Version 1.0

SMTES1 Cryptographic Key Management Policy for DLMS Devices

1. Introduction

This document constitutes the SMETS1 Cryptographic Key Management Policy for symmetric keys required to communicate with SMETS1 DLMS devices. The scope of the document covers DLMS devices which form part of the SMETS1 IOC and FOC cohorts.

The SMETS1 MOC cohort is not in scope of this policy as it utilises cryptographic controls provided by a S1SP Public Key Infrastructure (PKI) which falls under the governance of a S1SPKI Certificate Policy and S1SPKI Certification Practice Statement and is subject to TScheme certification and SMKI PMA approval.

Details relating to the cohort specific technical implementation of this policy are detailed in the SMETS1 Security Architecture Document and in each of the cohorts S1SP technical designs. The SMETS1 Security Architecture Document is controlled by the SEC Security Sub Committee (SSC).

DCC shall ensure that Symmetric Keys used in relation to communications with SMETS1 DLMS devices are managed and used in accordance with the requirements of this SMETS1 Cryptographic Key Management Policy.

The assurance of this policy forms a subset of the overarching security requirements defined in SEC Section G for the protection of Total System S1SP's and therefore is subject to the same level of assurance to DCC, SMKI PMA and SSC.

2. Requirement

The SEC requires in L14.7 that the DCC shall, in respect of each SMETS1 Symmetric Key Arrangement, develop a draft of a SMETS1 Cryptographic Key Management Policy, which shall:

(a) be in accordance with the requirements of "A10.1.2 - Key Management" of ISO 27001;

(b) set out the policy on the use, protection and duration of the Symmetric Keys throughout their entire lifecycle;

(c) make provision for managing those Symmetric Keys throughout their entire lifecycle, including in particular provision for generating, storing, archiving, distributing, retiring and destroying them;

(d) specify secure procedures and methods for:

i. generating Symmetric Keys for different cryptographic systems and different applications;
ii. distributing Symmetric Keys to intended recipients;
iii. activating the Symmetric Keys when received;
iv. storing Symmetric Keys and providing access to them for authorised users;
v. changing or updating Symmetric Keys, including provision for how and when they will be changed or updated;
vi. dealing with Compromised Symmetric Keys;
vii. revoking Symmetric Keys, including provision for how and when they are to be withdrawn or deactivated;
viii. recovering Symmetric Keys that are lost or corrupted;
ix. backing-up or archiving Symmetric Keys;
x. destroying Symmetric Keys; and
xi. the logging and auditing of key management related activities.

(a) be in accordance with the requirements of "A10.1.2 – Key Management" of ISO 27001;

This policy is in line with ISO 27001 A10.1.2 – Key Management which states:

A.10 Cryptography

A.10.1 Cryptographic controls

Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

A.10.1.1 A Policy on the use of cryptographic controls for protection of information shall be developed and implemented.

A.10.1.2 Key management: A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.

(b) set out the policy on the use, protection and duration of the Symmetric Keys throughout their entire lifecycle;

(b)(i) Use:

This document constitutes the SMETS1 Cryptographic Key Management Policy for SMETS1 DLMS devices.

DLMS meter types use four symmetric keys to send and receive instructions:

- Master Key (MK):
- Global Unicast Encryption Key (GUEK);
- Authentication Key (AK);
- Dedicated Key (DK)

SMETS1 DLMS devices have 5 separate 'clients' on the meter, these have defined roles:

- Public, used for unauthenticated access to non-sensitive information;
- Data Collection, a read-only interface to collect data from the meter;
- Extended Data Collection, a further interface to collect data from the meter;
- Management, used to make changes to the meter’ s configuration; and
- Firmware, used to update the firmware of the meter.

Each of these clients (except Public) on each SMETS1 DLMS Device must have separate AK and GUEK keys unique to the meter and each client associated with it.

The term 'packaged key' is used for a key that is in a format for storage by the S1SP and use by the DCO and/or S1SP, these will be encrypted using a HSM stored Key Encryption Key.

