

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.



DP207

‘Allowing Registered Supplier Agents to Maintain Meter Firmware’

Modification Report

Version 0.3

9 August 2022



About this document

This document is a draft Modification Report. It currently sets out the background, issue, assessment of the proposal and progression timetable for this modification, along with any relevant discussions, views and conclusions. This document will be updated as this modification progresses.

Contents

1. Summary.....	3
2. Issue.....	3
3. Assessment of the proposal	6
4. Appendix 1: Progression timetable	7
5. Appendix 2: Glossary	8

Contact

If you have any questions on this modification, please contact:

Elizabeth Woods

020 4566 8335

elizabeth.woods@gemserv.com

1. Summary

This proposal has been raised by Tom Woolley from SMS Plc.

Supplier Parties authorise Meter Operators (MOPs) and Meter Asset Managers (MAMs) to install and maintain Smart Meters. However, under the Smart Energy Code (SEC), MOPs and MAMs are not able to use the Data Communications Company (DCC) System to remotely manage the meters' Firmware.

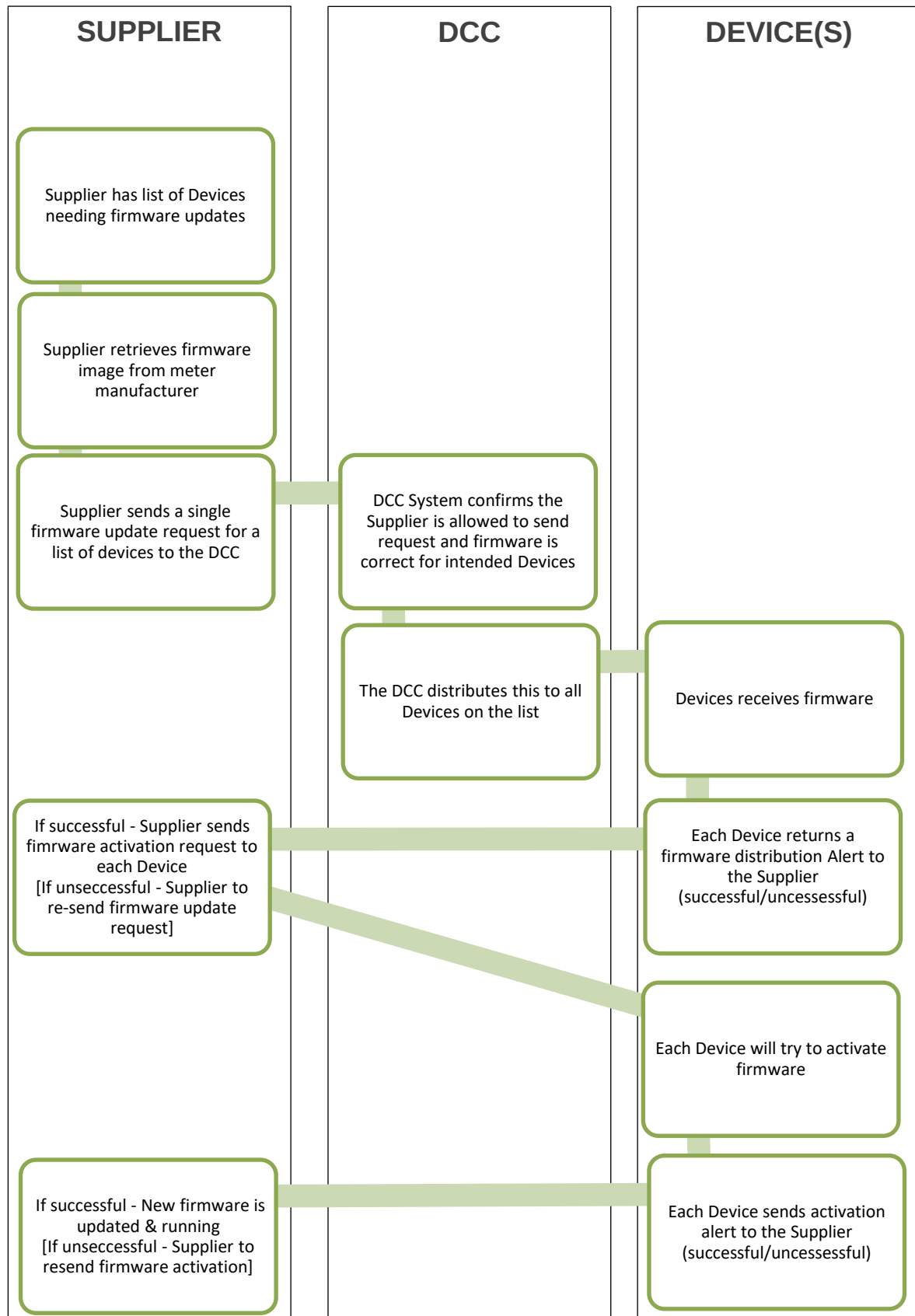
Device Firmware management is integral to the health of the Smart Metering ecosystem. The Proposer believes that MOPs and MAMs are in a better position than Suppliers to facilitate this, and that enabling Suppliers to outsource these operations to their Registered Supplier Agents (RSAs) will improve the overall Smart Metering service.

