Smart Energy Code

Responsible Officer Guidance

Version Number: v1.1 Date Published: December 2017

What Does This Guidance Cover?

This document provides guidance in relation to **Smart Metering Key Infrastructure (SMKI) Senior Responsible Officers (SRO)** and **Authorised Responsible Officers (ARO)**, and their roles and responsibilities. This document is based on content set out within the **SMKI Registration Authority Policies and Procedures (SMKI RAPP)**, and has been designed to provide assistance to SEC Parties, Registration Data Providers (RDP) and other interested Parties when nominating individuals to become SROs and AROs for the purpose of subscribing to SMKI Certificates.

Prerequisites – EUI-64 Compliant Identifiers and Signifiers for the use of SMKI Organisation Certificates and DCCKI Certificates

SMKI provides the means by which Parties, the DCC (in its role as DCC Service Provider) and RDPs establish trust across the DCC network, and is one of the ways in which communications to Devices are secured. The DCC provide a number of interfaces for SMKI that are secured using Infrastructure Key Infrastructure (IKI) Certificates, and are used by AROs and SROs authorised to interact with the SMKI Services and/or SMKI Repository Services. Equally, **DCC Key Infrastructure (DCCKI)** is used to provide Parties and RDPs with Certificates to authenticate and communicate securely with DCC interfaces, such as the DCC Gateway Connection and Self-Service Interface.

Parties, the DCC, and RDPs are required to request from the SEC Panel (via SECAS) two identification numbers: an ID (User ID, DCC ID and RDP ID), and a Signifier (Party and RDP Signifier). Both IDs and Signifiers are issued in accordance with the Panel's ID Allocation Procedure.

In order to use the SMKI Services and/or SMKI Repository Services, Parties, the DCC, and RDPS will require an EUI-64 Compliant identifier range, used within the 'UniqueIdentifier' field in an Organisation Certificate Profile. They will also require a Signifier, which is a SEC-unique, non EUI-64 Compliant identifier linked to specific Public Keys in DCCKI Certificates. Further information on EUI- 64 Compliant identifiers and Signifiers can be found in the 'ID Allocation Procedure, EUI-64, and Signifier Guidance' found on the SEC Website.

Authorised Subscribers

A Party, the DCC or an RDP may become an Authorised Subscriber of a Certificate once their organisational identity has been successfully verified at least one SRO and one ARO has been nominated, and the **SMKI and Repository Entry Process Testing (SREPT)** applicable to the Certificate has been successfully completed. The procedural steps required for a Party or RDP wishing to undertake SREPT can be found in the SMKI and Repository Test Scenarios Document, a SEC Subsidiary Document. On becoming an Authorised Subscriber the Party, RDP or DCC is **required to submit forecasts to the DCC**. The DCC will provide details of this process and reminders when forecasts are due.

Administered by Gemserv

SMKI Senior Responsible Officer

A **SMKI SRO** is an individual that is nominated by a Director or Company Secretary, and is a representative of a Party, the SMKI Policy Management Authority (SMKI PMA), the Panel, an RDP or DCC Service Provider.

The responsibilities of a SMKI SRO are:

- to nominate and authorise SMKI AROs;
- to provide authorisation in regards to the revocation of Credentials and/or creation or revocation of Organisation Certificates; and
- to be available to be contacted by the DCC to confirm whether a User's submitted Anomaly Detection Thresholds (ADT) should be applied, and if not, to identify who will resubmit ADTs to the DCC.

An SRO can only access SMKI Services and/or SMKI Repository Services if they also become an ARO.

How to become a SMKI SRO:

The SMKI SRO Nomination Form can be found on the DCC's SharePoint website and should be completed by the nominee and a Nominating Officer (Director or Company Secretary) from the Party, RDP or DCC Service Provider.

The SMKI PMA Chair and Panel Chair shall be the Nominating Officers for the SMKI PMA and Panel respectively, in relation to a SMKI SRO being nominated by the SMKI PMA or the Panel.

The SMKI RAPP states that, as part of the SMKI SRO nomination process, the SMKI SRO must undertake a verification meeting. The SMKI SRO's identity shall be verified to Level 3, as set out in CESG GPG45 (Identity Proofing and Verification of an Individual), or to an equivalent level within a comparable authentication framework as agreed by the SMKI PMA.

Considerations:

Parties, RDPs and the DCC may wish to consider having a number of nominated SMKI SROs in order to provide adequate coverage (e.g. to cover annual leave, sickness, etc.).

