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.

SECMP0009 'Centralised Firmware Library'

2nd September 2016

Meeting 4 Minutes

Attendees:

Working Group 3 Member	Organisation
Mark Pitchford (SECMP0009 Proposer)	Npower
Paul Saker	EDF
Rachel Goozee	SSE
Robert Williams	EON
Andrew Willman	BEAMA
Elias Hanna	Landis Gyr

Other attendees	Organisation
Adam Pearce	DCC
Jill Ashby (Chair)	SECAS
Sebastian Rattansen (Lead)	
Urszula Thorpe (SECAS)	
Keith Phakoe (Support/ Meeting Secretary)	

Apologies:

Working Group 3 Member	Organisation
Kay Houghton	Calvin Capital

1. Introduction

After welcoming the Working Group (WG) Members, the Chair informed the WG that the Refinement Process of SECMP0009 – Centralised Firmware Library (CFL) continued and the scope of this meeting was to solidify the requirements for SECMP0009.

1.1 General comments received on WG3-3 minutes

The Chair informed the WG Members that the draft minutes distributed after the last WG meeting were final and were published as such.

1.2 Revised Timelines

SECAS informed the WG that the Panel agreed the proposed timetable adjustments[1] for some Modification Proposals, including SECMP0009, at their August 2016 meeting. The proposed new target date for the draft Modification Report for SECMP0009 to be submitted to the Panel is April 2017.

The Chair highlighted that to meet the revised timetable, a WG consultation on SECMP0009 needs to take place in Q1 2017.

2. Objectives

SECAS and the Proposer recapped the objective of the CFL which is to have a single place to obtain firmware images in a standardised format. The CFL would replace the current ad hoc, and distributed arrangements for obtaining images that exist between energy Suppliers, Meter Asset Providers (MAPs), and manufacturers.

The WG noted that further work is needed to define the requirements for SECMP0009, and highlighted that the underlying commercial considerations will be considered bi-laterally by the relevant stakeholders. However, it was recognised that resolution to the commercial issues was necessary to support the business case for SECMP0009. It was further noted that consideration of an alternative may be prudent if the underlying issues could not be resolved.

3. SECMP0009 Solution Design

Prior to the WG considerations for further refining the solution definition, the Chair updated the WG regarding an informal discussion with the Security Sub-Committee (SSC) about potential security concerns. At this stage, indications were that a CFL, provided it utilised secure file exchange mechanisms, was not of itself a material security risk. However, the storage of all Release Notes in one place may pose more of a risk and require additional security controls. It was acknowledged that, once requirements for the CFL are firmed up, formal input will be sought from the SSCto help mitigate any risks to the end-to-end system.

ACTION SECMP09_01: WG to obtain SSC views on SECMP0009 solution at the appropriate stage during Refinement Process

The WG considered the requirements collated to date.

[1] See Panel paper SECP_35_1208_07

3.1 Suppliers requirements to upload images into the CFL

The WG considered two options:

a) Requiring Suppliers to upload images into the CFL – despite advancing the business case for this Modification Proposal, there were concerns that a lack of clarity on the contractual terms between Suppliers and MAPs could put Suppliers at risk of being in breach of such an obligation.

b) No obligation on Suppliers to upload images into the CFL – Suppliers argued that given their obligations to maintain devices' compliance, they would have an incentive to keep the CFL up to date, and therefore no obligation was necessary.

3.2 Sharing firmware images from the CFL

An underlying issue is sharing images with other Suppliers via the CFL. SECAS highlighted this could be a function of the CFL within the Smart Energy Code (SEC) consistent with the general obligation [in SEC Section F] on each Supplier to ensure compliance of a meter with the Technical Specifications and ensure that they can communicate with the DCC systems. SECAS took an action to pull out the key provisions of the SEC for device compliance within the SEC to highlight the accountability.

ACTION SECMP09_02: SECAS to draw out SEC obligations for assurance and compliance of devices.

Notwithstanding any SEC provisions, it was recognised that Suppliers would need to consider their contractual position with MAPs with the right to use images from the CFL. The WG agreed that Suppliers and manufacturers would discuss this matter outside of this WG, while this WG would focus on developing requirements for the CFL.

3.3 Types of images would to be uploaded into the CFL

Two options were discussed:

a) The CFL would only hold images that maintain devices' compliance with the applicable SMETS version plus any that address an identified vulnerability. This would mean that the CFL would only hold the images that, currently, would be made available to each Supplier on request., or

b) The CFL would hold all types of images but the CFL would have controls in place to ensure that a Supplier wishing to access an image has a right to view and download it.

The WG were of the view that option 3.3b would be difficult to manage, particularly if the CFL provider would need to have access to each MAP-Supplier-manufacturer contract as part of controlling access. Furthermore, monitoring whether a Supplier accessing an image was entitled to that image, i.e. as it had the relevant device in its portfolio, would be onerous. SECAS confirmed that a general rule could be applied such that a Supplier only accessed images that were relevant to devices in its estate, including where inherited through a Change of Supplier (CoS) event. The WG agreed that option 3.3a was easier to manage. Although option 3.3a was chosen, the WG agreed that should the controls surrounding the CFL be favourable to everyone's satisfaction, option b) could be explored.

