This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

MP168 'CPL Security Improvements'

Annex A

Business requirements – version 0.4

About this document

This document contains the business requirements that support the solution(s) for this Modification Proposal. It sets out the requirements along with any assumptions and considerations. The DCC will use this information to provide an assessment of the requirements that help shape the complete solution.

1. Business requirements

This section contains the functional business requirements. Based on these requirements a full solution will be developed.

Business Requirements	
Ref.	**Requirement**
1	The DCC shall publish the Infrastructure Key Infrastructure (IKI) Certificate Revocation List (CRL) on-line for a range of uses that require authentication via IKI (e.g. Central Products List (CPL) submissions)
2	Any organisation that needs to authenticate IKI Certificates is given access to and is required to check the CRL when receiving requests authenticated with an IKI Certificate
3	It shall be possible for non-Smart Energy Code (SEC) Parties (e.g. Device Manufacturers) to apply for Certificates

2. Considerations and assumptions

This section contains the considerations and assumptions for each business requirement.

2.1 General

This solution aims to improve the authentication of communications submitting new entries to the Central Products List (CPL) that include a Manufacturer Image Hash and/or if a Commercial Product Assurance (CPA) Certificate has been previously used. This will ultimately improve the CPL security controls.

This modification does not intend to alter current elements of the process that Device Manufacturers must follow when signing their Manufacturer Images, other than that they will be required to do this via IKI Certificates, rather than using another reputable Certificate Authority. Suppliers or the DCC will be required to countersign CPL submissions with an IKI Certificate using the X.509 format. These IKI Certificates must be compatible with standard software packages such as Microsoft.

2.2 Requirement 1: The DCC shall publish the IKI CRL on-line for a range of uses that require authentication of IKI

Use cases have arisen that would benefit from the IKI CRL being published on-line to allow non-DCC Users to use IKI as means of authentication. These would improve security controls and help parties maintain compliance with the SEC security arrangements. These use cases include using the IKI CRL to authenticate CPL submissions beyond all reasonable doubt.

The Security Sub-Committee (SSC), with support from the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA), wishes to address these use cases by publishing the IKI CRL on-line to enable non-DCC Users to use IKI as a secure means of authentication.

However, currently SEC Appendix Q 'IKI Certificate Policy' section 4.9.9 explicitly states that the IKI CRL shall not be supported on-line. Therefore, this area of the SEC must be updated if this solution is approved.

2.3 Requirement 2: Any organisation that needs to authenticate IKI Certificates is given access to and is required to check the CRL when receiving requests authenticated with an IKI Certificate

Parties will require access to an on-line version of the IKI CRL. However, organisations such as the SEC Panel and SECAS who going forward will rely on the IKI Certificates to verify CPL Submissions are not SEC Parties or Registration Data Providers (RDPs). Therefore, the SEC needs an amendment to support the IKI CRL being made available to any organisation that needs to authenticate IKI Certificates.

Appendix Q sets out the arrangements for **Relying Parties** to check the CRL, mainly in sections 4.9.6 and 4.9.7. However, the main reference is to Section L12 to define a Relying Party. Based on these SEC references, the DCC will need to make the CRL available to:

- Suppliers, in the case of a Device which relies on a Certificate;
- The DCC, in the case of a Communications Hub Function or Gas Proxy Function which relies on a Certificate;
- Device Manufacturers, who are Parties who must use IKI to sign CPL submissions;
- The SEC Panel, who are required to authorise CPL submissions; and
- The Smart Energy Code Administrator and Secretariat (SECAS) who carry out this activity on behalf of the Panel.

2.4 Requirement 3: It shall be possible for non-SEC Parties to apply for Certificates

Device Manufacturers do not currently need to become SEC Parties. Therefore, a process needs to be developed that allows non-SEC Parties to obtain Certificates. Whilst it is acknowledged that a new process will be required to deliver this requirement, it should not impact the requirements that Device Manufacturers must follow when signing their Manufacturer Images.

3. Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	**Full term**
CPA	Commercial Product Assurance
CPL	Central Products List
CRL	Certificate Revocation List
DCC	Data Communications Company

Glossary	
Acronym	**Full term**
IKI	Infrastructure Key Infrastructure
RDP	Registration Data Provider
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SSC	Security Sub-Committee