SEC Modification Proposal, SECMP0109

DCC CR 1366, ADT and Exit Quarantine File Delivery Mechanism

DCC Preliminary Impact Assessment

Version:	**1.11**
Date:	**28-09-2020**
Author:	**DCC**
Classification:	**DCC PUBLIC**

Contents

1 Introduction

1.1 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.

1.2 Previous information provided by DCC

None.

1.3 DCC Contact Details

Please raise any queries regarding this DCC Impact Assessment using the contact details provided below.

Name	DCC - SEC Modification queries
Contact email	mods@smartdcc.co.uk

1.4 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 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”. 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 electricity network by specifying the maximum number of Critical commands expected, which in turn ensures there are no unexpected or malicious surges or reductions in power on the National Grid.

The DCC also believes that using email to provide ADT Files and subsequent updates is not as secure as the SSI, 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. An additional benefit suggested by the DCC is a single system for the delivery of files, therefore resulting in less effort for end Users and DCC.

1.5 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.

Business 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.

Business Requirement 2

Retain the email delivery method for sending ADI and Exit Quarantine files as an alternative method if the SSI is unavailable or in a disaster recovery situation.

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

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**. Where the requirements or SEC obligations change, DCC will be required to carry out a further impact assessment.

2 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.

2.1 Business Requirement 1

For Business Requirement 1, the remaining sections of this Impact Assessment cover the DCC System impacts and costs of the proposed SSI based file delivery mechanism.

2.2 Business Requirement 2

DCC propose to retain the current methods and processes used in support of the fallback email file delivery mechanism. There are no DCC System Impacts or costs associated with this.

2.3 Description of Solution

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

2.3.1 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 included as the subject of the email is used to send the ADT files to DCC.

DSP proposes that the SSI interface used for creating the SMSR for ADT file submission be modified to allow the Service Users to upload the ADT file at the time as creation of the SMSR. This functionality would eliminate the need for the second step of sending the ADT files separately. DSP will manage the processing so that the uploaded ADT file is not attached to the SMSR created within the DSMS. Instead, the file will be copied to a folder within DSP and subsequently delivered to a specific folder within DCC via the Enterprise Systems Interface (ESI). The name of the file will be included in the SMSR to help the DCC Service Desk correlate between the SMSR reference and the ADT files. The SMSR reference will be added to the filename to guarantee unique filenames for the rest of the processing within DSP, which will also act as a second correlation mechanism for the DCC Service Desk.

2.3.2 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 (QCA) file, referred to as the Quarantine Exit file in this CR, which specifies the required actions needed for each quarantined Service Requests. Currently, the QCA 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.

DSP proposes that SSI is enhanced to provide the ability to upload the QCA files via the interface used to update the Quarantined Communication specific Service Management incident. This eliminates the first step of sending the QCA file separately via email to DCC. Similar to the handling of ADT files received via SSI, the uploaded QCA files will not be attached to the DSMS incident, rather the name of the file will be added to the incident. The QCA file will be copied to a folder within SSI and subsequently delivered to a specific folder within DCC via ESI. The incident reference will be added to the filename to guarantee unique filenames for the remainder of the processing within DSP.

2.3.3 Information Security Considerations

In case of both the ADT and Exit Quarantine files, the files received from the Service Users will be subject to anti-virus checks within DSP to mitigate the risk of any malicious content present in the file in the event of a Service User's systems being compromised. However, it shall be noted that DSP will not perform either cryptographic verification or content inspection on these files.

The primary security consideration in the solution presented here is storing the ADT and Exit Quarantine files received by SSI outside of the core components, i.e. within the SSI component itself before passing them on to ESI for delivery to DCC. This means that the Reporting Application Server that stores and tracks all the files delivered via ESI will, in the case of these new files, only be updated with the metadata and will not store the actual files. Updates are required to the network configuration to establish the communication channel between SSI and ESI for transferring the files from SSI.

When SSI prepares to move a file to the ESI server, the Reporting Application Server will be updated with the information about the file using a Web Service. The files will be delivered to DCC using the ESI file transfer component. DSP will store these files for a period of seven days, after which they will be deleted. During this period, DCC will be able to request redelivery of these files via SSMI using the File Transfers interface.

2.3.4 Affected Components

SSI/SSMI

SSI will need to enhance the Service Catalogue Request and the Update Service Management Incident interfaces to support the file handling as discussed above.

The File Transfers interface within SSMI will be configured to include the identifiers for the ADT and Exit Quarantine files 'File Type' drop down list. This is to allow DCC to request redelivery of these files.

Reporting Application Server

Reporting Application will need to receive the file metadata from the SSI via the Web Service and support the transfer requirements of ADT and Exit Quarantine files.

