SEC
Smart Energy Code

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.

SECMP0024

'Enduring Approach to Communication Hub Firmware Management'

Modification Report

Version 1.0

28 July 2021

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

This document also has five annexes:

- **Annex A** contains the business requirements for the solution.
- **Annex B** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.
- **Annex C** contains the full Data Communications Company (DCC) Impact Assessment response.
- **Annex D** contains the full responses received to the Refinement Consultation.
- **Annex E** contains the DCC statement around the costs. This annex is classified as **RED** – Parties can request a copy by emailing sec.change@gemserv.com.

Contact

If you have any questions on this modification, please contact:

Joe Hehir

020 7770 6874

joe.hehir@gemserv.com

1. Summary

This proposal has been raised by Rob Williams from E.ON.

The Proposer notes that there is nothing in place to automatically notify Suppliers once firmware updates have been activated on Communications Hubs (CHs). The Proposer also considers there to be a lack of a formalised process for managing firmware updates to CHs between the DCC and Suppliers.

The Proposed Solution is for the DCC to generate an Alert to Responsible Suppliers upon successful activation of CH firmware. This Alert will contain the firmware version of the newly activated firmware.

In addition, the DCC will update its CH Firmware Management Overview document and make this publicly available on the DCC website. This document is a DCC owned document and is not referenced in the SEC. It therefore does not require a Modification Proposal to amend and so does not form part of the Proposed Solution, but has been updated alongside SECMP0024 to further support the solution.

This modification's impacts will be limited to the DCC and Suppliers. It will incur a central implementation cost of approximately £512,000. This is a Self-Governance Modification and the targeted implementation date is the June 2022 SEC Release.

2. Issue

What are the current arrangements?

DCC obligations for SMETS2+ CH firmware

Section 5 of SEC Appendix AB 'Service Request Processing Document' contains the obligations for the DCC in relation to Smart Metering Equipment Technical Specifications (SMETS) 2+ CH firmware.

Before updating firmware on CHs, the DCC must notify relevant Users of its intention at least seven days in advance of any update.

Where the firmware updates are needed for "urgent security related reasons", the DCC must take all reasonable steps to notify Users in advance of making the updates but does not need to give seven days' notice. In these scenarios, where the DCC has not notified Users in advance, it shall notify them of having done so as soon as is reasonably practicable after the event.

The DCC must also validate the credentials of the firmware and its relevant entries in the Central Products List (CPL).

What is Hypercare?

DCC Change Request 203 'CH Firmware Upgrade Hypercare' was raised as an interim CH firmware management solution. However, no enduring solution is currently available. The processes put into place by this Change Request were intended to provide DCC Customers the ability to control the deployment of new CH firmware for six months after the firmware is made available. The objective of Hypercare is to ensure that DCC Customers have time to prepare and gain confidence that any new

CH firmware version will not affect their deployed Home Area Network (HAN) Devices. The initial Proposed Solution to SECMP0024 consisted of two solution options which were modelled on the Hypercare approach. These have both now been discarded due to the implementation costs and lack of a business case.

What is the issue?

The Proposer notes that there is nothing in place to automatically notify Suppliers once firmware updates have been activated on CHs.

In addition, the Proposer considers there to be a lack of a formalised process for managing firmware updates to CHs between the DCC and Suppliers.

What is the impact this is having?

The following impacts result from the lack of any notification to Suppliers of when a firmware update has been made to a CH:

- Suppliers are unable to track progress of their pilot CH firmware update rollout.
- Suppliers are not made aware of the new firmware version activated and therefore have to periodically query the Smart Metering Inventory (SMI) to obtain this information.
- The lack of a notification prevents Suppliers from being able to plan the deployment of firmware updates to other HAN Devices as a result of any CH firmware updates.

The DCC believes it follows a process for carrying out firmware updates to CHs that takes into consideration the impacts on Suppliers. This includes various decision points throughout that must be passed in order for the DCC to proceed with a CH release:

- Content agreement
- Development and testing
- Over-the-air (OTA) deployment
- Manufacturer supply chain

However, this process is not formalised and Parties do not have sight of it. This means Suppliers are unaware of how and why decisions are made.

The Proposer considers, due to the lack of a formalised process for managing firmware updates to CHs, that there is also a risk that a firmware update with defects or interoperability issues could be deployed and activated to significant numbers of CHs without Suppliers knowing in advance or Suppliers only being made aware sometime after the upgrade has taken place. This could create a range of issues arising from a DCC deployed CH firmware update occurring concurrently with:

- A programmed configuration change to a Supplier’s smart metering Device e.g. a Change of Supplier (CoS) event, price change, or tariff change;
- A Supplier’s scheduled firmware deployment to a smart metering Device;
- Historical consumption data being uploaded to Supplier systems on behalf of the consumer; or

- A consumer attempting to interface with the Smart Metering System (e.g. a delay in a prepayment top-up), leading to a poor customer experience.

Furthermore, the Proposer notes that these issues could go undetected entirely or be discovered at a later date. This would then require investigation to determine that the problems were a result of a firmware upgrade. In addition, delayed identification of problems resulting from a DCC firmware upgrade, could allow further tranches of defective firmware to be deployed and activated, further amplifying the problems outlined above.

Impact on consumers

If this issue is not resolved, it could increase the chance of defective firmware being deployed to CHs. This could lead to increased HAN stability issues which could lead to consumers' Devices not working as they should, a poor consumer experience and an additional consumer contact workload for the Supplier. Furthermore, it could add to lack of consumer confidence in the Supplier and the Smart Metering Implementation Programme (SMIP) leading to reputational issues to the Supplier and the SMIP.

3. Solution

Proposed Solution

The Proposed Solution is for the DCC to generate an Alert to Responsible Suppliers upon successful activation of CH firmware. This Alert will contain the firmware version of the newly activated firmware. Suppliers will then be aware of when CH firmware updates have been made.

In addition, the DCC will update its CH Firmware Management Overview document and make this publicly available on the DCC website. Although this does not currently require a change to the SEC, this piece of work has been monitored by the Working Group and will help to resolve the issue highlighted by the Proposer. As a result, the progression of this modification is not dependant on the document being available. However, SECAS will continue to monitor its progression and make it available to Parties once it has been approved by the DCC.

The business requirements for this solution can be found 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

Supplier Parties

Suppliers will receive a DCC Alert once firmware Images are activated on CHs. The Alert will contain the firmware version for the updated CH. The new Alert will result in the following benefits for Suppliers:

- Suppliers can track progress of pilot CH firmware update rollout;
- Suppliers can update back-office systems to record the active firmware version on each CH, avoiding the need to query the SMI periodically to obtain this information; and
- Suppliers can plan the deployment of firmware updates to other HAN Devices following activation of the new CH firmware.

In addition, with the DCC publishing its CH Firmware Management Overview document on the DCC website, the document will be easily accessible and the process more transparent. This benefit is not dependent upon this modification being approved.