The following symmetric key types and their uses are defined in this policy for use in SMETS1;

- Master Key (MK): the 'master' or 'key encryption' key for a single DLMS meter. Each SMTES1 DLMS device will have a Master Key (MK) that is used for key rotation.
- Global Unicast Encryption Key (GUEK): the encryption key for a single DLMS client on a single DLMS meter.

- Authentication Key (AK): the authentication key for a single DLMS client on a single DLMS meter.
- Dedicated Key (DK): the 'dedicated' or 'session' encryption key for an authenticated DLMS meter interaction.
- HSM Key: This is a Key Encryption Key stored inside a HSM for the encryption and decryption of symmetric DLMS meter keys stored by S1SPs outside of an HSM. There are two types of HSM Key Encryption Key defined in the SMETS1 Security Architecture:
- DCO Key: a HSM Key Encryption Key only stored in DCO HSM's and used to encrypt MKs and AKs stored at S1SPs.
- Shared Key: a HSM Key Encryption Key stored by both the DCO and S1SP in HSMs. Used to encrypt and decrypt GUEKs and DKs

Each SMETS1 S1SP shall only have access to the GUEK and (if used) DK.

For each command the DCO shall be provided by the S1SP the device specific AK, which must be stored by the S1SP in a packaged form where a DCO Key has been used to encrypt the AK.

In addition, for each command the DCO shall also be provided by the S1SP the GUEK and DK (if used) as required to perform cryptographic operations at the DCO.

(b)(ii) Protection & Cryptographic Processing

The DCC shall ensure that for Cryptographic Processing performed, that:

- is carried out by a SMETS1 Service Provider and involves the use of SMETS1 Global Unicast Encryption Key (GUEK); and
- after Post Migration Key Rotation has completed, is carried out by a DCO and involves the use of a packaged SMETS1 Authentication Key (AK);

Is, in each case, carried out within Cryptographic Modules that are compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

The following encryption schemes must be used:

Symmetric Keys used for SMETS1 Device communication:

- AES_GCM 128 must be used for MKs and AKs
- AES_GCM 128 must be used for GUEKs;

Symmetric keys used for packaging MKs, AKs and GUEKs at the S1SP

- AES_ECB 128 must be used for DCO HSM Keys
- AES_ECB 128 must be used for Shared Keys.

All SMETS1 systems that generate, handle, store or distribute symmetric keys must be protected in line with SEC Section G security controls and assurance requirements.

b(iii) SMETS1 Symmetric Key Lifetime

As soon as reasonably practicable (and in any event within 7 days subject to device connectivity) following the Commissioning of a SMETS1 Communications Hub Function or a SMETS1 Smart Meter or a SMETS1 Gas Proxy Function the S1SP shall, via the DCO, in relation to each such Device and where supported by that Device, re-generate and replace any Authentication Keys and any Encryption Keys held by that Device.

Authentication Keys and any Encryption Keys generated via the DCO, following device commissioning do not subsequently need to be periodically re-generated and replaced during the life of the device. The DCC shall ensure the keys are re-generated and replaced where it is instructed to do so by the SMKI PMA in the following situations;

- As instructed in order to recover from a Major Incident where a compromise of the DCO or S1SP has occurred. PMA will consider as part of this process the need and impact of rotating symmetric keys at the DCO and/or the S1SP.
- If, as part of periodic risk and assurance reviews of the Section G controls at the DCO and S1SPs, relating to the handling of symmetric keys, these controls fall short of the minimum DCC require and where material risks are introduced that would require the re-generation and replacement of device, S1SP and DCO managed symmetric keys.

DCC must complete periodic risk reviews, at no more than 5 year intervals, of all symmetric key use and controls at the DCO and S1SPs, and provide evidence and assurance to SMKI PMA on the continued effectiveness of those controls.

(c) make provision for managing those Symmetric Keys throughout their entire lifecycle, including in particular provision for generating, storing, archiving, distributing, retiring and destroying them;

This policy makes provision for managing Symmetric Keys throughout their entire lifecycle as outlined below in Section (d).