2. Issue

What are the current arrangements?

MOPs and MAMs are appointed by Suppliers to manage their Devices, including remote and on-site fault resolution and processes such as Install and Commissioning (I&C) procedures. They are able to become DCC Users in the 'Registered Supplier Agent' User Role. MOPs and MAMs are authorised by Suppliers to maintain the meters in the Suppliers' portfolios throughout the Device lifespan. However, they are not able to maintain the meters' Firmware versions.

The flow diagram below sets out the current step-by-step procedure of updating and activating firmware process, which only the Supplier is able to do:



What is the issue?

SEC Appendix E 'DCC User Interface Services Schedule' (UISS) and SEC Appendix AD 'DCC User Interface Specification' (DUIS) both state that only Parties with either the DCC User Role 'Import Supplier' or 'Gas Supplier' can send Service Reference Variant (SRV) 11.1 'Update Firmware', SRV 11.3 'Activate Firmware' and SRV 11.4 'Update PPMID Firmware'. Parties with the User Role 'Registered Supplier Agent' are unable to send these SRVs, and therefore unable to manage the Firmware version on Smart Metering Equipment Technical Specifications (SMETS) 2+ Devices they are registered to.

The responsibility for managing Device Firmware therefore sits solely with Supplier Parties, when it may be beneficial to outsource some of this functionality to RSAs.

Firmware management is essential for Suppliers and the wider industry, which relies on Smart Meter data for day-to-day processes and for the success of future programmes, such as Market-wide Half Hourly Settlement (MHHS) and achieving net-zero. It is also critical for asset funders, such as Meter Asset Providers (MAPs) and their investors, which rely on meters being installed and operated for many years.

What is the impact this is having?

Each Supplier has to implement varied processes to manage different Device Model Combinations, requiring investment of time and resource which could be outsourced to RSAs.

Placing the burden of maintaining meter Firmware versions solely on Suppliers, where a Supplier uses an RSA, causes inefficiencies in the Smart service, as there is an increased risk of Device Firmware becoming outdated. In addition, this can have a negative impact on the interoperability of Devices. This in turn increases the risk of disruption to message process pathways if Devices are not communicating as expected over the Home Area Network (HAN) or Wide Area Network (WAN). Out-of-date Firmware versions may also be more vulnerable to security breaches.

Impact on consumers

Outdated Firmware can impact the interoperability of HAN Devices such as In-Home Displays (IHDs) and Prepayment Meter Interface Devices (PPMIDs), negatively affecting consumers' access to information and prepayment functionality. The financial investment in time and resources required for Suppliers to manage Firmware versions across all their Devices may be greater than if they were able to outsource this functionality to RSAs, resulting in a higher cost to consumers for providing this service.

3. Assessment of the proposal

Areas for assessment

Sub-Committee input

SECAS has engaged with the Chairs from the Operations Group (OPSG), the Technical Architecture and Business Architecture Sub-Committee (TABASC), the Security Sub-Committee (SSC) and the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) to confirm what input is required from these forums. The Chairs of the Sub-Committees considered that the TABASC, the OPSG and the SSC should provide views on the modification to the Working Group.

SECAS believes the following Sub-Committees will need to input to this modification:

Sub-Committee input	
Sub-Committee	Input sought
OPSG	Will allowing RSAs to send SRVs 11.1, 11.3 and 11.4 have an impact on other operational processes?
SMKI PMA	No input needed.
SSC	Will security audits need to be adapted to meet the expanding scope of the RSA User Role?
TABASC	Will allowing RSAs to send SRVs 11.1, 11.3 and 11.4 require changes to the technical architecture?

Observations on the issue

Security Considerations

Change Sub-Committee (CSC) members noted concerns relating to security considerations, as the proposed changes would open up possible entry points for malicious activity. There were also concerns about the validation of RSAs as the appropriate Parties. The Proposer explained that they expected that this would be mitigated by contractual arrangements between Parties to ensure proper liability. It was also confirmed that meter manufacturers could be included if they registered as an RSA.