Refinement Consultation respondents noted that SEC Parties will be required to make system changes to receive the new Alert and process it accordingly. One respondent added that the benefits of this modification outweigh the costs that will be incurred.

Another respondent advised that the new Alert would help it to understand when new firmware has been updated on CHs and allow it to maintain Device details appropriately.

DCC System

This modification will impact the Data Services Provider (DSP) only.

The DCC User Interface Specification (DUIS) Extensible Markup Language (XML) Schema will be updated to include the definition of the new DCC Alert.

The full impacts on the DCC Systems and the DCC's proposed testing approach can be found in the DCC Impact Assessment response in Annex C.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Appendix AD 'DCC User Interface Specification'

- Schedule 11 'TS Applicability Tables'

The changes to the DUIS required to deliver the Proposed Solution can be found in Annex B.

SEC Schedule 11 and the Technical specification versions

Annex B does not include the Schedule 11 changes as any changes would only reference the version of the DUIS implemented in the given release, including its implementation. The new DCC Alert is expected to only impact the next Sub Version of the DUIS at the time of implementation. However, this is dependent upon the full scope of DUIS changes being implemented in the given release, including other modifications and/or the Department for Business, Energy and Industrial Strategy (BEIS) designations. The Technical Specification versions and the updates to Schedule 11 will be consulted upon with the DCC and the Technical Architecture and Business Architecture Sub-Committee (TABASC) prior to the given release.

Consumers

The new DCC Alert will make Suppliers aware of CH firmware updates and could allow them to address any HAN and Wide Area Network (WAN) issues more quickly if they arise. Suppliers may also be able to inform the DCC if a firmware upgrade is causing issues or has a defect to allow the DCC to stop the rollout escalating the magnitude of any problems. This will have consumer benefits as it will reduce the risk of any HAN stability issues that could arise from a CH firmware update.

Other industry Codes

This modification will not have any impacts on other industry Codes.

Greenhouse gas emissions

This modification will not have any impact on greenhouse gas emissions.

5. Costs

DCC costs

The estimated DCC implementation costs to implement this modification is £512,003. The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	**Cost**
Design, Build and Pre-Integration Testing (PIT)	£202,395
Systems Integration Testing (SIT), User Integration Testing (UIT) and Implement to Live	£309,608

More information can be found in the DCC Impact Assessment response in Annex C. A further breakdown of the DCC's costs is available in Annex E – this Annex is classified as RED in accordance with the Panel Information Policy and is only available to SEC Parties by emailing sec.change@gemserv.com.

SECAS costs

The estimated SECAS implementation costs to implement this modification is two days of effort, amounting to approximately £1,200. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.

SEC Party costs

If this modification is approved, the central implementation cost will be socialised across all SEC parties. Also, the new DCC Alert will need to be implemented in a new version of the DUIS. As a result, Parties that choose to uplift to this new version will incur additional internal costs to uplift to support new version, but this would include all modifications associated with this uplift.

Three Large Suppliers advised in the Refinement Consultation that they would incur costs as a result of this modification. This would be due to updating systems and business processes to utilise the new DCC Alert and to automatically update the firmware versions of CHs in their systems. One Supplier specified that there would be a cost to it to automatically process the firmware version from the Alert payload.

The Proposer noted effort and costs are thought to be relatively small compared to overall budgets.

6. Implementation approach

Approved implementation approach

The Change Sub-Committee (CSC) has agreed an implementation date of:

- **30 June 2022** (June 2022 SEC Release) if a decision to approve is received on or before 30 August 2021; or
- **2 November 2023** (November 2023 SEC Release) if a decision to approve is received after 30 August 2021 but on or before 2 December 2022.

This modification will impact the DUIS and, for efficiency, should therefore be implemented in a scheduled SEC Release in which other DUIS changes will be implemented. This would also minimise SEC Party costs. The June 2022 SEC Release will be the next DUIS impacting SEC Release.

The DCC has advised that it will need an 11-month lead time to implement this modification. Although a Change Board decision in August 2021 will only leave ten-months until the June 2022 SEC Release, the DCC has confirmed it could still implement SECMP0024 in the release if a decision to approve is received by the August Change Board meeting (25 August 2021).

The next DUIS impacting SEC Release following the June 2022 SEC Release is expected to be in 2023.

Refinement Consultation respondents advised that would need to make system changes to handle the new Alert. One respondent advised they would need a minimum of 6 months to do this.

7. Solution development

Previous proposed end-to-end CH firmware management solutions

This section covers the Working Group's assessment and development of the previous iterations of the Proposed Solution that were included in the first Preliminary Assessment. Following this Assessment, these options were discarded in favour of the current Proposed Solution (see pages 15-16).

The current existing CHs arrangements

The Working Group discussed the current arrangements for updating firmware on CHs, noting that the DCC and its Communication Services Providers (CSPs) are not constrained in how they deploy and activate such updates. The only requirements are that any updated firmware must pass the relevant testing set out in SEC Section T 'Testing During Transition' and that DCC Users are notified seven days in advance of the activation of any firmware Image.

The DCC highlighted the testing provisions that came into legal effect in early February 2017. It noted that there are currently no requirements for the extent of User testing of new CH versions against existing Devices. However, where a new firmware version is introduced, User testing requirements shall be set out in the applicable DCC Change Request associated with the firmware release.

Initial consideration of the solution

The initial Proposed Solution sought to develop and implement an agreed enduring process for the deployment and activation of CH firmware updates. This would see Suppliers being informed by the DCC when CH firmware updates were available and allow them to specify the date and time, within a period defined by the DCC, when these would be deployed. The requirements and specifications for this process included two solution options that were assessed by the DCC:

1. Use of DUIS Service Requests; and
2. Use of a DCC operated Web Portal.

The Proposer did not suggest that the responsibility for CH firmware management be transferred to Suppliers. This solution intended only to enhance the firmware deployment and activation process by allowing Suppliers to manage the time any updates were deployed by the DCC to mitigate the Proposer's identified risks. These options were eventually discarded in favour of the current Proposed Solution (see pages 15-16).

Discussions followed on whether Suppliers would also want to request firmware activation in addition to deployment. Several Working Group members highlighted that this would enable simultaneous activation on various Devices on a Smart Metering System. SECAS highlighted that this requirement would impact the SEC security arrangements and would be of interest to the Security Sub-Committee (SSC). It also noted that the requirement would likely increase the cost of the modification considerably. The Working Group asked how the cost to include activation would be justified. The Proposer confirmed that the scope of this modification is for Suppliers to request firmware deployment only.

The DCC highlighted that CSPs would deploy firmware in line with the Installation Validity Periods (IVPs) and Maintenance Validity Periods (MVPs), and in the most cost-effective manner. Therefore, considerations on how firmware updates could be classified by severity and priority would need to be made in relation to notifications prior to deployment.

