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.

DP127

'SMKI RAPP Security Screening clarification'

Modification Report

Version 1.0

12 June 2020

Corporate member of Plain English Campaign
Committed to clearer communication
592

About this document

This document is a Modification Report. It currently 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

This document also has one annex:

- **Annex A** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.

Contact

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

Joe Hehir

020 7770 6874

Joe.hehir@gemserv.com

1. Summary

This proposal has been raised by Gordon Hextall on behalf of the Security Sub-Committee (SSC).

The SSC has confirmed that the obligations in SEC Section G 'Security' G4.2 and G4.3 apply to Authorised Responsible Officers (AROs) and that AROs should be subject to security screening to British Standard (BS) 7858:2019 or equivalent. However, this obligation isn't made explicit in Appendix D 'SMKI Registration Authority Policies and Procedures' (SMKI RAPP) which is followed by Users and the Data Communications Company (DCC) Registration Authority in processing applications for the appointment of AROs. Failure to comply with the obligation in Section G4.3 will result in a non-compliance being raised during a User Security Assessment.

This could cause confusion for Users and the DCC when assessing if AROs should be subject to BS 7858:2019. This could also create a security risk if the appropriate screening of AROs is not undertaken.

The Proposed Solution is to amend the sections of the SMKI RAPP that explain the process of the becoming an ARO, making it clear that AROs must be subject to BS 7858:2019 or equivalent. SEC Parties should not be impacted by this modification as they should already be screening AROs under the obligation in Section G4.3.

This modification's costs will be limited to Smart Energy Code Administrator and Secretariat (SECAS) time and effort to implement the changes. If approved, it is targeted for implementation in the November 2020 SEC Release.

2. Issue

What is an ARO?

The DCC can only permit AROs to act on behalf of a Party, the Smart Metering Key Infrastructure (SMKI) Policy Management Authority (PMA), the Panel or a 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.

SEC Appendix D section 4.1.2 identifies the interfaces and functions that an ARO may carry out. These largely relate to having access to the DCC Gateway to obtain SMKI Organisation and/or Device Certificates and for submitting Comma Separated Variable (CSV) Files to notify Anomaly Detection Thresholds (ADTs), including notifying changes to ADTs during SMKI Recovery. An extract of figure 1 in SEC Appendix D Section 4.1.2 is shown below, showing the procedure for provision of credentials to AROs for accessing SMKI Services:

Interface	**Purpose** (detailed in the SMKI Interface Design Specification and SMKI Repository Interface Design Specification)	**Credential Type**
Via DCC Gateway		
SMKI Portal (org Certs) SMKI Portal (Device Certs) SMKI Ad-Hoc Device CSR Web Service SMKI Batched Device CSR Web Service SMKI Repository Portal SMKI Repository Web Service SMKI Repository SFTP	Authentication to SMKI Portal (manual submission of Organisation CSRs and retrieval of Org Certs) Authentication to SMKI Portal (manual submission of Ad Hoc and Batched CSRs for Device Certs and retrieval of Device Certs) Authentication to Ad Hoc Device CSR Web Service (automated submission of Ad Hoc Device CSRs and retrieval of Device Certs) Authentication to Batched Device CSR Web Service (automated submission of Batched Device CSRs and retrieval of Device Certs) Authentication to SMKI Repository Portal (manual access to Certificates, CRLs and ARLs) Authentication to SMKI Repository Web Service interface (automated access to Certificates, CRLs and ARLs) Authentication to the SMKI SFTP interface (access to Certificates, CRLs and ARLs)	IKI Certificate IKI Certificate IKI Certificate IKI Certificate Username/pwd API Key Username/pwd
Via Internet		
SMKI Portal (Org Certs) SMKI Portal (Device Certs)	Authentication to SMKI Portal (manual submission of Organisation CSRs) Authentication to SMKI Portal (manual submission of Ad Hoc and Batched CSRs for Device Certs)	IKI Certificate IKI Certificate
File-Signing		
Threshold Anomaly Detection / Certified Products list, etc	Digital Signing of ADT files, the CPL or communications related to the SMKI Recovery Procedures.	IKI Certificate

SEC Appendix D section 4.1.1(d) also permits an ARO to undertake duties for multiple SEC Parties which widens the scope for an ARO to have an impact.

What is the BS 7858:2019?

BS 7858:2019 details how to screen individuals who work in “secure” environments, defined as anywhere that an insider could steal or threaten the integrity of data, information, or other physical or intellectual assets, or could threaten people’s safety. Such screening is required by the SEC for certain personnel who could cause a Compromise to the DCC Total System, User Systems, any Registration Data Provider (RDP) Systems or any Device.

What are the current arrangements?

The SSC has confirmed that the obligations in SEC Section G4.3 apply to AROs and that AROs should be subject to security screening to British Standard BS 7858:2019 or equivalent:

G4.2 Each User shall comply with Section G4.3 in respect of any of its User Personnel who are authorised to carry out activities which:

(a) involve access to resources, or Data held, on its User Systems; and

(b) are capable of Compromising the DCC Total System, any User Systems, any RDP Systems or any Device in a manner that could affect (either directly or indirectly) the quantity of gas or electricity that is supplied to a consumer at premises.

G4.3 Each User shall ensure that any of its User Personnel who are authorised to carry out the activities identified in Section G4.2:

(a) where they are located in the United Kingdom are subject to security screening in a manner that is compliant with:

(i) British Standard BS 7858:2012 (Security Screening of Individuals Employed in a Security Environment – Code of Practice); or

(ii) any equivalent to that British Standard which updates or replaces it from time to time; and

(b)where they are not located in the United Kingdom are subject to security screening in a manner that is compliant with:

(I) the British Standard referred to in Section G4.3(a); or

(ii) any comparable national standard applying in the jurisdiction in which they are located.