It was queried how the DCC would validate which Party deployed the firmware to that Device, and if the security considerations will be directly affected, as there is no register for RSAs.

SSC members queried if the Proposer is intending that RSAs both distribute and activate firmware or only distribute it. SECAS advised this would be dependent on the complexity and cost of each option as the modification progresses and would be confirmed in the Refinement Process. The SSC advised that the solution would need an evaluation of whether RSAs having access to these critical and non-critical SRVs will affect security. The User Competent Independent Organisation (CIO) will need to provide an assessment on what assurance would need to be if an RSA was going to distribute firmware and an additional assessment on what assurance will be needed if the RSA will be distributing and activating firmware.

The SSC subsequently confirmed there will be no additional requirements to the usual security checks if RSAs intend to only deploy firmware. Any increased risk will be mitigated as the activation will remain with the Supplier. If RSAs want to activate firmware then they will need to be assessed to

the standards required of a Supplier. However the User CIO and the SSC's views are that the risk and cost would negate the benefits of introducing activation of firmware for this modification.

A Requirements Workshop attendee stated that only the Import Supplier can issue SRV 11.3, as it is a Critical Command containing security credentials. Therefore, the quickest way of resolving this issue is for the RSA to have a manual process with the Supplier to trigger the firmware activation after the RSA has deployed the firmware.

An SSC member also noted that PPMID firmware, once deployed, will be activated straight away without a need for an activation command. SECAS advised it will need to look into how this will affect security if RSAs are only allowed to deploy firmware.

Additional Trust Anchor Cell

The ideal way for an RSA to implement firmware upgrades would be for there to be another Trust Anchor Cell, whereby the Supplier controls that key and allows access to an appointed RSA to use it. However, there is no appetite for this change as it would be expensive and complex to retrofit. It would also require DUIS changes to support this. An alternative would be to implement this through the Supplier systems or DCC systems.

Benefits

The CSC queried how many Supplier Parties would benefit from this change and how much they are currently affected by the issue. The Proposer did not disclose the number of Supplier Parties they are aware of, but did advise the biggest challenge for the Suppliers they work with is which version of firmware goes to which Device and when. RSAs being able to deploy the firmware would help mitigate this and therefore improve the overall Smart Metering service.

The OPSG was also presented with the issue and had no comments at this stage.

4. Appendix 1: Progression timetable

This Proposal will be returned to the CSC on 16 August 2022 for further discussion and agreement to convert this to a Modification Proposal. Following this, SECAS and the Proposer will develop the detailed business requirements. Once the requirements are agreed, SECAS will seek feedback from the Working Group.

Timetable	
Event/Action	Date
Draft Proposal raised	10 May 2022
Presented to CSC for initial comment	17 May 2022
Business requirements developed with Proposer	May 2022 – Jun 2022
Present to SEC Sub-Committees for initial comment	Jul 2022
Business requirements workshop	11 Jul 2022
<i>Propose CSC to convert Draft Proposal to Modification Proposal</i>	<i>16 Aug 2022</i>

Timetable	
Event/Action	Date
<i>Further develop business requirements with Proposer</i>	<i>Aug 2022</i>
<i>Business requirements discussed with Working Group</i>	<i>7 Sep 2022</i>
<i>Business requirements discussed with TABASC</i>	<i>6 Oct 2022</i>
<i>DCC Preliminary Assessment requested</i>	<i>7 Oct 2022</i>
<i>DCC Preliminary Assessment returned</i>	<i>31 Oct 2022</i>
<i>Update CSC</i>	<i>15 Nov 2022</i>

5. Appendix 2: Glossary

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

Glossary	
Acronym	Full term
CIO	Competent Independent Organisation
CPA	Commercial Product Assurance
CSC	Change Sub-Committee
DCC	Data Communications Company
DUIS	DCC User Interface Specification
GBCS	Great Britain Companion Specification
HAN	Home Area Network
IHD	In Home Display
MAM	Meter Asset Manager
MAP	Meter Asset Provider
MHHS	Market-wide Half Hourly Settlement
MOP	Meter Operator
OTA	over-the-air
OPSG	Operations Group
PPMID	Prepayment Meter Interface Device
RSA	Registered Supplier Agent
SEC	Smart Energy Code
SECAS	The Smart Energy Code Administrator and Secretariat
SMETS	Smart Metering Equipment Technical Specifications
SMKI	Smart Metering Key Infrastructure
SRV	Service Reference Variant
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
UISS	User Interface Services Schedule

Glossary	
Acronym	Full term
WAN	Wide Area Network