

This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.



MP207

‘Allowing Registered Supplier Agents to Maintain Meter Firmware’

Modification Report

Version 1.0

22 May 2024

Corporate member of
Plain English Campaign
Committed to clearer
communication

592



About this document

This document is a Modification Report. It sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views and conclusions.

Contents

1. Summary.....	3
2. Issue.....	4
3. Solution	6
4. Impacts	6
5. Costs	8
6. Implementation approach	10
7. Assessment of the proposal	10
Appendix 1: Progression timetable	18
Appendix 2: Glossary	19

This document also has seven annexes:

- **Annex A** contains the business requirements for the Proposed Solution.
- **Annex B** contains the Data Communications Company (DCC) Preliminary Assessment response.
- **Annex C** contains the Energy UK (EUK) Consultation responses.
- **Annex D** contains the full responses received to the Refinement Consultation.
- **Annex E** contains the Change Board comments on the rejection of the DCC Impact Assessment request.
- **Annex F** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.
- **Annex G** contains the diagram of the current step-by-step procedure of updating and activating firmware.

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.

Device firmware management is integral to the health of the Smart Metering ecosystem. The DCC is responsible for updating firmware on Communications Hubs, but the responsible Supplier has an obligation to update the firmware on all other Devices.

Supplier Parties authorise Meter Operators (MOPs) and Meter Asset Managers (MAMs) to install and maintain Smart Meters as Registered Supplier Agents (RSAs). However, the SEC does not allow MOPs and MAMs to use the DCC System to remotely manage the meters' firmware.

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 RSAs will improve the overall Smart Metering service.

Originally the Proposed Solution was to allow RSAs to send SRV 11.1 'Update Firmware', SRV 11.3 'Activate Firmware' and SRV 11.4 'Update PPMID Firmware', however the Security Sub-Committee believed that allowing RSAs to send SRV 11.3 and 11.4 was a security risk and stated that it would only support the solution if these were not included so the Proposer agreed to remove the SRV 11.3 and SRV 11.4 from the Solution.

The Proposed Solution, therefore, only applies to Smart Metering Equipment Technical Specification (SMETS) 2+ Devices (excluding Prepayment Meter Interface Devices (PPMIDs)). The aim is to add capability for RSAs to send, Service Reference Variant (SRV) 11.1 'Update Firmware' to Electricity Smart Metering Equipment (ESMEs) and Gas Smart Metering Equipment (GSMEs) where they are the appointed RSA for the Device. The SRV 11.1 can also be sent to Standalone Auxiliary Proportional Controllers (SAPCs) and Home Area Network (HAN) Connected Auxiliary Load Control Switches (HCALCSs). The RSA will also receive Alerts related to the Device regarding firmware management.

This modification has received significant criticism from industry and the Change Board did not approve the costs to request a DCC Final impact Assessment. The Change Board believed that there are many reasons why Firmware is not up to date on Devices and the Proposed Solution (allowing RSAs to send SRV 11.1 'Update Firmware') will not resolve the issues identified as Suppliers will still be required to send the SRV 11.3 'Activate Firmware' and 11.4 'Update PPMID Firmware'. Furthermore, the Change Board and the Working Group believe that allowing RSAs to send SRV 11.1 but Suppliers having to send SRV 11.3 will 'muddy the water' around who is responsible for updating firmware and any issues that result from incorrect firmware upgrades. The Smart Energy Code Administrator and Secretariat (SECAS) has included more information on the Change Board decision to reject the Impact Assessment request in Annex E.

This change will require a new version of SEC Appendix AD 'DCC User Interface Specification' (DUIS) and will require Parties that want to use the solution to upgrade to that version of DUIS. Those Parties wishing to move onto the latest version of DUIS will incur costs for this business transition.

The estimated cost of the DCC System changes up to the end of Pre-Integration Testing (PIT) is between £151,000 and £350,000. However, SECAS has worked with the DCC to establish that the costs of this modification are likely to be between £450k and £650k (see Section 5).

It has also been highlighted that having an additional Party (RSA) working to resolve firmware issues, means more DCC resource and cost in dealing with that additional Party.

No benefits case has been provided by the Proposer, but they believe that if they are able to offer this service this will allow some Suppliers to outsource some of their firmware responsibilities. They believe that this may lead to an increase in firmware health and potentially better operation and interoperability of the smart metering estate.

This modification will impact Other SEC Parties, Suppliers and the DCC. If approved, this modification is targeted for the June 2026 SEC Release and will be progressed as an Authority Determined Modification.

2. Issue

What are the current arrangements?

Up to date firmware ensures that Devices operate effectively. There are known issues with out-of-date firmware preventing Devices communicating with the DCC, or with each other. There is a drive within industry to improve the firmware health of Devices across the UK. Firmware updates are also needed to fix security vulnerabilities and other Device defects as well as make improvements in functionality. Devices can still operate on older Firmware, but they may not be operating at their full potential.

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 ultimately 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.

Suppliers are responsible for maintaining the firmware on Devices, which is a Licenced obligation within the Electricity and Gas Supply Standard Licence Conditions¹. MOPs and MAMs can be 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. Under the security model, the Supplier is responsible for the firmware on the Device. The SSC has confirmed during discussions on this modification that it does not want responsibility split between Parties.

The flow diagram in Annex G sets out the current step-by-step procedure of updating and activating firmware for ESMEs and GSMEs (including HCALCS and SAPCs), which currently only the Supplier can do.

What is the issue?

To update firmware on SMETS2 ESME, GSME, HCALCS and SAPCs the Supplier must first send the SRV11.1 'Update Firmware'. Once a response is received to confirm that the firmware has been received by the Communications Hub the Supplier must then send the SRV 11.3 'Activate Firmware' which activates the update. For PPMIDs the Supplier must send SRV11.4 'Update PPMID Firmware' which sends and activates the firmware on a PPMID.

¹ [Gas Supply Standard Licence Condition](#) 33.15 and [Electricity Supply Standard Licence Condition](#) 39.15

The Supplier is responsible for ensuring that the firmware is up to date on Devices, however Suppliers have reported that there are many reasons why the firmware may not be up to date.

These reasons include, but are not limited to:

- failure of firmware update to complete at the Communications Hub (see [MP211 'Aligning the SMI with the CPL'](#))
- concerns around firmware updates resulting in further firmware failures (resulting in a worse service)²
- multiple firmware updates required in a specific order to get to latest firmware (see [MP231 'Firmware upgrade pathways'](#))
- failure of SRVs relating to firmware update

The Proposer believes that RSAs should be given the ability to send SRVs to update firmware to support and provide a more efficient and effective service to Supplier Parties to manage the firmware.

SEC Appendix E 'DCC User Interface Services Schedule' (UISS) and 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 SMETS2+ Devices they are registered to.

What is the impact this is having?

There are approximately 56,000 different Device Model Combinations that are possible, and each Supplier must implement varied processes to manage these, requiring investment of time and resource which could be outsourced to RSAs.

The Proposer believes that placing the burden of maintaining meter firmware versions solely on Suppliers, where a Supplier uses an RSA, causes inefficiencies in the Smart service, and 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 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), negatively affecting consumers' access to information. The Proposer believes 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. There was no indication of this in the Refinement Consultation responses.

² See [MP207 Working Group meeting summary - February 2023](#) for more details.

3. Solution

Proposed Solution

The Proposed Solution will add capability for RSAs to send SRV 11.1 to ESMEs and GSMEs (and HCALCS and SAPCs) where they are the appointed RSA for the Device. If the RSA sends the SRV 11.1 'Update Firmware' it will receive all the Alerts related to the firmware distribution 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 via the Self-Service Interface (SSI) for Devices where the other Party (Supplier or RSA) has sent the SRV 11.1 'Update Firmware' using the 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 (ESMEs, GSMEs, HCALCS and SAPCs).

The change will only apply to SMETS2 Devices.

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 Agents		Meter Data Retrievers

As the Proposed Solution aims to allow RSAs to send SRV 11.1 'Update Firmware' they will be impacted if they chose to offer the service.

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 the DCC User Gateway Interface Design Specification (DUGIDS). The DUIS Guidance document may need to be updated.

Integration Impact

An appropriate level of Systems Integration Testing (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. However, since the Change Board rejected the request for the costs to perform the DCC Impact Assessment SECAS has included an estimate of these costs in Section 5.

Service Impact

The changes noted above are not expected to alter traffic volumes significantly as RSAs will be sending the 11.1 instead of Suppliers, nor will they add to message processing time, but are expected to amend 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'. Usually, a draft of the changes to SEC Appendix AD 'DCC User Interface Specification' (DUIS) is provided by the DSP as part of the Final Impact Assessment with the draft legal text being confirmed during the detailed design phase (post decision). However, due to the Change Board rejecting the request for the Final Impact Assessment this is only available in draft form.

