

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’

Modification Report

Version 0.5

XX May 2023



About this document

This document is a draft Modification Report. It currently sets out the background, issue, solution, impacts, costs, implementation approach 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. Solution	5
4. Impacts	6
5. Costs	8
6. Implementation approach	9
7. Assessment of the proposal	9
8. Appendix 1: Progression timetable	13
9. Appendix 2: Glossary.....	14

This document also has seven annexes:

- **Annex A** contains the business requirements for the solution.
- **Annex B** contains the full DCC Preliminary Assessment response.
- **Annex C** contains the Energy UK (EUK) Consultation responses.

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, the Smart Energy Code (SEC) does not allow MOPs and MAMs 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.

The Proposed Solution aims to add capability for RSAs to send Service Reference Variant (SRV) 11.1 to Electricity Smart Metering Equipment (ESMEs) and Gas Smart Metering Equipment (GSMEs) where they are the appointed RSA for the Device. RSAs will receive all the Alerts related to the Firmware distribution if they send the SRV 11.1 and will also receive copies of the Firmware receipt Device Alerts sent from the Device to the Supplier. RSAs will also receive DCC Alerts relating to changes of Firmware on Devices. RSAs and Suppliers will be able to see the Firmware tracking for Devices where the other Party has sent the SRV 11.1 using the Self-Service Interface (SSI).

The definition of invalid device check W110101 (used when device does not exist, or sender is not the registered Supplier) will be extended to include checking that an RSA is appointed to the Device (which must be an ESME or GSME).

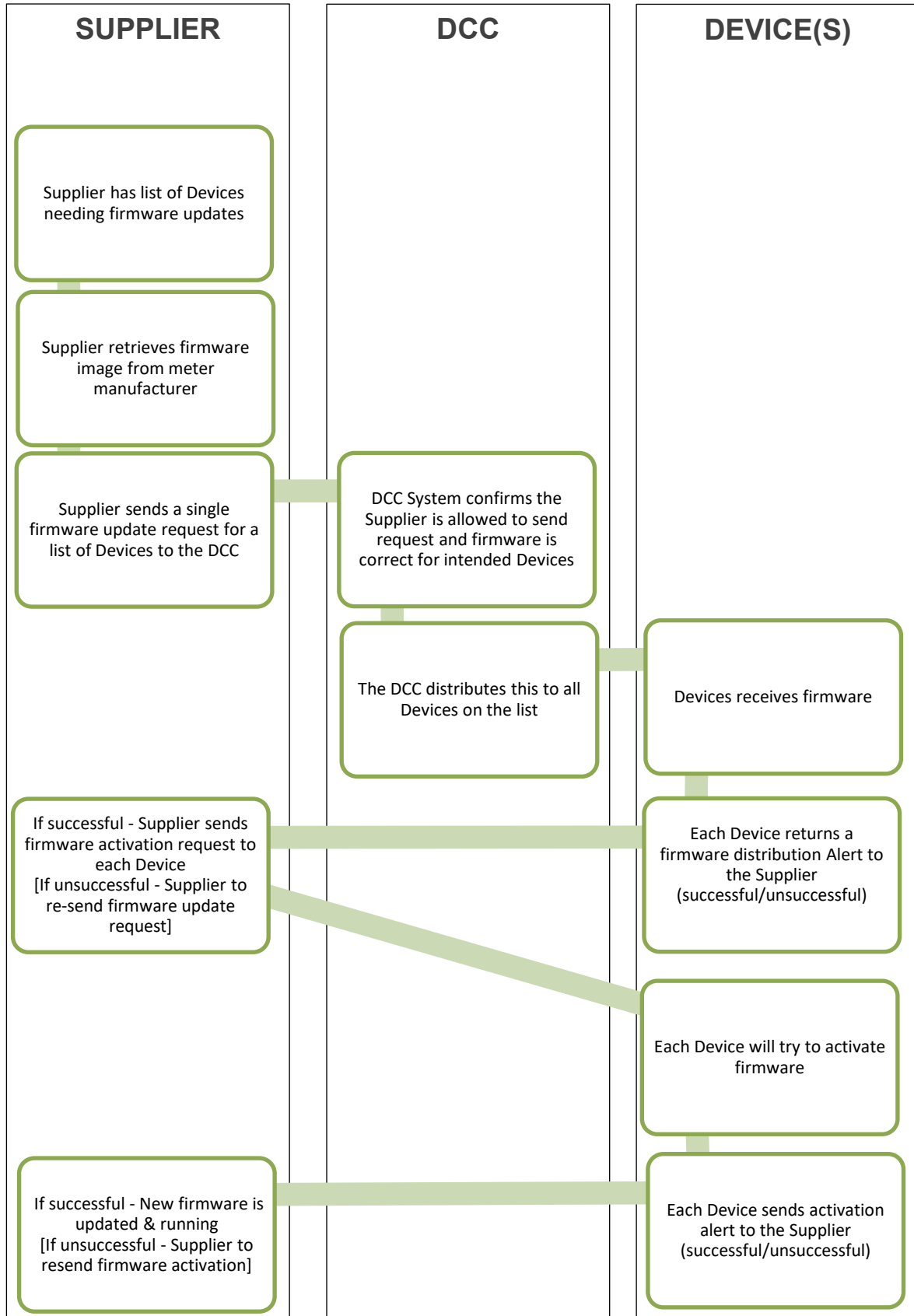
This modification will impact Other SEC Parties, Suppliers and the DCC. The estimated cost of the DCC System changes up to the end of Pre-Integration Testing (PIT) is between £151,000 and £350,000. Post-PIT costs will be assessed in the DCC Impact Assessment. This modification is targeted for the November 2024 SEC Release and will be progressed as a Self-Governance Modification.

