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'

February 2023 Working Group – meeting summary

Attendees

Attendee	Organisation
Ali Beard (AB)	SECAS
Kev Duddy (KD)	SECAS
Rachel Black (RB)	SECAS
Elizabeth Woods (EW)	SECAS
Mike Fenn (MF)	SECAS
Abhijit Pal (AP)	DCC
Chris Thompson (CT)	DCC
David Walsh (DW)	DCC
Patricia Massey (PM)	BEAMA
Tracey Foxley (TF)	BEBOC
Julie Brown (JB)	British Gas
Beth Davey (BD)	Calvin Capital
Steve Blackler (SB)	E Gas & Electricity
Alex Hurcombe (AH)	EDF
Robert Williams (RW)	EON
Daniel Davies (DD)	ESG Global
Martin Bell (MB)	EUA
Alastair Cobb (AC)	Landis+Gyr
Matt Roderick (MRo)	n3rgy ltd
Ralph Baxter (RBa)	Octopus Energy
Audrey Smith-Keary (ASK)	OVO Energy
Mafs Rahman (MR)	Scottish Power
Joanne Rush (JR)	SSE
Shuba Khatun (SK)	SSE Networks
Tom Woolley (TW)	SMS Plc
Kevin Clark (KC)	Utilita
Karen Jacks (KJ)	Vantage Meters
Luke Brady (LB)	Vantage Meters
Kelly Kinsman (KK)	WPD

Overview

The Smart Energy Code Administrator and Secretariat (SECAS) provided a summary of the issue and potential solution, Energy UK (EUK) feedback, business requirements, Proposed Solution and Data Communications Company (DCC) Preliminary Assessment.

Issue

- Meter Operators (MOPs) and Meter Asset Managers (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

Potential Solution

- Only deploy Firmware (SRV 11.1 'Update Firmware').
- Suppliers will still need to activate Firmware following the deployment.
- No changes to User Competent Independent Organisation (CIO) Assessment.

EUK Member feedback

Based on questions asked by SECAS to EUK member organisations, whether they will make use of this change if it is approved and if their organisation would require anything additional to facilitate the change. There were five respondents, and none said they would use this facility if the change went ahead. Key comments are outlined below:

- 'Existing process of automated Firmware activation would be broken'
- 'Not something we support or believe there is a need for'
- 'We cannot see how this suggestion addresses anything as all the issues of managing the upgrade will need to be done by the Supplier. The RSA cannot manage most items.'
- 'Opening up critical commands to RSA's that are not also subject to the IS/GS security arrangements should be avoided in principle'
- 'As an organisation not expecting to make use of this change we would need certainty that a MOP/MAM could NEVER install Firmware on any meters operated by a Supplier without explicit permission from the Supplier (in the form of system-based approval).'

Business requirements

All instances of 'Update/updating Firmware' means only the deployment of Firmware, as per Service Reference Variant (SRV) 11.1 'Update Firmware'.

1. Enable Energy Supplier appointed RSAs (Registered Supplier Agents) to Update Firmware on SMETS1 and SMETS2+ Devices (ESME and GSME only)
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

Proposed Solution

- Appointed RSAs
    - Adds capability for RSAs to send SRV11.1s to ESME/GSME
    - Receive all Alerts related to distribution & changes of Firmware on Devices
    - RSAs & Suppliers will receive confirmation of delivery
- SSI
    - RSAs and Suppliers able to see Firmware tracking for Devices where the other Party has sent the SRV 11.1 using SSI
- Definition change
    - Invalid Device check (W110101 – currently used when Device does not exist or sender is not the Registered Supplier) to include checking an RSA is appointed to the Device (ESME/GSME)

DCC Preliminary Assessment Summary

- **Cost (Design, Build & PIT)**
    - £151,000 - £350,000
- **Implementation**
    - Release timeline to be confirmed in Full Impact Assessment.
    - Full Impact Assessment - £13,127
    - Expected to be completed in 40 Working Days
- **Impact**
    - Only DSP component impact and cost are included in this PIA.
    - Possible impact on S1SPs, CSPs and DCC Data Science and Analytics (DS&A) team will be included in the Full Impact Assessment (FIA).

Working Group Discussion

SECAS (EW) provided an overview of the issue and potential solution, EUK feedback, business requirements, Proposed Solution and DCC Preliminary Assessment.

While discussing the business requirements, a member (JB) noted that the slides stated that RSAs are allowed to ‘update’ the firmware which implied they could ‘activate’ it. However, the proposal is that RSAs can only ‘deploy’ firmware but not ‘activate’ it. The member (JB) recommended that this be changed from 'update' to just to 'deploy’ to avoid confusion. Another member (MRo) suggested that the member's statement could also be considered incorrect as SRV 11.1 ‘Update Firmware’ is used to ‘deploy’ the firmware. The group agreed that there is a misalignment with the language in the Smart Energy Code (SEC) and that any documentation should include a caveat to show the ‘update’ as per

SRV11.1 means ‘deploy’ only, not ‘activate’. The DCC (DW) noted the business requirements being discussed had been updated to add clarity since the feedback at the last Working Group meeting.

While discussing the Proposed Solution summary, a member (JB) asked for clarification on ‘RSAs receiving all Alerts’ and if all Device Alerts and DCC Alerts up to and including N62 would be received by the RSA. The DCC (AP) advised that it has confirmation that the Alerts from N49 to N52 will be included but will confirm about the rest. The member (JB) highlighted that those Alerts will determine the next steps, and questioned whether all the Alerts need to be exposed to the RSA. The DCC (AP) advised that they can see how many Alerts need to be shared with Parties. Another member (RBa) raised concerns around the cost of implementing this and maintaining these costs in the future. The member (RBa) noted that Suppliers do not pay for RSA costs but was concerned with the cost Suppliers have to pay to implement this change. The member noted that they would incur costs even if no RSAs used the solution. The DCC (AP) acknowledged these comments.