Devices

Devices impacted			
✓	Electricity Smart Metering Equipment	✓	Gas Smart Metering Equipment
	Communications Hubs		Gas Proxy Functions
	In-Home Displays		Prepayment Meter Interface Devices

Devices impacted			
✓	Standalone Auxiliary Proportional Controllers	✓	Home Area Network Connected Auxiliary Load Control Switches
	Consumer Access Devices		Alternative Home Area Network Devices

This would affect GSMEs and all variations of ESMEs including SAPCs and HCALCS, as it is stated 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

Preliminary Assessment

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 (from the DCC Preliminary Assessment)	
Activity	Cost
Design, Build and PIT	£151,000 – £350,000
SIT	TBC
UIT	TBC
Implement to Live	TBC
Application Support	TBC

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

Creation of new DUIS error code

The DCC Preliminary Assessment stated there was the option to create a new DUIS error code 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. SECAS noted that a decision to create a new error code could increase costs and extend the project duration therefore the Proposer agreed not to include this to keep cost down.

A final DCC Impact Assessment has not been performed as the Change Board rejected the request for the Impact Assessment which would have cost industry £13,127 (see Annex E). However, SECAS has used previous DCC Assessments to help understand the likely costs.

Estimate of Impact Assessment costs

Preliminary Assessments provide an estimate of the design, build and PIT costs. These costs are individual to each change and usually do not change significantly between the Preliminary Assessment and the final Impact Assessment.

The Impact Assessment is a quotation of the cost to implement the change as a standalone implementation. This includes the full costs of System Integration Testing and User Integration Testing. MP207 would only be implemented as part of a release which had other DUIS impacting changes (unless there was an extremely strong business case for implementing it alone, such as an urgent requirement for the functionality, which there is not). Where more than one modification is included in a release the SIT and UIT costs are spread amongst those modifications included in the release.

Working with the DCC, SECAS has identified that a modification with similar functionality changes and costs is [MP202 'Enduring Solution for SMETS1 and SMETS2+ PPMIDs'](#). MP202 had similar DUIS impacts to MP207 and therefore will have similar testing requirements (SIT, UIT and implementation).

MP202 DCC implementation costs (from the DCC Impact Assessment)							
£	Design	Build	PIT	SIT	UIT	TTO	SP Total
Phase Total	80,841	250,633	62,078	283,714	72,126	9,160	758,552

Forecast of MP207 DCC implementation costs based on MP202							
£	Design	Build	PIT	SIT	UIT	TTO	SP Total
Phase Total	151,000 – 350,000			Approx 250,000		50,000-70,000	461,000 – 680,000

The DCC agree that using this information SIT and UIT for MP207 is estimated to be around £250k. In addition to the £10k required for TTO, MP207 requires some minor changes to the Self-Service Interface which are estimated to cost £40-60k, giving a range of £50,000 to £70,000 for TTO. This estimate is based on the Impact Assessment for [MP169 'Managing SEC Obligations and the Consumer's Right to refuse a Smart Meter'](#) which requiring similar changes to the SSI at this cost. There is also some minor reporting changes for the DCC Data Science and Analytics (DS&A) team which the DCC estimate to be approximately £10k. This gives a range of £4610-680k for a standalone modification as per a DCC Impact Assessment.

SECAS costs

The estimated SECAS implementation cost to implement this as a stand-alone modification is one day 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 Parties that responded to the Refinement Consultation highlighted that their costs would be their share of the costs to implement this modification. One Large Supplier noted that if they were to use this service, they would incur substantial costs to change their automated processes that are already in place. There were no other costs identified.

6. Implementation approach

Recommended implementation approach

If this modification were to be implemented, SECAS recommends an implementation date of:

- **25 June 2026** (June 2026 SEC Release) if a decision to approve is received on or before 25 August 2025; or
- **24 June 2027** (June 2027 SEC Release) if a decision to approve is received after 25 August 2025 but on or before 24 August 2026.

This modification will impact the DUIS which is only updated annually. It is not possible to target the June 2025 SEC Release, which is the next scheduled DUIS uplift, due to the length of time required for Authority Determination and 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.

The following Sub-Committees were requested 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?

Solution development

Business Case and scale of the issue

The Change Sub-Committee (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. No further specific details were provided by the Proposer. The Proposer believes that RSAs being able to deploy the firmware would help mitigate this and therefore improve the overall Smart Metering service.

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, but no evidence was given. A Working Group member added that the value is identifying which upgrades haven't worked. The Proposer noted that where their organisation is the appointed RSA, they will take responsibility for managing the firmware updates. These cover firmware upgrades that haven't worked and added that this is an additional route for Suppliers to manage their estate. This is a commercial agreement and will not automatically apply to all RSAs.

Working Group members questioned which Suppliers wanted to use this new proposed change, how they would ensure it works and how they would understand the hash on the firmware sent is the same as the hash on the activation message when sending the SRV11.3. The Proposer did not provide any information for which Suppliers wanted to use the proposed change. They stated the other issues are resolved on a case-by-case basis.

A Working Group member noted this would make the process clunkier and add multiple points of failure. Another Working Group member agreed that this modification is looking to add more complexity to firmware distribution and activation which would potentially add confusion around responsibility and liability. They commented that PPMIDs are not included so a Supplier would still need additional processes to cover those (by sending SRV 11.4), as well as the activation of firmware by sending the SRV11.3. They noted this would further complicate the process for some Suppliers as they would still need to activate the firmware and rebuild their processes to accommodate this. Working Group members agreed that this would add another level of complexity and are not seeing the demand for this change.

The TABASC discussed the potential use case of the Modification Proposal and agreed that it might be advantageous to Small Supplier Parties to have additional support in deploying firmware. 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 the Communications Hubs (SRV11.1) and manage

distribution. Consequently, it is unlikely that RSAs will be able to deal with other firmware-related issues. The TABASC concluded that it seems unlikely that the RSAs in the revised scope (only deployment but not activation of firmware) would be able to operate to a useful degree on behalf of Small Supplier Parties. It further considered 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.

The TABASC also noted that, similar to the way in which RSAs currently carry out I&C activities for Suppliers, they queried if it would be possible for RSAs to utilise a Supplier Party's system as meter installers currently do, but for firmware maintenance. If this is possible, it would not require a SEC Modification Proposal to implement. The Proposer responded that this is possible, however due to the DCC Adapter being a competitive market, there are multiple DCC Adaptors in play and integration to all will be at a higher cost and not interoperable for industry.

SECAS asked Working Group members if there were any outstanding issues that needed to be resolved prior to requesting an Impact Assessment. A Working Group member noted that although they appreciated the Proposer's enthusiasm for this proposal, that the Refinement Consultation responses do not show any support. Neither have any Suppliers shown support, nor any intention to use the service, either by attending the Working Group, or responding to the Refinement Consultation. They added, this was an example of high costs with a highly debatable Proposed Solution and no support for the change nor for paying the costs.

Several Working Group members believed that industry should not spend £13,000 on an Impact Assessment as the solution doesn't solve the problem that has been identified. The Working Group Chair advised that the Change Board would be made aware of the Working Group's comments, but the Change Board will make the final decision on requesting an Impact Assessment.

A Working Group member advised they believed that there is no clear needs statement for this change and therefore does not think this modification will ever be in a position to request an Impact Assessment. They added that the scope has been reduced to such an extent that this is only assisting in a limited part of the process, which still requires Suppliers to do the rest.

The Proposer advised that they believed that this modification would help address the three million meters noted in the National Audit Office (NAO) report³ which are SMETS compliant but are not functioning as Smart Meters. They added that doing so, would assist in protecting assets in industry and address poor performing portfolios. The Proposer expressed their frustration that there are issues with the whole Smart Metering estate in terms of firmware, however they believed that members of the Working Group were indicating that there was no problem to fix. The Proposer added that their organisation has created a smart meter health checker due to Suppliers not handling the full extent of the issue.

The Proposer has sought feedback from energy Suppliers across the industry directly for their views regarding maintenance of firmware of Smart Meters on their portfolios. The Proposer stated that most respondents agreed that firmware maintenance plays a part in their Smart Meter performance and were interested in a solution that would assist with testing and assuring firmware. The Proposer said that whilst the majority indicated interest, there were split views on a solution that shares the responsibility and liability of Smart Performance with a third party. The Proposer further said that respondents displayed interest in having more detailed conversations about the solution. SECAS has not received any direct interest from Suppliers.

³ <https://www.nao.org.uk/wp-content/uploads/2023/06/update-on-the-rollout-of-smart-meters.pdf>

Working Group members agreed that the Proposer needed to provide evidence of support from prospective users of this service, and for these Parties to respond in the Refinement Consultation of their support and desire for this change.