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 can 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 can 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 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.

RSAs may be able to support and provide a more efficient and effective service to Supplier Parties to manage the Firmware.

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 must 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. Solution

Proposed Solution

The Proposed Solution will add capability for RSAs to send SRV 11.1 to ESMEs and GSMEs where they are the appointed RSA for the Device. RSAs will receive all the Alerts related to the Firmware distribution as they are the sender of SRV 11.1 and will also receive copies of the Firmware receipt Device Alerts sent from the Device to the Supplier. RSAs will also receive DCC Alerts relating to

changes of Firmware on Devices. RSAs and Suppliers will be able to see the Firmware tracking for Devices where the other Party has sent the SRV 11.1 using SSI.

The definition of invalid device check W110101 (used when device does not exist, or sender is not the registered Supplier) to be extended to include checking that an RSA is appointed to the device (which must be an ESME or GSME).

It is noted that it may also be necessary to create a new DUIS error code to report validation failures when an RSA attempts to download firmware to a device type for which they are not authorised. This could result in a requirement to revise the DUIS schema.

A decision to create a new error code could increase costs and extend the project duration. This will be discussed with the Working Group and Industry views will be sought as part of the Refinement Consultation.

The change will apply to SMETS1 and SMETS2 Devices, and to all versions of DUIS.

The full business requirements are in Annex A.

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
✓	Large Suppliers	✓	Small Suppliers
	Electricity Network Operators		Gas Network Operators
✓	Other SEC Parties	✓	DCC

Breakdown of Other SEC Party types impacted			
	Shared Resource Providers		Meter Installers
	Device Manufacturers		Flexibility Providers
✓	Registered Supplier Agent		Meter Data Retriever

As the Proposed Solution aims to allow RSAs to send SRV 11.1, therefore it is believed they will be impacted; however more Industry views will be sought as part of the Refinement Consultation.

Suppliers will be indirectly impacted as well, due to allowing RSAs to deploy Firmware on their behalf, if they choose to do so.

The DCC will have to make system and internal process changes, therefore would also be impacted.

DCC System

Technical Specifications

There will be changes in DUIS and corresponding changes in DCC User Gateway Interface Design Specification (DUGIDS) for the changes in DUIS. The DUIS Guidance document may need to be updated.

Integration Impact

An appropriate level of Systems Integration (SIT) and User Integration Testing (UIT) will be carried out prior to progressing the release of this change to the Production environment, but this is not included in the Preliminary Impact Assessment. A more detailed integration impact will be carried out as part of the Full Impact Assessment to evaluate Communications Services Providers (CSPs) and SMETS1 Service Providers need to carry out any integration testing or not.

Service Impact

The changes noted above are not expected to alter traffic volumes significantly, nor to add to message processing time but amends functionality of core Data Service Provider (DSP) processing components. No changes to Service Level Agreements (SLAs) or reporting are expected because of this change.

The full impacts on DCC Systems and DCC's proposed testing approach can be found in the DCC Preliminary Assessment response in Annex B.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Appendix E 'DCC User Interface Services Schedule'
- Appendix AD 'DCC User Interface Specification'

Technical specification versions

This modification will impact Appendix AD 'DCC User Interface Specification'. The proposed changes will be made clear after the Impact Assessment is returned by the DCC.

Devices

Devices impacted			
✓	Electricity Smart Metering Equipment	✓	Gas Smart Metering Equipment
	Communications Hubs		Gas Proxy Functions
	In-Home Displays		Prepayment Meter Interface Devices
✓	Standalone Auxiliary Proportional Controllers	✓	Home Area Network Connected Auxiliary Load Control Switches
	Consumer Access Devices		Alternative Home Area Network Devices

This would affect all variations of ESME including Standalone Auxiliary Proportional Controllers (SAPC), GSME, and Home Area Network Connected Auxiliary Load Control Switches (HCALCS), as it is set out in the DUIS that these Device types are applicable for SRV 11.1.