The Working Group agreed that Registered Supplier Agents (RSAs) should also be included within the scope of the modification.

Notifications and classifications of CH firmware updates

The Working Group discussed the business requirement where the DCC would notify Parties of an impending CH firmware update. Members agreed the DCC should notify Parties of an impending firmware update at least six months in advance of doing so. The Working Group agreed that this timeframe would need to be flexible because of the level of unknown possibilities with firmware updates. It suggested that an existing Sub-Committee, such as the Operations Group, could be used to decide and review roll-out timeframes on a release-by-release basis.

The DCC advised that Users would be informed of CH firmware updates via release “road maps” and release notes. For core Releases, Release Notes would be published following SIT and UIT. Users would be notified of maintenance Releases once the Release was ready for production. Release Notes are available to all DCC Users on the DCC’s operational SharePoint.

The Working Group considered that classifying each CH firmware upgrade within the Release Note could slow the User’s decision to deploy CH firmware using the proposed safe launch process. Release Notes may be too granular, and Small Suppliers may not have the time or resources to interrogate each Release Note.

Discussions followed on whether the DCC should also notify Users of CH firmware updates for security or emergency Releases. SECAS highlighted the DCC does not need to notify Users if the firmware update is required for urgent security related reasons but that such updates are considered by the SSC. However, the DCC advised that in the event of a security/emergency incident, a Release Note would be issued as early as possible.

The Working Group agreed that Users’ priority was to be able to use the proposed new safe launch process for CH firmware updates included in core and maintenance Releases. It was agreed that the classification of all firmware updates (including security/emergency events), and necessary timescales, should be requirements of this modification. However, the ability to safe launch security/ emergency CH firmware updates would not be a requirement of this modification. It was also agreed that the DCC would need to develop the framework for classifications and define them with a priority criterion.

SSC views on security related Communication Hub releases

Prior to the request of the first Preliminary Assessment, the SSC was provided with an update on the business requirements and the two solution variants to be assessed by the DCC. SSC members noted the importance in making sure the DCC maintained the right to override the timescale for a firmware update in case there was a risk of a security issue which needed to be implemented urgently. SECAS confirmed this had already been specified for security purposes and explicitly stated in the business requirements noting that, ‘where necessary the DCC can set the date on which the firmware version will be automatically deployed earlier or later than the normal date of six months from the point of notification’.

The SSC agreed that, to be able to assess the security implications arising from the proposed solution, the DCC would need to carry out a risk assessment once the solution has been confirmed, and that this should be made available to the SSC. The risk assessment should include:

- Any security risks and proposed mitigations arising from the solution itself; and
- Any risks arising from failed firmware upgrades via the new solution (recognising that there is still the potential for upgrade failures due to a variety of circumstances and which could lead to stranding of assets etc).

Safe launch process

The Proposer and the Working Group discussed which Supplier would be responsible for the proposed safe launch process where there are different Suppliers for the Electricity Smart Metering Equipment (ESME) and the Gas Smart Metering Equipment (GSME). It was suggested that the Working Group should agree requirements for a single Supplier scenario for both ESME and GSME, before considering requirements and communications for a split Supplier scenario. The Proposer and Working Group also agreed that participation in the safe launch process should be optional for Suppliers.

The Working Group agreed that a new Service Request to instruct the safe launch process was the most efficient method. The proposed new Service Request would specify the Device IDs that the DCC should deploy and activate firmware to. The new Service Request would have a similar design to the current SR11.1 ‘Update Firmware’ and the DCC would be required to deploy the firmware within a five-day Target Response Time (TRT). However, Suppliers would not send another Service Request to activate the firmware, unlike the process for firmware updates on ESME and GSME.

Incident Management

The Working Group discussed how the DCC and DCC Users could extend the safe launch process duration, in order to fix issues prior to mass deployment of CH firmware updates. The Working Group noted that a reporting procedure was required for when problems occurred during the deployment of CH firmware updates. Currently, all issues must be raised via the DCC Service Desk and are pooled and attended to as and when they are picked up. A suggestion was raised that the Incident Management Process be reviewed as a process would be required to enable Suppliers to be able to escalate problems with Communication Hub firmware upgrades more quickly within the DCC Service Desk, with the DCC categorising these in order of severity level. The DCC would take on the responsibility of monitoring issues with the roll-out and updating Suppliers on the status.

The DCC highlighted that an incident “ticket” could be raised if a CH firmware update impacted the HAN. However, the DCC noted that it needed to understand the impacts of a safe launch process from an operational perspective, as some issues may not necessarily be for the DCC to resolve. Therefore, the DCC agreed to investigate its problem management procedure further to see how it could feedback issues to Suppliers, subject to competition law.

SECAS highlighted an assumption that the DCC would not mass deploy firmware updates if Suppliers raised incidents in relation to broken HANs or other defects or vulnerabilities. The Working Group agreed that no further requirements were needed in relation to incident management, and the DCC would confirm via its future assessments.

Major Incidents and Major Security Incidents

The Proposer advised that the intention of the modification was to manage CH firmware deployment for all types of CH releases. This was because firmware updates to fix Major Incidents and Major Security Incidents could still cause HAN stability issues.

The Working Group noted that the Suppliers are ultimately responsible for the HAN, and the DCC will only be in breach if it did not meet its SEC obligations. Therefore, the risk still applies to Major Incidents and Major Security Incidents and the Working Group agreed that all types of CH releases should be within the scope of this modification.

Amendments to the roll-out of CH firmware updates

In order to manage the impacts of an incident, the DCC must be able to amend the roll-out of CH firmware updates during deployment. Working Group members suggested a review process be established based on the severity of the incidents reported during the early roll-out phase of new CH firmware. The outcome of the review process would then result in:

- Proceeding with the roll-out as planned;
- Pausing the roll-out;
- Delaying the end-date of the roll-out; or
- Stopping the roll-out completely.

The Working Group suggested that the governance should sit with the Operations Group.

Split Supplier scenarios

The Working Group discussed four options for handling split Supplier scenarios, with an additional option to exclude Split Supplier premises from the scope of the modification;

- Option 1: Lead Supplier instructs firmware updates
- Option 2: Supplier collaboration on firmware updates
- Option 3: Service Requests for all Responsible Suppliers
- Option 4: Excluding Split Supplier Premises from firmware updates

The Working Group raised concerns as to how liabilities resulting from each option would be managed. The consensus was that Option 1, Option 2 and Option 4 were essentially the same solution from a DCC perspective, and so would be included as a single option in the first Preliminary Assessment. The Working Group believed that Option 1 would be the easiest option to implement, but liability would be the biggest issue here.

Members noted that the least impactful solution for customers was collaboration between Suppliers. The Proposer opted to progress a business requirement whereby in a split Supplier scenario, both the Import and Gas Suppliers needed to coordinate CH firmware deployments. The solution would provide the functionality that requires both Suppliers to agree to proceed in the event that one Supplier wishes to deploy earlier than the DCC's planned deployment date.