They considered the following points did not support the modification:

- No evidence of support from Parties who want this service, either in writing or engagement in forums like the Working Group (the Proposer should provide evidence of support from prospective Parties for this modification). During Refinement Consultation, none of the Supplier respondents were supportive of this modification nor indicated a desire for this service.
- Suppliers will still need to have expertise for activation of all firmware and also a full process in place for PPMID firmware updates.
- If this was such a large issue as the Proposer claimed to be, why was this not raised by a Supplier.
- Only a percentage of those three million meters identified in the NAO report are known to not be able to have the firmware upgraded, there is also no breakdown of how many of these are SMETS2 meters and therefore would be in scope of this modification.
- Supplier issues with Firmware are a mixed bag, of which some Suppliers are managing their portfolio well.
- This is more of an OPSG issue rather than a need for a modification.

They considered the following places where more information could be provided:

- If the costs of asset removals could be gathered in order to build a business case for requesting the Impact Assessment.
- Helpful to have feedback from within The Community of Meter Asset Providers (CMAP), as there has been a range of costs collated for SMETS1 and SMETS2 estates, to better understand the cost of an unnecessary removal of assets (CMAP has fed back to Department for Energy Security and Net Zero (DESNZ), Office of Gas and Electricity Markets (Ofgem) and the Strategic Working Group) without any comments returned.
- Relevant metric is 'how many SMETS2 meters across DCC are on unsupported firmware?', although that number might be less if the Firmware had been updated historically.

The Proposer has provided information but noted it was commercially sensitive, and preferred it wasn't shared. There is an industry group, Smart Meters Not Operating in Smart Mode (SMNOSM), that has been initiated following the NAO report, recently set up to tackle these questions.

The Proposer provided a figure of approximately £200 per meter removal with an average removal rate of 5-7%. i.e. for every 10,000 meter installs 500-700 are removed (£100,000 - £140,000). SECAS notes that not all meter removals are due to out-of-date firmware.

Scope

The CSC queried why this modification is only factoring in RSAs and asked why it would not apply to all Party roles, not just Suppliers. For efficiency, it would be appropriate to include the Other User role, as MAPs and meter manufacturers could benefit from being able to maintain meter firmware as well.

It was highlighted that 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 Competent Independent Organisation (CIO) Assessment of all Other Users. By adding another User Role into the Proposed Solution, this would add more complexity and cost to what has already been assessed in the DCC Preliminary Assessment. The Proposer did not want to add this into the scope of the Proposed Solution.

The initial solution was to incorporate both deployment and activation of firmware (SRV 11.1 'Update Firmware', SRV 11.3 'Activate Firmware' and SRV 11.4 'Update PPMID Firmware') as part of this modification. Following feedback and guidance of the SSC and TABASC (shown below), the current solution is only to deploy firmware (SRV 11.1 'Update Firmware'), as this is a non-critical request. (See Security Considerations below for more detailed discussions)

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. The Proposer did not want to add this into the scope of the Proposed Solution.

Firmware updates

The NAO report states that three million meters are not operating in smart mode but does not breakdown how many are SMETS2 meters. There is also a lack of detail as to whether these are only due to outdated firmware or non-communicative for other reasons. Industry has advised that there are a multitude of issues which can lead to a meter not being on the latest firmware.

It is also noted that in order for this Proposed Solution to help with the wider out-of-date firmware issue, Supplier and RSA systems would need to upgrade onto new version of DUIS that would result from this change.

Trust Anchor Cell needed for Activation

The TABASC reviewed the original solution which included activation of firmware, they highlighted that there is currently no Trust Anchor Cell for RSAs, which is vital in holding the Organisational Certificate of the party which wishes to send messages for activation. As this would entail a physical change to Devices, there was no appetite for making a change to the Trust Anchor Cells, and would be expensive with far reaching costs from many parties within industry and complex to retrofit. It would require changes to Devices and DUIS to support it.

Security Considerations

The initial solution was to incorporate both deployment and activation of firmware (SRV 11.1 'Update Firmware', SRV 11.3 'Activate Firmware' and SRV 11.4 'Update PPMID Firmware') as part of this modification. Following feedback and guidance of the SSC and TABASC (shown below), the current solution is only to deploy firmware (SRV 11.1 'Update Firmware'), as this is a non-critical request.

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. This has been addressed by with the DCC Preliminary Assessment to extend the SRV 11.1 authorisation check to include the RSA role.

SSC members queried the Proposer about the original Proposal and if it 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 CIO would need to provide an assessment on what assurance would be needed 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 were allowed 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. They were not supportive of this solution.

A Requirements Workshop attendee stated that only the Import Supplier or Gas 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. The Proposer agreed to amend the solution to only sending SRV11.1, not the SRV11.3 which is a Critical Command. The SRV11.3 would still need to be sent by the Responsible Supplier.

An SSC member also noted that SRV 11.4 'Update PPMID Firmware', once deployed, will be activated straight away without a need for an activation Command. Due to activation of firmware being a Critical Command, the Proposer has decided to remove PPMIDs 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. SSC members did not see any added risks of an RSA versus a Supplier deploying firmware onto a Supplier's estate.

Cost and DCC system usage

A Working Group member noted that the changes proposed are not costing the RSAs nor Other Users anything, and that Supplier and Network Parties would be subsidising 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 an additional Party working to resolve the issue, means more DCC resource and cost in dealing with that additional Party who are not currently charged for DCC resource.

DCC Elective Service

The Proposer advised that they had offered to pay for this change however have been told it is not possible. SECAS and the DCC have considered if this change could be delivered under an Elective Service, however due to this requiring a DUIS change it is not a viable option to be a DCC Elective Service. SECAS added that even if the Proposer wanted to pay for the Impact Assessment and implementation costs, there are other factors to consider, including costs to other SEC Parties who will be impacted by this change. A Working Group member noted that if the Proposer is willing to pay for all Industry changes, including SEC Parties internal changes, then they believed that they should be able to.

The Proposer stated that they were not solely looking to introduce a commercial offering but also wanted to protect their assets and other MAPs assets. The Proposer added, if this was £500,000, their organisation would be more than willing to pay it and get this moving forward, which they believed pales in comparison to non-functioning Smart Meters being decommissioned and removed.

Change Board

The Change Board unanimously rejected the request for an Impact Assessment. Change Board members acknowledged that there are problems with Firmware however stated that these are wider ranging than simply sending firmware updates (as specified in Section 2). Change Board members highlighted that even when SRVs are sent these do not always result in updated firmware and can result in further errors to firmware versions which can compound the problem. Change Board members further cited lack of business case, and that the solution does not solve the problem as Suppliers would still need to send the SRV11.3 to activate the firmware. The comments received at Change Board can be seen in Annex E.

Views of the Energy UK Members

SECAS asked EUK member organisations whether they will make use of this service if the modification was approved and whether 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 available in Annex C. SECAS notes that EUK is only a subset of the Supplier community and has reiterated to the Working Group and the Proposer that the interested Parties need to engage to show their support of this modification.

Views from the SECAS Small Supplier engagement session

During an engagement session in May 2023, SECAS asked Small Suppliers if their organisation was interested to take up these services if they were offered to them. There were seven attendees who said they would not use this service if the change went ahead and was offered to their organisation. There were no votes for using the service.

Views of the OPSG

SECAS also presented the issue to the OPSG, which had no comments.

Views of the CSC

At the May 2024 CSC, members noted the issue stated already has a solution, therefore this Modification provided an additional solution path. They also noted that the three million Devices quoted in the NAO was inaccurate at the SMNOSM. They noted that of the three million Devices non-communicating, 1.7 million are non-enrolled SMETS1 Devices and therefore would not benefit from this modification. The CSC also noted there has been no support from Suppliers, who would be the users of this commercial service, nor from the rest of industry for this modification.

Final Comments

There are many problems with firmware which the industry is seeking to address. The original solution requested by the Proposer was for RSAs to be able to send both SRV11.1 and SRV11.3 to update and active new firmware on behalf of Suppliers (and SRV 11.4 for PPMIDs). The SSC highlighted a security risk due to SRV11.3 and SRV 11.4 being Critical Commands and the Proposer agreed to restrict the solution to SRV11.1. This means that the Supplier that uses the RSA will still need to validate and check the firmware update and send a SRV11.3 as well as send a SRV11.4 to update and activation the firmware on PPMIDs. This has reduced the usefulness of this solution significantly.

SEC Parties are further concerned about the splitting/blurring of responsibility with regard to ensuring firmware is updated.

The TABASC identified a workaround to avoid this modification and SECAS is aware that the Proposer is already working with some Supplier organisations as a work around to this problem.

SECAS has received no feedback in support of the modification and no evidence from the Proposer of support.

