G2 SYSTEM SECURITY: OBLIGATIONS ON THE DCC

Cryptographic Processing

G2.44 The DCC shall ensure that all Cryptographic Processing which:

(a) is for the purposes of complying with its obligations as CoS Party;

(b) results in the application of a Message Authentication Code to any message in order to create a Command to be sent to a SMETS2+ Device;

(c) is carried out by a DCO and involves the use of a SMETS1 Symmetric Key;

~~(b)~~(d) involves the use of a DCC Private Key to establish any Transport Layer Security for the purposes of communicating with a SMETS1 Device; or

~~(c)~~(e) (other than in any of the circumstances set out in paragraph G2.44A) is carried out by a SMETS1 Service Provider and involves the use of a SMETS1 Symmetric Key,

is 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).

G2.44A For the purposes of Section G2.44(e), the circumstances set out in this Section shall be those in which one of the following occurs:

(a) Cryptographic Processing is carried out by a SMETS1 Service Provider to generate a Command to "add credit" (as specified in a Version of the SMETS with a Principal Version number of 1) to a SMETS1 Device;

(b) a SMETS1 Symmetric Key is used by a SMETS1 Service Provider to generate an Instruction where the target Device is identified in the SMETS1 Supporting Requirements as a Category 1 Device for the purposes of this paragraph (b); and

(c) a SMETS1 Symmetric Key is used by a SMETS1 Service Provider where:

(i) that Symmetric Key is valid only for the duration of a single Application Association; and

(ii) the target Device is identified as a Category 2 Device for the purposes of this sub-paragraph in the SMETS1 Supporting Requirements.

G2.45 The DCC shall ensure that it carries out all ~~other~~ Cryptographic Processing which does not fall within the scope of Section G2.44 only within Cryptographic Modules established in accordance with its Information Classification Scheme.

Section A1 – New and Amended Definitions

Application Association

has the meaning given to that expression in the Green Book (DLMS UA 1000-2 Ed. 8), published by the DLMS User Association.

Authentication Key

has the meaning given to that expression in the Green Book (DLMS UA 1000-2 Ed. 8), published by the DLMS User Association.

Cryptographic Processing

means the generation, storage (other than of Secret Key Material used in relation to communications with a SMETS1 Device, where that Secret Key Material is encrypted) or use of any Secret Key Material.

Instruction

means, in respect of a SMETS1 Device, a communication generated by the SMETS1 Service Provider or a DCO following receipt of a SMETS1 Service Request by the DCC that is designed to instruct the Device to execute the functionality necessary to permit the DCC to take the necessary Equivalent Steps.

SMETS1 Symmetric Key

means an Authentication Key or a symmetric key which is in either case used to process communications with SMETS1 Devices.

Transport Layer Security

means TLS 1.2 as defined in the Internet Engineering Task Force (IETF) Request For Change (RFC) 5246 or any equivalent to that document which updates or replaces it from time to time.