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.

# MP261 'Extending the Organisation Certificate Validity Period'

# 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.

# Section L 'Smart Metering Key Infrastructure and DCC Key Infrastructure'

These changes have been redlined against Section L version 21.0.

## Amend Section 11.4 as follows:

**Certificate Signing Requests**

L11.4 No Eligible Subscriber may make a Certificate Signing Request for the Issue of:

(a) a Device Certificate or DCA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other Device Certificate or DCA Certificate;

(b) subject to Section 11.4A, an Organisation Certificate or OCA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other Organisation Certificate or OCA Certificate (except in the case of the Root OCA Certificate to the extent to which it is expressly permitted in accordance with the Organisation Certificate Policy); or

(c) an IKI Certificate or ICA Certificate which contains the same Public Key as a Public Key which that Eligible Subscriber knows to be contained in any other IKI Certificate or ICA Certificate.

L11.4A Subject to 11.4B, the DCC may submit a Certificate Signing Request for, and may Issue, an Organisation Certificate that has the same Public Key as an existing Organisation Certificate.

L11.4B The circumstances in which 11.4A applies are:

(a) that the SMKI PMA (having taken into account the views of the Security Sub-Committee) has given approval for a Certificate to be Issued that contains the same Public Key as an existing Organisation Certificate; and

(b) the Remote Party Role Code for that Certificate is either: "recovery", "transitionalCoS", "wanProvider", or "accessControlBroker".

# Appendix B 'Organisation Certificate Policy'

These changes have been redlined against Appendix B version 8.0.

**Amend Section 6.3 as follows:**

## 6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

### 6.3.1 Public Key Archival

(A) The OCA shall ensure that it archives OCA Public Keys in accordance with the requirements of Part 5.5 of this Policy.

### 6.3.2 Certificate Operational Periods and Key Pair Usage Periods

(A) The OCA shall ensure that the Validity Period of each Certificate Issued by it shall be as follows:

(i) in the case of an Organisation Certificate, 10 years or, a different duration in circumstances approved by the SMKI PMA (having taken into account the views of the Security Sub-Committee);

(ii) in the case of an Issuing OCA Certificate, 25 years; and

(iii) in the case of a Root OCA Certificate, 50 years.

(B) For the purposes of paragraph (A), the OCA shall set the `notAfter` value specified in Annex B in accordance with that paragraph.

(C) The OCA shall ensure that no OCA Private Key is used after the end of the Validity Period of the Certificate containing the Public Key which is associated with that Private Key.