The SEC is an unusual Code as it requires the DCC to be paid to provide the Final Impact Assessment of the costs of a modification. To ensure oversight of these potentially significant costs the Change Board is tasked with the responsibility to act as the gate keeper for requesting Impact Assessments. In this instance the Change Board considered that the lack of business case, lack of support and lack of the ability to offer a complete solution deemed the costs unjustifiable. Whilst no Impact Assessment has been provided, SECAS and the DCC have been able to use historical comparisons to estimate a cost. The Preliminary Assessment costs have been established. Only SIT and UIT have been estimated. It is worth noting that SIT and UIT costs provided in the DCC Impact Assessments are estimates anyway as they are costed for a standalone release and expected to reduce (by an unknown amount) when included in a release with multiple modifications.

Legal text changes to DUIS are normally prepared as part of the DCC Impact Assessment. However, since the Change Board rejected the request for the DCC Impact Assessment this has not been completed. Whilst this could be considered to be missing from a complete assessment, it is fairly common that further amendments are made to DUIS text following the Change Board's final approval once the DCC begin detailed design of the solution. SECAS has prepared some Proposed legal text for consideration.

There are many reasons why Suppliers may not have updated the firmware on a Device. For instance, there are some firmware versions which introduce more problems than they resolve, and Suppliers are known to be actively avoiding a firmware upgrade to ensure the continued functionality of their Devices rather than a detrimental update. Therefore, to simply report that firmware is not up to date is an inaccurate measure of whether Suppliers are effectively managing their Device estate.

SECAS is recommending that this modification is not approved, especially in light of the ongoing industry work on SMNOSM that has been initiated following the NAO report.

The CSC noted the issue stated already has a solution, therefore this Modification is an additional solution path. They also noted there has been no support from industry nor Suppliers for this modification.

Appendix 1: Progression timetable

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
Modification discussed with SSC	13 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
Modification discussed with Working Group	3 May 2023
Refinement Consultation	31 May 2023 – 22 Jun 2023
Modification discussed with Working Group	5 Jul 2023
Impact Assessment costs rejected by Change Board	20 Sep 2023
Modification Report approved by CSC	21 May 2024
Modification Report Consultation	22 May – 13 Jun 2024

Timetable	
Event/Action	Date
Change Board Vote	26 Jun 2024
Authority decision (anticipated date expected by)	Aug 2024
Implementation Date	25 June 2026 SEC Release

Italics denote planned events that could be subject to change

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
CMAP	The Community of Meter Asset Providers
CSC	Change Sub-Committee
DCC	Data Communications Company
DESNZ	Department for Energy Security and Net Zero
DSP	Data Service Provider
DS&A	Data Science and Analytics
DUGIDS	DCC User Gateway Interface Design Specification
DUIS	DCC User Interface Specification
ESME	Electricity Smart Metering Equipment
EUK	Energy UK
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
NAO	National Audit Office
Ofgem	Office of Gas and Electricity Markets
OPSG	Operations Group
PIT	Pre-Integration Testing
PPMID	Prepayment Meter Interface Device
ROM	Rough order of magnitude
RSA	Registered Supplier Agent
SAPC	Standalone Auxiliary Proportional Controller

Managed by

Glossary	
Acronym	Full term
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 Specification
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SMNOSM	Smart Meters Not Operating in Smart Mode
SRV	Service Reference Variant
SSC	Security Sub-Committee
SSI	Self-Service Interface
TABASC	Technical Architecture and Business Architecture Sub-Committee
TTO	Transition to Operations
UISS	User Interface Services Schedule
UIT	User Integration Testing
WAN	Wide Area Network

MP207 ‘Allowing Registered Supplier Agents to Maintain Meter Firmware’

Annex A

Business requirements – version 0.5

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 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

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 (Registered Supplier Agents) to Update Firmware on SMETS1 and SMETS2+ Devices (ESME and GSME only)

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. Targeted Smart Metering Equipment Technical Specifications 1 (SMETS1) and SMETS2+ Devices are only for Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME) due to Prepayment Meter Interface Device (PPMID) *Update Firmware* SRV automatically *Activates Firmware*. Energy Suppliers will still be required to activate the firmware.

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.

For example, check could be performed by the DCC, to provide an indication that the Device is for a contracting Party, in this case an Import Supplier, and the RSA is the appointed Party for said Import Supplier.

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 Competent Independent Organisation (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. Ideally current reports should be used if the appropriate information is provided.

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 Update Firmware on SMETS1 and SMETS2+ Devices (ESME and GSME only)	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
ESME	Electricity Smart Metering Equipment
GSME	Gas Smart Metering Equipment
HCALCS	HAN connected auxiliary load control switch
PPMID	Prepayment Meter Interface Device
RSA	Registered Supplier Agent
SEC	Smart Energy Code
SMETS	Smart Metering Equipment Technical Specifications
User CIO	User Competent Independent Organisation

SEC Modification Proposal, SECMP0207, DCC CR4875

Allowing Registered Supplier Agents to Maintain Meter Firmware

Preliminary Impact Assessment (PIA)

Version:	0.3
Date:	30th November 2022
Author:	DCC
Classification:	DCC PUBLIC

Contents

1	Executive Summary	3
2	Document History	4
2.1	Revision History	4
2.2	Associated Documents	4
2.3	Document Information.....	4
3	Context and Requirements	5
3.1	Current Arrangements.....	5
3.2	What is the Issue?	5
3.3	Impact of the Issue	5
3.4	Business Requirements	6
4	Description of Solution	8
4.1	Impacts on DSP	8
4.2	Impacts on CSPs	9
4.3	Impacts on S1SPs.....	9
4.4	Impacts on DCC DS&A Reporting	9
5	Impact on DCC Systems, Processes and People	10
5.1	Security Impact.....	10
5.2	Technical Specifications	10
5.3	Integration Impact.....	10
5.4	Infrastructure Impact.....	10
5.5	Service Impact	10
6	Implementation Timescales and Approach.....	11
6.1	Implementation Approach.....	11
6.2	Testing and Acceptance.....	11
7	Costs and Charges.....	11
7.1	Design, Build and Testing Cost Impact.....	11
8	Risk, Assumptions, Issues, and Dependencies	12
8.1	Risks and Issues.....	12
8.2	Assumptions	12
8.3	Dependencies	12
	Appendix A: Glossary	13

1 Executive Summary

The Change Board are asked to approve the following:

- Cost to complete the Full Impact Assessment of **£13,127**.
- The timescales to complete the Full Impact Assessment of 40 working days.
- ROM costs for SECMP0207, up to the end of Pre-Integration Testing (PIT) of £151,000 to £350,000.

Only DSP component impact and cost are included in this PIA. Possible impact on SMETS1 Service Providers (S1SPs), Communications Services Providers (CSPs) and DCC Data Science and Analytics (DS&A) team will be included in the Full Impact Assessment (FIA).

Problem Statement and Solution

Meter Operators (MOPs) and Meter Asset Managers (MAMs) are appointed by Suppliers to maintain a Supplier's portfolio throughout the lifespan of the Devices. MOPs and MAMs can issue Service Requests to the DCC in a Registered Supplier Agent (RSA) user role. As per the current Smart Energy Code (SEC), the responsibility for managing Device Firmware sits solely with Supplier Parties. 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 services, as there is an increased risk of Device Firmware becoming outdated.

This Modification is proposing the RSA should be able to deploy firmware updates on behalf of the Supplier without compromising any security, whilst ensuring all relevant parties are able to have an overview of their current Device estate.

Modification Benefits

RSAs being able to deploy the firmware would help mitigate the challenge faced by Suppliers to maintain firmware updated for different Device Model Combinations. This reduces the risk of Devices being out of communications and vulnerable to security breaches.

2 Document History

2.1 Revision History

Revision Date	Revision	Summary of Changes
29/11/2022	0.1	Initial version, for DCC internal review
29/11/2022	0.2	Updated following DCC internal review
30/11/2022	0.3	Updated following further DCC internal review

2.2 Associated Documents

This document is associated with the following documents:

Ref	Title and Originator's Reference	Source	Issue Date
1	MP207 Modification Report v0.4	SECAS	31/08/2022
2.	MP207 Business Requirements v0.5	SECAS	28/09/2022

References are shown in this format, [1].

2.3 Document Information

The Proposer for this Modification is Tom Woolley of the SMS Plc. An Initial Modification Report was prepared and published in August 2022.

The Preliminary Impact Assessment (PIA) was requested of DCC on 1st November 2022.

3 Context and Requirements

In this section, the context of the Modification, assumptions, and the requirements are stated.

The requirements have been provided by SECAS, the Proposer and the Working Group.

3.1 Current Arrangements

Supplier Parties authorises Meter Operators (MOPs) and Meter Asset Managers (MAMs) to maintain their Smart Meters including remote and on-site fault resolution and processes such as Install and Commissioning (I&C) procedures. MOPs and MAMs are able to become Data Communications Company (DCC) Users in the 'Registered Supplier Agent' User Role, however, under the Smart Energy Code (SEC), MOPs and MAMs are not able to use the DCC System to remotely manage the meters' Firmware.

3.2 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.

3.3 Impact of the Issue

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.

