Data Communications Company

SEC Modification Proposal, SECMP0170, DCC CR4435

Firmware updates to Point to Point Alt HAN Devices

Preliminary Impact Assessment (PIA)

Version:	**1.0**
Date:	**30th September 2021**
Author:	**DCC**
Classification:	**DCC PUBLIC**

Contents

1   Executive Summary

The Change Board are asked to approve the following:

- Total cost to complete the Full Impact Assessment of £86,007.

- The timescales to complete the Full Impact Assessment of 40 working days.

- ROM costs for MP170 (using DCC recommended Option 1 solution approach), up to the end of Pre-Integration Testing (PIT) of up to £636,500.

Problem Statement and Solution

Point to Point (P2P) Alt HAN Devices are being developed that will act as a range extender to offer a solution in situations where one, or both, of the gas meter (GSME) or In Home Display (IHD)/ Prepayment Metering Interface Device (PPMID) are out of range of the Home Area Network (HAN).

The SEC does not currently support remote firmware updates to Alt HAN P2P Devices.

Without the ability to perform a remote firmware upgrade, new innovations and functionality to improve the service to consumers will not be cost effective. Additionally, if a security defect is identified then an Over-the-Air (OTA) firmware update to fix the defect would be quicker and cheaper than a site visit and thus reduces the length of time that a consumer's premise is a security risk.

The objective of this Modification is to introduce support for OTA firmware updates for the Alt HAN P2P Devices within DCC Total Systems.

Modification Benefits

Following are the benefits of providing remote firmware updates to Alt HAN P2P Devices.

- Risk mitigation - OTA firmware updates enable the User to remedy faults, fix security issues without a site visit which can avoid partial/mass recall of Alt HAN P2P Devices.

- Delivering future change – OTA firmware updates are also needed to support and deliver innovative advancements within the Alt HAN and DCC ecosystems. If OTA firmware updates are not possible, this would limit the opportunity for future innovation for Alt HAN P2P Devices as well as other Devices that would rely on them.

- Reduces Impact on Consumers – Without OTA firmware updates, any changes needed will rely on Engineer's site visits to consumer premises which is inconvenience to consumers and incur additional cost to industry Parties.

2   Document History

2.1   Revision History

Revision Date	Revision	Summary of Changes
29/09/2021	0.1	Initial version, for DCC internal review
30/09/2021	0.2	Updated following DCC internal review
30/09/2021	0.3	Updated following further DCC internal review
30/09/2021	1.0	For SECAS review

2.2   Associated Documents

This document is associated with the following documents:

Ref	Title and Originator's Reference	Source	Issue Date
1	DP170 Modification Report	SECAS	17/06/2021
2.	MP170 Business Requirements v0.3	SECAS	17/08/2021

References are shown in this format, [1].

2.3   Document Information

The Proposer for this Modification is David Jones of AltHANCo. The proposal was submitted in June 2021. Following the Working Group meeting, the business requirements were discussed at the Technical Architecture and Busines Architecture Sub-Committee (TABASC) and the Preliminary Impact Assessment (PIA) was requested of DCC on 13th August 2021. This is issued as DCC CR 4435.

3   Context and Requirements

In this section, the context of the Modification, assumptions, and the requirements are stated.

The requirements have been provided by SECAS, the Proposer and the Working Group.

3.1   Current Arrangements

The Alternative Home Area Network (Alt HAN) solution is being developed to address situations where one, or both, of the gas meter or In Home Display (IHD)/Prepayment Metering Interface Device (PPMID) are out of range of the Communications Hub (Comms Hub), using Alt HAN Point to Point (P2P) Devices.

AltHANCo. uses four different P2P Device Types (B1, B2, B3, B4) known as 'bridges' - these acts as range extender and are configured in different ways depending on the set up of the premises. There will be either two or three P2P Devices at each premise to provide a solution – this is dependent on a number of factors:

- Whether it is the IHD or GSME that is out of range of the HAN;
- Whether the IHD and GSME are close together;
- Whether the GSME has a nearby electricity source.

Each bridge joins the ZigBee network as a range extender to transfer traffic. This is achieved via whitelist functionality and performed by Service Users by sending existing DCC User Interface Specification (DUIS) Service Requests.

