Smart Energy Code

SEC Overview - SMKI / IKI / DCCKI

Definitions

- **Smart Metering Key Infrastructure (SMKI)** - provides Certificates used for the means of establishing trust and secured communications between Known Remote Parties and Smart Metering Devices traversing the End-to-End Smart Metering System.
- **Infrastructure Key Infrastructure (IKI)** – provides DCC Users and non-DCC Users with credentials used for the purpose of authenticating and securing connection to the SMKI Service Interfaces, and which are used for Digital Signing purposes.
- **DCC Key Infrastructure (DCCKI)** – provides SEC Parties and Registration Data Providers (RDPs) with Certificates used to authenticate and communicate securely with DCC interfaces such as the DCC Gateway Connection, Self-Service Interface (SSI), the Registration Data Interface and the DCC User Interface.

Infrastructure Key Infrastructure (IKI)

Infrastructure Key Infrastructure (IKI) are used to authenticate to the SMKI Interfaces for the purposes of submitting Certificate Signing Requests (CSRs) to the Organisation Certificate Authority (OCA) and/or Device Certificate Authority (DCA) to receive Certificates.

The SMKI Interfaces used by IKI to secure connections are:

- SMKI Portal access over a DCC Gateway Connection
- SMKI Portal Web Service over a DCC Gateway Connection
- SMKI Portal Batched CSR Web Service over a DCC Gateway Connection
- SMKI Portal over the Internet

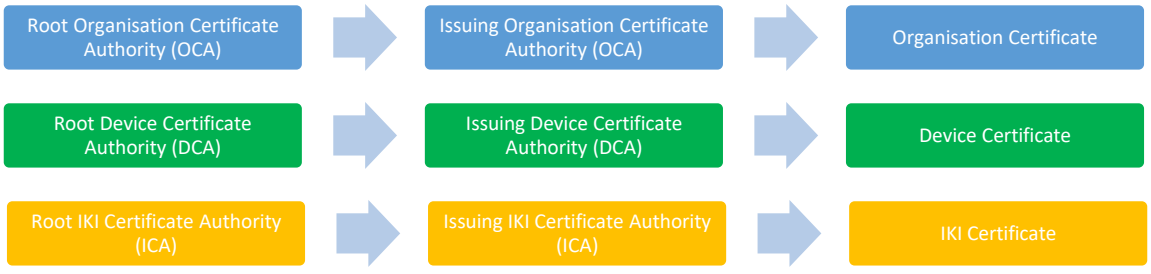
IKI Certificates shall also be used to Digitally Sign files (e.g. Threshold Anomaly Detection (TAD) Files and the Certified Products List (CPL).

Smart Metering Key Infrastructure (SMKI)

Smart Metering Key Infrastructure (SMKI) provides 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.

SMKI is based on existing industry and international Public Key Infrastructure (PKI) standards, mechanisms and principles. PKI is used widely across business sectors where secure transactions are needed (e.g. internet trading and banking transactions).

SMKI effectively 'binds' the identity of Devices and Organisations to (Public) cryptographic keys contained within SMKI Certificates, thereby allowing these to be trusted.



March 2016
Version Number: 1.1

Administered by
Gemserv

DCC Key Infrastructure (DCCKI)

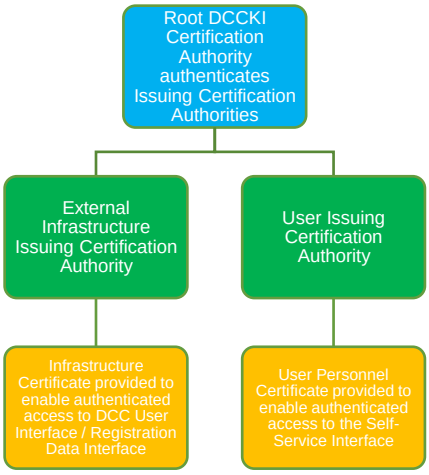
The DCC Key Infrastructure (DCCKI) is a separate key infrastructure arrangement used to manage the identities of SEC Parties and RDPs to secure communications to the DCC interfaces.

DCCKI provides authentication and secure communication between DCC Users and the DCC in relation to Service Requests and associated Service Responses. These communications are subject to specific additional Transport Layer Security (TLS) protection, and which are used established TLS sessions to the DCC User Interface and Registration Data Interface.

DCCKI Certificates are also used to sign the Security Assertion Mark-up Language (SAML) assertions of SEC Parties who wish to use their own Identity Provider Service (IDP) to authenticate SEC Party personnel to the Self Service Interface (SSI).