Also 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.

3.4 Business Requirements

The business requirements are as follows.

Ref.	Requirement
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

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

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. Targeted Smart Metering Equipment Technical Specifications 1 (SMETS1) and SMETS2+ Devices are only for Electricity Smart Metering Equipment (ESME) and Gas Smart Metering Equipment (GSME) due to Prepayment Meter Interface Device (PPMID) Update Firmware SRV automatically Activates Firmware. Energy Suppliers will still be required to activate the firmware.

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.

For example, check could be performed by the DCC, to provide an indication that the Device is for a contracting Party, in this case an Import Supplier, and the RSA is the appointed Party for said Import Supplier.

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 Competent Independent Organisation (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.

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. Ideally current reports should be used if the appropriate information is provided.

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.

4 Description of Solution

The primary change to the DCC solution is on Data Services Provider (DSP) component. Communications Service Providers (CSPs), SMETS1 Service Providers (S1SPs) and DCC's Data Science and Analytics (DS&A) team could also be impacted.

4.1 Impacts on DSP

The following changes are required to the DSP solution to meet the requirements mentioned in section 3.4

Requirement 1

Allow a Registered Supplier Agent (RSA) to send Service Request Variant (SRV) 11.1 to ESME and GSME devices.

Requirement 2

Extend SRV 11.1 authorisation check to include the RSA role.

Requirement 3

No impact – activation of firmware is not in scope.

Requirement 4

No impact – likely impact the DCC's DS&A team.

Requirement 5

Update the Self Service Interface (SSI) component such that both the Supplier and their appointed RSA can see each other's SMETS2 firmware tracking data.

Deliver copy of firmware receipt alerts (8F72 & 8F1C) to RSAs.

Add RSAs to recipients for DCC Alerts N49 N50 N51 N52 where these relate to ESMEs or GSMEs.

Amend SRV 11.3 processing to send N49 to RSAs when the firmware on an ESME or GSME is updated to an active version.

In summary, this change adds the capability for RSAs to send 11.1s to ESMEs and GSMEs where they are the appointed RSA for the meter. RSAs will receive all the alerts related to the distribution as they are the sender of the 11.1, and will also receive copies of the firmware receipt device alerts sent from the device to the Supplier.

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.

RSAs will receive DCC Alerts relating to changes of firmware on devices.

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).

Note 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. This will need to be discussed with the Business Proposer and Working Group prior to the Full

Impact Assessment (FIA). A decision to create a new error code could increase costs and extend the project duration.

4.2 Impacts on CSPs

SECMP0007 already introduced validation on SRV 11.1 to check that there is no firmware update already in progress to a given Device when an SRV 11.1 is submitted and this validation is not User specific. This existing validation should prevent the scenario where Supplier and RSA are invoking the same firmware download request which could have impact Communications Services Providers (CSPs). Any other impact of inclusion of *SR11.1-Update Firmware* for SMETS1 and SMETS2+ Devices in RSA role on CSPs will be assessed as part of the FIA.

4.3 Impacts on S1SPs

Inclusion of *SR11.1-Update Firmware* for SMETS1 Devices in RSA role are likely to impact SMETS1 Service Providers. This will be assessed as part of the FIA.

4.4 Impacts on DCC DS&A Reporting

Inclusion of *SR11.1-Update Firmware* in RSA role are likely to impact reporting produced by the DCC Data Science and Analytics (DS&A) team. This will be assessed as part of the FIA.

5 Impact on DCC Systems, Processes and People

This section describes the impact of SECMP0207 solution on DCC Services and Interfaces that impact Users and/or Parties.

5.1 Security Impact

The implementation will be security assured during the implementation phase. This includes reviewing designs, test artefacts and providing consultancy to the implementation and test teams.

A more detailed security impact will be carried out as part of the Full Impact Assessment.

5.2 Technical Specifications

There will be changes in DUIS and corresponding changes in DUGIDS for the changes in DUIS. The DUIS Guidance document may need to be updated.

5.3 Integration Impact

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

5.4 Infrastructure Impact

No infrastructure impact is expected from this Modification. It should be noted that the aggregated impact of many such changes to the DSP solution will ultimately result in a reduction of the available processing headroom assumed as part of the original Agreement. As such, it may be necessary for DSP to raise a Business as Usual (BAU) CR for the provision/ of additional infrastructure to ensure the DCC Total System does not experience performance problems that are the direct result of the accumulation of such changes.

The change does not impact the DSP resilience or Disaster Recovery implementation.

5.5 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 DSP processing components. No changes to Service Level Agreements (SLAs) or reporting are expected as a result of this change.

A detailed service impact will be completed as part of the Full Impact Assessment.

6 Implementation Timescales and Approach

This Modification is expected to be implemented in a future SEC Release. Design, Build, and PIT is expected to take approximately four months to complete after the CAN is signed.

Details of the implementation will be finalised in the FIA.

6.1 Implementation Approach

Implementation of this change is assumed to follow a hybrid of agile and waterfall methodology. The release lifecycle duration will be confirmed as part of the FIA.

6.2 Testing and Acceptance

It is assumed that the change will be implemented and tested as part of a major release and will include release based regression testing in SIT and UIT.

7 Costs and Charges

The scope of supply under this PIA includes design, development (build), system testing, and performance testing within the PIT environments.

The Rough Order of Magnitude cost (ROM) shown below describes indicative costs to implement the functional and non-functional requirements as assumed above. The price is not an offer open to acceptance. It should be noted that the change has not been subject to the same level of analysis that would be performed as part of a Full Impact Assessment and as such there may be elements missing from the solution or the solution may be subject to a material change. As a result, the final offer price may result in a variation.

7.1 Design, Build and Testing Cost Impact

The table below details the cost of delivering the changes and Services required to implement this Modification. For a PIA, only the Design, Build and PIT indicative costs are supplied.

£	Design, Build and PIT
SECMP0207	£151,000 to £350,000

Based on the existing requirements, the total fixed price cost for a Full Impact Assessment by the DSP is **£13,127** and would be expected to be completed in 40 working days.

8 Risk, Assumptions, Issues, and Dependencies

In the following sections, Risks, Assumptions, Issues, and Dependencies have been identified.

8.1 Risks and Issues

Ref.	Assumption	Impact
MP207-IS1	This PIA draft includes DSP component impact only. Other DCC components (such as S1SPs, CSPs and DS&A Reporting) could be impacted and this will be assessed prior to the FIA.	Total cost of the Modification and the price to complete the FIA may increase based on wider impacts.

8.2 Assumptions

None at this time.

8.3 Dependencies

Ref.	Dependency	Impact
MP207-AD1	Adding new error code may have impact on DUIS schema as mentioned in Section 4.1	This should be discussed with the Business Proposer and Working Group to agree or avoid the DUIS schema change.

Appendix A: Glossary

The table below provides definitions of the terms used in this document.

Acronym	Definition
BaU, BAU	Business As Usual
CAN	Contract Amendment Note
CR	DCC Change Request
CSP	Communications Services Provider
DCC	Data Communications Company
DS&A	Data Science and Analytics
DSP	Data Service Provider
DUGIDS	DCC User Gateway Interface Design Specification
DUIS	DCC User Interface Specification
FIA	Full Impact Assessment
HAN	Home Area Network
IHD	In-Home Display
MAM	Meter Asset Manager
MOP	Meter Operator
PIA	Preliminary Impact Assessment
PIT	Pre-Integration Testing
PPMID	Prepayment Meter Interface Device
RAID	Risks, Assumptions, Issues, and Dependencies
ROM	Rough Order of Magnitude (cost)
RSA	Registered Supplier Agent
S1SP	SMETS1 Service Provider
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SLA	Service Level Agreement
SMETS	Smart Metering Equipment Technical Specification
SR	Service Request
SRV	Service Request Variant
SSI	Self Service Interface
UIT	User Integration Testing
WAN	Wide Area Network

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’

Annex C

EUK Consultation responses – version 0.4

About this document

This document contains the full anonymised collated responses received to the MP207 EUK Consultation.

Question 1: Do you think your organisation will make use of this change if it is approved?

Question 1			
Respondent	Category	Response	Rationale
1	Other SEC Party	-	-
2	Small Supplier	-	a. Established systems/business processes for firmware upgrade including system-enforced approval of both firmware/device combinations and individual upgrade batches – these safeguards would be difficult (maybe impossible) to replicate effectively with a 3rd party MOP/MAM b. Existing process of automated firmware activation would be broken. c. Firmware upgrade is a business-critical activity with potentially severe negative consequences if not carefully controlled (eg large numbers of prepay customers off supply with no means of resolution other than large number of meter replacements in short timescales). As firmware upgrades progress through pilot into full roll-out monitoring of meter performance and customer feedback is critical – only the Supplier can do this (cannot delegate to MOP/MAM). Introducing MOP/MAM to ‘facilitate’ the process would extend the chain of communications making the process far more difficult to control.
3	Large Supplier	No	-
4	Large Supplier	No	-
5	Large Supplier	-	-

Question 2: Would your organisation require anything additional to facilitate the change?

