

This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.

# DP296 ‘Alignment with updated ISO standards’

## Annex A

### Legal text – version 0.1

#### About this document

---

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

## Section L ‘Smart Metering Key Infrastructure and DCC Key Infrastructure’

---

These changes have been redlined against Section L version 24.0.

### Amend Section L14.7 as follows (housekeeping change):

#### **The SMETS1 Cryptographic Key Management Policy: Document Development**

L14.7 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 A8.24 "Use of cryptography"~~ of ISO 27001 and 27002;
- (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  - (vii) revoking Symmetric Keys, including provision for how and when they are to be withdrawn or deactivated;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; and

- (e) be developed in accordance with the process set out at Section L14.8. All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorised use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected.
- (f) In addition to integrity, for many use cases, the authenticity of public keys [Symmetric Keys] should also be considered; and
- (h) be developed in accordance with the process set out at Section L14.8.

## Appendix AT 'SMETS1 Cryptographic Key Management Policy for DLMS Devices'

---

These changes have been redlined against Appendix AT version 2.0.

### Amend Section 2 'Requirement' as follows (housekeeping change):

#### 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 A8.24 "Use of cryptography"~~ OF ISO 27001 and 27002;

(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.

(e) All cryptographic keys should be protected against modification and loss. In addition, secret and private keys need protection against unauthorised use as well as disclosure. Equipment used to generate, store and archive keys should be physically protected.

(f) In addition to integrity, for many use cases, the authenticity of public keys [Symmetric Keys] should also be considered; and

(h) be developed in accordance with the process set out at Section L14.8.

~~(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;~~

### **3. Use**

~~(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 ~~SMETS1~~ SMETS1 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.

#### 4. Protection and Cryptographic Processing

##### (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.

## **5. SMETS1 Symmetric Key Lifetime**

### **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.

**(ea) 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 **(bd)**.

**(bd) 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, regenerates 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 Device's 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