3.2   What is the issue?

The SEC does not currently support firmware updates to Alt HAN P2P Devices. Without the ability to perform a remote firmware upgrade new innovations and functionality to improve the service to consumers will not be cost effective. Additionally, if a security defect is identified then an OTA firmware update to fix the defect would be quicker than a site visit and thus limits the length of time that a consumer's premise is a security risk.

3.3   Impact of the issue

Risk mitigation - OTA firmware updates enable the User to remedy faults on a Device without the need for a site visit. There is a risk that an Alt HAN P2P Device may lose its ability to communicate if there is a ZigBee stack upgrade that needs to be applied to fix a security related issue. This would lead to a mass recall of Alt HAN P2P Devices if there was not a remote firmware update capability.

The costs associated with either of these events would vary depending on the stage of the rollout but highlighted as significant should there be an issue that requires either a partial or a mass recall. If the capability for an OTA firmware update is available, then it is envisaged that these issues could be addressed remotely and in a much shorter timeframe than Device replacement.

Future changes - Smart Metering requirements continue to change as the Smart Metering Implementation Programme (SMIP) evolves. OTA firmware updates are needed to support and deliver innovative advancements within the Alt HAN and DCC ecosystems. If OTA firmware updates are not

possible this would limit the opportunity for future innovation for Alt HAN P2P Devices as well as other Devices that would rely on them. Additionally, developments in security features would not be able to be rolled out without a Device being physically exchanged via site visit.

Impact on Consumers - If OTA firmware updates are not possible then any changes needed will rely on site visits to consumer premises. This is an inconvenience to consumers to accommodate an onsite visit and additional cost to Industry Parties.

3.4 Business Requirements

After the discussion of this proposal in different fora such as Working Group (WG), Technical Architecture and Business Architecture and Sub-Committee (TABASC), the following list of business requirements are identified.

Ref	Requirement	Impacted Party
1	AltHANCo shall be able to develop and assure firmware upgrades for Alternative Home Area Network (Alt HAN) Point to Point (P2P) Devices.	AltHANCo
2	Energy Suppliers shall be able to deploy Over-The-Air (OTA) firmware upgrades for Alt HAN P2P Devices over the Smart Metering System.	DCC/ Suppliers
3	Energy Suppliers shall keep AltHANCo up to date following any Alt HAN P2P Device firmware upgrades.	DCC/ Suppliers
4	DCC shall provide AltHANCo with reports on deployed firmware versions.	DCC
5	The DCC shall be able to maintain records on firmware deployments and current firmware versions of Alt HAN P2P Devices.	DCC
6	Energy Suppliers shall be able to confirm that Firmware upgrades for Alt HAN P2P Devices have been successful.	DCC/ Suppliers
7	Energy Suppliers shall be able to read the current Firmware version on Alt HAN P2P Devices.	DCC/ Suppliers
8	Energy Suppliers shall be able to replace any Smart Metering Key Infrastructure (SMKI) credentials on Alt HAN P2P Devices.	DCC/ Suppliers
9	Alt HAN P2P Devices shall be resilient to the deployment of firmware to other Alt HAN P2P Devices in any order of deployment within a Home Area Network (HAN).	AltHANCo
10	Alt HAN P2P Devices shall minimise the impact to other Devices on the HAN.	AltHANCo
11	DCC and Energy Suppliers shall be able to distinguish Alt HAN P2P Devices from other Devices	DCC/Suppliers
12	The DCC shall ensure that only known Firmware images are sent to Alt HAN P2P Devices	DCC/AltHANCo

4 Description of Solution

The following sections give an overview of the high-level outline solution created to support the PIA discussion and associated PIA responses from DCC and its Service Providers, along with considerations of design assumptions with the solution.

4.1 High Level Architecture

The objective of this Modification is to add support for OTA firmware updates to the Alt HAN P2P Devices for SMETS2+ Devices. Two solution options are proposed.

- **Option 1**, where the Alt HAN P2P Device is considered as a Prepayment Metering Interface Device (PPMID), and;

- **Option 2**, where the Alt HAN P2P Device acts as if it were a Consumer Access Device (CAD).

4.1.1 Option 1: Alt HAN P2P Device is considered as a Prepayment Metering Interface Device (PPMID)

In this approach, assumption is that the Alt HAN P2P Devices will be treated in the same way as PPMIDs by the Comms Hubs. Comms Hub allows up to six Type 1 Devices (PPMID or HCALCS) and this approach reuses SECMP0007 capability and avoids the need for making any changes to the Comms Hub firmware. Changes to Comms Hub firmware typically are expensive and time consuming.

