MP251 'Transfer of Secret Key Material'

Annex A

Legal text – version 1.0

About this document

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

Appendix S 'DCCKI Certificate Policy'

These changes have been redlined against Appendix S version 5.0.

Amend Clause 1.4 as follows:

1.4 USAGE OF DCCKI CERTIFICATES

1.4.1 Appropriate Certificate Uses

(a) The DCCKICA shall ensure that DCCKICA Certificates are Issued only to:

(i) the Root DCCKICA for use in its capacity as, and for the purposes of, exercising its functions as the Root DCCKICA; and

(ii) the EII DCCKICA and the UI DCCKICA, in their capacity as, and for the purposes of exercising the functions of, issuing authorities.

(b) Subject to 1.4.1 (e), the DCCKICA shall ensure that DCCKI Infrastructure Certificates are Issued only:

(i) by the EII DCCKICA, and to DCCKI Eligible Subscribers; and

(ii) for the purposes of:

(1) establishing TLS communications with the DCC over a DCC Gateway Connection; or

(2) the signing of SAML assertions of a User that chooses to Authenticate its User Personnel to the Self Service Interface using an Identity Provider Service that is not provided by the DCC~~.~~; or

~~(2)~~(3) supporting the Transfer of Secret Key Material as defined in Section G2.22F to G2.22I.

(c) Subject to 1.4.1 (e), the DCCKICA shall ensure that Personnel Authentication Certificates are Issued only:

(i) by the UI DCCKICA, and to DCCKI Eligible Subscribers; and

(ii) for the purpose of Authenticating User Personnel of Users intending to use the Identity Provider Service provided by the DCC to the Self Service Interface.

(d) Further provision in relation to Parties and RDPs obligations in respect of the use of DCCKI Certificates is made in Sections L13.43 to L13.47 (The DCCKI Subscriber Obligations) of the Code and Sections L13.48 to L13.52 (The DCCKI Relying Party Obligations) of the Code.

(e) Nothing in this DCCKI Certificate Policy shall prevent DCC from:

(i) using the Root DCCKICA Certificate for the purposes of issuing additional issuing authority certificates;

(ii) using those issuing authorities to issue additional end entity certificates; or

(iii) issuing DCCKI Infrastructure Certificates or Personnel Authentication Certificates to DCC or DCC Service Providers other than in accordance with this Policy;

provided that in any of the above cases DCC may only do so:

(iv) for the purposes of issuing DCCKI Certificates or other certificates as may be required to establish secure communications between DCC and DCC Service Providers, or to secure communications and data within DCC Service Providers, but not between either DCC or a DCC Service Provider and any other Party or RDP; ~~and~~

(v) to the extent set out in the DCCKI Certification Practice Statement~~.~~; and

~~(v)~~(vi) other than in the cases specified in 1.4.1(a) to (c) above, subject to SMKI PMA approval.