Post DCC Firmware Management Consultation – A web-portal based solution

In November 2018, in parallel with this modification, the DCC issued a separate consultation asking how firmware management should work. After noting the responses to this, the Proposer confirmed the updated iteration of the SECMP0024 proposed solution would allow Suppliers to carry out firmware upgrades at different times via scheduling, rather than all together, and the entire process could be voluntary until there was a need for a compulsory firmware upgrade. The DCC noted there may also be a point in the future when all CH firmware upgrades return to being managed solely by the DCC; however as stated within the DCC Firmware Management Consultation this will only be after an appropriate consultation with all SEC Parties.

The DCC approach would be loosely modelled on that used for the Hypercare project and would use a web-portal type interface for Suppliers. This portal would not require Service Requests, which is a considerable difference to the original solution proposed under SECMP0024. Additional tooling will be required to replace the spreadsheets used currently with Hypercare and to move to an interface similar to that of the Self-Service Interface (SSI). Notifications and alerts would then be managed via the web-portal.

It was confirmed there would be a pilot phase to ensure Suppliers were in control of deciding which of their customers would be upgraded and when, protecting those at risk such as vulnerable customers to ensure they were not part of any early deployments. There would also be split Supplier approvals whereby Suppliers could use the interface to see where one Supplier has approved an upgrade to the CH and react as appropriate, without disclosing details of the Suppliers to each other.

How will firmware be tested?

One Working Group member queried the testing approach that would be taken for CH firmware updates prior to them being released. They wanted to understand the details of the testing that would be used and what User testing would be involved, as previous new CH firmware versions could not be deployed in Production despite initially passed testing. The Working Group queried whether there was a role for a group such as the Testing Advisory Group (TAG) in this. However, it concluded this was not a matter for SECMP0024 to resolve, as it was raised to resolve the issue of the firmware being deployed. The DCC also noted workshops were being set up to gather more detail in this space.

How would the solution be governed?

Suppliers questioned whether they would be able to upgrade a CH if Devices joined to that CH could not be upgraded, e.g. In-Home-Displays (IHDs) and Prepayment Metering Interface Devices (PPMIDs)[1]. Should the solution be optional rather than mandatory, there could be a risk of Suppliers not carrying out upgrades to CHs if they thought the upgrade might negatively affect the HAN and cause disruption to other devices and the connection in general. Suppliers queried whether there was the potential for the solution to be implemented in alternative ways should there be little governance in place.

[1] SMETS2+ PPMIDs will be over-the-air (OTA) upgradeable following the implementation of SECMP0007 'Firmware updates to IHDs and PPMIDs' which has now been approved.

Suppliers raised concerns over the DCC having sole responsibility of upgrades in the future and a potential lack of governance should this not be passed through as a Modification Proposal. The DCC acknowledged SEC Parties' concerns and agreed with the process for the implementation of upgrades to be documented in the SEC so that the industry could be confident in the agreed solution. As a result, the DCC brought its proposals from the DCC Firmware Management consultation into SECMP0024 to ensure appropriate governance and to allow SEC Parties to select the most appropriate solution.

The solution proposed by the DCC would need to be enduring, and it was questioned whether a Modification Proposal would be required to implement a web-portal. The Working Group agreed that it would be beneficial to have a process written down and governed via the SEC, to prevent changes from taking place in the future without adequate warning or consultation.

How will Suppliers' systems be affected?

The Working Group questioned how Suppliers would be able to manage and merge the web-portal with their internal systems and firmware portfolios. The Working Group requested a side-by-side comparison of the two solutions to be presented, as well as cost expectations for both, in order to make an informed decision. This would also assist in understanding the impacts to Supplier systems, the scale of the change required and the timescales. The Working Group asked whether the implementation for the DCC's web-portal solution and the original Service Request-based solution would have the same impact on the CSPs. Members considered that the lead time to implement the web-portal could be much shorter than introducing new Service Requests. The lead times for each option would be drawn out in the first Preliminary Assessment response.

Members raised concerns over how user friendly the web-portal would be. Suppliers were already well-versed in how to use Service Requests, and members felt that the consensus could be to use these based on experience.

The Working Group highlighted the need to avoid any clashes or problems with firmware upgrades in CoS situations. There would need to be a marrying up of information between Customer Relationship Management (CRM) systems and the portal, potentially to have information updates in real-time.

Will the proposed solution be a uniform approach?

The DCC confirmed the proposed solution was modelled on Hypercare. However, Suppliers noted they had experienced different levels of service from the CSPs when it should be a uniform approach, e.g. some CSPs ask for a list of locations to be upgraded with a planned approach while others upgraded without warning. The DCC recognised the experience SEC Parties referred to, as an interim manual Hypercare approach was used. However, the automated solution would introduce the uniform approach SEC Parties had requested.

With Hypercare, Suppliers also noted that they had not received Alerts from the CSPs once an upgrade was carried out, meaning that they had been unable to carry out further work. Suppliers agreed they needed assurance that all CSPs would follow the same process, should the proposed solution be implemented, to be achieved via Service Level Agreements (SLAs). Members noted that the solution developed would need to be consistent and reliable so that Suppliers could build their processes with confidence.

Do the costs of any proposed solution outweigh the option of maintaining the interim approach?

One member also queried whether this solution was just a variant of what was already in place, but with a huge cost attached to it. However, it was noted the costs of doing nothing and maintaining the Hypercare approach would need to account for the spreadsheets used in this approach being scaled to millions of CHs, which could quickly become unfeasible. Ultimately, the solution would involve the CSPs being presented with a list of CHs to upgrade and a time period for each upgrade.

TABASC feedback prior to the first Preliminary Assessment

Prior to the request of the first Preliminary Assessment, the TABASC was provided with an update on the business requirements and the two solution variants to be assessed by the DCC. TABASC members raised queries around the lack of detail the requirements held in terms of setting out SLAs for split Supplier scenarios as well as exception handling. The DCC advised that it would be unusual to investigate SLAs and exception handling prior to any DCC Assessment and that these would be investigated following the Preliminary Assessment via industry workshops and/or Working Groups.

The TABASC also advised that it would like to see more context regarding the option proposing the use of a DCC operated web portal to manage CH firmware updates. The TABASC Chair preferred the web portal solution variant, believing it would be quicker and easier for Parties to implement. SECAS advised further detail to each solution variant would be defined as part of the Preliminary Assessment and that prior to the assessment, the aim was to define the business requirements for the proposed solution.

Consideration of first Preliminary Assessment (CH firmware management)

The first Preliminary Assessment comprised of two management options:

- **Option 1: CH Firmware Management with Service Request: £2.7m – £3.7m**

  The general principle behind Option 1 was to allow Service Users to share relevant data in support of the CH firmware management process via Service Requests. The success and failure of any processing stage would be communicated back to the Service Users via either DCC Alerts or emails.

