Smart Energy Code
Section L: Smart Metering Key Infrastructure and DCC Key Infrastructure

SEC Section L provisions concern:

- SEC Parties
- Smart Metering Key Infrastructure Policy Management Authority
- Data and Communications Company
- SEC Panel
- Registered Supplier Agents
- Registered Data Providers

SMKI Policy Management Authority (SMKI PMA)

The SMKI PMA is a **Sub-Committee** of the SEC Panel, and has been established to govern the **SMKI Document Set**, to gain assurance of the DCC's operation and implementation of **SMKI Services,** and to review the **DCCKI Document Set**. **SEC Section L1** sets out the Membership of the SMKI PMA, in addition to its duties and proceedings at meetings.

SEC Section L1.19 outlines the provision for the SMKI PMA and any SMKI PMA Member to be able to submit Modification Proposals in respect of the SMKI SEC Documents.

What Does SEC Section L Cover?

SEC Section L outlines the cryptography related services that will provide GB Smart Metering with a secure and effective means of ensuring that messages to and from Smart Metering Equipment are properly authenticated, provide integrity and, where applicable, provide non-repudiation through the use of Public Key cryptography and Certificates. The Public Key Infrastructures (PKIs) used are referred to as **Smart Metering Key Infrastructure (SMKI), DCC Key Infrastructure (DCCKI) and Infrastructure Key Infrastructure (IKI)**.

SEC Section L outlines the requirements and related services for SMKI, DCCKI and IKI, as well as:

- the duties of the SMKI Policy Management Authority (SMKI PMA);
- the interfaces for SMKI services and obligations on SMKI Participants;
- the assurance of SMKI Services;
- the definition and requirements of the SMKI Recovery Procedure and the SMKI Document Set;
- the Obligations on Eligible Subscribers and the subsequent Relying Party Obligations.

SMKI Assurance

SEC Section L2 sets out obligations on the SMKI PMA and SMKI Participants in relation to the assurance of **SMKI Services**, and how they will demonstrate compliance with the **SMKI Document Set**.

When a SMKI Participant is in material breach of the SMKI Document Set, **SEC Section L2.5** outlines the **Events of Default** of process. For more information, please refer to Events of Default Guidance document.

Emergency Suspension of SMKI Services

SEC Section L2.14 highlights the **Emergency Suspension** of SMKI Services. The SMKI PMA can instruct the DCC to suspend SMKI Services and/or any use of Certificates when it believes there is an immediate threat and risk of material compromise to:

- The DCC Total System;
- Any User System;
- Any Smart Metering System; and/or
- Any Registration Data Provider System.

SMKI Participants

The term **SMKI Participants** refers to:

- The DCC (acting in its capacity as the provider of the SMKI Services);
- Authorised Subscribers; and
- Relying Parties.

All SMKI Participants must comply with the requirements of the SMKI SEC Documents.

Authorised Subscriber

An **Authorised Subscriber** means a Party who can obtain a SMKI Certificate. To become an Authorised Subscriber, a Party must have:

- Organisation Identity successfully verified;
- At least one Senior Responsible Officer (SRO) and Authorised Responsible Officer (ARO); and
- Successfully completed the SMKI and Repository Entry Process Tests.

For more information on the registration process for becoming an Authorised Subscriber please see the **Certificate Policies** and the **Registration Authority Policies and Procedures** (RAPP).

Relying Party

A **Relying Party** is a person who receives and relies upon a SMKI Certificate for the purpose of creating, sending, receiving or processing communications sent to and from a Device or another Party or Registration Data Provider (RDP).

The SMKI Services

The **SMKI Services** means all activities undertaken by the DCC in its capacity as the:

- Device Certification Authority (DCA);
- Organisation Certification Authority (OCA); or
- The IKI Certification Authority (ICA).

Within this capacity, the DCC is required to make available the **SMKI Service Interface**, **SMKI Repository** and **SMKI Repository Interface**.

SMKI Service Interface

SEC Section L4 sets out the provisions for the SMKI Service Interface; a **communications interface** designed to allow messages to be sent between an Authorised Subscriber and the DCC for the purposes of the SMKI Services. The SMKI Service Interface is built according to the **SMKI Interface Design Specification**, which is a SEC Subsidiary document. The **SMKI Code of Connection** explains how an Authorised Subscriber may access the SMKI Service Interface.

