SEC
Smart Energy Code

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.

Smart Energy Code

MP109

‘ADT and Exit Quarantine file delivery mechanism’

Modification Report

Version 1.0

19 January 2022

Corporate member of Plain English Campaign
Committed to clearer communication
592

About this document

This document is a Modification Report. It sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views, and conclusions.

Contents

1. Summary 3
2. Issue 3
3. Solution 4
4. Impacts 5
5. Costs 6
6. Implementation approach 6
7. Assessment of the proposal 6

Appendix 1: Progression timetable 9

Appendix 2: Glossary 10

This document also has five annexes:

- **Annex A** contains the business requirements for the solution.
- **Annex B** contains the Data Communications Company (DCC) Preliminary Assessment response.
- **Annex C** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.
- **Annex D** contains the Anomaly Detection Threshold (ADT) User Guidance document.
- **Annex E** contains the Refinement Consultation responses.

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. is the Proposer believes 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 has 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 the DCC SharePoint. The legal text also removes references to sending emails to the 'DCC Service Desk'.

This modification will affect the DCC and DCC Users. There are no DCC, or SEC Party 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. Several 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.

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 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.

Impact on consumers

This change will benefit consumers as moving away from email to SharePoint is a safer method providing privacy and security.

3. Solution

Proposed Solution

The DCC proposes that a secure delivery method could be via DCC SharePoint which all Service Users have access to as part of the onboarding process. To mitigate the potential security risk posed by email, the DCC proposes a change of SEC Appendix AA wording from "Email" to "DCC's preferred secure delivery method of choice". The wording change to the SEC would also allow future improvements to the ADT process without another SEC Modification. Changes would be communicated via DCC normal operational communications:

- the Customer Operations Forum
- business wide mass communications
- detailed explanations on the delivery method will also be added to the ADT User Guidance document available to all Service Users via DCC SharePoint and the SSI.

The business requirements can be found in Annex A and the ADT User Guidance document reflecting this solution can be found in Annex D.

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 will impact all DCC Users that submit Critical Service Requests.

DCC System

There are no impacts on the DCC Systems. These is a small change proposed to the SSI, but the modification is not dependant on that change, and it is being consulted on separately[1].

The DCC's Preliminary Assessment response can be found in Annex B. As there are no DCC costs to implement this solution, the DCC has confirmed that no subsequent Impact Assessment was needed.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Appendix AA 'Threshold Anomaly Detection Procedures'.

The redlined changes to deliver this modification can be found in Annex C.

Consumers

No impacts of Consumers have been identified.

Other industry Codes

No other industry Codes are impacted by this proposal.

[1] The DCC SSI consultation can be found here Consultation on proposed changes to the Self-Service Interface (1) | Smart DCC

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

Agreed implementation approach

The Change Sub-Committee (CSC) has agreed an implementation date of:

- **24 February 2022** (February 2022 SEC Release) if a decision to approve is received on or before 10 February 2022; or
- **30 June 2022** (June 2022 SEC Release) if a decision to approve is received after 10 February 2022 but on or before 16 June 2022.

As the change will be a document-only change, the February 2022 SEC Release is the earliest release this can be targeted for.

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 developed so that it could remain updated on its progress and ensure that it would be fit for purpose.

The CSC, on its initial viewing of the modification, was supportive of the issue and agreed that it was clear in what was looking to be addressed. SECAS and the CSC agreed that if converted to a Modification Proposal, it should proceed to a decision under Self-Governance.

Solution development

The DCC initially proposed that 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 Proposed Solution which was presented to Working Group[2].

The Working Group members discussed this option and highlighted they would consider to a move to the SSI, on the condition it wouldn't create any duplication of efforts for the User. This was due to ADT files 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.

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. It was suggested that a SIP be run in parallel with a Refinement Consultation for the Modification Proposal; however, since the SSI solution is no longer the Proposed Solution this is no longer needed to deliver the modification.

Overall though, the Working Group considered the SSI solution to be too expensive compared to the benefits it would bring and the availability of another, less expensive option. The Smart Energy Code Administrator and Secretariat (SECAS) and the DCC explored alternative methods. 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 more supportive of this method.

Working Group members noted the DCC had not stated a secondary method in the solution for use if SharePoint is suffering an outage. The DCC advised the secondary method of email was not recommended as it was unsecure. The DCC proposed the term 'preferred secure delivery method of choice' be used in SEC Appendix AA as this would allow changes to be made in the future without the need for a SEC modification.