- **Option 2: CH Firmware Management via Web Portal: £1.9m – £2.7m**

  Option 2 was the Web Portal based solution and would be built using the existing SSI and Self-Service Management Interface (SSMI) suite. The SSI and SSMI would be updated to provide new interfaces to manage all stages of the CH firmware update process. The solution would not require any amendments to existing or the introduction of new Service Requests.

The Assessment was presented to the TABASC for feedback. The TABASC advised that it preferred option 2 as it would be easier to implement for both the DCC and Users. It also believed it would be more cost effective than option 1. However, overall, it still felt that option 2 was too expensive as it was simply formalising processes already in place via email.

The TABASC asked the Working Group to consider a SharePoint option or a solution that would only provide an Alert to Users upon the activation of CH firmware.

The Working Group agreed and preferred option 2, but again thought that overall, it would not be cost effective. However, a member expressed concern with any solution that utilised the SSI due to the periods of maintenance that it may need.

The Working Group also considered exploring a SharePoint option but did not believe it would reduce costs enough to warrant using it and the time it would take to assess it.

Conclusion
Considering the TABASC and Working Group feedback, the Proposer dropped the initial solution and pursued a solution that would notify Suppliers upon CH firmware activation (see below).

Agreed DCC Alert for CH firmware activation notification

The Working Group agreed that a second Preliminary Assessment should be requested specifically for an Alert to Responsible Suppliers upon the activation of CH firmware. Suppliers felt that this was the minimum it needed to improve the visibility of CH firmware updates and that this would improve Supplier experience. It agreed that the Alert only needed to be sent to Suppliers and not Network Parties.

The Proposer agreed with the points raised and for the proposed revised solution to be assessed further.

Consideration of second Preliminary Assessment (new DCC Alert)

The TABASC reviewed the DCC Preliminary Assessment (Annex C) and agreed that the DCC's solution delivered the business requirements.

The Working Group agreed with the following Supplier benefits highlighted in the DCC's Preliminary Assessment of the proposed new Alert:

- Suppliers can track progress of CH firmware update pilots
- Suppliers can update back-office systems to record the active firmware version on each CH, avoiding the need to query the SMI periodically to obtain this information
- Suppliers can plan the deployment of firmware updates to other HAN Devices following activation of the new CH firmware

Members also agreed with the consumer benefit highlighted by SECAS, where the new Alert would make Suppliers aware of CH firmware updates and therefore would be able to address any HAN issues more quickly if they arose. This would have an indirect consumer benefit as it should reduce the risk of HAN instability issues.

One Supplier Party noted that there had been several CH releases in 2020, two of which it believed had led to HAN instability issues. The Supplier agreed that the proposed new Alert would aid Suppliers in identifying and resolving such issues.

Noting the rough order of magnitude cost for Design, Build and PIT of £151,000 to £350,000 in the Preliminary Assessment, the Proposer and other Suppliers in the Working Group believed the new Alert should be implemented as soon as possible.

Refinement Consultation respondent view

One respondent believed an addition should be made to the solution with an additional DCC Alert notifying Responsible Suppliers once a CH firmware update is initiated. This was due to the rare scenario a User may attempt a firmware update whilst a CH firmware update is already in progress. SECAS and the DCC advised the respondent that this scenario would be prevented by SECMP0007 'Firmware updates to IHDs and PPMIDs'. SECMP0007 is pending implementation and the first phase will be implemented in the November 2021 SEC Release.

The first phase of SECMP0007 will introduce added DSP validation for when a User attempts a firmware update to check if another firmware update is already in progress. For ESME/GSME, this will be placed under the W110101 Response Code in the DUIS. Whilst Users will not get an Alert when the CSPs initiate a CH firmware update, they will be notified if they attempt a firmware update whilst a CH (or any other SMETS2 Device) firmware update is in progress. The User's attempted update would be rejected and the User would receive a notification with a clear reason.

Both the Proposer and the respondent agreed that SECMP0007 would prevent the scenario raised by the respondent and agreed there was no need to add any additional Alerts to the SECMP0024 Proposed Solution.

Consideration of the Impact Assessment (new DCC Alert)

SECAS presented the DCC's final Impact Assessment to the TABASC, the Operations Group and the Working Group. The Operations Group and the Working Group had no comments on the proposal or its implementation cost.

TABASC views

The TABASC provided views against the solutions impact on the technical infrastructure and the implementation costs. A TABASC Member queried whether there are any details about the firmware of the Communications Hub contained within the Alert. The DCC advised that the new active firmware version will be included in the body of the Alert.

The TABASC Chair queried when this modification is likely to be implemented. SECAS advised that it is targeted for the June 2022 SEC Release along with other DUIS impacting modifications. The next cut-off date for a decision is the Change Board meeting on 25 August 2021, any decision after this point will likely mean targeting this modification for the next DUIS impacting release which is likely to be in 2023. The TABASC Chair raised that with DSP re-procurement ongoing, should this be applied to the future DSP rather than the current DSP which sunsets in two years. The TABASC Chair queried whether the TABASC and the Working Group can be provided with a comparative Impact Assessment for implementing as part of the future DSP design. SECAS advised it would be very unlikely the DCC would be able to complete the comparative Impact Assessment in time for the Change Board meeting on 25 August 2021, which if missed would risk the targeted implementation date. The DCC advised that the current cost is based on a stand-alone SEC Release and noted that the post-PIT cost may reduce through synergies as a result of other modifications in the same release. The DCC still expects DUIS changes to be aligned despite the modification being applied to the current or new DSP.

Following the meeting, the DCC advised currently it would not be feasible to reassess the modification as part of DSP re-procurement. This is given that the re-procurement has not started yet, and, as it is not part of the existing DSP, it will in theory cost the same or more. Therefore, the DCC did not believe there is any benefit in delaying SECMP0024. As a result, SECAS recommended to the Proposer that SECMP0024 not be reassessed, in order to not risk the targeted implementation date of the June 2022 SEC Release. The Proposer agreed with this approach.

MP122B crossover

SECAS noted with industry that the functionality within SECMP0024 is also part of the scope of CR1423 'Comms Hub Firmware Image Data' under MP122B 'Operational Metrics – Part 2'. The changes under SECMP0024 affect the DSP only, whereas the changes under CR1423 have dependencies on the CSPs. If approval is gained for CR1423 to go ahead under MP122B, the overlap of functionality and any reduction in costs will be accounted for in the MP122B Impact Assessment.

CH Firmware Management Overview document

Although the Working Group agreed that a Preliminary Assessment should be requested for a new DCC Alert, the Proposer expressed concern that the DCC still could deploy firmware updates to CHs with seven days' notice. Other Suppliers agreed and advised that seven days does not give them time to test sufficiently. They also felt the process lacked enough formality as its not contained in the SEC.

