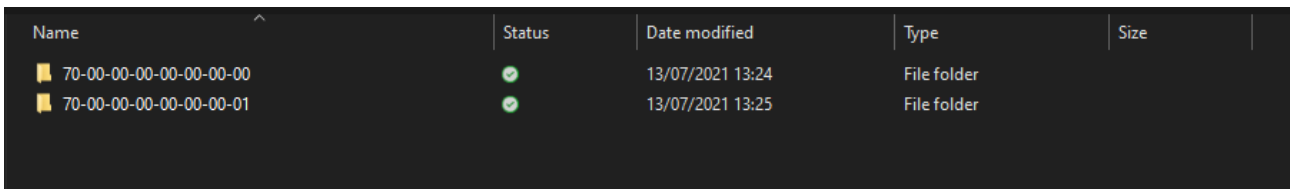
Step 2: Choose the folder. This location has two sub-folders.

- 'ADT File Submissions' for submitting Service User's ADT files
- 'QCAF Submissions' for submitting QCAF files



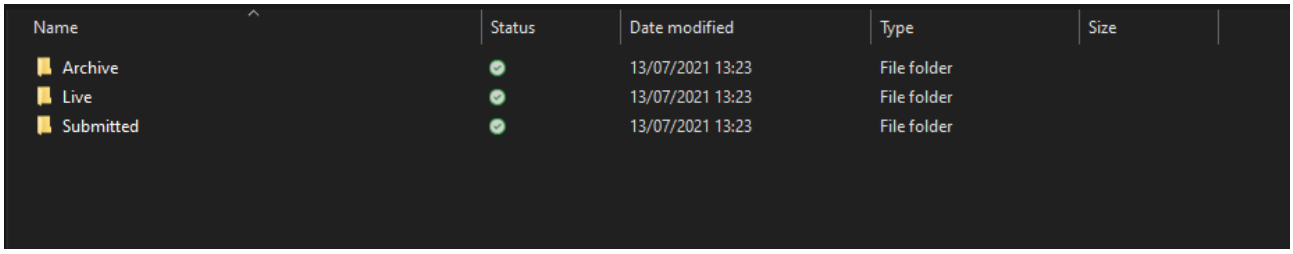
Step 3: For submitting a new ADT file, select 'ADT File Submissions'.

In the 'ADT File Submissions' folder, a list of your SEC Party EUI64 Ids is available. If your SEC Party has only one current EUI64, then a subfolder for that EUI64 will be in place.



Step 4: Select the appropriate EUI64 subfolder for the thresholds you wish to update.

In each of the EUI64 folders, there will be three subfolders as shown below:



Context:
Archive – a store of old submitted User ADT files.
Live – This folder contains the current User ADT file loaded in live.
Submitted – Area for new submitted ADT files ready to be processed by DCC and loaded into live.

Step 5: Choose the Submitted folder and Upload the new ADT submissions file.

In a separate step, DCC will then pick up the request from the Submitted folder and process accordingly.

1.4 Submitting a QCAF

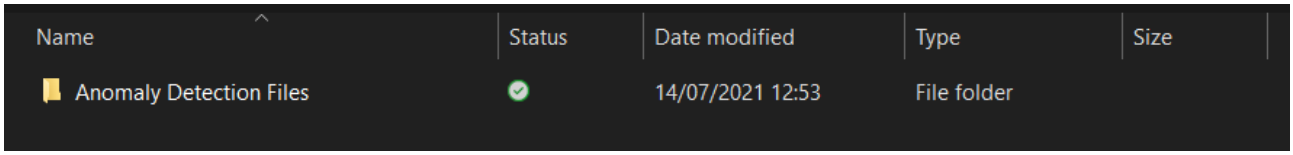
Before uploading the Quarantine Communications Action File (QCAF), the submission filename should be formatted as:

SEC Party EUI64 – RequestId – QCAF

For Example: **70-00-00-00-00-00-00-01–REQ000000000001-QCAF**

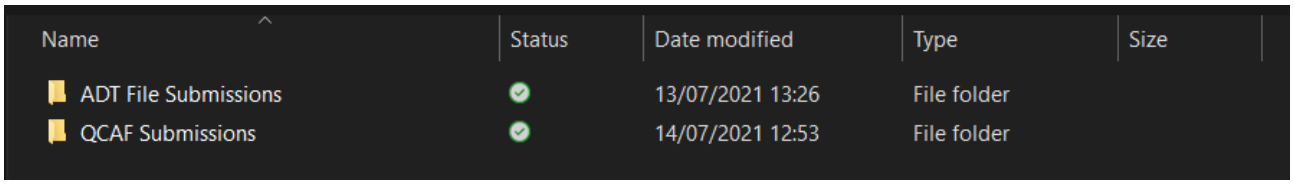
The images following illustrate the folder structure for each EUI64s QCAF submission.

Step 1: Initially access your SEC Party SharePoint page, where you will find the 'Anomaly Detection Files' folder as below:



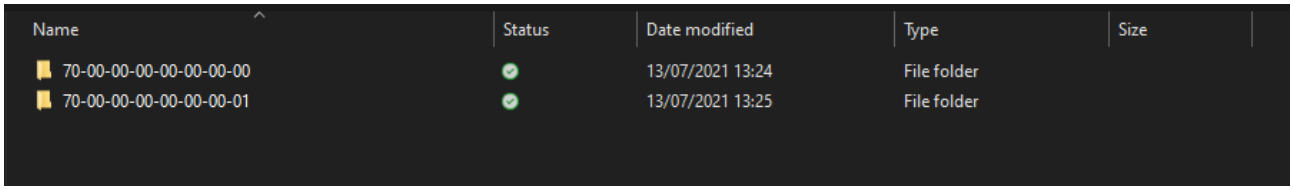
Step 2: Choose the folder. This location has two subfolders.

- 'ADT File Submissions' area is for submitting Service Users ADT Files.
- 'QCAF Submissions' area is for submitting QCAF files for DCC to process.



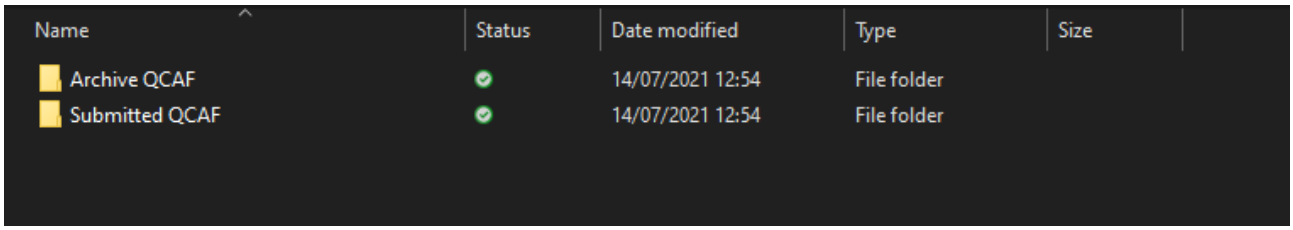
Step 3: For submitting a new QCAF select 'QCAF Submissions'.

In the 'QCAF Submissions' folder, a list of your SEC Party EUI64 Ids is available. If your SEC Party has only one current EUI64, then a subfolder for that EUI64 will still be in place.



Step 4: Select the appropriate EUI64 subfolder for the thresholds you wish to update.

In each of the EUI64 folders, there will be three subfolders seen below:



Context:
Archive QCAF – a store of old submitted QCAFs containing details on already released Service Requests
Submitted QCAF – Area for new QCAFs ready to be actioned by the DCC

Step 5: Choose the Submitted folder and Upload the new QCAF submission.

DCC will then pick up the request from your created Service Request and process accordingly.

SEC Modification Proposal, SECMP0109

DCC CR 1366, ADT and Exit Quarantine File Delivery Mechanism

DCC Preliminary Impact Assessment (Updated)

Version:	**1.41**
Date:	**16th 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. However licenses will need to be obtained for the use of Premium Egress, and will form the basis of Application Support and Business as Usual charges as shown following.

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