(d) specify secure procedures and methods for:

(i) generating Symmetric Keys for different cryptographic systems and different applications;

Keys must be generated in line with each cohort's S1SP solution and in accordance with Clause 20.1 of SEC Appendix AM (SMETS1 Supporting Requirements) which states that as soon as reasonably practicable (and in any event within 7 days subject to devices connectivity) following the Commissioning of a SMETS1 Communications Hub Function or a SMETS1 Smart Meter or a SMETS1 Gas Proxy Function or a SMETS1 PPMID, the S1SP shall, via the DCO, in relation to each such Device and where supported by that Device, re-generate and replace any Authentication Keys and any Encryption Keys held by that Device.

Symmetric Keys will be automatically requested by each S1SP from the DCO as part of the Device commissioning process, where in relation to each such Device and where supported by that Device, the DCO will generate new Authentication Keys and Encryption Keys for each device DLMS client, with all cryptographic processing being carried out in Cryptographic Modules which are compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

(ii) distributing Symmetric Keys to intended recipients;

Where supported by that Device each Device will have a Master Key (MK) that is used for key rotation and distribution. When AK and GUEK rotation is required as part of the SMETS1 commissioning obligations,

the S1SP and DCO will, where supported by that Device, re-generate and replace any Authentication Keys and any Encryption Keys held by that Device and create a new Key value.

Where supported by that Device the Master Key will be rotated. Details relating to the cohort specific technical implementation of this rotation policy are detailed in the SMETS1 Security Architecture Document and in each of the cohorts S1SP technical designs and security management plans.

In the case of DCO and Shared HSM Key Encryption Keys, where the intended recipient is the DCO or the S1SP, keys will be distributed using appropriate secure transport mechanisms and digital signatures to sign the key packages to ensure the integrity and authentication of the symmetric key material as defined in the security architecture and agreed with the SMKI PMA.

(iii) activating the Symmetric Keys when received;

Where the S1SP, via the DCO, in relation to each such Device and, where supported, by that Device, re-generates and replaces any Authentication Keys and any Encryption Keys held by that Device, all such Symmetric Keys will be considered to be activated immediately.

(iv) storing Symmetric Keys and providing access to them for authorised users;

SMETS1 Symmetric Keys must be stored in compliance with SEC Section G security controls and with all cryptographic processing being carried out within Cryptographic Modules which are compliant with FIPS 140-2 Level 3 (or any equivalent to that Federal Information Processing Standard which updates or replaces it from time to time).

Access to any packed keys must be limited to S1SP Privileged Persons and only for support reasons.

All keys stored in HSMs shall be subject to controls where access is restricted to nominated ACS card holders only.

(v) changing or updating Symmetric Keys, including provision for how and when they will be changed or updated;

Authentication Keys and any Encryption Keys generated via the DCO, where supported by that Device following device commissioning, do not need to be periodically re-generated and replaced during the life of the Device other than as set out under **(b)(iii) SMETS1 Symmetric Key Lifetime** and they will not be changed or updated other than as set out in that section.

(vi) dealing with Compromised Symmetric Keys;

This policy only considers the compromise of SMETS1 Symmetric Keys held at the DCO and S1SP

In accordance with that set out under **(b)(iii) SMETS1 Symmetric Key Lifetime** of this policy, SMKI PMA may consider the need and impact of rotating one or more SMETS1 Symmetric Keys at the DCO and/or the S1SP.

(vii) revoking Symmetric Keys, including provision for how and when they are to be withdrawn or deactivated;

The SMETS1 Security architecture and DLMS Devices do not support the capability to revoke symmetric keys.

(viii) recovering Symmetric Keys that are lost or corrupted;

Should any of a Devices DLMS symmetric keys be corrupted or compromised, the S1SP and DCO will, where supported by that Device, re-generate and replace any Authentication Keys and any Encryption Keys held by that Device and create a new Key value. .

(ix) backing-up or archiving Symmetric Keys;

As laid out in (viii) there is no requirement to backup or archive Symmetric Keys

(x) destroying Symmetric Keys;

The SMETS1 Security Architecture and DLMS Devices do not support the capability to destroy symmetric keys. Instead, the S1SP and DCO will, where supported by that Device, re-generate and replace any Authentication Keys and any Encryption Keys held by that Device and create a new Key value.