Noting the Party feedback, the DCC gave an overview of the process it currently follows and broke this down into stages:

1. The DCC will work with the CSPs and the CH Manufacturers to agree what changes should be included in the release e.g., Change Requests, modifications, manufacturer enhancements.
2. The DCC will then submit a plan to build and test the firmware, including PIT, SIT and UIT.
3. Once the CSPs have designed the firmware release, a "micro pilot" will be carried out, whereby around 10-20 Globally Unique Identifiers (GUIDs) are used to test the Over-The-Air (OTA) release.
4. Next a "pilot" will be carried out with around 5,000 GUIDs. Here the DCC will identify any category 1 and 2 Incidents raised and decide whether to proceed with the roll-out.

The DCC noted that at each of the above stages, decisions are made with Parties as to whether to proceed to the next stage.

The DCC also advised that the seven days' notice referenced in SEC Appendix AB 'Service Request Processing Document' is an absolute minimum. However, the "micro pilot" and "pilot" tend to take between two to four weeks at least. The DCC also noted that in its most recent (circa October 2020) CH firmware release, one month's notice was given to Parties.

The Proposer acknowledged the process but noted that in 2016 it did not exist, hence the need for a modification to be raised at the time. However, even with this process now in place, the Proposer noted that it is yet to be documented and the DCC is not obligated to abide by it. The Proposer felt it should be governed like other processes are in the SEC.

Working Group members noted that in some cases the process gets expedited e.g., for urgent security related reasons. The DCC advised that it must have this flexibility in place for it to act on such scenarios in a timely manner. The Working Group agreed, but again felt the rules should be documented. The DCC advised that appropriate governance was already in place and that it works with Parties to make sure they are aware of such scenarios.

The DCC acknowledged that its CH Firmware Management Overview required an update and made a commitment to do this by January 2021. SECAS suggested that once updated, the document be published on the SECAS website as with several other DCC-owned documents. This would ensure ease of accessibility. The Working Group agreed with this approach. However, the DCC later considered that as the CH Firmware Management Overview is a DCC owned document, it should be held on the DCC website only. This is due to the risk that having two copies on different websites could lead to them being out of sync if one is updated and not the other. Also, putting it on the DCC website indicates that DCC are the owners of it. Therefore, this would indicate to readers that any questions or comments on the document should go to the DCC and not SECAS. SECAS agreed with this approach.

Conclusion
The DCC will update and provide its CH Firmware Management Overview for publication on the DCC website. It will not be referenced in the SEC.

8. Assessment of the proposal

Support for Change

Working Group views

The Proposer and the Working Group considered the costs up to the end of PIT, which following the Impact Assessment resulted in costing less than the DCC's estimated upper range in its Preliminary Assessment. The Proposer and the Working Group agreed with the following benefits highlighted in the DCC's assessment. These could also have indirect benefits for consumers by preventing any HAN stability issues associated with CH firmware updates:

- Suppliers can track progress of CH firmware update pilots
- Suppliers can update back-office systems to record the active firmware version on each CH, avoiding the need to query the SMI periodically to obtain this information
- Suppliers can plan the deployment of firmware updates to other HAN Devices following activation of the new CH firmware

The Proposer, DCC and the Working Group also agreed with SECAS' view that CH Firmware Management Overview should be publicly available online but not referenced in the SEC.

TABASC views

The TABASC reviewed the final DCC Impact Assessment and believed the solution to be beneficial to the technical infrastructure. However, it questioned whether the solution could be implemented via the DSP procurement. The DCC advised reassessing based on DSP re-procurement would unlikely result in a cost saving and that any would be insignificant. Considering the time this would take, SECAS and the Proposer opted not to reassess the modification and instead progress to the Report Phase with the target of meeting the June 2022 SEC Release. This was considering the following DUIS impacting release isn't expected until 2023.

Refinement Consultation responses

All three Refinement Consultation respondents supported this modification. This was considering the costs associated with it and the Proposed Solution.

Views against the General SEC Objectives

Proposer's views

Objective (a)[2]

The Proposer believes that SECMP0024 will better facilitate SEC Objective (a). The SMIP relies on the coordinated involvement of many different Parties. The provision of a CH firmware update framework that is coordinated, controlled and transparent to the relevant parties will facilitate the efficient provision, installation, and operation and interoperability of Smart Metering Systems at Energy Consumers' premises within Great Britain.

Objective (b)[3]

The Proposer believes that SECMP0024 will better facilitate SEC Objective (b). The DCC Licence conditions state the following:

> *5.4 The Interim General Objective of the Licensee is to contribute (taking all reasonable steps for that purpose) to the achievement of a full, timely, efficient, economical, and secure Completion of Implementation in accordance with such requirements as may be imposed on the Licensee under or by virtue of Parts D to F of Condition 13.*
>
> *5.5 For the purposes of paragraph 5.4, the Interim General Objective includes a duty:*
>
> *a) to co-ordinate the activities, systems, and procedures of SEC Parties and, if applicable, SECCo Ltd in such manner and to such extent as may be necessary with respect to the requirements to which that paragraph refers;*
>
> …
>
> *5.9 The First Enduring General Objective of the Licensee is to carry on the Mandatory Business in the manner that is most likely to ensure the development, operation, and maintenance of an efficient, economical, co-ordinated, and secure system for the provision of Mandatory Business Services under the Smart Energy Code.*

Based on the above three clauses, the new DCC Alert will enable Suppliers to monitor firmware updates to CHs.

Industry views

Refinement Consultation respondents agreed with the Proposer's views on the SEC Objectives. However, one respondent believed this modification would only better facilitate SEC Objective (a) and did not give any views against SEC Objective (b).

[2] Facilitate the efficient provision, installation, and operation, as well as interoperability, of Smart Metering Systems at Energy Consumers' premises within Great Britain

[3] Enable the DCC to comply at all times with the General Objectives of the DCC (as defined in the DCC Licence), and to efficiently discharge the other obligations imposed upon it by the DCC Licence

Views against the consumer areas

Improved safety and reliability

This modification would provide a positive impact in this area. The reliability of firmware updates will be improved as Suppliers will be notified when CH firmware has been activated and can then proactively monitor for that these updates are not affecting any other parts of the Smart Metering System.

Lower bills than would otherwise be the case

This modification will be neutral against this consumer benefit area.

Reduced environmental damage

This modification will be neutral against this consumer benefit area.

However, there could be reduced carbon dioxide (CO_2) emissions if visits by meter technician to premises can be avoided by a coordinated approach to CH firmware updates.

Improved quality of service

This modification would provide a positive impact in this area by lowering the risk of defective CH firmware updates leading to HAN stability issues. The new DCC Alert would give Suppliers more awareness over when CH firmware updates take place and therefore quicker to prevent any issues that may arise. Overall, this increases the quality of service for the consumer as it lowers the risk of consumer Device not operating as they should be.