SMKI Repository

The SMKI Repository performs a **directory and library function** for SMKI Certificates, Certificate Revocation Lists (CRLs), Authority Revocation Lists (ARLs) and key related SMKI documents, as detailed in **SEC Section L5**.

SMKI Repository Interface

SEC Section L6 establishes the SMKI Repository Interface, the **communications interface** which allows communications to be sent from and received by the SMKI Repository. It is regulated by the **SMKI Repository Interface Design Specification** and **SMKI Repository Code of Connection**.

For more information on the different SMKI Services, please refer to the Overview of SMKI / IKI and DCCKI Guidance.

SMKI and Repository Testing

SMKI and Repository Testing (SRT) tests that the communication systems operated by the DCC, SEC Parties and RDPs can interoperate with each other for SMKI Services and SMKI Repository Services.

A SEC Party or RDP will not be entitled to apply to become an Authorised Subscriber of a Certificate, or access the SMKI Repository, until it has completed the **SMKI and Repository Entry Process Tests (SREPT)**, as set out in **SEC Section L7**.

SREPT (**SEC Party, RDP and non-DCC User(s)**)

- SEC Parties, RDPs and non-DCC Users must successfully complete SREPT on the SMKI Test Service before Live Certificates can be obtained by Authorised Subscribers.
- Once the DCC has confirmed a SEC Party or RDP has completed SREPT, the DCC will confirm this to the SEC Panel.