Due to the ability of SROs to revoke Certificates, a SMKI SRO is likely to be an individual who holds a managerial and/or decision making responsibility within their organisation. Parties, RDPs and the DCC may wish to consider internal protocols to decide who within their organisation should have the ability to revoke Certificates, and whether or not individuals may revoke all Certificates, or be accountable for a single Certificate.

A SMKI SRO may be an individual who is contracted by the Party, RDP or DCC. This may be dependent on the Party, RDP or DCC ensuring appropriate 'risk appetite' for the individuals nominated, and ensuring that appropriate measures are in place to ensure SMKI SRO powers are not misused.

The SMKI SRO's responsibilities should be included as part of the individual's daily role(s), to be employed as and when required by Parties, RDPs or the DCC to nominate new SMKI AROs, or create or revoke Organisation Certificates.

An SRO is likely to be an individual who holds a managerial and/or decision making responsibility within their organisation, due to the ability of SRO's to revoke Certificates. Each Party, RDP and DCC (in its role as DCC Service Provider) may wish to consider internal protocols on who, within their organisation, has the ability to revoke Certificates, and whether or not individuals may revoke all Certificates, or be accountable for a single Certificate held by that Party, RDP or the DCC (in its role as DCC Service Provider).

SMKI Authorised Responsible Officer

A **SMKI ARO** is an individual that is nominated by a SMKI SRO, and is a representative of a Party, the SMKI PMA, the Panel, an RDP, or the DCC.

The responsibilities of an ARO are:

- To access the SMKI Services and/or SMKI Repository Services on behalf of Parties, the SMKI PMA, the Panel, RDPs or the DCC;
- To Digitally Sign, using a Private Key issued to the SMKI ARO, a Comma Separate Variable (CSV) file in order for the DCC to set the ADT; and
- To Digitally Sign, using a Private Key issued to the SMKI ARO, a valid CSV file with the required action for each communication to resolve the ADT quarantined threshold exceeded event.

Depending on the processes followed, a SMKI ARO may also become an Authorised Subscriber for Organisation Certificates and/or Devices Certificates, following the successful completion of SREPT. The ARO shall be the only authorised individual (unless an SRO has equally been authorised) to access and use the SMKI Services and/or SMKI Repository Services on behalf of a Party, the SMKI PMA, the Panel, an RDP or the DCC.

How you become a SMKI ARO:

The SMKI ARO Nomination Form can be found on the DCC's SharePoint website and should be completed by the nominee and a SMKI SRO (i.e. the nominating officer) from the Party, RDP or DCC Service Provider.

The SMKI PMA Chair and Panel Chair shall be the nominating officers for the SMKI PMA and Panel respectively, in relation to a SMKI ARO being nominated by the SMKI PMA or the Panel.

The SMKI RAPP states that, as part of the SMKI ARO nomination process, the SMKI ARO must undertake a verification meeting. The SMKI ARO's identity shall be verified to Level 3, as set out in CESG GPG45 (Identity Proofing and Verification of an Individual), or to an equivalent level within a comparable authentication framework as agreed by the SMKI PMA.

Considerations:

Parties, RDPs and the DCC may wish to consider having a number of nominated SMKI AROs in order to provide adequate coverage (e.g. to cover annual leave, sickness, etc.).

A SMKI ARO is likely to be an individual who holds an 'analyst' or 'data entry' role within their organisation. Depending on the processes followed, an ARO may be an Authorised Subscriber for a number of Certificates, and will also be the only individual (alongside other AROs of that organisation) to use the SMKI Services and/or SMKI Repository Services.

The SMKI SRO's responsibilities should be included as part of the individual's daily role(s). As the ARO will have direct access to the SMKI Services and/or SMKI Repository Services, Parties, RDPs and the DCC may wish to consider the individuals nominated, and ensure suitable processes are in place for the levels of access they have within the SMKI Services and/or SMKI Repository Services on behalf of their Party, RDP or DCC.

In order to provide sufficient coverage (e.g. to cover annual leave, sickness, etc.) –Parties, the SMKI PMA, the Panel, an RDP or the DCC (in its roles as DCC Service Provider) may want to nominate a number of individuals to become AROs to act on their behalf. An ARO is required to fill in the SMKI ARO Nomination Form, which is found on the DCC's SharePoint. Each ARO Nomination Form will also need to be completed by an SRO on behalf of the Party, the RDP or the DCC Service Provider. Equally, the SMKI PMA Chair and Panel Chair shall be the Nominating Officers for the SMKI PMA and Panel respectfully in relation to an ARO being nominated by either the SMKI PMA or the Panel.

