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 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 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	Overall view:

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). Our comments and objections are as follows: 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 download 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 *downloading* 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:

Question 3		
Respondent	**Category**	**Response and rationale**
		We believe that the mod will require: • 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.