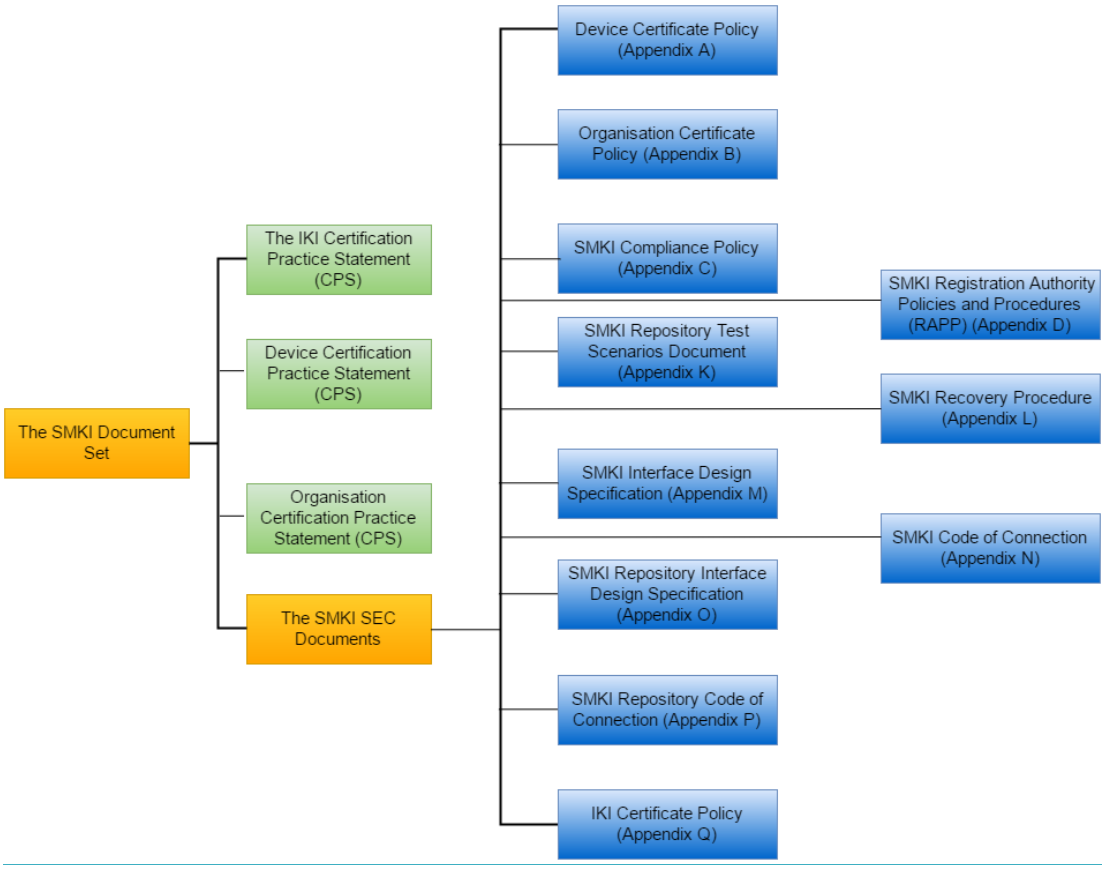
SMKI and Repository Entry Guide

A **SMKI and Repository Entry Guide** will be developed by the DCC to assist SEC Parties or RDPs with the SREPT process. This guide will be published on the DCC website.

The SMKI Document Set

Given the importance of SMKI as a security control on GB smart metering, the SEC Panel, on behalf of SEC Parties and other users of the SMKI Service, need assurance that SMKI Service is being operated in accordance with the **SMKI Document Set**.

Below is a diagram which shows the structure of the **SMKI Documents** within the **SMKI Document Set**. The Document Set also includes relevant sections of SEC itself.



Relying Party Obligations

Relying Parties are required to check Cryptographic Protection in respect of the Organisation **Authority Revocation List** (ARL), **Certificate Revocation List** (CRL) and **IKI CRL and IKI ARL** before relying on a Certificate. Relying Parties should not rely on Certificates that appear on any ARL or CRL, nor rely on Certificates which have expired or are suspected of being Compromised.

Relying Parties also shall take reasonable steps to verify Digital Signatures, check Cryptographic Protection, confirm Validity, and perform all appropriate cryptographic operations before relying on any Organisation Certificate, OCA Certificate, IKI Certificate or ICA Certificate.

SMKI Performance Standards

As provider of the SMKI Services, the DCC are required to meet a number response times for certain activities. These **Target Response Times** are detailed in **SEC Section L8.1**.

Certificate Signing Requests

Upon receipt of a **Certificate Signing Request (CSR)** through the SMKI Service Interface from an Eligible Subscriber, the DCC must send either an Organisation Certificate or Device Certificate within **30 seconds**.

For a **Batched CSR** (a single communication containing CSRs for the issue of more than one but no more than 50,000 Device Certificates), the response time can either be:

- By no later than 08:00 on the following day, if the Batched CSR occurred between the hours of 08:00 and 20:00 on any day over the SMKI Service Interface from an Eligible Subscriber; or
- Within 24 hours of the receipt received, if the Batched CSR did not occur between the hours of 08:00 and 20:00 on any day over the SMKI Service Interface from an Eligible Subscriber.

SMKI Repository Service

The DCC shall send to a SEC Party, the SEC Panel or the SMKI PMA a copy of any document or information stored on the SMKI Repository within **3 seconds** of receipt over the SMKI Repository Interface.

SMKI Recovery Procedure

As the SMKI Service relies on a secure environment, the DCC must ensure that they have a suitable 'recovery plan' in place in the event of failure or Compromise of certain Private Keys. To fulfil this need, the DCC has produced the **SMKI Recovery Procedure**, a SEC Subsidiary Document that forms part of the SMKI SEC Documents.

SEC Section L10 sets out the requirements and provisions for the SMKI recovery process; the proceedings relating to various Compromises for different Private Keys; and, outlines the obligations on the DCC, Parties, RDPs, the SMKI PMA and the Panel.

What will Recovery mitigate?

Recovery will be invoked in any incident where a Relevant Private Key is (or suspected of) being compromised and can involve affected Keys and Certificates, as well as the types of Devices that will be affected. These include, but are not limited to:

- Organisation Certificates;
- Issuing Authorities;
- Root Certificate Authorities; and
- DCC Key used for Recovery.

DCC Key Infrastructure

SEC Section L13 sets out the DCCKI and looks at the Services and activities undertaken by the DCC in its capacity as the **DCCKI Certification Authority**.