In addition, the DCC believed a secondary method was not required as the DCC uses the Microsoft Office 365 cloud subscription to host the service. The DCC believed that in Q2 2021 there was a worldwide 99.98% uptime. There had only been one major incident related to DCC Customer SharePoint in the last year, on 11 December 2020, due to a full Microsoft outage across the UK for all of Office 365, disrupting the Service for under an hour. A Working Group member stated while they heard the DCC's comments about SharePoint being reliable they did not agree, and it would be good to have an alternative method in the event of an emergency.

SECAS asked the Working Group if members wanted something specific written into the SEC and a Working Group member confirmed it would be better to have this updated into the ADT User Guidance document. The DCC agreed it would be able to put some wording in the guidance

[2] The DCC Preliminary Assessment against the initial proposed solution can be found here https://smartenergycodecompany.co.uk/modifications/adt-and-exit-quarantine-file-delivery-mechanism/

document with the agreement to use email if SharePoint is unavailable. Following the Working Group, the DCC have updated the ADT User Guidance to reflect the User request. This will be released when the modification goes live.

The CSC queried in the instances members are not able to send documents via the DCC SharePoint, and instead send the documents via email, would they be breeching any rules or law. and members sent the documents via email be breeching the law. SECAS advised the DCC have updated the ADT User Guidance to reflect an addition of a contingency option of email in the unforeseen circumstance that DCC SharePoint is unavailable to Users. The CSC agreed to progress the modification to report phase.

The full DCC Preliminary Assessment response can be found in Annex B. Furthermore, as there are no DCC costs associated to implement the change the DCC confirmed an Impact Assessment was not required.

Support for Change

The SSC expressed support of the revised solution using SharePoint.

Once SECAS presented the revised solution and the updated Preliminary Assessment findings, the Working Group provided full support. 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 DCC confirmed that this would be updated when the modification was implemented to reflect the requirement of the use of SharePoint – these updates can be found in Annex D.

Business case

Moving away from email to SharePoint is a safer method providing privacy and security. Since this is a very low-cost option, the benefits outweigh the costs.

Views against the General SEC Objectives

Proposer's views

The Proposer believes that this Modification Proposal would help better facilitate SEC Objective (f)[3]. 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.

Industry views

Four responses were received to the Refinement Consultation. One Large Suppliers confirmed although they preferred email, they had no material issues with moving to the new method od using SharePoint. One Network Party agreed the new method would improve the security of the ADT and Exit Quarantine file delivery mechanism. Another Network Party highlighted while they agreed with

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

the intent of the solution, they queried what would happen in the instance the SharePoint suffers an outage.

The general view of the Refinement Consultation responses was that MP109 would better facilitate SEC Objective (f). If individuals who currently upload the ADT files have access to the DCC SharePoint and respective folders, the change can be implemented immediately. Three respondents agreed MP109 should be approved. However, one Network Party highlighted they believed the modification is neutral against the SEC objectives. Whilst they understand email is not secure, they believed that the files do not contain any personal data. As they are signed the DCC would know if they had been tampered with before actioning them.

The full Refinement Consultation responses can be found in Annex D.

Views against the consumer areas

Improved safety and reliability

This modification will ensure increased safety of the Smart Metering system by maintaining DCC User documents secure and private.

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.

Appendix 1: Progression timetable

A Modification Report Consultation (MRC) has been issued on 6 December 2021 and will close on 7 January 2022. The Change Board vote under Self-Governance will take place 26 January 2022.

Timetable	
Action	**Date**
Business requirements agreed with the Proposer	16 Mar 2020

Timetable	
Action	**Date**
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
Modification Report approved by CSC	30 Nov 2021
Modification Report Consultation	6 Dec – 7 Jan 2022
Change Board vote	26 Jan 2022

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
MRC	Modification Report Consultation
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

Business requirements – version 1.0

About this document

This document contains the business requirements that support the Proposers solution for this Modification. It sets out the requirements along with any assumptions and considerations. The DCC use this information to provide an assessment of the requirements that help shape the complete solution.

1. Business requirements

This section contains the functional business requirements. Based on these requirements a full solution will be developed.

Business Requirements	
Ref.	**Requirement**
1	Replace the main delivery method of ADT and Exit Quarantine files of emails with the SSI.
2	Retain the email delivery method for sending ADT and Exit Quarantine files as an alternative method if the SSI is unavailable or in a disaster recovery situation.