Question 2			
Respondent	Category	Response	Rationale
1	Other SEC Party	-	-
2	Small Supplier		As an organisation <u>not</u> expecting to make use of this change we would need certainty that a MOP/MAM could <u>NEVER</u> install Firmware on any meters operated by a Supplier without explicit permission from the Supplier (in the form of system-based approval). The reason for this is that unsolicited firmware upgrades/firmware upgrades applied in error) can have severe consequences including prepayment customers off supply and emergency meter replacement (potentially emergency meter replacement on very large numbers of meters).
3	Large Supplier	No	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.
4	Large Supplier	N/A	For us, but as per above, I think it's likely work would be required.
5	Large Supplier	-	-

Question 3: Any other comments or queries?

Question 3		
Respondent	Category	Response and rationale
1	Other SEC Party	The proposal to allow RSA access to manage firmware upgrades and the Supplier for firmware activation is not something we support or believe there is a need for. The product and process changes to implement this would be significant and costly to our product. As a result of this, it's not something we support and we have no intentions of adding the MOD, even if approved, to our product roadmap. If a supplier and their contracted RSA agent wanted to manage firmware in this manner, we would strongly recommend it's an elective service only.
2	Small Supplier	-
3	Large Supplier	Considerable feedback was given at the Working Group on the challenges this requirement creates. It seems to be a partial solution looking for requirements. With very little benefit to anyone. How is the RSA sending the Deploy Firmware going to help anyone?
4	Large Supplier	Firstly, the proposal is to only send the 11.1, and suppliers will then have to read the firmware and activate it I don't really see the point. If anything, based on my understanding of the process, it would add a step as the supplier would need to obtain the list of "updated" devices regularly, then craft batch commands to read and activate. Whereas if the 11.1 is already in the system, follow up SR's can be automatically triggered and fully tracked on system. Secondly, given the metering contract is between the MAP and the supplier and that's where the liabilities fall, it's not clear why anyone would let their MOP loose on their estate (unless they were the MAP of course but still). Choice of individual suppliers of course but struggling to see a scenario where MOP's are signing up to pay PRC's if they mess up an OTA, and suppliers accept that risk. More generally, I think opening up critical commands to RSA's that are not also subject to the IS/GS security arrangements should be avoided in principle - not just due to security risk but also increasing the risk of functional issues caused by diluted expertise.
5	Large Supplier	<u>Overall view:</u>

Managed by

Question 3		
Respondent	Category	Response and rationale
		This mod seems to be a “sledgehammer to crack a nut” and we do not support. The requirement within the mod could be better achieved by the RSA personnel being granted access to utilise a Supplier’s firmware deployment tool (i.e. a contractual / personnel agreement between a Supplier Party and their RSA). This would not require a SEC Modification Proposal to implement. Suppliers already delegate this kind of activity. e.g. A Supplier has a contractual arrangement for an external MOP agent to perform smart meter installations on their behalf. The MOP agent sends the required service requests on their behalf for install and commissioning purposes. The benefits of the proposed mod are very limited, and it does not cover PPMIDs (they are out of scope as firmware activation is automatic with download). <u>Our comments and objections are as follows:</u> We are not aware that this is a widespread issue / essential requirement needed by industry. There seems to be only 1 Smaller Supplier customer of the proposer (SMS plc). The Preliminary Assessment has been done but hasn’t been seen. However, the vast majority of the cost would be placed on large Suppliers who don’t want this service. Any cost should be carried by the party benefitting i.e. in the recovery mechanism from RSA service pricing. There are benefits to just one party maintaining an asset to reduce errors. Would there be any control to prevent both RSA and Supplier sending firmware download requests at the same time to the same asset? We have seen issues where sending a firmware <u>download</u> has caused significant numbers of assets to fall off the HAN. Only the Supplier has the holistic view of a customer’s assets and account status. Most firmware deployment systems treat “Download and Activation” as one business control. Therefore, the Supplier system would need to be modified to split up the 2 activities (at extra cost and be non-standard). The Mod doesn’t seem to be justified if only <i>downloading</i> firmware is the solution – the Supplier will still need to activate the firmware themselves. However, the Mod would still require a technical and business architecture change. The detailed issues/points that we have with the mod are described below:

Managed by

Question 3		
Respondent	Category	Response and rationale
		<u>We believe that the mod will require:</u> • Allocation of RSA privileges to only certain supplier portfolio assets and to ensure that the permissions don't persist on CoS Loss from that Supplier. • Extra auditing of who's done what & when to assets, in the case of any disputes over asset issues / Premature Replacement Charges. • Precise coordination between RSA and Supplier in terms of the Supplier sending the SR11.3 activate with the correct hash that has been used by the RSA in the SR11.1 firmware download. • Secure transfer of firmware between Supplier and RSA and that will require contractual agreements to be in place for this transfer. • The hash on the firmware downloaded needs to be the same as the hash within the activation message. • A reporting mechanism to track who has done what action. • RSA access to alerts that are triggered by updating firmware (0x8F72 / 0x8F1C). The RSA would probably also need access to SR11.2 to read the current firmware image and SR 8.1 to read the SMI inventory.

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’

Annex D

Refinement Consultation responses

About this document

This document contains the full collated responses received to the MP207 Refinement Consultation.

Question 1: Do you agree that the solution put forward will effectively resolve the identified issue?

Question 1			
Respondent	Category	Response	Rationale
EON UK	Large Supplier	Yes	Yes, but only in a technical way. We do not believe that the fundamental issue of improving firmware update success will be achieved, plus there are much easier ways of achieving the end-goal without this SEC Mod.
OVO Energy	Large Supplier	No	We are yet to see evidence that there is an issue that Parties are seeking a solution to. From the discussions had through the modification process we are also yet to see or hear that there is a demand for this service, which is what this is, a service that is being provided at the expense of Suppliers. The issue outlined in the mod report is that only Suppliers can deploy and activate Firmware. The proposal is for RSA's to be able to deploy the Firmware, but this does not resolve the issue specified as Suppliers will still need to activate it. We believe that the solution only adds a level of complexity and ambiguity.
Utility Warehouse	Large Supplier	No	We do not support the opinion that MOPs and MAMs are in a better position than Suppliers to facilitate the upload of firmware to meters.
Utilita Energy Ltd	Large Supplier	No	We do not agree with the framing of the issue as identified. Outsourcing these operations would not simplify matters, as claimed. Suppliers must make considered and informed decisions as to which versions of firmware to deploy – this modification would not remove this requirement, and would simply outsource the issuance of a single command. Furthermore, this mod aims to remove the need for suppliers to deploy firmware updates to their estate, thus potentially removing the need to have processes and expertise built up for this purpose. However, the mod only deals with deploying firmware to ESME and GSME, which would still leave suppliers

Question 1			
Respondent	Category	Response	Rationale
			requiring processes to monitor and deploy firmware to IDHs, PPMID etc. As these processes are functionally the same, there would be no reason to not also build those processes to handle ESME\GSME at the same time.
ENGIE (ENGIE Power Limited, ENGIE Gas Limited)	Small Supplier	No	We are not persuaded that there is a significant issue to address or a pressing need for RSAs to be able to update firmware, but in any case the modification does not provide a complete solution – the RSA would only be able to do the preliminary deployment of the firmware, not activate it – this would remain with the Supplier. Further, there is no control in the modification for errors if an RSA were to attempt to apply firmware to a supplier's meters without authorisation– to fix this with an error message would add more cost and complexity to the solution. We are also concerned that this proposal could add more complexity to Security Assessments if there is another party involved in firmware upgrades. We also note that without needing to outsource the actual deployment of firmware to third parties, there are already good commercial options for Suppliers to obtain support with preparation for firmware deployment via software service providers. As the RSA firmware service would remain optional for suppliers, if there was limited take up (as seems likely from other negative supplier reactions documented in the report) MP207 would simply be a cost to the industry for little benefit.

Question 2: Do you agree with the proposed implementation approach?

Question 2			
Respondent	Category	Response	Rationale
EON UK	Large Supplier	No	The requirements within the SEC Mod could be better achieved by the RSA personnel being granted access to utilise a Supplier's firmware deployment tool (i.e. a contractual / personnel agreement between a Supplier Party and their RSA). This would not require a SEC Modification Proposal to implement. Suppliers already delegate this kind of activity... e.g. it is common for Suppliers to have contractual arrangements for an external MOP agent to perform SMART installations on the Supplier's behalf. The MOP agent sends the required service requests on behalf of the Supplier for installation and commissioning purposes, using the Supplier's IT systems.
OVO Energy	Large Supplier	-	-
Utility Warehouse	Large Supplier	No	The proposed implementation approach would add unnecessary complexity to the firmware update process as it would require coordination with an additional party with additional tracking of the Service Requests.
Utilita Energy Ltd	Large Supplier	No	We do not believe that the modification as it stands should be implemented, as the benefits as set out in the modification report cannot be realised.
ENGIE (ENGIE Power Limited, ENGIE Gas Limited)	Small Supplier	No	We do not support the proposal.

