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 0.1

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

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 Security Sub-Committee (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 the 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 BS7858:2019. This could also create a security risk if the appropriate screening of AROs is not undertaken.

2. Issue

What is an ARO?

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

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 CSV Files to notify Anomaly Detection Thresholds (ADTs), including notifying changes to ADTs during SMKI Recovery. An extract of figure 1 in 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

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 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 BS7858:2019 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.

Section 5.3 of Appendix D 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 BS7858:2019 or equivalent. However, this obligation isn't made explicit in the 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 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.

This would require a relatively straightforward addition to the Appendix D to clarify the need for security screening to BS7858:2019 or equivalent as part of the ARO appointment process. There are no DCC System or User System changes required.

Appendix 1: Progression timetable

Timetable	
Event/Action	**Date**
Draft Proposal raised	11 May 2020
Presented to CSC for initial comment	26 May 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
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
SSC	Security Sub-Committee