**Version 2.1**

**Appendix AS**

**ECoS Transition and Migration Approach Document**

# Introduction and General Obligations

This Appendix is the ECoS Transition and Migration Approach Document (**ETMAD**), the first version of which is developed by the Secretary of State pursuant to Section G11 of the Code.

Where directed to do so by the Secretary of State from time to time, the DCC shall develop and consult upon a further draft or drafts of this ETMAD and submit it to the Secretary of State in accordance with the process set out in Section G11.6 of the Code

# Defined Terms and Interpretation for the purposes of ETMAD

|  |  |
| --- | --- |
| XML User Role MPID Signing Key | means a Private Key associated with a Public Key that is contained within an Organisation Certificate that:   1. has a Remote Party Role of “xmlSign”; and 2. has within the X520 Common Name field (with the meaning ascribed to that term in the Organisation Certificate Policy) one or two Market Participant Identifiers by which the Subscriber for that Certificate may be identified in the Party Details. |

1. **Transitional Application of Sections of the Code**

Whilst this ETMAD remains in force:

* 1. In Section G2 (System Security: Obligations on the DCC):
     1. Sections G2.20 and G2.21 shall be replaced with the following paragraphs: “G2.20 The DCC shall ensure that:
        1. all DCC Systems which form part of the DCC Total System are Separated from any other Systems;
        2. the DCC IT Testing and Training Systems and DCC IT Supporting Systems are Separated from the DCC Live Systems; and
        3. subject to the provisions of Sections G2.21 and G2.22, each DCC Individual Live System is Separated from each other such System.

G2.21 The DCC Individual Live System referred to at paragraph (c) of the definition of DCC Live Systems in Section A1 (Definitions) need not be Separated from the DCC Individual Live System referred to at paragraph (a) of that definition to the extent that it uses that System referred to at paragraph (a) solely for the purposes of confirming the relationship between:

1. an MPAN or MPRN and any Party Details;
2. an MPAN or MPRN and any Device; or
3. any Party Details and any User ID.”.
   * 1. Sections G2.22A to G2.22E shall not apply.
   1. Section G2.52 shall not apply and in section G2.54, the words “and shall publish the replacement version on the DCC Website” shall not apply, and instead, the DCC shall ensure that the latest version of the ECoS Interface Specification, any previous changes to it, and the supporting Security Impact Assessments are made available to the DCC Independent Security Assessment Service Provider on request for the purposes of carrying out a DCC Security Assessment.
   2. In Section G6 (Anomaly Detection Thresholds: Obligations on the DCC and Users), Section G6.6A shall not apply.
   3. In Section L3 (The SMKI Services), remove the row relating to the coSPartyXmlSign from the table immediately following Section L3.18 (b)(ii).











* 1. In Section L3 (The SMKI Services), Section L3.18 (b) shall be replaced with the following:

‘(b) if the value of the X520OrganizationalUnitName field in that Certificate is a Remote Party Role corresponding to that listed in the table immediately below, either:

* + 1. that person is the DCC, it is the Party identified with that Remote Party Role in the second column of that table, the Certificate Signing Request originates from the individual System referred in the paragraph of the definition of DCC Live Systems identified in the fourth column of that table, and the Certificate is to be issued to the same individual System from which the Certificate Signing Request originates; or
    2. that person is identified with that Remote Party Role in the second column of that table, and the value of the subjectUniqueID field in the Certificate is a User ID or RDP ID associated with any such User Role or with an RDP as may be identified in the third column of that table; or
    3. subject to the requirements of sub-paragraph L3.18(c), that person is the ECoS Service Provider, the Remote Party Role is “transitionalCoS” and the Certificate Signing Request originates from the ECoS Service Provider systems.
  1. In Section L3 (The SMKI Services), Section L3.18 shall be supplemented with the following:

‘(c) For the purposes of subparagraph L3.18(b)(iii):

* + 1. ECoS Service Provider has the meaning given to that term in Appendix AR (SEC Variation Testing Approach Document for the Enduring Change of Supplier Arrangements); and
    2. prior to the submission of any Certificate Signing Request, and having taken account of the views of the Security Sub-Committee, the SMKI PMA has given approval for an Organisation Certificate to be issued to the ECoS Service Provider systems; and
    3. the DCC shall comply with any conditions that may be specified by the SMKI PMA in its approval under L3.18(c)(ii).
  1. In Annex A to Section L (Smart Metering Key Infrastructure and DCC Key Infrastructure) remove the row relating to coSPartyXmlSign from the table.



# Reporting

The DCC shall, within one week of the last day of (i) November 2021 (or such later month as may be directed by the Secretary of State), and (ii) every month thereafter, produce and submit to the Secretary of State and Security Sub-Committee, a report setting out which Users that have submitted one or more “CoS Update Security Credentials” Service Requests in that month, did not Digitally Sign all such Service Requests with an XML User Role MPID Signing Key.

# Provision of Information to the DCC

Each Supplier Party shall, on request from the DCC and within such reasonable time period as the DCC may specify, provide such information as may be reasonably required by the DCC to enable it to plan, co-ordinate, and undertake (and provide ongoing support for) ECoS Migration.

For the purposes of clause 5.1, 'ECoS Migration' shall have the meaning given to that term in Section G11 of this Code.