The DCCKI Services

In order to submit DCCKI Certificate Signing Requests (CSRs), SEC Parties and RDPs must first become an Authorised DCCKI Subscriber. They do this by following the relevant procedures as set out in the **DCCKI Certificate Policy** and the **DCCKI Registration Authority Policies and Procedures (DCCKI RAPP)** documents. A DCCKI Authorised Subscriber is then recognised as a **DCCKI Eligible Subscriber**.

The DCCKI Service Interface

The DCCKI Service interface is a communication interface to allow DCC Authorised Subscribers and the DCC to send messages between each other. The **DCCKI Code of Connection** obliges the DCC to maintain the DCCKI Service Interface for SEC Parties and RDPs, whilst keeping it available for DCCKI Authorised Subscribers to be able to send and receive communications. Excluding *Planned Maintenance* (**SEC Section H8.3**) the DCC is also to ensure it remains available at all times. Much like the SMKI Interface, the DCCKI Service Interface's technical details are constructed to the requirements of the **DCCKI Interface Design Specification**.

The DCCKI Repository Service

Much like the SMKI Repository, the DCCKI Repository acts as a library and directory for DCCKI CRLs, ARLs and other DCCKI materials such as the DCCKI RAPP as outlined in **SEC Section L13.17**.

The DCCKI Repository Interface

SEC Section L13.24 highlights the provisions for the DCCKI Repository Interface, which is the **communications interface** designed to allow communications to be sent from and received by the DCCKI Repository for the purposes of the DCCKI Repository Service.

The DCCKI PMA Functions

The DCCKI PMA Functions group is responsible for reviewing the effectiveness of the DCCKI Document Set and the related DCCKI CPS, so that they align with SEC Objectives.

The DCCKI PMA members will also ensure they make the SMKI PMA and **Security Sub Committee (SSC)** aware of any notifications or recommendations reached at their meetings, and make available all agendas and supporting documentation to SMKI PMA and SSC members where required.

Certification Practice Statements (CPS)

The DCC, as provider of the SMKI Service, must produce **Certification Practice Statements (CPS)**. A CPS outlines the ways in which the DCC shall issue various SMKI Certificates. There are three CPS in the SEC – the **Device CPS**, **Organisation CPS** and the **Infrastructure Key Infrastructure (IKI) CPS)** (Section L9.7 - L9.19).

The Device CPS sets out the rules and procedures used by the DCC to operate in its capacity as the Device Certification Authority (DCA), who issue Device Certificates. Similarly, **the Organisation CPS** sets out the rules and procedure used by the DCC whilst operating in its capacity as the Organisation Certification Authority (OCA), who issue Organisation Certificates. **The IKI CPS** sets out the policies and procedures of the DCC designed to operate in its capacity as the IKI Certificate Authority (ICA).

Unlike the SMKI SEC Documents, the Device CPS, Organisation CPS and IKI CPS are confidential in nature, and as a result, are approved by the SMKI PMA and are not available to the public.

SMKI Services: Managing Demand (Forecasting)

By the **15th Working Day** for **December, March, June and September**, each Authorised Subscriber of the Device Certificate Policy shall forecast the number of CSRs that they will send to the DCC. This forecast shall contain a breakdown of the total number of single and/or batch CSRs for a Device Certificate.

By no later than the **10th Working Day** following the end of each month, the DCC shall provide reports to the following participants:

- **Each Authorised Subscriber** setting out:
  - The number of CSRs sent by that Authorised Subscriber for Device Certificates during that month; and
  - The actual numbers sent against the numbers most recently forecast for the applicable month.

- The **SEC Panel** setting out:
  - The total number of CSRs sent by all Authorised Subscribers for Device Certificates during that month;
  - A comparison of the actual numbers sent against the numbers most recently forecast for the applicable month; and
  - The number of CSRs sent by any Authorised Subscriber for Device Certificates during that month that is greater than or equal to 110% of the Authorised Subscribers most recent monthly forecast. This should include the identity of each Authorised Subscriber and the number of CSRs sent.

Contact Us:

For all enquires or further advice, please contact SECAS at:

W: smartenergycodecompany.co.uk

T: 020 7090 7755

E: secas@gemserv.com