2. Considerations and assumptions

This section contains the considerations and assumptions for each business requirement.

2.1 General

The following business requirements should be adhered to, where possible using the most cost-effective means and uses the existing architecture to maintain simplicity. If this cannot be done, reasons should be given as to why the requirements could not be followed through with.

2.2 Requirement 1: Replace the main delivery method of ADT and Exit Quarantine files of emails with the SSI

For this requirement, it should provide the most simple and cost-effective means of changing the email method of delivering ADT and Exit Quarantine files with the SSI.

2.3 Requirement 2: Retain the email delivery method for sending ADT and Exit Quarantine files as an alternative method if the SSI is unavailable or in a disaster recovery situation

For this requirement, it should allow the existing email method to be retained. This way, in the event of disaster recovery or a User being unable to use the SSI that a User will still have the ability to deliver ADT and Exit Quarantine files.

Data Communications Company

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 3
2 Introduction 4
3 Impact on DCC's Systems, Processes and People 6
4 Impact on Security 7
5 Testing Considerations 8
6 Implementation Timescales and Releases 8
7 DCC Costs and Charges 8
Appendix: Glossary 9

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

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 C

Legal text – version 1.1

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. Notification of Anomaly Detection Thresholds

User and DCC Responsibilities: ADT submissions

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 4.3 as follows:

4. Exceeding Anomaly Detection or Warning Thresholds

User and DCC Responsibilities: User Warning Threshold

4.3. Each User shall investigate, and then update and assign the Incident to the ~~Service Desk~~DCC using the "Update Service Management Incident" Functional Component within the SSI.

Amend Section 4.7 and 4.8 as follows:

4. Exceeding Anomaly Detection or Warning Thresholds

User and DCC Responsibilities: User Set Anomaly Detection Threshold

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.

4.8. Each User shall update the Incident using the "Update Service Management Incident" Functional Component within the SSI and assign to the ~~Service Desk~~DCC for further action. The DCC shall:

(a) Check Cryptographic Protection applied to the CSV file, Confirm Validity of the Certificate used to Check Cryptographic Protection for the CSV file; and
(b) check that the format of the data is correct.

Amend Section 4.13 as follows:

4. Exceeding Anomaly Detection or Warning Thresholds

User and DCC Responsibilities: DCC Set Anomaly Detection Threshold

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

DRAFT File Submission User Guidance

Version: 0.1
Date: 18.11.21
Author: DCC
Classification: Draft

Document Control

Revision history

Revision date	Summary of changes	Changes marked	Version number
18/11/21	Drafted Guidance	N	0.1
08/12/2021	Minor edits	N	0.2

Information:

This document contains a drafted Anomaly Detection User Guidance section 5 that provides information on how to submit a User ADT file or QCAF to the DCC via the DCC's Preferred Secure Delivery Method.

Also included is the addition of a contingency option of email in the unforeseen circumstance that DCC SharePoint is unavailable to Users.

Table of Contents

1 How to Submit an ADT File/ QCAF 4
1.1 Quick Rules for ADT File 4
1.2 Quick Rules for QCAF 4
1.3 Raising a Service Catalogue Request for Action 5
1.4 Submitting an ADT File 6
1.5 Submitting a QCAF 7
1.6 Contingency Option for Submitting ADT Files and QCAFs 9

1 How to Submit an ADT File/ QCAF

1.1 Quick Rules for ADT File

The ADT submissions process from Users to the DCC has been designed using relatively simple files and design assumptions to keep its population and submission as easy as possible for Users with four stages as described in the TADP.

1. Determine the number and values for Anomaly Detection Thresholds to set
2. Export ADTs to CSV
3. Sign the Anomaly Detection Thresholds File
4. Raise Service Request via the SSI.
5. Supply signed ADT File to DCC via **DCC SharePoint** (see section 5.3).

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 that are not contained within the ADT submission file (i.e. were in a previous version) 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.

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

1.2 Quick Rules for QCAF

The QCAF creation and submissions process must be completed within 120 hours of the point of quarantine. After 120 hours, the Service Requests are achieved for a 30-day period but are not available for release. The basic stages are:

1. Download RSMI006 (Quarantined Requests Report) from the SSI as CSV.
2. Input action type for each SRV.
3. Sign the QCAF.
4. Raise Service Request via the SSI.
5. Supply signed QCAF to DCC via **DCC SharePoint** (see section 5.3).