3.4 Administering duplicate images in the CFL

The WG discussed how the CFL provider would manage duplicates. The WG discussed the following three options:

a) 'Synchronisation': in this option, all images would be uploaded. There would be synchronisation of the images in the CFL, identification, and reporting. Duplicates would be deleted manually by the CFL Provider.

b) 'Sweep': in this option, all images would be uploaded. A periodic sweep of contents of the CFL would occur to see if any duplicates had been uploaded. The system would then automatically delete duplicates.

c) 'Gateway': here images being uploaded would be checked against the contents of the CFL. If a duplicate is identified, the image would be held there and not uploaded. The WG favoured this 'gateway' process.

3.5 CFL access / download procedure

The WG considered issues concerning the download procedure. Two options were set forth:

a) Upon a request to download an image, the CFL Provider would check whether the Supplier has the right to download it.

b) Suppliers would have access to view and download all images.

For the avoidance of doubt, in order to access the CFL (under both options), the Supplier would need to demonstrate that they are a User in the User Role of Import Supplier or Gas Supplier before they were given access to the CFL (previous WG discussions had agreed that there would be varying permission levels for access).

The WG suggested that compliance monitoring under option 3.5a could be achieved on an ad hoc and ex post basis. For example, it might be that an audit could verify whether a Supplier had the right to download an image, similar to the Independent Privacy Auditor audit for privacy under the SEC. However, option 3.5a could be complex to manage if it extended to verifying contractual arrangements. However, under option 3.5b, a universal right to all images would not offer a compliance regime and so may not meet the desired objective of controls.

A question arose of whether, in order to maximise the benefits of this Modification Proposal, Suppliers should be prohibited from obtaining firmware images via means other than the CFL. The WG concluded that such exclusion was not necessary as Suppliers would be naturally incentivised to use the CFL.

Access and download controls can be considered further following the offline discussions referenced in Section 2 of these Minutes.

3.6 Liability

The WG then focused its discussion on liability; specifically, recovery for loss if a firmware image downloaded from the CFL caused physical damage to a device. This was an issue even if the image was obtained directly from the manufacturer. It was noted that firmware images would likely be tested during their development, and Suppliers may test them as part of their ongoing assurance of devices for which they are responsible. It would be prudent for checks to be made before deployment to installed devices that the image works as expected, and that any deployment instructions are

understood. In the case of damage, if a Supplier had an issue with a manufacturer or MAP, this would be outside the SEC.

3.7 Scenarios: When this process will be used

The WG agreed that the only use cases that need to be consolidated for SECMP0009 concern firmware images with the potential to be deployed to meters for reasons of an upgrade (noting that it may not be required to upgrade a meter to e.g. a new Technical Specification version[2]) or to deal with known issues such as reported security vulnerabilities and defects in the existing firmware. The WG agreed that a firmware upgrade would not be an automatic outcome of a CoS event, rather, it would mean that the new Supplier may need to check whether any images in the CFL relates to a meter it has gained. It would be for the incoming Supplier to determine the appropriate time to do this.

The WG discussed elective services and came to the conclusion that they were beyond the scope of SECMP0009 due to their bi-lateral nature.

3.8 End to End Considerations

An update from the MAP representatives noted that they are supportive but neutral on SECMP0009, and will continue to facilitate liaison with manufacturers as long as no additional operational requirements fall to them.

The scope of this WG is a purely process driven solution to meet the aims of SECMP0009. Suppliers will be responsible for ensuring that they use the correct firmware, whether it be from the CFL or directly from the manufacturer and have appropriate commercial arrangements to underpin use of firmware images. In light of the discussion around the business case, the Proposer acknowledged that there might be other mechanisms (outside of the Modifications Process) to procure a CFL.

The CFL would have to have a secure solution for the appropriate handling of release notes and the Egress system used by the SSC was mentioned as an example of a secure system of information transfer. It was not intended as a basis for this solution, rather a way of indicating a working procedure that was secure and effective for all interested parties.

3.9 Procurement of the CFL

The WG then considered who would procure the CFL. Two options were discussed:

a) DCC

b) The Panel

It was noted that in order to make an informed choice on the above options, a complete solution, including SSC input, needed to be worked out. Key points to consider were how access control to the CFL would work, and a clear definition of the contents and functions of the CFL.

[2] Under Transition governance, rules for the version configuration of concurrent Technical Specifications, and when change are retrospective or forward are in development – see Changes to the Supply Licence Conditions, the DCC Licence and the SEC to accommodate multiple versions of Technical Specifications and multiple versions of DUIS section of the consultation issued by BEIS on 22nd September at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/554627/16_09_22_September_2016_SEC_Consultation.pdf.

4. Next Steps

The WG concluded that a process diagram was needed in order to map the solution, for discussion at the next meeting.

ACTION SECMP09_03: SECAS to build a strawman process flow that maps SECMP0009 proposed solution

Noting the forthcoming DCC Live will be a focus for many of the WG members in the coming weeks, it was decided to hold the next WG in late October/November 2016. This will give time to develop the process diagram. The Proposer noted that the progression of SECMP0009 will be discussed at the next Supplier forum where the CFL concept was first raised, and the WG will be updated on their views.