SECAS Consultation

|  |  |
| --- | --- |
| SMETS2 Interoperability – Suppliers Firmware Consultation | |
| Issued: 24 July 2020  Response due: 21 August 2020  Response to: [SECAS@gemserv.com](mailto:SECAS@gemserv.com) | Contact: Joey Manners  Tel: 020 3314 1441  Email: [Joey.Manners@Gemserv.com](mailto:Joey.Manners@Gemserv.com) |

Summary

In autumn of 2019 BEIS undertook an independent review of assurance for SMETS2 device interoperability on change. The final report was submitted to BEIS on 29 October 2019 and set out ten recommendations relating to test assurance and firmware management. On the request of BEIS the SEC Panel accepted to investigate and action six of these recommendations.

Of the six recommendations three relate to firmware management:

|  |  |
| --- | --- |
| Recommendation 5 | Consider options for increasing monitoring and reporting of device model combinations and interoperability testing |
| Recommendation 6 | Develop and communicate good practice guidance for updating firmware on devices |
| Recommendation 7 | Monitor energy supplier firmware management processes over time and monitor developing commercial arrangements to ensure necessary access to firmware images |

In order to support the delivery of these recommendations we are seeking a better understanding of firmware management arrangements and any issues with them.

SECAS is therefore requesting assistance from Suppliers to understand:

* the maturity of firmware management processes across industry,
* the challenges and issues that Suppliers may be facing with accessing and deploying firmware, and
* the scale and extent of testing against device and firmware version combinations for both installed and gained devices.

SECAS intends to use this information to develop a Best Practice Guidance for industry on the testing, deployment and management of firmware that will be made available to all SEC parties. The information will also be used to compile a report to be discussed at SEC Sub-Committees and SEC Panel to consider the issues raised by industry and to agree solutions and recommendations for any improvements.

A final report will then be compiled for BEIS providing an overview of the analysis, outputs and suggested recommendations.

Responding to this consultation

A set of seven survey questions, and a response form, can be found in Annex A.

To help us process your response efficiently, please email your completed response form to [SECAS@gemserv.com](mailto:SECAS@gemserv.com) with the subject line ‘Firmware Consultation’.

If you have any questions or you wish to respond verbally, please contact Joey Manners on 020 020 3314 1441 or email [joey.manners@gemserv.com](mailto:joey.manners@gemserv.com).

Suppliers are asked to provide responses by 21 August 2020.

Annex A – Consultation Questions and Response Form

| Respondent details | |
| --- | --- |
| **Name** | Click and insert your name |
| **Organisation** | Click and insert the name of the organisation you are responding for |
| **Phone number** | Click and insert a phone number we can call you on with any queries |

|  |  |  |  |
| --- | --- | --- | --- |
| **Q1. Can you access the latest firmware versions for devices within your Smart Metering portfolio?** | | | |
| Yes |  | No |  |
| **1a)** If yes, do you receive firmware from MAP or direct from Meter Manufacturers? | | | |
|  | | | |
| **1b)** If no, is the constraint Technical or Commercial? | | | |
|  | | | |
| **1c)** If unsure, are you aware you can check for the latest firmware on the Certified Products List (CPL)? | | | |
|  | | | |
| **Context:** The aim is to understand whether Suppliers have access to the relevant firmware images for devices installed and gained and if not, what issue(s) they are facing that is preventing access to firmware images | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Q2. Do you undertake checks / testing before deploying Firmware to your Smart Meters?** | | | |
| Yes |  | No |  |
| **2a)** Do you carry out any testing on firmware pre pilot / deployment? | | | |
|  | | | |
| **2b)** Do you use Pilot deployments before mass deployment? If so, what are these? (Duration/volume of Pilot, Variations by payment mode?) | | | |
|  | | | |
| **2c)** What do you consider are the common success criteria for Pilots? (e.g. % devices successfully upgraded; time taken for upgrade; Meter read or Top up success after upgrade) | | | |
|  | | | |
| **2d)** What prerequisites do you have before mass deploying firmware to your smart meters? | | | |
|  | | | |
| **Context:** The aim is to understand what processes, activities, and control mechanisms (or stage gating) that Suppliers utilise to assure, test, and deploy firmware to their portfolio of SMETS2 devices. We are looking to understand what business processes users test to assure firmware, whether that varies by payment mode or device type and the success criteria to proceed to the next phase. We are also keen to understand whether Suppliers utilise Pilot deployments where limited devices are upgraded, and a set criterion of ‘success’ is monitored to provide confidence to proceed with mass deployment. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Q3. Do you utilise baseline\* firmware versions for devices installed and gained?**  \*The definition of baseline within the context of firmware is whether users have a minimum version for firmware that they have tested and approved that users try to ensure their portfolio of devices are on. There may be later firmware versions for that device | | | |
| Yes |  | No |  |
| 3a) For Gained Smart Meters, do you identify and attempt upgrade on gaining devices on older firmware versions or batch upgrade at a later date or volume? | | | |
|  | | | |
| 3b) For installed meters on older firmware, do you upgrade shortly after installation or batch upgrade at a later date or volume? | | | |
|  | | | |
| **Context:** The aim is to understand whether Suppliers utilise firmware versions that they have assured and feel comfortable with or just look to upgrade to the latest version for devices installed or gained through Change of Supply. The aim is also to understand whether Suppliers upgrade devices on installation or gain, or whether the activity of downloading and activating firmware is done at a set time or upon reaching a set volume of devices that require upgrading | | | |

|  |
| --- |
| **Q4. What action do you take if the upgrade is unsuccessful? (either that the firmware image delivery or activation has failed)** |
|  |
| **Q5. When Upgrading Firmware, are there specific "good practices" you always consider in planning, e.g. ESME before GSME, Time of day, per region, post code, other please specify?** |
|  |
| **Q6. How many firmware deployments are you completing a year currently?** |
|  |
| **6a)** Do you have a view as to whether this is likely to reduce or increase in the future (next 6-12 months)? |
|  |

|  |
| --- |
| **Q7. To what extent do you test against Device Model Combinations (DMC)\* within your portfolios?**  \*The SMETS2 Device Model Combination(s), represents the combination of CHF, ESME, GSME and if applicable an IHD/PPMID devices and firmware version |
|  |
| **7a)** Do you know how many DMCs are within your portfolio as a result of installs and gains? |
|  |
| **7b)** Do you actively execute testing against Device Model Combinations that you gain? If so, to what extent? (e.g. what types of test cases are executed) |
|  |
| **7c)** Do you actively execute testing against Device Model Combinations that you install? If so, to what extent? (e.g. what types of test cases are executed) |
|  |
| **Context:** The aim is to understand the scale of unique SMETS2 DMCs that exist within Suppliers portfolios (Installed and Gained) and to what extent that Suppliers are currently testing against these DMCs, to identify whether there is a risk that untested SMETS2 DMCs are being operated in Production |