SEC Appendix AA informs that the Service User must submit an ADT File or 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**.

1.3 Raising a Service Catalogue Request for Action

Before uploading an ADT Submissions File or a QCAF to DCC SharePoint, the initial steps of creating a Service Catalogue Request prior must be completed.

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

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 5.3 for ADT submission files and section 5.4 for QCAF submissions.

In the unforeseen scenario that DCC SharePoint is unavailable, as a contingency option, an email containing the ADT file to the Service Centre should act as the delivery method. For more information on this see section 5.6.

1.4 Submitting an ADT File

Before uploading the ADT File, the submissions name should be formatted as:

SEC Party EUI64 – RequestId – ADT

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

The below illustrates the folder structure for each EUI64s ADT File Submissions.

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

Name	Status	Date modified	Type	Size
Anomaly Detection Files	✓	14/07/2021 12:53	File folder	

This location has a further two sub-areas.

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

For submitting a new ADT file select 'ADT File Submissions'.

Name	Status	Date modified	Type	Size
ADT File Submissions	✓	13/07/2021 13:26	File folder	
QCAF Submissions	✓	14/07/2021 12:53	File folder	

Once in the 'ADT File Submissions' area, there will be three subfolders seen below:

Name	Status	Date modified	Type	Size
Archive	✓	13/07/2021 13:23	File folder	
Live	✓	13/07/2021 13:23	File folder	
Submitted	✓	13/07/2021 13:23	File folder	

Context:

Archive – This is a store of old submitted ADT files.

Live – This folder contains the current User ADT file loaded in production.

Submitted – Area for new submitted ADT files ready to be processed by DCC and loaded into production.

Upload the new ADT submissions file to the 'Submitted' area.

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

If there any queries on the above, please contact

DCC Service Centre: ServiceCentre@smartdcc.co.uk

1.5 Submitting a QCAF

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

SEC Party EUI64 – RequestId – QCAF

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

The below illustrates the folder structure for each EUI64s ADT File Submissions.

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

Name	Status	Date modified	Type	Size
Anomaly Detection Files		14/07/2021 12:53	File folder	

This location has a further two sub-areas.

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

For submitting a new QCAF select 'QCAF Submissions'.

Name	Status	Date modified	Type	Size
ADT File Submissions		13/07/2021 13:26	File folder	
QCAF Submissions		14/07/2021 12:53	File folder	

Once in the 'QCAF Submissions' area, there will be two subfolders seen below:

Name	Status	Date modified	Type	Size
Archive QCAF		14/07/2021 12:54	File folder	
Submitted QCAF		14/07/2021 12:54	File folder	

Context:

Archive QCAF – store of old submitted QCAFs containing details on already released service requests.

Submitted QCAF – Area that new QCAFs should be submitted ready to be actioned by the DCC.

Upload the new QCAF submission the 'Submitted QCAF' area.

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

If there any queries on the above, please contact

DCC Service Centre: ServiceCentre@smartdcc.co.uk

1.6 Contingency Option for Submitting ADT Files and QCAFs

In the unforeseen scenario that DCC SharePoint is unavailable to Users, as a contingency option both ADT files and QCAFs may be submitted via an email to the DCC Service Centre at the address ServiceCentre@smartdcc.co.uk.

This should be viewed as a contingency option and not the preferred method.

To complete this:

1. Generate the signed ADT File / QCAF ready to submit.
2. Create a Service Request via the SSI as described in section 5.3 of this document.
3. Quoting the newly created Service Request Id in the subject line and body of the email send via email the ADT file/ QCAF to ServiceCentre@smartdcc.co.uk

Once received, DCC will action the Service Request as necessary.

This option should only be used in the scenario of DCC's preferred secure delivery method (DCC SharePoint) being unavailable to Users for file submission.

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'

Refinement Consultation responses

Annex E

About this document

This document contains the full collated responses received to the MP109 Refinement Consultation.

Question 1: Do you agree with the solution put forward?

Question 1			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	Yes	The solution sounds reasonable however will not impact our organisation and therefore we are neutral.
Western Power Distribution	Network Party	No	Whilst we agree with the intent we don't agree that the solution is fit for purpose. The updated wording states that Users 'shall' provide the file via the DCC's secure delivery method of choice. This does not allow for instances when this is not possible.
OVO	Large Supplier	Yes	Although we prefer email, we have no material issues with moving to this method.
Scottish and Southern Electricity Networks	Network Party	Yes	Although this modification is making minimal changes to the current process, SSEN agree that this will improve the security of the ADT and Exit Quarantine file delivery mechanism.