Benefits for society as a whole

This modification will be neutral against this consumer benefit area.

Business Case for change

By Suppliers receiving an Alert upon the activation of CH firmware, they will receive the following benefits:

- Suppliers could track progress of their pilot CH firmware update rollout
- Suppliers will automatically be notified of the new CH firmware version and no longer need to periodically query the SMI
- Suppliers will be able to better plan the deployment of firmware updates to other HAN Devices as a result of any CH firmware updates

The above benefits could all further prevent any HAN stability issues arising or escalating by enabling Suppliers to monitor firmware updates to CHs. This will help to identify any issues caused by those firmware updates and improve the efficiency of the smart meter rollout and its operation. This will reduce the likelihood of issues relating to interoperability of CH firmware updates with other HAN devices, and thus the likelihood of asset replacements or other subsequent firmware updates being required. This will ultimately benefit consumers as well.

This proposal would reduce the risk of CH firmware updates causing issues with Supplier installations of metering equipment in terms of both financial measurements and customer experience (within the premises and in billing/settlements).

The ability of a Supplier to be aware of a CH firmware update immediately upon activation would:

- Reduce the risk of large-scale corrective action and remediation following inappropriate deployment and activation of firmware to significant numbers of CHs;
- Reduce the risk of impact to consumers through issues related to CH firmware performance issues;
- Reduce the risk of large-scale interoperability issues;
- Allow DCC and Suppliers to monitor and provide feedback on successes and failures;
- Reduce financial expenditure on meter technician visits to resolve interoperability issues;
- Assist the journey to technical excellence in the SMIP program; and
- Reduce the risk of reputational damage to the SMIP.

Customers would benefit from:

- A more reliable customer journey with minimal disruption caused by meter technician visits to resolve interoperability issues; and
- Increased customer confidence in the SMIP program.

Noting the costs and benefits of this modification, all three Refinement Consultation respondents believed this modification should be approved. The Proposer noted cost savings are difficult to calculate. However, the alternative of not having accurate and quick access to a customer's CH firmware version can lead to poor customer service, longer customer contact times and inefficient asset deployment planning. The Proposer added the DCC implementation costs are relatively small and noted Supplier costs will be incurred only if the Supplier wishes to take advantage of the new Alert to better serve customers.

Appendix 1: Progression timetable

The Modification Report will be issued for Modification Report Consultation. It will then be presented to the Change Board for vote on 25 August 2021 under Self-Governance.

Timetable	
Event/Action	**Date**
Modification Proposal raised	27 Oct 2016
Modification discussed with Working Group	9 Jan 2017
Modification discussed with Working Group	3 Jul 2017
Modification discussed with Working Group	2 Nov 2017
Modification discussed with Working Group	1 Mar 2018
Update provided to the SSC	28 Mar 2018

Timetable	
Event/Action	**Date**
DCC Firmware Management consultation	5 Nov 2018 – 17 Dec 2018
Modification discussed with Working Group	25 Feb 2019
Business requirements developed with Proposer and DCC	Mar 2019 – Apr 2019
Business requirements discussed with TABASC	18 Apr 2019
Business requirements discussed with SSC	24 Apr 2019
Business requirements discussed with the Working Group	1 May 2019
First Preliminary Assessment requested	17 May 2019
Preliminary Assessment returned	21 Feb 2020
Modification discussed with TABASC	4 Jun 2020
Modification discussed with Working Group	2 Sep 2020
Business requirements developed with Proposer and DCC	Sep 2020
Preliminary Assessment requested	23 Sep 2020
Modification discussed with Working Group	7 Oct 2020
Preliminary Assessment returned	23 Oct 2020
Modification discussed with Working Group	2 Dec 2020
Modification discussed with Working Group	6 Jan 2021
Modification discussed with TABASC	7 Jan 2021
Refinement Consultation	18 Jan 2021 – 5 Feb 2021
Impact Assessment costs approved by Change Board	24 Mar 2021
Impact Assessment	25 Mar 2021
Modification discussed with TABASC	1 Jul 2021
Modification discussed with Operations Group	6 Jul 2021
Modification discussed with Working Group	7 Jul 2021
Modification Report approved by CSC	27 Jul 2021
Modification Report Consultation	28 Jul 2021 – 16 Aug 2021
Change Board Vote	25 Aug 2021

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**
BEIS	Department for Business, Energy and Industrial Strategy
CH	Communications Hub
CoS	Change of Supplier
CPL	Central Products List

Glossary	
Acronym	**Full term**
CRM	Customer Relationship Management
CSC	Change Sub-Committee
CSP	Communication Service Provider
DCC	Data Communications Company
DSP	Data Service Provider
DUIS	DCC User Interface Specification
XML	Extensible Markup Language
ESME	Electricity Smart Metering Equipment
GSME	Gas Smart Metering Equipment
GUID	Globally Unique Identifiers
HAN	Home Area Network
IHD	In-Home Display
IVP	Installation Validity Period
MVP	Maintenance Validity Period
OTA	Over-the-air
PIT	Pre-Integration Testing
RSA	Registered Supplier Agent
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SMI	Smart Metering Inventory
SMIP	Smart Metering Implementation Programme
SSC	Security Sub-Committee
SSI	Self-Service Interface
SSMI	Self-Service Management Interface
TABASC	Technical Architecture and Business Architecture Sub-Committee
TAG	Testing Advisory Group
TRT	Target Response Time
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.

SECMP0024 'Enduring Approach to Communication Hub Firmware Management'

Annex A

Business requirements – version 2.0

About this document

This document contains the business requirements and solution design specification for this Modification Proposal. It provides detailed information on the business requirements for the proposed solution agreed by the Proposer with input from the Data Communications Company (DCC), Sub-Committees and the Working Group, and the considerations and assumptions for each business requirement with respect to this Modification Proposal.

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	The DCC is to generate an Alert to the Service User upon successful activation of Communications Hub firmware, containing the firmware version of the newly activated firmware.

2. Considerations and assumptions

2.1 General

Originally, this modification proposed an approach to Communications Hub firmware management that gave Suppliers more oversight over the process. This included the following requirements:

1. The DCC will notify all relevant Users of a Communications Hub (CH) firmware update being available
2. The DCC shall trigger the firmware update to a 'pilot group' of CH prior to mass deployment
3. The Supplier(s) can choose to trigger the firmware update at an earlier time than the DCC's specified deployment date
4. Any solution shall be able to accommodate split Supplier scenarios
5. The DCC will update Suppliers regularly at different stages of firmware processing
6. If issues are identified with deployed firmware, the DCC shall investigate and determine whether to proceed with the roll-out

The first Preliminary Assessment proposed to deliver these requirements via:

- new Service Request(s) on the DCC User Interface Specification (DUIS); and
- use of a the Self-Service Interface (SSI).

