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.

MP104 'Security Improvements'

Legal text – version 0.1

About this document

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

Section A 'Definitions and Interpretation'

These changes have been redlined against Section A version 14.0.

Add Section A as follows:

Wide Area Network (WAN) Provider	means the DCC, acting in the capacity and exercising the functions of the Kn Remote Party role identified as such in the GB Companion Specification.
Working Day	means any day other than a Saturday, a Sunday, Christmas Day, Good Friday, or a day that is a bank holiday within the meaning of the Banking and Financial Dealings Act 1971.
Working Group	has the meaning given to that expression in Section D6.2 (Establishment of a Working Group).
Working Group Terms of Reference	has the meaning given to that term in Section D6.2 (Establishment of a Working Group).
XML User Role Signing Key	means a Private Key associated with a Public Key that is contained within an Organisation Certificate with a remote Party Role of "xmlSign".
Zigbee Alliance	means the association of that name administered by ZigBee Alliance Inc (2400 Camino Ramon, Suite 375, San Ramon, CA 94583, USA) (see - www.zigbee.org).

Formatted: Font: Expert Sans, 9.5 pt

Formatted: Font: Expert Sans, 9.5 pt

Formatted: Font: Expert Sans, 9.5 pt

Formatted: Font: Expert Sans, 9.5 pt

Formatted: Font: Expert Sans, 9.5 pt

Formatted: Font: Expert Sans, 9.5 pt

Formatted: Font: Expert Sans, 9.5 pt

Appendix AD 'DCC User Interface Specification'

These changes have been redlined against Appendix AD version 4.0.

Add Section 3.3.1 as follows:

3.1. Key Cryptographic Operations

The following cryptographic operations protect all DUIS XML format messages that are sent and received by Users across the DCC User Interface and are in addition to those specified within the GB Companion Specification which are used to Digitally Sign Commands.

The DCC and each User shall Digitally Sign all DUIS XML format messages using the following method for each of the DUIS signing activities listed below. All these DUIS signing activities shall be performed using the Elliptic Curve Digital Signature Algorithm (ECDSA) on the P-256 curve, with the corresponding public keys being certified under the auspices of the Smart Meter Key Infrastructure (SMKI).

Each DUIS XML format message shall be signed with a Digital Signature (XMLDSig). There are a number of parameters that are required as part of the algorithm, these parameters define the transform, canonicalization, signing, and digest algorithms to be used, as well as the XML node which is signed. Note that the Reference URI is defined as "", which indicates that signature applies from the root of the document.

Parameter	**Value**
Reference URI	""
Transform Algorithm	http://www.w3.org/2000/09/xmldsig#enveloped-signature
CanonicalizationMethod Algorithm	http://www.w3.org/2001/10/xml-exc-c14n
SignatureMethod Algorithm	http://www.w3.org/2001/04/xmldsig-more#ecdsa-sha256
DigestMethod Algorithm	http://www.w3.org/2001/04/xmlenc#sha256

3.3.1. DUIS XML Service Request Signing

The User shall Digitally Sign each~~every~~ XML ~~format~~ Service Request and Signed Pre-Command ~~sent to the DCC~~ using an XML User Role Signing Private Key. ~~This must be a separate dedicated Key that shall not be used for communication with Devices (i.e. different to that used to sign the GBCS Payload held within Signed Pre-Commands). A separate User Role Signing Private Key must be used per User Id in use for each User."~~

~~Each User shall notify the DCC of the Organisation Certificate corresponding to each User Role Signing Private Key that they wish to use for Digitally Signing communications to the~~

~~DCC in accordance with the paragraph above.~~The DCC shall check that the User has used an XML User Role Signing Private Key to Digitally Sign each Service request and Signed Pre-Command and shall cease processing the communication if this is not the case and shall notify the User.

3.3.2. Transform Service Response Signature Validation

The DCC shall Digitally Sign all XML format Service Responses containing Pre-Commands sent to Users using a DCC Transform Private Key. This must be a separate dedicated key that shall not be used for communication with Devices.

The DCC shall notify Users of the Organisation Certificate used for Digitally Signing communications to Users in accordance with the above paragraph.

The User shall verify the Digital Signature of Pre-Commands sent by the DCC (this includes Certificate status checking and the Confirm Validity check of the Public Key Certificate of the DCC Transform Service).

3.3.3. DCC Signed Service Responses

The DCC shall Digitally Sign the following XML format Service Responses sent to Users, using a DCC Access Control Broker Private Key. This will be a separate dedicated key that shall not be used for communication with Devices.

- DCC Alert messages originating from the DCC;
- Service Responses to Non-Device Service Requests that return data within the body of the Response;
- Service Responses returning a Command for Local Delivery;
- Service Responses containing Responses to Commands created by a DCC Schedule; and
- Service Responses containing Responses to DCC issued Commands on behalf of an Unknown Remote Party. Also applicable to Service Requests 6.21 (Request Handover Of DCC Controlled Device), 6.23 (Update Security Credentials (CoS)), 6.24.1 (Retrieve Device Security Credentials (KRP)), 8.5 (Service Opt Out), 8.9 (Read Device Log) where the Target Device Type is HCALCS and 8.12.2 (Restore GPF Device Log)

The DCC shall notify Users of the Organisation Certificate used for Digitally Signing communications to Users in accordance with the above paragraph.

The User shall verify the Digital Signature of DCC Signed Service Responses (this includes Certificate status checking and the Confirm Validity check of the Public Key Certificate of the DCC Access Control Broker).

3.3.4. Requests

This section defines the formats for Service Requests and Signed Pre-Commands and the Common Objects (i.e. header data items, data types) contained within them.

The Request Types described in this section are as follows:

- Device Requests (Critical)
- Device Requests (Non Critical)
- Non-Device Requests
- Signed Pre-Commands

The more detailed data attributes associated with each Service Request are contained within clause - **Error! Reference source not found.**.

Users shall construct Service Request and Signed Pre-Commands in accordance with the description within this section (general requirements) and **Error! Reference source not found.** (request specific requirements).

The DCC shall respond to all Service Requests and Signed Pre-Commands from Users synchronously. All other responses (solicited and unsolicited) are returned asynchronously.