Question 3: Will there be any impact on your organisation to implement MP207?

Question 3			
Respondent	Category	Response	Rationale
EON UK	Large Supplier	Yes	Our organisation, along with other large Suppliers, would need to pay for the SEC Mod, but have no use for it.
OVO Energy	Large Supplier	No	Apart from the cost of this modification, we would not opt to use this service.
Utility Warehouse	Large Supplier	Yes	Firmware updates are triggered upon our request only after internal testing to ensure compliance with our adaptor and back-end systems. The new process would remove an element of control of that decision. Our current process utilises support from our adaptor host who initiates upgrades on our request. Our adaptor host would have to redevelop their automated solution that applies and tracks the progress of the firmware updates, and then we would need to redevelop the joint processes.
Utilita Energy Ltd	Large Supplier	Yes	If we were to utilize a service enabled by this modification, we would have to completely rebuild our current automated processes and system that deal with firmware updates, as the activation portion of these processes would need an alternative trigger.
ENGIE (ENGIE Power Limited, ENGIE Gas Limited)	Small Supplier	Yes	There would be a cost implication for introducing the necessary industry changes to facilitate the RSA firmware service which we will incur whether or not we actually use the RSA firmware service.

Question 4: Will your organisation incur any costs in implementing MP207?

Question 4			
Respondent	Category	Response	Rationale
EON UK	Large Supplier	£100k-£250k	This would be our share of the SEC Mod costs and we would not gain any value from this.
OVO Energy	Large Supplier	Yes	Yes, if approved we would be paying for a service that we have no intention of using.
Utility Warehouse	Large Supplier	Less than £100k	If the modification is not implemented, we will continue with the current process, with costs that we are prepared to incur. We have not identified any cost savings we may achieve as a result of implementation of this modification. We will incur costs in redeveloping the automated process utilised by our adaptor provider if this modification were to be implemented.
Utilita Energy Ltd	Large Supplier	£250k-£500k	As previously mentioned, we would need to extensively overhaul our automated processes and systems. Additionally, there would be further ongoing costs in the form of contracting these services out to an offering party.
ENGIE (ENGIE Power Limited, ENGIE Gas Limited)	Small Supplier	Less than £100k	There will be a cost implication for introducing the necessary industry changes to facilitate the RSA firmware service which we will incur whether or not we actually use the RSA firmware service.

Question 5: How long from the point of approval would your organisation need to implement MP207?

Question 5			
Respondent	Category	Response	Rationale
EON UK	Large Supplier	We would not implement the solution	The issue being addressed would be of potential use to perhaps a very small number of Suppliers.
OVO Energy	Large Supplier	Immediately	We would not make use of this service
Utility Warehouse	Large Supplier	-	-
Utilita Energy Ltd	Large Supplier	6 – 8 Months	Due to the scope of changes to systems and processes we would require significant time to build and test these. Time would additionally be required to negotiate and agree contracts to replace these processes.
ENGIE (ENGIE Power Limited, ENGIE Gas Limited)	Small Supplier	6 months	The long lead time from approval noted in the Modification Report would cover our required lead time.

Question 6: Do you believe that MP207 would better facilitate the General SEC Objectives?

Question 6			
Respondent	Category	Response	Rationale
EON UK	Large Supplier	No	We do not believe that any fundamental improvements would be forthcoming from MP207
OVO Energy	Large Supplier	No	-
Utility Warehouse	Large Supplier	No	We believe we are already meeting the objective of N or N-1 firmware as best we can with 95% of meters satisfying this requirement. Therefore, we don't believe that implementation of this modification would better facilitate the General SEC Objectives.
Utilita Energy Ltd	Large Supplier	No	We believe that this modification would negatively affect General SEC Objectives: Objective (a) would be negatively affected as a supplier would have to have two different processes for maintaining firmware depending on the device – E\GMSE vs IHD or PPMID, for example. Additionally these suppliers would still need a process to activate the deployed firmware. We recognise that a Supplier would be under no obligation to outsource their processes, however the paragraphs above applies whether they chose to or not.
ENGIE (ENGIE Power Limited, ENGIE Gas Limited)	Small Supplier	No	We believe that MP207 would not better facilitate Objective (a) as it is not likely to lead to efficiency in the operation of smart metering systems.

Question 7: Do you believe there will be any impacts on or benefits to consumers if MP207 is implemented?

Question 7			
Respondent	Category	Response	Rationale
EON UK	Large Supplier	No	Additional costs on industry to implement and support MP207 will eventually be paid by consumers. There are more cost-efficient ways to achieve the same goal without MP207.
OVO Energy	Large Supplier	No	-
Utility Warehouse	Large Supplier	No	Impacts would only be worsened by implementation of this modification as it would require coordinating a process that would include an additional party, making it more difficult to ensure the latest firmware is applied to a consumer's meter.
Utilita Energy Ltd	Large Supplier	No	We believe that the majority of consumers will not see a noticeable difference from this modification, as the proposal simply changes who does parts of an already existing process.
ENGIE (ENGIE Power Limited, ENGIE Gas Limited)	Small Supplier	No	There is no discernible benefit to consumers from this modification, and there may be a disbenefit if the involvement of RSAs in firmware upgrades leads to inefficiencies in the process which result in non-functioning meters.

Question 8: Noting the costs and benefits of this modification, do you believe MP207 should be approved?

Question 8				
Respondent	Category	Response	Rationale	SECAS Response
EON UK	Large Supplier	No	MP207 provides a very limited benefit and does not cover firmware activation, PPMID deployments or interactions with customer data or direct with the end-customer.	-
OVO Energy	Large Supplier	No	Ultimately if this modification was approved, we would be paying for a service that we would not be utilising. We are yet to see any evidence of any demand for this service either. Until those that wish to use the service come forward, we cannot fully understand the benefits of this modification. We feel that this would be far better suited as an Elective Service.	SECAS has explored the Elective Services route with the DCC, however, as there are changes to SEC Appendix AD 'DCC User Interface Specification' (DUIS) required, the Proposed Solution would not be viable for an Elective Service. (Any DUIS changes must be done via a SEC Modification)
Utility Warehouse	Large Supplier	No	-	-
Utilita Energy Ltd	Large Supplier	No	Taking into account that suppliers who choose to take up a service enabled by this mod would still have to have processes in place to deploy and activate firmware, the cost to implement far outweighs the benefits that would be provided.	-
ENGIE (ENGIE Power Limited,	Small Supplier	No	Please see comments on Question 1.	-

Question 8				
Respondent	Category	Response	Rationale	SECAS Response
ENGIE Gas Limited)				

Question 9: Please provide any further comments you may have.

Question 9		
Respondent	Category	Comments
EON UK	Large Supplier	The costs for MP207 will eventually be paid for by energy consumers to allow RSAs to make profits via an additional revenue stream. The same end-result can be achieved by the RSA using Supplier systems under contractual arrangements. The RSA personnel could be granted access to utilise a Supplier's firmware deployment tool (i.e. a contractual / personnel agreement between a Supplier Party and their RSA). This would also allow continued automation of the download-activate sequence of firmware deployment which would be broken under MP207 if the RSA downloaded the firmware image using their own deployment system. Under MP207, there would still need to be contractual agreements in place to allow the RSA to obtain the Manufacturers' firmware images for deployment and to cover the scope of the RSA activities.
OVO Energy	Large Supplier	-
Utility Warehouse	Large Supplier	A supplier could maintain an even higher level of firmware update by being able to readily access the latest firmware from the full range of manufacturers, without each supplier having to negotiate separate contracts with each manufacturer.
Utilita Energy Ltd	Large Supplier	-
ENGIE (ENGIE Power Limited, ENGIE Gas Limited)	Small Supplier	No further comments.

This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.

SECCB_82_2009 – MP207 Impact Assessment Request responses

The Change Board were unanimous in their rejection of the recommendation to request the Impact Assessment for MP207. This document summarises each members vote and the reasons given for the rejection of the Request for the Impact Assessment.