Consumers

There will be no impact on consumers.

Other industry Codes

There will be no impact on other Codes from this modification.

Greenhouse gas emissions

There will be no impact on greenhouse gas emissions.

5. Costs

DCC costs

The DCC's Service Providers have provided a rough order of magnitude (ROM) cost shown below, which describes the indicative costs to implement the functional and non-functional requirements as assumed above. The scope of supply under the DCC Preliminary Assessment includes design, development (build), system testing, and performance testing within the PIT environments.

The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	Cost
Design, Build and Pre-Integration Testing (PIT)	£151,000 – £350,000
Systems Integration Testing (SIT)	TBC
User Integration Testing (UIT)	TBC
Implement to Live	TBC
Application Support	TBC

More information can be found in the DCC Preliminary Assessment response in Annex B.

SECAS costs

The estimated Smart Energy Code Administrator and Secretariat (SECAS) implementation cost to implement this as a stand-alone modification is one days of effort, amounting to approximately £600.

This cost will be reassessed when combining this modification in a scheduled SEC Release. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.

SEC Party costs

SEC Party costs will be sought as part of this Refinement Consultation.

6. Implementation approach

Recommended implementation approach

SECAS is recommending an implementation date of:

- **26 June 2025** (June 2025 SEC Release) if a decision to approve is received on or before 26 August 2024; or
- **25 June 2026** (June 2025 SEC Release) if a decision to approve is received after 26 August 2024 but on or before 25 August 2025.

This modification will impact the DUIS which is only updated annually. It is not possible to target the June 2024 SEC Release, which is the next scheduled DUIS uplift, due to the length of time required for implementation.

7. 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?

Sub-Committee input	
TABASC	Will allowing RSAs to send SRVs 11.1, 11.3 and 11.4 require changes to the technical architecture?

Creation of new DUIS error code

The DCC Preliminary Assessment stated there is a possibility to necessitate creation of a new DUIS error code, in order to report validation failures when an RSA attempts to download Firmware onto a Device type for which the RSA is not authorised by the Supplier to do so. It is noted that a decision to create a new error code could increase costs and extend the project duration.

This will need to be discussed with the Working Group and Industry views will be sought as part of the Refinement Consultation, before concluding if a new DUIS error code should be requested.

Observations on the issue

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 Operations Group (OPSG) was also presented with the issue and had no comments.

Solution development

The initial solution was to incorporate both deployment and activation of Firmware as part of this modification. Following feedback and guidance of the SSC and Technical Architecture and Business Architecture Sub-Committee (TABASC), the current solution is only to deploy Firmware, as this is a non-critical request.

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.

Due to activation of firmware being a critical command, the Proposer is considering removing this from the scope of this modification, due to the cost factors involved in allowing RSAs access to a critical command.

Working Group members requested a review by the SSC on security concerns of RSAs potentially distributing faulty Firmware onto a Supplier's estate and to return to the Working Group with findings.

The SCC views will be sought and an update will be provided to the Working Group for discussion.

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.

Additional Users

The CSC queried why this modification is only factoring in RSAs and why it would not apply to all Party roles, not just Suppliers. For efficiency, it would be appropriate to include the Other Users role, as MAPs and meter manufacturers could benefit from being able to maintain meter firmware as well. CSC also requested to change the name of the modification to expand the scope of Users which should be included.

The Other User role is primarily used for 'Read Only' functions for DCC systems and usually would not intend on using the deployment of firmware function. The SSC has confirmed that, if the deployment of firmware were to be added as a function for an Other User, it would mean a negligible increase in the User CIO Assessment of all Other Users.

An alternative option would be to include additional SEC Parties wishing to deploy firmware by expanding the RSA role to include, e.g. MAPs and meter manufacturers.

A Working Group member 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.

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 advised that this had been driven by some Suppliers and represents one to two million Devices initially. A Working Group member added that the value is identifying which upgrades haven't worked. The Proposer noted RSAs will take responsibility for upgrades that haven't worked and added this is an additional route for Suppliers to manage their estate.

SECAS 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.

Alerts

A Working Group member 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.

Cost and DCC system usage

A Working Group member noted that the changes proposed are not costing the RSAs nor Other Users anything, and other Parties are subsidising 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. A Working Group member 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 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.

Terminology

Upon the return of the DCC Preliminary Assessment and discussing the business requirements, a Working Group member noted that the business requirements stated that RSAs are allowed to 'update' the firmware which implied they could 'activate' it. The Working Group agreed that there is a misalignment with the language in the SEC and that any documentation should include a caveat to show the 'update' as per SRV11.1 means 'deploy' only, not 'activate'.