SMKI Authorised Responsible Officer cont.

Considerations:

SECAS and the DCC consider that Parties, RDPs and the DCC (in its role as DCC Service Provider) may wish to consider having a number of AROs nominated, in order to provide sufficient coverage. As such, it may be prudent to assume that these roles are aligned with each businesses requirements, and that a sufficient number of AROs are nominated to provide cover across business procedures and operations.

An ARO is likely to be an individual who holds an 'Analyst' or 'Data Entry' role within a Party, RDP and/or the DCC (in its role as DCC Service Provider). Depending on the processes followed, an ARO may be an Authorised Subscriber for a number of Certificates, and will also be the only individual (alongside other ARO's of that organisation) to use the SMKI Services and/or SMKI Repository Services.

An ARO's role and responsibilities are likely to be part of their enduring day-to-day roles and responsibilities they are contracted to do with their Party, RDP or DCC (in its role as DCC Service Provider). As the ARO will have direct access to the SMKI Services and/or SMKI Repository Services, each Party, RDP and the DCC (in its role as DCC Service Provider) may wish to consider the individuals nominated, and ensure suitable processes are in place for the levels of access they have within the SMKI Services and/or SMKI Repository.

Additional Information for Responsible Officers

SMKI and Repository Entry Process Testing (SREPT):

Any Party or RDP wishing to undertake SREPT must comply with the security requirements applicable and required of **Testing Participants** set out in the **Enduring Testing Approach Document (ETAD)**. As part of these requirements, and in order for a Party or RDP to gain access to Test Systems, the following must be undertaken:

- The organisation must have completed the procedure(s) to verify their organisational identity for testing purposes as part of the SMKI RAPP;
- An organisation must have at least one **test SMKI SRO** and at least one **test SMKI ARO** appointed for test purposes; and
- Organisations that wish to use the SMKI test Service, must have a test SMKI ARO who has obtained their test credentials for accessing test SMKI Services and/or test SMKI Repository Services.

In November 2014, the SMKI PMA agreed that the SMKI test Service should be assured and separate to the 'Live' SMKI Systems. Consequently, organisations must declare if they are acting as 'Test' or 'Live' SMKI SRO/ARO.

The SMKI Recovery Procedure:

The SMKI Recovery Procedure is a SEC Subsidiary Document, and sets out the procedural requirements and the rights and obligations of the DCC, Parties and the SMKI PMA regarding recovery from the Compromise (or suspected Compromise) of a Relevant Private Key. The scope of the SMKI Recovery Procedure is set out in SEC Section L10 of the Code.

The SMKI Recovery Procedure states that the DCC are required to raise an Incident in the event of a Compromise (or suspected Compromise) of a Relevant Private Key, as set out in the **Incident Management Policy**. As a part of this process, the DCC will contact the Subscriber for any Certificate associated with a Compromised (or suspected Compromised) Relevant Private Key as soon as reasonably practicable, using the contact details held by the SMKI Registration Authority (RA). The DCC shall request confirmation from the Subscriber as to whether they reasonably believe that a Compromise has occurred, and if they wish to proceed with one or more of the recovery processes, which shall be confirmed by:

a) The organisation's SMKI SRO; or

b) In the case of the DCC not operating in its role as a service provider, a SMKI SRO, SMKI RA Manager, or member of SMKI RA Personnel.

Additional Information for Responsible Officers cont.

SMKI Services

The SMKI Interface Design Specification (IDS) is a SEC Subsidiary Document that contains the protocols and technical standards based on open standards. The SMKI IDS defines the technical details of the interfaces to the SMKI Services relating to Authorised Subscribers. As per the SMKI Code of Connection, which is also a SEC Subsidiary Document, only SMKI AROs issued with the appropriate IKI credentials shall be able to access SMKI Services on behalf of their organisation.

The SMKI Portal interface accessed via a DCC Gateway Connection provides an asynchronous mechanism for SMKI AROs to submit Organisation Certificate Signing Requests (CSRs), and Device CSRs, on behalf of their Authorised Subscriber.

The SMKI Portal interface via the Internet provides an asynchronous mechanism for SMKI AROs not accessing the SMKI Service through a DCC Gateway Connection. This provides the means by which Organisation CSRs and Device CSRs can be submitted and retrieved.

The SMKI Repository Interface is designed to allow communications to be sent from, and received by, the SMKI Repository for the purposes of the SMKI Repository Service. Only SMKI AROs are issued with Credentials for accessing the interface on behalf of their organisation.