The diagram below shows an end-to-end view of the OTA firmware delivery and the mechanisms used to communicate between different systems.
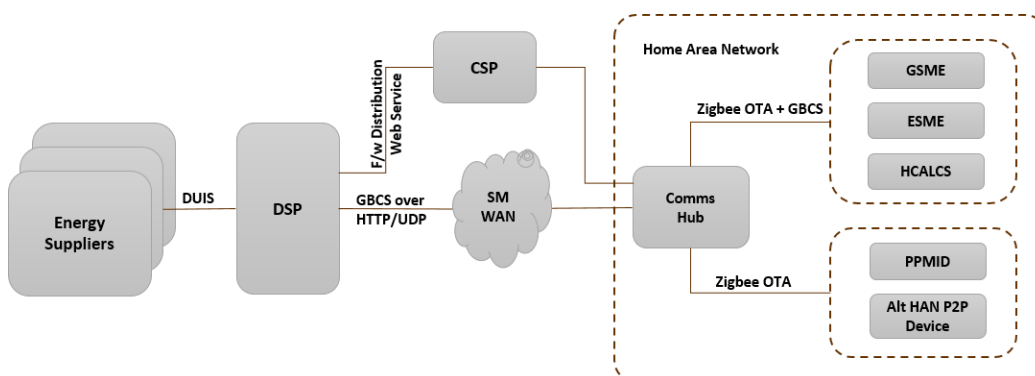
Identifying P2P Devices differently

DCC Total Systems will build the capability to differentiate the Alt HAN P2P Devices from the regular PPMID Devices. To support this, the existing SMETS Variant Type attribute (available to ESME Devices for recording ESME Variant) will also be made available to PPMID Devices for recording the 'Alt HAN Device Variant' information. There are four main types of Alt HAN P2P Devices (also known as bridges) namely B1, B2, B3 and B4 and for each type there will be a unique 'Alt HAN Device Variant' value.

Device Management

DCC Total Systems rely on 'Alt HAN Device Variant' information to identify an Alt HAN P2P Device and the same needs to be provided as part of device pre-notification using SRV 12.2. While it would be possible to include the Alt HAN Device Variant information in the Central

Product List (CPL) record, DSP will use only the data received via SRV 12.2 as the mechanism to identify an Alt HAN P2P Device.

After an Alt HAN P2P Device has been successfully pre-notified, the Service Users may update (SRV 8.4 Update Inventory) and read (SRV 8.2 Read Inventory) the Alt HAN P2P Device information stored in the Smart Metering Inventory (SMI). The Service Users will also be able to view the Alt HAN P2P Device information using the Self-Service Interface (SSI). No changes are required to the format of CPL to allow Alt HAN P2P Devices.

Some of the Service Requests that are applicable to PPMIDs will not be applicable to Alt HAN P2P Devices and Service Users shall not be allowed to submit those such as SRV 8.7.2 – Join Service (Non-Critical) and SRV8.8.2 – Unjoin Service (Non-Critical). New validation check will be introduced to enforce this for AltHAN P2P Devices. The existing DSP internal credentials management mechanism used for managing the certificates in PPMIDs will also be applicable to the Alt HAN P2P Devices.

Firmware Distribution Management

The OTA firmware update for Alt HAN P2P Devices will make use of the same method used for updating the firmware of PPMIDs. The Service Users will send firmware images using the existing Service Request 11.4 - Update PPMID Firmware. DCC Total Systems will determine the Device Type using the data held in SMI.

DCC Total Systems will process the received request that contains the firmware image and the list of devices, and forward that to the Communication Service Providers (CSPs) along with the corresponding Comms Hub identifiers. DSP will make use of the existing Web Service interface at CSP SMWAN Gateway to deliver the firmware image to the CSPs. DSP will mark the Device Type of the Alt HAN P2P Devices as PPMID for the subsequent processing.

The CSPs will deliver the firmware image to the corresponding Comms Hubs and the Comms Hubs will in turn deliver it to the target device within the HAN using the ZigBee OTA delivery currently used for PPMIDs. Although the Alt HAN P2P Devices are a different type of Device, they are joined to a HAN as though they are PPMIDs and therefore a Comms Hub will not be able to differentiate Alt HAN P2P Devices from a PPMID.