Question 2: Will there be any impact on your organisation to implement MP109?

Question 2			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	No	We fix the ADT internally and resend a new request rather than the existing quarantined request (as it would be out of date). Therefore this change in non-applicable to our processes.
Western Power Distribution	Network Party	Yes	We will be impacted as we will need to submit files via a different method.
OVO	Large Supplier	Yes	Sending a email was far more straightforward and less complex to achieve than using the very un-userfriendly Sharepoint. We will need to change our processes to do so. Not onerous or problematic to us but we have issues with the DCC Sharepoint and hope that all who currently provide ADTs via email all will have rights to be able to publish documented and files onto the
Scottish and Southern Electricity Networks	Network Party	No	-

Question 3: Will your organisation incur any costs in implementing MP109?

Question 3			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	No	-
Western Power Distribution	Network Party	No	-
OVO	Large Supplier	No	n/a
Scottish and Southern Electricity Networks	Network Party	No	-

Question 4: Do you believe that MP109 would better facilitate the General SEC Objectives?

Question 4			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	Yes	For those required to use the process, it appears a more secure method and supports SEC objective F.
Western Power Distribution	Network Party	-	We feel that this modification is neutral against the SEC Objectives. We don't feel that the argument for better facilitating the SEC Objectives is clear. Whilst we understand that email is not as secure a method of sharing information as SharePoint, the files do not contain any personal data and also, as they are signed the DCC know whether they have been tampered with before they action them and therefore we are not convinced that this modification is better facilitating any of the SEC Objectives.
OVO	Large Supplier	Yes	Moving away from email to using Sharepoint is more secure which aligns to the SEC Objectives set out in the Report.
Scottish and Southern Electricity Networks	Network Party	Yes	SSEN agree that this modification will better facilitate SEC Objective (f) as detailed in the modification report.

Question 5: Noting the costs and benefits of this modification, do you believe MP109 should be approved?

Question 5			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	Yes	-
Western Power Distribution	Network Party	No	As per our comments under Question 1 we believe that the legal text is not appropriate and as per our comments under Question 4, we are not convinced this modification will better facilitate the SEC Objectives.
OVO	Large Supplier	Yes	We have no material issues with moving to this solution.
Scottish and Southern Electricity Networks	Network Party	Yes	SSEN note the standard legal text costs and no DCC costs.

Question 6: How long from the point of approval would your organisation need to implement MP109?

Question 6			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	N/a	-
Western Power Distribution	Network Party	N/A	-
OVO	Large Supplier	ASAP	As long as the current individuals that provide ADTs via email are able to do so via Sharepoint, we should be able to implement this immediately.
Scottish and Southern Electricity Networks	Network Party	N/A	-

Question 7: Do you agree with the proposed implementation approach?

Question 7			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	Yes	-
Western Power Distribution	Network Party	Yes	We note under Section 6 it states there is work required with updates made to the SSI which will be covered outside the modification, however we are presuming that this is just uploading the updated ADT User Guide.
OVO	Large Supplier	Yes	As detailed in previous answers.
Scottish and Southern Electricity Networks	Network Party	Yes	SSEN Agree with the proposed implantation approach.

Question 8: Do you agree that the legal text will deliver SECMPMP109?

Question 8			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	Yes	-
Western Power Distribution	Network Party	No	The updated wording states that Users 'shall' provide the file via the DCC's secure delivery method of choice. This does not allow for instances when this is not possible.
OVO	Large Supplier	Yes	The wording delivers the intent.
Scottish and Southern Electricity Networks	Network Party	Yes	SSEN agree that the legal text is clear and unambiguous.

Question 9: Please provide any further comments you may have?

Question 9			
Respondent	**Category**	**Response**	**Rationale**
British Gas	Large Supplier	-	-
Western Power Distribution	Network Party	-	We note that the guidance will be made available on the SSI, however there is currently ADT Guidance on SharePoint. Is the intent to move it all across to the SSI? Might it be appropriate to keep the documentation in the current location, or put it in both locations?
OVO	Large Supplier	-	Not at this time.
Scottish and Southern Electricity Networks	Network Party	N/A	-