Change Board Member	Vote	Comments
Large Supplier 1 (AH)	Reject	There is no benefits case ¹ , this is not a solution to the problem and a waste of industry time.
Large Supplier 2 (EL)	Reject	No use case has been provided, no business case, the benefits do not align with SEC Objectives, costs do not align to the solution, this will not fix the problem.
Large Supplier 3 (DR)	Reject	We acknowledge there is a firmware problem, but this solution does not solve the problem. The business benefits are not here.
Large Supplier 4 (KC)	Reject	There is no business case
Large Supplier 5 (EJ)	Reject	We acknowledge there is a problem, no point in asking for the IA as the benefits of this solution are not clear or appear to be negative.
Large Supplier 6 (SA)	Reject	There is no viable business case, this doesn't resolve the problem. The proposal has no clear support. It is not helpful that the Proposer is not here,

¹ The Proposer has not provided any evidence and SECAS has not been able to find enough evidence to show a positive benefits/business case.

		they appear to have a conflict of interests as they are looking to enable services they can sell to Parties and no evidence of Parties really needing it.
Small Supplier 1 (CB)	Reject	The solution provided does not address the issue. There is an assumption that Small Suppliers need this, but Small Suppliers have rejected it and it has had no support.
Small Supplier 2 (CT)	Reject	There is no support from Small Suppliers. This is not a good use of industry time and money.
Network Party 1 (JDA)	Reject	This does not solve the issue. There is no support from key Parties. It is a drain on DCC resources and will muddy the waters with respect to responsibility for firmware upgrades.
Network Party 2 (AC)	Reject	There is a lack of business case.
Other SEC Party 1 (NW)	Reject	This does not solve the problem and has no support.
Other SEC Party 2 (IL)	Reject	We agree there is a problem, but this solution will not solve it. There is no evidence that the Suppliers can activate the upgrade once sent. This will be a dilution of accountability on firmware upgrades. We agree with everything already stated by other Change Board members.
Other SEC Party 3 (PCS)	Reject	We are very supportive of the additional services concept, but this is only a partial solution. We cannot support requesting an Impact Assessment when no support has been shown.

This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.

MP207 ‘Allowing Registered Supplier Agents to Maintain Meter Firmware’

Annex F

Legal text – version 1.0

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

Appendix E 'DCC User Interface Services Schedule'

These changes have been redlined against Appendix E version 8.0.

Amend the following rows in the table in DCC User Interface Services Schedule as follows (extract of full table):

DCC USER INTERFACE SERVICES SCHEDULE

Service Reference	Service Reference Variant	Description	Eligible Users	SMETS2+Target Response Time	SMETS1 Target Response Time	Non-Device Services	Notes
11.1	11.1	Update Firmware	Import Supplier, Gas Supplier, <u>Registered Supplier Agent</u>	24 hours	24 hours	✓	In respect of SMETS2+ Devices the DCC must ensure that the associated firmware update has been delivered to all relevant Communications Hub Functions within 5 days of receipt of the Service Request. <u>A Registered Supplier Agent cannot send Update Firmware for a SMETS1 Device.</u>

Amend Section 9 as follows:

- 9 The Monthly Service Metrics and Monthly Service Thresholds (referred to in Section H3.24 for reporting) are as set out in the table below. These shall not apply in respect of SMETS1 Smart Metering Systems. Accordingly, SMETS1 Service Requests and SMETS1 Smart Metering Systems shall be excluded from each of the calculations set out below.

Monthly Service Metric applies to Users acting in the following User Roles**	Monthly Service Metric applies to Service Requests for the following Services	Monthly Service Metric (excluding SMETS1 Service Requests and SMETS1 SMS)	Monthly Service Threshold
Import Supplier Gas Supplier <u>Registered Supplier Agent</u>	11.1 Send Firmware	The total over month m and the previous eleven months of the number of Service Requests; divided by the User ASMSm.	6

Appendix AD ‘DCC User Interface Specification’

These changes have been redlined against Appendix AD version 5.2.

3 MESSAGES SENT OVER THE INTERFACE

Amend the following rows in the table in Section 3.1 as follows (extract of full table):

Service Request Name	Service Reference	Service Reference Variant	Critical	Modes of Operation				Eligible User Roles	Available in relation to SMETS1 Devices
				On Demand	Future Dated Response Pattern	DCC Scheduled	Non-Device Request		
Update Firmware	11.1	11.1	No	No	No	No	Yes	IS GS <u>RSA</u>	Yes

3.8 Service Request Definitions

Amend Section 3.8.17 as follows:

3.8.123 Update Firmware

3.8.123.1 Service Description

Service Request Name	UpdateFirmware
Service Reference	11.1
Service Reference Variant	11.1
Eligible Users	Import Supplier (IS) Gas Supplier (GS) <u>Registered Supplier Agent (RSA)</u>
Security Classification	Non Critical
BusinessTargetID - Device applicable to this request	DCC Access Control Broker
Can be future dated?	No

On Demand?	No	
Capable of being DCC Scheduled?	No	
Command Variants applicable to this Request (Only one populated)	8 – Non-Device	
Common Header Data Items	See clause 3.4.1.1	
Data Items Specific to this Service Request	See Specific Data Items Below	
Possible responses from this Service Request	These are the possible responses applicable to this Service Request. Please see clause 3.5 for more details on processing patterns • Acknowledgement • Response to a Non-Device Service Request Also see Response Section below for details specific to this request	
Response Codes possible from this Service Request	See clause 3.5.10 for Common Response Codes	
GBCS Cross Reference	Electricity	Gas
GBCS MessageCode	N/A	N/A
GBCS Use Case	N/A	N/A

Specific Data Items for this Request

UpdateFirmware Definition

Data Item	Description / Allowable values	Type	Mandatory	Default	Units
FirmwareImage	The Firmware Image corresponding to the Firmware Version This is a base64 encoded version of the GBCS defined Firmware “OTA Upgrade Image”. The Firmware Image is the full OTA Upgrade Image as defined in GBCS. Note that this includes not only the Manufacturer Image but also additional signature and OTA Header information. Please see GBCS for details of how to construct the OTA Upgrade Image	Restriction of xs:base64Binary (max Length = 10240000)	Yes	None	N/A
FirmwareVersion	An identifier representing a firmware image that has been approved for release by the User concerned. The Firmware version as held in the CPL and presented in the format XXXXXXXX where each X is one of the characters 0 to 9 or A to F. This value must align with the firmware version value listed on the Central Products List (excluding the colon separator between octet values) and the Firmware Hash held on the CPL must match the Manufacturer Image Hash pursuant to clause 6.1(i) of the Service Request Processing Document. For avoidance of doubt, there is no direct comparison made between this FirmwareVersion value to the File Version value contained in the OTA Header (as defined by GBCS).	sr:FirmwareVersion (Restriction of xs:string (minLength=1, maxLength = 8))	Yes	None	N/A

DeviceIDList	Comma separated list of Device IDs. Containing a minimum of 1 and a maximum of 50000 Device IDs, each as defined by sr:EUI	Restriction of xs:string (minLength = 23 maxLength = 1199999 pattern = “([A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2}-[A-Fa-f0-9]{2})”)	Yes Minimum 1 and Maximum 50,000 Device IDs	None	N/A
--------------	--	---	--	------	-----

Table 1 : UpdateFirmware (sr:UpdateFirmware) data items

Specific Validation for this Request

See clause 3.2.5 for general validation applied to all Requests.

For this Service Request and as an exception, the Authorisation Check associated to E5 allows the Device's SMI Status to be 'Suspended'

Response Code	Response Code Description
E110101	The Firmware Version is not approved. The Firmware version ID does not align with an entry on the Central Products List.
W110101	<u>A Registered Supplier Agent cannot send Update Firmware for a SMETS1 Device</u> The Update Firmware Warning contains between one and five lists of Device IDs for which the validation failed for each DeviceID: - InvalidDeviceIDList . The DeviceID does not exist or the User is not the Meter or HCALCS Import Supplier - NotCommissionedDeviceIDList. The Meter status is not ‘Commissioned’ or ‘Suspended’ or the Device is not a Meter or a HCALCS - NotApplicableFirmwareDeviceIDList. The Firmware Version is not applicable to the Device - OtherRequestsInProgressList. The Device already has another Firmware update request in progress.InvalidGBCSVersionList. The CHF associated with the HCALCS Device has a GBCS Version prior to v4.1,or the HCALCS Device currently has a GBCS Version that is prior to v4.1.

E110102	The firmware is not marked as active in the Central Products List and Smart Meter Inventory.
E110103	The DCC Systems calculated Hash value over the Manufacturer Image part of the FirmwareImage provided by the User within the Service Request differs from that held in the CPL for the specified FirmwareVersion.
E110105	The firmware image is not constructed as per the GBCS definition, i.e. the FirmwareImage does not contain both an OTA Header and a Firmware Image concatenated together , or where the Target Device is a SMETS2+ Device, the Length of the base64 encoded version of the GBCS defined Firmware “OTA Upgrade Image” exceeds 1024000.

Specific Data Items in the Response

This Service Request synchronous response is defined in the XSD DSPUpdateFirmwareWarning XML element, which contains the list(s) of Device IDs that failed DCC Authorisation / Validation.

Firmware Upgrade using SR11.1 and SR11.3

Step 1: Firmware Distribution

Step 2: Firmware Activation

