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.

DP108

'SSI Job Type Role for SRO/ARO'

Modification Report

Version 0.2

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

1. Summary 3
2. Issue 4

Appendix 1: Progression timetable 6

Appendix 2: Glossary 7

Contact

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

Joe Hehir

020 7770 6874

Joe.hehir@gemserv.com

1. Summary

This proposal was raised by Gary Fairclough from the Data Communications Company (DCC).

The access specifications for the Self-Service Interface (SSI) can be found in SEC Appendix AH 'Self Service Interface Access Control Specification'. There are several procedures that only Senior Responsible Officers (SROs), or Authorised Responsible Officers (AROs) are empowered to undertake with or request of the DCC. However, the Appendix AH currently has no restrictions available to limit access to these processes/requests to SROs and AROs only.

Therefore, anyone who has access to the SSI could in theory submit requests on behalf of an SRO or ARO for which only an SRO or ARO should have access to.

The DCC believes that by creating a Job Type Role specifically for SRO and ARO profiles, it can restrict access to non-authorised DCC Users from requests they are not empowered to submit and/or information deemed not relevant to their roles.

2. Issue

What is the SSI?

The SSI allows authorised Users, using supported web browsers, to perform a range of self-service functions including raising and monitoring the status of incidents, viewing Smart Metering Inventory (SMI) data and accessing external systems.

Appendix AH specifies how the SSI access rights permitted by the SEC are applied in practice and defines the information available to Users.

What are the current arrangements?

SROs

An SRO is an individual that is nominated to become a SRO by anyone of the following:

- A Director;
- Company Secretary; or
- Chief Information Security Officer (CISO).

SRO's are nominated for a SEC Party or DCC Service Provider, the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) or the SEC Panel.

Once an individual has become a SRO, the SRO may at any time nominate individuals to become Authorised Responsible Officers and to access SMKI Services and/or SMKI Repository Services.

AROs

The DCC can only permit AROs to act on behalf of a Party, the SMKI PMA, the Panel or DCC Service Provider for the purposes of accessing SMKI Services and/or SMKI Repository Services.

An ARO may be authorised to act on behalf of a Party or DCC Service Provider to be an Authorised Subscriber for Organisation Certificates, Device Certificates or both, following SMKI and Repository Entry Process Tests. All AROs are also permitted to access certain SMKI Repository Services on behalf of the organisation that they represent.

Functional Components

A Functional Component is a specific item or set of functionalities provided by the SSI which is subject to the access controls set out in Appendix AH.

When a DCC User requests access to a Functional Component, it must advise the Job Type Role for which it is applying for. The DCC must then ensure that the Job Type Role identified by the DCC User is authorised to access the Functional Components requested by the DCC User.

What is the issue?

There are several procedures that only SROs, or AROs are empowered to undertake with or request of the DCC. However, Appendix AH currently has no restrictions available to limit access to these

processes/requests to SROs and AROs only. For example, there are no restrictions to submit Anomaly Detection Threshold data to a SRO or ARO.

What is the impact this is having?

There are several procedures in the SSI that only SROs, or AROs are empowered to undertake with or request of the DCC. However, Appendix AH currently has no restrictions available to limit access to processes/requests SROs and AROs only.

There is a low risk that an individual that has access to the SSI who is not an SRO or ARO, could submit requests on behalf of an SRO or ARO.

The DCC believes that by creating a Job Type Role specifically for SRO and ARO profiles, it can restrict access to non-authorised DCC Users from requests they are not empowered to submit and/or information deemed not relevant to their roles.

Appendix 1: Progression timetable

This proposal will go to the Change Sub-Committee (CSC) on 28 January 2020 for initial discussion. It will then be reviewed by the Security Sub-Committee (SSC) on 12 February 2020.

It will then be returned to the CSC for a decision on the subsequent progression.

Timetable	
Action	**Date**
CSC provide initial views on the proposal	28 Jan 20
SSC review the issue outlined in the Modification Report	12 Feb 20
CSC recommendation that Panel convert into a Modification Proposal	25 Feb 20
Panel convert Draft Proposal to a Modification Proposal	13 Mar 20

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 Thresholds
ARO	Authorised Responsible Officer
CISO	Chief Information Security Officer
CSC	Change Sub-Committee
DCC	Data Communications Company
SSC	Security Sub-Committee
SMI	Smart Metering Inventory
SMKI	Smart Metering Key Infrastructure
SRO	Senior Responsible Officer
SSI	Self-Service Interface