There are two types of certificates available through the DCCKI:

- **Infrastructure Certificates** – used to establish secure communication channels to DCC interfaces e.g. Registration Data Interface, DCC User Interface, etc.
- **User Personnel Certificates** – obtained via an automated interface to authenticate SEC Party personnel to the Self-Service Interface (SSI).



SMKI Certificates

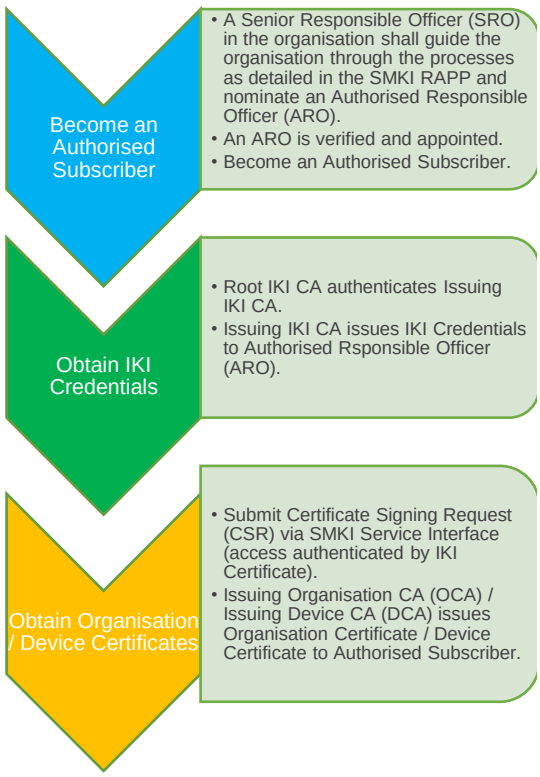
Organisation Certificates are required by DCC Users to sign Great Britain Companion Specification (GBCS) commands to Smart Metering Systems, in a similar way to Devices requiring **Device Certificates** to sign Command responses.

In order to obtain an Organisation Certificate, an **Authorised Subscriber** (a User who has undergone the relevant process as detailed in the SMKI Registration Authority Policies and Procedures (SMKI RAPP) document) will submit a Certificate Signing Request (CSR) via the SMKI Service Interface to the **Organisation Certification Authority (OCA)**.

Each Device will also require a Device Certificate issued by the **Device Certification Authority (DCA)** to the Authorised Subscriber.

The **Certificate Policies** detail the structure and the requirements applicable to each of the Certificate Authorities (CA) – setting out the rules for how the CA operates and how Certificates should be used and issued.

Obtaining SMKI Certificates



Administered by
Gemserv

SMKI / IKI / DCCKI Documents

A number of documents which detail the requirements, policies and procedures for the Key Infrastructure Arrangements are to be included within the SEC as SEC Subsidiary Documents and governed by the SMKI Policy Management Authority (PMA) and the DCCKI PMA.

The table below provides an outline as to the status of each SMKI / IKI / DCCKI document, as if SEC 4.9.

Document	Status
Device Certification Practice Statement (CPS)	Approved
Organisation CPS	Approved
IKI CPS	Approved
Device Certificate Policy	Designated – SEC Appendix A
Organisation Certificate Policy	Designated – SEC Appendix B
IKI Certificate Policy	Designated - SEC Appendix Q
SMKI Compliance Policy	Designated – SEC Appendix C
SMKI RAPP	Designated – SEC Appendix D
SMKI Recovery Procedure	Designated – SEC Appendix L
SMKI Interface Design Specification	Designated – SEC Appendix M
SMKI Code of Connection	Designated – SEC Appendix N
SMKI Repository Interface Design Specification	Designated – SEC Appendix O
SMKI Repository Code of Connection	Designated – SEC Appendix P
SMKI and Repository Test Scenarios Document	Designated – SEC Appendix K
SMKI Recovery Key Guidance	In Development
DCCKI CPS	Approved
DCCKI Certificate Policy	Approved – Awaiting Designation
DCCKI RAPP	Approved – Awaiting Designation
DCCKI Interface Design Specification	Approved – Awaiting Designation
DCCKI Code of Connection	Approved – Awaiting Designation
DCCKI Repository Interface Design Specification	Approved – Awaiting Designation
DCCKI Repository Code of Connection	Approved – Awaiting Designation

The designated SEC Subsidiary Documents can be found here.

Disclaimer

These guides are intended to provide a simple overview of the SEC and any supporting or related arrangements and do not replace or supersede the SEC or these related arrangements in any way. The author does not accept any liability for error, omission or inconsistency with the SEC.

Contact Us:

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

W: smartenergycodecompany.co.uk

T: 020 7090 7755

E: secas@gemserv.com