DCC Total Systems tracks the progress of the firmware update request at a device level. If a firmware update request is already in progress for a given Alt HAN P2P Device, any further firmware update requests will be blocked and the Service Users will be notified using the already existing functionality.

The Device Alerts received from the Alt HAN P2P Devices will be delivered to the Service Users using the DCC Alert N39, as with PPMIDs.

Service Users will be able to read the version of an Alt HAN P2P Device firmware by using the Service Request 11.2 Read Firmware Version. If the SRV 11.2 is targeted at an Alt HAN P2P Device, then DCC Total Systems will employ the URP (Unknown Remote Party) pattern to process this, as with the PPMIDs.

If the Response to SRV11.2 contains a version of firmware different to the version in SMI, the SMI will be updated with the new version subject to the rules applicable for the other Devices. Therefore, Service Users could use SRV11.2 also as a vehicle for updating the firmware version of PPMIDs in the SMI.

It is assumed that the Alt HAN P2P Device will implement the existing GBCS Use Case CS08 (*Read PPMID Firmware Version*) and the 0x8F8B Alert, which are currently implemented by the PPMID.

Summary

- Alt HAN P2P Devices will be treated like PPMIDs for processing within DCC Total Systems. The Alt HAN Device Variant information will be used to differentiate an Alt HAN P2P Device from a real PPMID.
- Service Requests 12.2, 8.4 and 8.2 will be modified to include the Alt HAN Device Variant information.
- Service Users will be able to use SRV 11.4 to send the firmware update requests for Alt HAN P2P Device. No changes are needed to this Service Request definition.
- Service Users will receive notifications at different stages of processing across DSP, CSP and the Comms Hubs.
- Service Users will be able to use SRV 11.2 to read the firmware version of Alt HAN P2P Device as well.
- The existing DCC Alert N39 will be used to notify the firmware activation of Alt HAN P2P Device.
- No changes required on Comms Hub firmware.
- Additional volume for CSPs to support firmware download and associated services to AltHAN P2P Devices.

4.1.1.1   Impact on DSP

DUIS, DUGIDS

DUIS and DUGIDS require updates to describe the changes to the behaviour of the impacted Services Requests 12.2, 8.4 and 8.2. DUIS XML Schema will need to be updated to revise the definition of SRVs 12.2, 8.4 and 8.2.

Request Management

Request Management will need changes to support the changes to the Service Request processing described above.

Data Management / Data Model

Data Model will need changes to support the additional values of the existing SMETS Variant attribute to identify an Alt HAN P2P Device.

SSI

SSI will be amended to present the real device type of an Alt HAN P2P Device when queried by a Service User.

ESI Reports

The ESI Reports ESI-034 and ESI-034i will need to be updated to be updated describe the revised usage of the field SMETS Variant Type.

CPL

No change is expected to the structure of the CPL for this Option 1.

Transform

No changes are expected to the Transform libraries for this Option 1.

Anomaly Detection

No changes are required within the Anomaly Detection component. Anomaly Detection volume thresholds for SR11.4 will need to account for the new and added volume of Alt HAN P2P Devices as well.

CSP SMWAN Gateway

No changes are required to the CSP SMWAN Gateway.

CSP Management Gateway

No changes are required to the CSP Management Gateway.

4.1.1.2 Impact on CSP Central & South

For Option 1, CSP-Central & South would be impacted in the following areas:

- Technical analysis is required to assess system requirements based on the increase in volumes of firmware downloads.
- PIT activity
    - o Setup of PIT environments to support testing of increased volumes of firmware downloads.
    - o PIT Performance and IT regression testing of the end-to-end use cases associated with P2P device firmware downloads.
    - o Technical support for test phases up to completion of PIT, including test case reviews, problem resolution and test sign-off activities.
    - o Additional support activities from the service management team for the Alt HAN devices, covering ongoing monitoring of the firmware download activities and the generation of the PM 2.2 monthly performance measures for firmware downloads.
- Design, use case and performance measure documentation updates to support these changes

4.1.1.3 Impact on CSP North

For Option 1, CSP-N would be impacted as follows:

- Technical analysis required to assess impact on message motorway (SMWAN) based on the volume increase of firmware download.

- Impact on PIT environments for performance and regression testing of the end-to-end use cases associated with P2P device firmware downloads.

4.1.1.4 Impact on Critical Software

Critical software identified Parse & Corelate software needs to be updated due to the change in DUIS schema.