Use cases and scale of the issue

Views of the TABASC

The TABASC discussed the potential use case of the Modification Proposal and agreed that it would be advantageous to Small Supplier Parties to have additional support in deploying firmware.

However, the TABASC noted that it would require substantial changes to most components of the Smart Metering System for RSAs to be involved in the end-to-end process. This is due to security limitations meaning that RSAs are only able to send firmware to Communications Hub (CH) Devices

and manage distribution. Consequently, it is unlikely that RSAs will be able to deal with other firmware related issues.

Furthermore, the Trust Anchor Cell, which is vital in holding the organisational certificate of the party which wishes to send messages for activation, is also missing. When all of these omissions are considered, it seems unlikely that the RSAs in the revised scope would be able to operate to a very useful degree on behalf of Small Supplier Parties

The TABASC suggested that the Modification Proposal does not seem to address a widespread issue or meet an essential need faced by industry and noted that to add the User Roles and make the associated system changes would require a significant technical and business process change. The TABASC queried the use case of the Modification in its current form and considered whether further clarity on the use of this proposed functionality is required and noted requests of this nature should be a good candidate for an DCC Elective Communications Service (ECS).

The TABASC also noted that, similar to the way in which RSAs currently carry out install and commission activities, there is the scope for them to utilise a Supplier Party's system as meter installers would, which is agreed between a Supplier Party and their RSA and would not require a SEC Modification Proposal to implement.

Views of the Energy UK Members

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).'

The full EUK member responses are in Annex C.

8. Appendix 1: Progression timetable

Following the Refinement Consultation, SECAS will be presenting this Modification Proposal for the Change Board to approve the Impact Assessment costs. This will be the final stage of the Refinement Process, after which the Modification Report can be returned to the CSC for approval to move to the Report Phase.

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
Presented to SEC Sub-Committees for initial comment	Jul 2022
Business requirements workshop	11 Jul 2022
Propose CSC to convert Draft Proposal to Modification Proposal	16 Aug 2022
Further develop business requirements with Proposer	Aug 2022
Business requirements discussed with Working Group	7 Sep 2022
Business requirements discussed with TABASC	6 Oct 2022
DCC Preliminary Assessment requested	1 Nov 2022
DCC Preliminary Assessment returned	30 Nov 2022
Discussed DCC Preliminary Assessment with Working Group	1 Feb 2023
Modification discussed with SSC	26 Apr 2023
<i>Modification discussed with Working Group</i>	<i>3 May 2023</i>
<i>Refinement Consultation</i>	<i>10 May 2023 – 31 May 2023</i>
<i>Update CSC</i>	<i>20 Jun 2023</i>
<i>Impact Assessment costs approved by Change Board</i>	<i>21 Jun 2023</i>
<i>Impact Assessment requested</i>	<i>22 Jun 2022</i>
<i>Impact Assessment returned</i>	<i>31 Aug 2023</i>
<i>Modification discussed with Working Group</i>	<i>4 Oct 2023</i>
<i>Modification Report approved by CSC</i>	<i>17 Oct 2023</i>
<i>Modification Report Consultation</i>	<i>18 Oct 2023 – 7 Nov 2023</i>
<i>Change Board Vote</i>	<i>22 Nov 2023</i>

Italics denote planned events that could be subject to change

9. 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
CH	Communications Hub
CIO	Competent Independent Organisation
CPA	Commercial Product Assurance
CSC	Change Sub-Committee
CSP	Communications Services Provider
DCC	Data Communications Company
DSP	Data Service Provider
DUGIDS	DCC User Gateway Interface Design Specification

Managed by

Glossary	
Acronym	Full term
DUIS	DCC User Interface Specification
DUISS	DCC User Interface Services Schedule
ECS	Elective Communications Service
ESME	Electricity Smart Metering Equipment
EUK	Energy UK
GBCS	Great Britain Companion Specification
GSME	Gas Smart Metering Equipment
HAN	Home Area Network
HCALCS	HAN Connected Auxiliary Load Control Switch
I&C	Installation & Commission
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
PIT	Pre-Integration Testing
PPMID	Prepayment Meter Interface Device
ROM	Rough order of magnitude
RSA	Registered Supplier Agent
SEC	Smart Energy Code
SECAS	The Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SLA	Service Level Agreement
SMETS	Smart Metering Equipment Technical Specifications
SMKI	Smart Metering Key Infrastructure
SAPC	Standalone Auxiliary Proportional Controllers
SRV	Service Reference Variant
SSC	Security Sub-Committee
SSI	Self-Service Interface
TABASC	Technical Architecture and Business Architecture Sub-Committee
TSIRS	Technical Specification Issue Resolution Subgroup
UISS	User Interface Services Schedule
UIT	User Integration Testing
WAN	Wide Area Network