

MP207 ‘Allowing Registered Supplier Agents to Maintain Meter Firmware’

Business requirements – version 0.3

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	Enable Energy Supplier appointed RSAs (Registered Supplier Agents) to <i>Update Firmware</i> on Devices
2	Validation of Devices which the appointed RSAs are responsible for and have permission to manage
3	Current firmware management security requirements must be maintained
4	Reporting mechanism to monitor and ensure Energy Suppliers are aware of the current state of their Device portfolio
5	RSAs can access Alerts that are triggered by updating firmware

2. Considerations and assumptions

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

2.1 General

Allowing RSAs to maintain firmware on behalf of Energy Suppliers mean there would be improved management of firmware deployment and maintenance across the Smart Metering estate.

This modification aims to find a path which is feasible for a non-Supplier Party to be able to maintain Firmware without compromising any security, whilst ensuring all relevant parties are able to have an overview of their current Device estate. This would entail Energy Supplier appointed RSAs to Update Firmware. Currently RSAs are expected to maintain meters, however there is a gap in their ability to provide this service any capacity other than reporting on the firmware estate. The solution will allow RSAs, who are authorised by Energy Suppliers, to manage and maintain their Devices in a larger capacity than they are currently able to.

2.2 Requirement 1: Enable Energy Supplier appointed RSAs to *Update Firmware on Devices*

RSAs are being instructed to maintain the meters, however, currently only an Energy Supplier is able to update or activate firmware for their Device portfolio. By allowing RSAs to update firmware, they are able to assist the Energy Supplier to ensure the correct firmware is on Devices within their portfolio, and therefore better able to maintain their meters in the process.

2.3 Requirement 2: Validation of Devices which the appointed RSAs are responsible for and have permission to manage

RSAs are contracted by Energy Suppliers to maintain the Devices within their portfolio. Validation will be needed to ensure that only the correct RSA has access to Devices which are within the Energy Supplier's portfolio and restricted from those for which they are not appointed. This would ensure Devices are not being accessed by unauthorised Parties.

2.4 Requirement 3: Current firmware management security requirements must be maintained

In order to maintain current security requirements, the Proposer is only pursuing deployment of firmware due to implications of firmware activation being a critical command. By only allowing RSAs to deploy firmware, no additional User CIO Assessments would be needed and that the Supplier would remain accountable for the mitigation of this risk, as they are under the current model.

If firmware activation is added to the scope, it would need a new User Role to be needed to help facilitate the Firmware management by appointed RSAs. This new role would also be added to the Trust Anchor Cells to ensure Security is maintained and no malicious activity occurs.

2.5 Requirement 4: Reporting mechanism to monitor and ensure Energy Suppliers are aware of the current state of their Device portfolio

As Energy Suppliers who use RSAs to manage their Device portfolio, it would be ideal if the exact state of their Device portfolio is known and an obligation added to the Smart Energy Code (SEC) to

facilitate this. This is to ensure there is a up to date report to understand and determine the exact state of all Devices at any one time.

2.6 Requirement 5: RSAs can access Alerts that are triggered by updating firmware

Currently Energy Suppliers are sent these Alerts, however, to enable RSAs to effectively manage an Energy Supplier's Device portfolio, they will need access to Alerts which will be triggered following any updating of firmware on Devices. This modification does not intend to stop Alerts being received by Energy Suppliers, but allow RSAs access to these Alerts as well. Without these Alerts, the RSA would need to obtain this information from the Energy Supplier and this would impede their management of the Device portfolio effectively and in a timely manner.

3. Solution development

This section contains a must-have, should-have, could-have, won't-have (MoSCoW) analysis for the different requirement components to be considered as part of the solution.

MoSCoW Analysis		
Requirement Ref.	Description	MoSCoW
1	Enable Energy Supplier appointed RSAs (Registered Supplier Agents) to <i>Update Firmware</i> on Devices	M
2	Validation of Devices which the appointed RSAs are responsible for and have permissions	M
3	Current firmware management security requirements must be maintained	M
4	Reporting mechanism to monitor and ensure Energy Suppliers are aware of the current state of their Device portfolio	S
5	RSAs can access Alerts that are triggered by updating firmware	C

Key

- M = Must have
- S = Should have
- C = Could have
- W = Won't have

4. Glossary

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

Glossary	
Acronym	Full term
DCC	Data Communications Company
HCALCS	HAN connected auxiliary load control switch
PPMID	Prepayment Meter Interface Device
RSA	Registered Supplier Agent
SEC	Smart Energy Code