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 QCA specific Service Management Incident template.

Enterprise Services Interface

No changes to the file transfer mechanism are required.

Infrastructure Impact

Network configuration changes are required to establish a communications channel between SSI and ESI.

Service Impact

This change introduces some automation to what is currently a manual process, some changes to Service Design will be required.

3 Impact on Security

It shall be noted that receiving a file via SSI and transferring it via ESI is a new processing pattern within DSP. The files received in this scenario are to be checked for the presence of any malicious content in order to protect the DCC Data Systems. The design of this requires security review and approval. The implementation will be security assured during the implementation phase. This includes reviewing designs, test artefacts and providing consultancy to the implementation and test teams.

As part of initial data privacy and security reviews, it is thought that it will be necessary to apply data encryption in the form of a product called Vormetric.

A more detailed Security impact will be carried out as part of the Full Impact Assessment.

4 Testing Considerations

This section outlines the testing required to complete the Design, Build and Test phases for this SEC Modification.

4.1 Pre-integration Testing

During Pre-Integration Testing (PIT), each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. Specifically, the development team will carry out unit testing and the build will be subject to continuous build and automated testing to identify build issues at the earliest opportunity.

PIT will operate as a single phase of activity with a single drop. It will consist of a defined subset of system tests being observed by DCC.

4.2 Systems Integration Testing

Systems Integration Testing (SIT) is the testing of the DCC Total System, which brings together the components, e.g., DSP and CSP Systems, to allow testing of the end-to-end solution by DCC. SIT is carried out for every DCC System release and incorporates the test

and integration of multiple changes. The SEC Modification and associated system changes will need to be demonstrated and tested as part of the integration test phases.

4.3 User Integration Testing

User Integration Testing (UIT) is referred to as User Testing in the SEC. User Testing of Modification Proposals is provided using the Modification Implementation Testing Service. It enables Users to run specific tests to support their implementation of a change. DCC expects that User Testing will be required to support User's implementation of this modification.

5 Implementation Timescales and Releases

5.1 Change Lead Times

From the date of approval, (in accordance with Section D9 of the SEC), in order to implement the changes proposed DCC requires a lead time of **6 months.**

6 DCC Costs and Charges

6.1 Cost Impact

6.1.1 Implementation Costs

The table below details the cost of delivering the changes and Services required to implement this Modification Proposal.

Implementation costs							
ROM	**Design**	**Build**	**PIT**	**SIT**	**UIT**	**Implementation to Live**	**Total**
SECMP0109	£150,000- 350,000						**£150,000 - 350,000**

Implementation costs – supplementary information	
Implementation cost assumptions	*A. Costs are exclusive of VAT and any applicable finance charges* *B. Majority of the costs above represent labour costs.* *C. Costs provided for Design, Build and Pre-Integration Testing are quotes provided by the Service Providers and assuming there is no scope change can be considered the final costs. DCC have reviewed and challenged the costs from the Service Providers to ensure this reflects best price to date.* *D. Costs will be refined during future assessments.*
Explanation of Implementation Phases	*DCC's implementation costs are provided by implementation phases. The following describes the purpose of each phase:* • *Design: The production of detailed System and Service design to deliver all new requirements.* • *Build: The development of the designed Systems and Services to create a solution (e.g. code, systems, or products) that can be tested and implemented.* • *Pre-integration Testing: Each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. This is assured by DCC.* • *System Integration Testing: All Service Providers' PIT-complete solutions are brought together and tested as an integrated solution, ensuring all Service Provider solutions align and operate as an end to end solution.* • *User Integration Testing: Users are provided with an opportunity to run a range of pre-specified tests in relation to the relevant change.*

- *Implementation to Live Costs: The solution is implemented into production environments and ready for use by Users as part of a live service. This service is subject to implementation costs.*

The fixed price cost for a Full Impact Assessment is **£14,551.58**, and is expected to take 30 days.

6.2 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. DCC has made the assumption that, in the absence of an agreed alternative arrangement by the Working Group, the costs associated with the implementation of SECMP0109 will be allocated to DCC's fixed cost based and passed through to Parties via Fixed Charges.

Subject to the commercial arrangements put in place to support the relevant Release, DCC expects the increase in Charges associated with the implementation of MP109 to commence in the month following the modification's implementation.

7 RAID

7.1 Risks

Ref.	Risk Description	Risk Impact
R-001	None identified	n/a

7.2 Assumptions

Ref.	Description	Impact
A-001	None identified	n/a

7.3 Dependencies

Ref.	Description	Impact
D-001	None identified	n/a