In relation to the new error code, a member (JB) asked how the DCC will know that a specific RSA is permitted to deploy firmware to a specific meter. The DCC (AP) advised that it is Device dependant, but it would confirm the functionality of the solution. The Proposer (TW) advised that at present, RSAs are not validated by DCC systems [i.e. they can sent SRVs to any Device], it depends on an RSA’s commercial contract with the Suppliers. The member (JB) had concerns if a Responsible Supplier had yet to decide on a commercial agreement with an RSA, that RSA could start downloading Firmware to the Suppliers’ meters. She questioned how the DCC would know if it is authorised or not. A member (DD) advised that authorisation by the Responsible Supplier isn’t needed, it’s dependant on the RSA being registered to that supply point. The member (JB) noted this but advised that they believed that the Responsible Supplier needed to give explicit permission for RSAs to download Firmware. The DCC (AP) advised that they would investigate this and report back to the Working Group. A member (AC) suggested that a benefit of the RSA deploying Firmware on behalf of the Supplier is that it would ensure that the right OTA paths are followed. The member (AC) asked for clarity on if RSAs need to determine the current Firmware on a Device before loading the next Firmware. A member (MRo) advised that RSAs can already read the current firmware via SRV 8.4 and that any User is able to read the current Firmware on a Device and the Smart Meter Inventory (SMI).

A member (SB) raised a security concern with MP207, noting that they have seen Firmware variants that have passed testing and still resulted in faulty Firmware that then has had negative effects on consumers. The member (SB) noted that these issues will not come to light until a Supplier or consumer complains about a non-functioning Device. SECAS (AB) advised that they will seek advice from the Security Sub-Committee (SSC). The Proposer (TW) noted that any RSA contracted by a Supplier will have to take on board a large amount of liability to help with managing Firmware. The member (SB) advised that they were not concerned about the commercial arrangements, but rather the ability of the RSA to spread faulty Firmware, which will affect consumers. SECAS (AB) acknowledged these concerns and advised that these concerns would be discussed at the SSC. A member (MRo) highlighted that SRV11.1 is a non-critical command that cannot affect meters until they have received the command to activate the firmware (SRV 11.3/11.4) but agreed that it needs to go back to the SSC. The Proposer (TW) stated that he cannot speak on behalf of all RSAs, but that their company runs Smart Metering Equipment Technical Specifications (SMETS) assurance and compliance tests. They then test the Firmware upgrades to various Home Are Network (HAN) combinations and Alt HAN. From this, they get data for the change and the basic HAN assurance. The Proposer (TW) advised that they take full liability. The member (JB) suggested that there will either be a significant development to build that change in to Suppliers' adaptors, or there will have to be a manual process to replace what is currently an automated response. The member (JB) raised concerns around the costs involved in this. A member (MRo) advised that there are many Suppliers using shared DCC adaptors, and all those Suppliers have zero to little costs as a result. Another

member (RW) observed that although the SRV 11.1 update is a non-critical demand, it can still result in meters being removed from the HAN.

The member (TW) asked the other members to consider the current level of compliance availability of SMART and state of the portfolios, not the costs. The member (TW) pointed out that, they have collected data and produced a heatmap which looks at level of compliance within the whole UK portfolio. Based on this data, it is clear that this is a problem across the industry that needs to be solved. A member (JB) noted that there are various reasons why the portfolios are not as up to date as they could be, and this proposed change will add significant complexity to an already complicated process. A member (SBlac) asked if the member (TW) mentioned the portfolios because of compliance issues or Firmware not being up to date. The Proposer (TW) advised that it highlights that the portfolios are defective regardless of it being a compliance or Firmware issue. The Proposer (TW) added that the portfolios are not GBCS or SMETS compliant, and therefore are not operating as they should be. The member (SBlac) acknowledged this, but agreed with JB that there are a lot of reasons for this being the case. For instance, some Firmware is considered to have extremely negative impacts, so Suppliers will not upgrade to them. The member (TW) advised that it related to where there is a fundamental problem with the HAN combination, and how this affects consumers and Suppliers. SECAS (AB) advised that the Working Group needs to view the information the Proposer (TW) has. However, SECAS (AB) noted that some of the information would need to be anonymised and advised that TW send SECAS the information to check it over before sending it to the Working Group members present for this discussion.

When considering if new error code needs to be creating, a member (JB) suggested that it depends on the clarification of the RSA role in the error code. The DCC (AP) advised that the business requirements will have to be updated.

Next Steps

The following actions were recorded from the meeting:

- SECAS (EW) to clarify business requirements which state ‘Update Firmware’ to mean only deployment and not activation of Firmware.
- The DCC to confirm the following:
    - If Alerts 49 to 52 will be included in MP207’s Proposed Solution and how many Alerts need to be shared with Parties.
    - What costs Suppliers will be paying for MP207’s Proposed Solution and what on-going costs will be incurred if no RSAs take on MP207’s Proposed Solution.
    - How the DCC will be able to determine if an RSA has been authorised/given explicit permission by a Supplier and given explicit permission for appointed RSA to download Firmware.
- The Proposer to provide SECAS with data on the current state of Firmware portfolios for all Devices.
- SECAS to anonymise data provided by the Proposer before sending to Working Group members.
- SECAS will seek advice and review from SSC on security concerns of RSAs potentially distributing faulty Firmware onto a Supplier’s estate; and
- Following the review by SSC and clarifications, SECAS will return to the Working Group.