4.1.1.5 Impact on DCC TOC

DCC Technical Operation Centre (TOC) will need to create new reports for stakeholders on firmware distribution to AltHAN P2P devices.

4.1.2 Option 2: Alt HAN P2P Device is considered as a Consumer Access Device (CAD)

DCC and Service Provider recognised Option 1 as the primary/preferred solution option and is believed to be better in terms of cost effectiveness. However, the Business Proposer and SECAS have also requested DCC to provide a complexity analysis (in relation to the primary solution) for an alternative solution option, where an Alt HAN P2P Device will be treated as a CAD.

This Option will require a number of changes and a very high-level view of the changes is provided below.

a. Requires all the changes described in the Option 1 section *"Identifying P2P Devices differently"* with the difference of Alt HAN P2P Device being treated as a CAD instead of a PPMID.
b. Requires changes to CPL to allow Alt HAN P2P Devices to be included as CAD Devices.
c. Requires extending the Access Control Broker (ACB) certificate management to include the Alt HAN P2P Device (CAD).
d. Requires changes to the Service Request processing of SRV12.2 and SRV8.4 in order to treat the Alt HAN P2P Devices as different types of CAD Devices.
e. Requires a separate Service Request for distribution of firmware images (equivalent of SRV11.4).
f. Requires a new DCC Alert to deliver the Device Alerts from Comm Hubs (on behalf of the Alt HAN P2P Devices) to the Service Users.
g. The existing processing and validation rules treat CAD as Type2 Devices. The Alt HAN P2P Devices will be Type1 CAD Devices and therefore the existing implementation will require updates to separate the behaviour. This may demand modelling the Alt HAN P2P Devices as a separate Device Type within DSP and present them as CAD to the external users.
h. Comms Hub firmware update is required to ensure the Comms Hub can manage firmware updates for Alt HAN devices, which will be managed differently from PPMIDs.

i. Changes in SMWAN Gateway to support firmware download to a Type 2 Device.
j. Changes in multiple internal systems of both CSPs to support firmware download to a Type 2 Device.

Please note that a detailed analysis of this Option 2 is required to be conducted as part of the FIA process, if this option is chosen over the preferred solution – Option 1.

5 Impact on DCC Systems, Processes and People

This section describes the impact of SECMP0170 solution Option 1 on DCC Services and Interfaces that impact Users and/or Parties.

5.1 System Components

Change in system components are highlighted in Section 4.1.1.

5.2 Security Impact

The implementation will be security assured during the implementation phase. This includes reviewing designs, test artefacts and providing consultancy to the implementation and test teams.

A more detailed security impact will be carried out as part of the Full Impact Assessment.

5.3 Technical Specifications

For Option 1, there will be changes in DUIS and corresponding changes in DUGIDS for the changes in DUIS. The DUIS Guidance document also needs to be updated.

For Option 2, changes are expected in DUIS, DUGIDS, GBCS and SMWAN Gateway specifications.

5.4 Integration Impact

An appropriate level of Systems Integration and User Integration Testing (SIT and UIT) will be carried out prior to progressing the release of this change to the Production environment, but this is not included in the PIA.

5.5 Infrastructure Impact

There will be no change to the infrastructure design as a result of this change using Option 1. Additional processing and storage will be required; however, they are not sufficiently large to warrant the procurement of additional compute power or storage.

The change does not impact the DSP resilience or DR implementation. It will be necessary to deploy the revised DUIS schema to Data Power devices.

This Modification does not impact DSP resilience or Disaster Recovery implementation.

CSP's PIT environment update might be required to support increased volume of firmware download. Details of any infrastructure uplift and associated impact on Application Support will be established in the FIA.

5.6 Service Impact

A detailed service impact will be completed as part of the Full Impact Assessment.

5.7 Safety Impact

No impact is expected, but a full Safety Impact Assessment will be carried out as part of the production of the FIA.

5.8   Contract Schedules

Service Providers have indicated changes may be required in number of Contract schedules based on the solution option selected and these will be detailed during the FIA.

6 Implementation Timescales and Approach

This Modification is expected to be implemented in a future SEC Release. Design, Build, and PIT for Option 1 is expected to take about three months to complete after the CAN is signed.

Details of the implementation will be finalised in the FIA.

6.1 Implementation Approach

Implementation of this change is assumed to follow a hybrid of agile and waterfall methodology. The release lifecycle duration will be confirmed as part of the FIA.

