

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



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 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
HICALCS	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