(xi) the logging and auditing of key management related activities

The S1SP and DCO systems and infrastructure that process SMETS1 DLMS symmetric keys form part of the wider DCC Total System and are therefore subject to the same obligations relating to Monitoring and Audit as outlined in **SEC Section G Monitoring and Audit (G2.26-G2.30).**

There are two types of logs generated as part of Symmetric key management activities:

- Environment and Infrastructure logs e.g. HSM and ACS access logs, which are subject to protective monitoring requirements.
- Logs generated during application transaction activities (e.g. all actions which involve interaction between DCO, S1SPs and devices for the creation or processing of symmetric keys)

Details relating to the cohort specific technical implementation of this policy are detailed in the SMETS1 Security Architecture Document and in each of the cohorts S1SP technical designs and security management plans.

Defined terms for the purposes of this SMETS1 Cryptographic Key Management Policy

Defined Term	Definition
Administrative Card Set (ACS)	Through smart card sets, security teams establish quorums, or a minimum number of cards that are required to perform a specific task on a HSM. There are two categories of smart card sets in HSM use : an ACS, which is used to authorise administrative tasks and disaster recovery, and one or more Operator Card Sets (OCS), which authorise HSMs to use specific application keys.
AES ECB	Advanced Encryption Standard (AES) Electronic codebook (ECB) is a block cipher mode of operation and is used for efficiency and speed for the packaging of symmetric keys.
AES GCM	Advanced Encryption Standard (AES) Galois/Counter Mode (GCM) is a mode of operation for symmetric-key cryptographic block ciphers which is widely adopted for its performance. AES-GCM is included in the NSA Suite B Cryptography as included in the DLMS specification.
Authentication Key (AK)	An authentication key for a single DLMS client on a SMETS1 Device.
DCO Key	DCO Key: a HSM Key Encryption Key only stored in DCO HSM's and used to encrypt MKs and AKs stored at S1SPs.
Dedicated Key (DK)	A 'dedicated' or 'session' encryption key for an authenticated DLMS meter interaction. Similar to an ephemeral TLS symmetric session key.
DLMS	Device Langue Message Specification. DLMS/COSEM (IEC 62056, EN13757-1) is the global standard for energy & water smart management, advanced control and innovative metering.
Final Operating Capability (FOC)	has the meaning set out in DCC's delivery plan for SMETS1 services produced pursuant to condition 13 of the DCC Licence.
Gamma	Means the secure communications network supported by Gamma Telecom Limited acting as a DCC Service Provider, or any such replacement network.
Global Unicast Encryption Key (GUEK)	An encryption key for a single DLMS client on a single SMETS1 Device.
Hardware Security Module (HSM)	means a Cryptographic Module.
HSM Key	This is a Key Encryption Key stored inside a HSM for the encryption and decryption of symmetric DLMS meter keys stored by S1SPs outside of an HSM. There are two types of HSM Key Encryption Key defined in the SMETS1 Security Architecture. DCO and Shared Keys.
Initial Operating Capability (IOC)	has the meaning set out in DCC's delivery plan for SMETS1 services produced pursuant to condition 13 of the DCC Licence.
Master Key (MK).	An encryption key that is unique to a single SMETS1 Device and that is used for key rotation.
Middle Operating Capability (MOC)	has the meaning set out in DCC's delivery plan for SMETS1 services produced pursuant to condition 13 of the DCC Licence.
Packaged Key	The term 'packaged' is used for a key that is in a format for storage by the S1SP and use by the DCO and/or S1SP, these will be encrypted using a HSM key.
Shared Key.	a HSM Key Encryption Key stored by both the DCO and S1SP in HSMs. Used to encrypt and decrypt GUEKs and DKs.
SMETS1 DLMS Device	A SMETS1 Device that uses DLMS and AES GCM Authenticated encryption. a SMETS1 Communications Hub Function or a SMETS1 Smart Meter or a SMETS1 Gas Proxy Function.

Wrapped Key	The term 'wrapped key' means a new key wrapped using the meter master key for transmission to the meter during key rotation via DLMS