6.2 Testing and Acceptance

It is assumed that the change will be implemented and tested as part of a major release and will include release based regression testing in SIT and UIT.

7   Costs and Charges

The table below details the cost of delivering the changes and Services required to implement this Modification Proposal.

The scope of supply under this PIA includes design, development (build), system testing, and performance testing within the PIT environments.

The Rough Order of Magnitude cost (ROM) shown below describes indicative costs to implement the functional and non-functional requirements as assumed above. The price is not an offer open to acceptance. It should be noted that the change has not been subject to the same level of analysis that would be performed as part of a Full Impact Assessment and as such there may be elements missing from the solution or the solution may be subject to a material change during discussions with the DCC. As a result, the final offer price may result in a variation.

7.1   Design, Build and Testing Cost Impact

The table below details the cost of delivering the changes and Services required to implement this Modification. For a PIA, only the Design, Build and PIT indicative costs are supplied.

£	Design, Build and PIT	
	Option 1	Option 2
Firmware updates to Point to Point Alt HAN Devices	£636,500	High

Based on the existing requirements, the total fixed price cost of Option 1 for a Full Impact Assessment by all Service Providers is £86,007 and would be expected to be completed in 40 working days. The fixed price FIA cost of solution Option 2 is significantly higher than Option 1 and expected to take longer time to complete.

8 Risk, Assumptions, Issues, and Dependencies

In the following sections, Risks, Assumptions, Issues, and Dependencies have been identified. Two clarifications are also requested.

Further RAID may be established as part of the Working Group reviews and the FIA.

8.1 Risks

None at this time.

8.2 Issues

None at this time.

8.3 Dependencies

Ref.	Area	Dependency	Impact
MP170-DD01	IA	The solution Option 1 is dependent on the full delivery of SECMP007.	High
MP170-DD02	IA	SECAS and the Working Group are to advise on which option they will be progressing prior to commencement of the FIA.	High

8.1 Assumptions

Ref.	Area	Assumption	Impact
MP170-AS01	IA	It is assumed that the Alt HAN P2P Device will implement the existing GBCS Use Case CS08 (Read PPMID Firmware Version) and the 0x8F8B Alert, which are currently implemented by the PPMID.	High
MP170-AS02	IA	Managing separate ADT thresholds for Alt HAN P2P Devices is excluded from the scope of solution Option 1.	Low
MP170-AS03	IA	Systems Integrator activity is assumed to be part of release costs and as such is not included in this Impact Assessment.	Low
MP170-AS04	IA	CSPs are not required to differentiate between PPMIDs and Alt HAN devices for Option 1 in its systems and therefore for CSP, this Modification are centred around managing the volume increases of firmware downloads.	High
MP170-AS05	IA	DCC's ROM for this Modification is based on the volumetric information (in terms of number of P2P Devices and frequency of firmware download per year per device) provided along with the Business Requirement as in [1]. These will be reviewed as part of the FIA.	High

Appendix A: Glossary

The table below provides definitions of the terms used in this document.

Acronym	Definition
ADT	Anomaly Detection Threshold
AltHAN	Alternative Home Area Network
AltHANCo.	Alt HAN Company
CAD	Consumer Access Device
CAN	Contract Amendment Note
CPL	Central Product List
CR	DCC Change Request
CSC	Change Sub-Committee
CSP	Communication Service Provider
DCC	Data Communications Company
DSP	Data Service Provider
DUGIDS	DCC User Gateway Interface Design Specification
DUIS	DCC User Interface Specification
ESME	Electricity Smart Metering Equipment
FIA	Full Impact Assessment
GBCS	Great Britain Companion Specification
GSME	Gas Smart Metering Equipment
HAN	Home Area Network
IHD	In Home Display
HCALCS	HAN Connected Auxiliary Load Control Switch
OTA	Over the Air
P2P	Point to Point
PIA	Preliminary Impact Assessment
PIT	Pre-Integration Testing
PPMID	Prepayment Metering Interface Device
ROM	Rough Order of Magnitude (cost)
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SMETS	Smart Metering Equipment Technical Specification
SMI	Smart Metering Inventory
SMIP	Smart Metering Implementation Programme
SMWAN	Smart Metering Wider Area Network
SP	Service Provider
SR	Service Request

SRV	Service Request Variant
TABASC	Technical Architecture and Business Architecture and Sub-Committee
UIT	User Integration Testing