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.

MP207 'Allowing Registered Supplier Agents to Maintain Meter Firmware'

September 2022 Working Group – meeting summary

Attendees

Attendee	Organisation
Ali Beard	SECAS
Kev Duddy	SECAS
Anik Abdullah	SECAS
Bradley Baker	SECAS
Elizabeth Woods	SECAS
Ben Giblin	SECAS
Gordon Hextall	SSC Chair
David Walsh	DCC
Tom Rothery	DCC
Chris Thompson	DCC
Mark Pitchford	DCC
Julie Brown	British Gas
Emma Johnson	British Gas
Beth Davey	Calvin Capital
Martin Bell	EUA
Alastair Cobb	Landis+Gyr
Mark Powell	Macquarie
Ralph Baxter	Octopus Energy
Audrey Smith-Keary	OVO Energy
Mafs Rahman	Scottish Power
Michael Snowden	Secure Meters
Matt Alexander	SSE Networks
Shuba Khatun	SSE Networks
Robert Johnstone	Utilita
Kelly Kinsman	WPD
Tom Woolley	SMS Plc
Matt Roderick	n3rgy ltd
Kevin McIntyre	Geo
Patricia Massey	BEAMA

Overview

The Smart Energy Code Administrator and Secretariat (SECAS) provided an overview of the issue identified, impact, the Proposed Solution options, and business requirements.

Issue

- MOPs and MAMs are able to become DCC Users in the User Role 'Registered Supplier Agent (RSA)'
- Only Suppliers are currently able to deploy and activate firmware
- RSAs are authorised to maintain the Supplier's meters but unable to maintain Device Firmware

Impact

- Greater variance in Firmware versions leads to decreased DCC System performance
- Placing the burden of maintaining meter Firmware versions solely on Suppliers reduces flexibility and increases cost to serve

Proposed Solution options

Based on the business requirements, SECAS and the Proposer has developed two Proposed Solution options as outlined below:

- Option 1
    - Expand RSA role to include Device/Meter Manufacturers & MAPs
    - Only deploy firmware
    - No changes to User CIO Assessment
- Option 2
    - RSAs and include Other Users into the scope
    - Only deploy firmware
    - Negligible cost increase for User CIO Assessments for Other Users
    - Possible increased internal processes for Other Users

Business requirements

1. Enable Energy Supplier appointed RSAs (Registered Supplier Agents) to *Update Firmware* 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.

Working Group Discussion

SECAS (EW) provided an overview of the issue and Proposed Solution options and business requirements. The Security Sub-Committee (SSC) noted that the User CIO (Competent Independent Organisation) Assessments for either RSAs or Other Users to deploy firmware will cause a negligible/no increase in assessment cost.

A Working Group member (DW) queried if this would be for SMETS1 and SMETS2 or only SMETS2 firmware updates. Working Group member (MR) advised at a high level, they would like both, however, there is a need to ensure there are no blockers in doing so.

SECAS (EW) asked Working Group Members which Proposed Solution option was preferable in terms of incorporating Device/Meter Manufacturers and MAPs into the RSA role, or if this modification should expand its scope to include Other Users.

Working Group members queried the number of Parties and volume of Devices that this represents, and if this is something which can already be managed within the Adaptor solution. The Proposer (TW) advised that this had been driven by some Suppliers and represents one to two million Devices initially. Working Group member (JB) added that the value is identifying which upgrades haven't worked. The Proposer (TW) noted RSAs will take responsibility for upgrades that haven't worked. (MR) added this is an additional route for Suppliers to manage their estate.

Working Group member (RB) queried as to why are we adding in more Users to manage firmware, as there is an outstanding over-the-air (OTA) firmware upgrade issue being discussed at Technical Specification Issue Resolution Subgroup (TSIRS) and reported by DCC. Adding additional Users to this, it might cause more issues. (JB) noted there are issues with Alerts which is ongoing and it's a wider issue than with the meter itself, not just access to OTA failure Alerts but wider Alerts to Devices.

A Working Group member (JB) asked if the solution would interfere with current Alerts received by Suppliers (if an RSA/Other User were to deploy the firmware) or if it can be sent to both the Supplier and RSA/Other User. Supplier's systems rely on receipt and in 40% of cases, non-receipt, of the firmware download Alert, in order to auto-trigger an activation. They stated they would not want the Alert to be removed for Suppliers as part of the solution of this modification.

SECAS (AA) noted concern, as the system of OTA updates is based on one Party maintaining the client to service relationship to reduce errors. They questioned which Suppliers wanted to use this new proposed change and how they would ensure it works. How would they understand the hash on the firmware sent is the same as the hash on the activation message.

A Working Group member (RB) noted that the changes proposed are not costing the RSAs nor Other Users anything, and other Parties are subsiding for this additional service. They were concerned this would add additional strain to the DCC systems and believed the parties benefiting should be paying for set up and running costs. Working Group member (MR) advised that RSAs would be replacing the Supplier in this instance and therefore should not be an additional strain to the system. A Working Group member (JB) added that having two non-DCC parties working to resolve the issue, means more DCC resource and cost in dealing with those additional parties, both of whom are not currently charged.

Next Steps

The following actions were recorded from the meeting:

- SECAS to clarify if this modification will include SMETS1 and SMETS2 firmware updates.

- SECAS will present the business requirements and Proposed Solution options to the TABASC for review; and
- Following the review by TABASC, SECAS will request the Preliminary Assessment.