SEC Appendix D section 5.3 describes the process to become an ARO.

What is the issue?

The SSC has confirmed that the obligations in SEC Sections G4.2 and G4.3 apply to AROs and that AROs should be subject to security screening to BS 7858:2019 or equivalent. However, this obligation isn't made explicit in SEC Appendix D which is followed by Users and the DCC Registration Authority in processing applications for the appointment of AROs. Failure to comply with the obligation in Section G4.3 will result in a non-compliance being raised during a User Security Assessment.

What is the impact this is having?

The SMKI PMA and the DCC support the SSC's view that not making the obligation explicit in the SMKI RAPP could:

- cause confusion for Users and the DCC;
- lead to appropriate screening not being undertaken which is a security risk; and
- lead to potential SEC non-compliances identified during a User Security Assessment.

This would require a relatively straightforward addition to SEC Appendix D to clarify the need for security screening to BS 7858:2019 or equivalent as part of the ARO appointment process.

3. Solution

Proposed Solution

Figure 1 of the SMKI RAPP gives an overview of the SMKI access registration processes, including the procedure for becoming an ARO. The Proposed Solution is to amend this figure so that it clearly states AROs must be subject to security screening as required in SEC Section G4.3.

In addition, section 5.3 ‘Procedure for becoming an Authorised Responsible Officer’ of the SMKI RAPP further details the steps required to become an ARO. An amendment will also be made to the table in this section. This will explicitly state that a Senior Responsible Officer (SRO) must confirm that an ARO Nominee has been subject to security screening compliant with BS 7858:2019 or an equivalent standard as required by SEC Section G4.3.

There are no DCC System or User System changes required.

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

SEC Parties should not be impacted by this modification as they should already be screening AROs under the obligation in Section G4.3. However, this obligation will be made clearer in the SMKI RAPP which is followed by Users and the DCC Registration Authority in processing applications for the appointment of AROs.

DCC System

There is no impact on the DCC System.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Appendix D 'SMKI Registration Authority Policies and Procedures'

The changes to the SEC required to deliver the proposed solution can be found in Annex A.

Consumers

This modification will not impact consumers.

Other industry Codes

This modification will not impact any other industry Codes

Greenhouse gas emissions

This modification will not impact greenhouse gas emissions.

5. Costs

DCC costs

There are no DCC costs associated with this modification.

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

This modification is not expected to have any SEC Party costs associated with it.

6. Implementation approach

Recommended implementation approach

SECAS is recommending an implementation date of:

- **5 November 2020** (November 2020 SEC Release) if a decision to approve is received on or before 22 October 2020; or
- **25 February 2021** (February 2021 SEC Release) if a decision to approve is received after 22 October 2020 but on or before 11 February 2021.

The November 2020 SEC Release is the earliest release this modification can be targeted for. If a decision is not received in time for the November 2020 SEC Release, it will be targeted for the next scheduled SEC Release which is the February 2021 SEC Release.

7. Assessment of the proposal

Observations on the issue

The Change Sub-Committee (CSC) unanimously agreed that the issue is clearly defined and understood. It recommended that the Panel should covert this Draft Proposal into a Modification Proposal and that it should move directly to the Report Phase.

Solution development

SSC views

The SSC has confirmed that the obligations in SEC Sections G4.2 and G4.3 apply to AROs and that AROs should be subject to security screening to BS 7858:2019 or equivalent. It therefore agreed that this obligation should be made clearer in the SMKI RAPP.

Support for Change

The SSC, the SMKI PMA and the DCC agree that making the obligation explicit in the SMKI RAPP will:

- remove confusion for Users and the DCC;
- will mitigate a security risk that appropriate screening is not undertaken; and
- will reduce the potential for SEC non-compliances to be identified during a User Security Assessment.

Views against the General SEC Objectives

Proposer's views

Objective (f)[1]

The Proposer believes that MP127 will better facilitate SEC Objective (f). Failure to comply with the security screening obligation in Section G4.3 will result in a non-compliance being raised during a User Security Assessment. This modification would ensure all Parties understand that AROs must be subject to BS 7858:2019 or equivalent.

Objective (g)[2]

The Proposer believes that MP127 will better facilitate SEC Objective (g). This would give Parties clarity that AROs are subject to BS 7858:2019 or equivalent, as stated under Section G4.3.

[1] To ensure the protection of Data and the security of Data and Systems in the operation of this Code.
[2] To facilitate the efficient and transparent administration and implementation of this Code.

Appendix 1: Progression timetable

This Proposal will be presented to the Panel on 19 June 2020. If the Panel agree it will then proceed to the Report Phase and be issued for Modification Report Consultation. The Change Board would then vote on the proposal under Self-Governance on 24 July 2020.

Timetable	
Event/Action	**Date**
Draft Proposal raised	11 May 2020
Presented to CSC for initial comment and recommendation	26 May 2020
Modification Report approved by Panel	19 Jun 2020
Modification Report Consultation	22 Jun – 13 Jul 2020
Change Board vote	24 Jul 2020

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
BS	British Standard
CSC	Change Sub-Committee
CSV	Comma Separated Variable
DCC	Data Communications Company
RDP	Registration Data Provider
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator & Secretariat
SMKI	Smart Metering Key Infrastructure
SMKI PMA	SMKI Policy Management Authority
SMKI RAPP	SMKI Registration Authority Policies and Procedures
SRO	Senior Responsible Officer
SSC	Security Sub-Committee