However, the scope of this modification has significantly decreased following reviews from the Technical Architecture and Business Architecture Sub-Committee (TABASC) and the Working Group. This was due to concerns over the costs of both solutions and whether there was a business case.

Therefore, this modification has been reduced to a single requirement explained below.

2.2 Requirement 1: The DCC is to generate an Alert to the Service User upon successful activation of Communications Hub firmware, containing the firmware version of the newly activated firmware

The Proposer requests as an absolute minimum that the solution introduces an Alert to Service Users notifying them when a firmware update has been made to a Communications Hub.

The Proposer and the Working Group agree that the minimum requirement is for Suppliers to receive an Alert upon activation of Communications Hub firmware with the newly activated firmware version.

SECAS note the solution provided by the DCC its first Preliminary Assessment would have delivered this Alert. However, the Proposer is now asking for this requirement to be delivered on its own.

3. Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	**Full term**
CH	Communications Hub
DCC	Data Communications Company
DUIS	DCC User Interface Specification
GUID	Globally Unique Identifier
HAN	Home Area Network
SMI	Smart Metering Inventory
TABASC	Technical Architecture and Business Architecture Sub-Committee

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.

SECMP0024 ‘Enduring Approach to Communication Hub Firmware Management’

Annex B

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 AD ‘DCC User Interface Specification’

These changes have been redlined against Appendix AD version 4.0.

These changes have been redlined on the basis that SECMP0007 ‘Firmware updates to IHDs and PPMIDs’ will be implemented before SECMP0024. The new DCC Alert therefore follows on numerically from the Alerts introduced by SECMP0007.

Add DCC Alert N64 to Table 41 ‘DCC Alert Codes’:

N58	ALCS/HCALCS configuration change	ALCS/HCALCS configuration changed on ESME	Upon successful completion of Service Request 6.14.2 Update Device Configuration (Auxilliary Load Control Scheduler) OR Upon successful completion of Service Request 6.14.1 Update Device Configuration (Auxilliary Load Control Descriptions) OR Upon successful completion of Service Request 6.14.3 Update Device Configuration (Auxiliary Controller Scheduler) OR Future Dated Execution Of Instruction Alert (DLMS COSEM) Alert (Alert Code 0x8F66 and Message Code 0x00CC) corresponding to AuxiliaryLoadControlSwitches Calendar received by the DCC Data Systems	ED	SMETS 2+
N64	Comms Hub Firmware Activation	Successful Comms Hub Firmware Activation	Upon receiving a Response from Comms Hub in response to the Activate Firmware request (GBCS Use Case CS06) sent by the CSP via DCC Data Systems.	All Responsible Suppliers	SMETS 2+
N999	DUIS Version Mismatch	User’s DUIS version is incompatible with the DCC Alert or Service Response to be sent	The DCC Alert or Service Response is not compatible with the DUIS version used by the User	Recipient of the incompatible DCC Alert or Service Response	All

Table 41 : DCC Alert Codes

Add DCC Alert N64 to Table 42 ‘DCC Alert Codes / Response Codes cross-reference’

3.6.4 Relationship between DCC Alert Codes and Response Codes

The DCC shall populate one of the following Response Codes in each DCC Alert in accordance with the allowable Response Codes for each DCC Alert Code as detailed below.

Alert Code	Response Code
AD1	I0
N1	I0
N2	I0
N3	I0
N4	I0
N5	I0
N6	I0
N7	E1,E2,E3,E4,E5,E19,E56 (Please note this Response Code is not applicable to this version of DUIS), E57,E1007, E060502
N8	I0
N9	I0
N10	E30
N11	E31
N12	E20
N13	E21
N14	E43,E46,E47
N15	E44
N16	I0
N17	I0
N18	I0
N19	I0
N20	I0
N21	I0
N22	E20
N23	E21
N24	I0
N25	I0
N26	E1,E2, E3,E4,E5,E19,E1007,E062304
N27	I0
N28	I0
N29	I0
N30	I0
N31	I0
N33	I0
N34	I0
N35	I0
N36	I0
N37	I0
N38	I0
N39	I0
N40	I0
N41	I0

Alert Code	Response Code
N42	I0
N43	I0
N44	I0
N45	I0
N46	I0
N47	I0
N48	I0
N49	I0
N50	I0
N51	I0
N52	I0
N53	E58
N54	I0 (for Alerts 0x8F21, 08F23, 0x8F25, 0x8F26, 0x8F27, 0x8F28, 0x8F2A), E59 (for Alerts 0x8F20, 08F22 , 0x8F24, 0x8F29, 0x8F2B, 0x8F2C, 0x8F2D)
N55	E62
N56	I0
N57	I0
N58	I0
N64	I0
N999	I0

Table 42 : DCC Alert Codes / Response Codes cross-reference

Amend Section 3.9 'DCC Alert Messages' as follows:

Note, the reference to clause 3.9.20 in Table 262 below may need adjusting following the implementation of SECMP0007. This is due to SECM0007 adding sections that would consequently alter the numbering of this added section.

3.9 DCC Alert Messages

3.9.1 Specific Data Items in the DCC Alert Message

Each Alert Code being reported as a DCC Alert shall conform to the DCC Alert format as defined in 3.6.3 DCC Alerts - DCCAlertMessage Format. The DCC shall ensure that the Body of each DCC Alert (DCCAlert XML element) conforms to one of the~~se fourteen~~ DCC Alert formats as defined in the table below:

DCCAlert Definition

DCC Alert Format / Data Item	Description / Allowable values	Type	Mandatory for Alert Codes	Default	Units
PowerOutageEvent	The trigger event indicates that a device power has failed	sr:PowerOutageEvent See 3.9.2	AD1	None	N/A
DeviceStatusChangeEvent	The trigger event indicates that a Device's SMI Status has changed	sr:DeviceStatusChangeEvent See 3.9.3	N1, N2, N8, N9 , N16, N28 and N29, N44, N45	None	N/A
DSPScheduleRemoval	The trigger event indicates that a DCC Schedule is to be deleted	sr:DSPScheduleRemoval See 3.9.4	N4, N5, N6, N17, N37 and N40	None	N/A
CommandFailure	The trigger event indicates that a Command has failed	sr:CommandFailure See 3.9.5	N3, N7, N10, N11, N12, N13, N14, N15, N33, N34, N35, N36, N38, N41 and N53	None	N/A
FirmwareDistributionFailure	The trigger event indicates that a Firmware Distribution Command to the CSP has failed, at least for some of the Devices	sr:FirmwareDistributionFailure See 3.9.6	N18, N19, N20, N21, N22 and N23	None	N/A
UpdateHANDeviceLogResult	The trigger event indicates if a Command to Update a Communications Hub Whitelist Update. (addition ONLY) has succeeded or no Alert has been received by the DCC. .	sr:UpdateHANDeviceLogResult See 3.9.7	N24 and N25	None	N/A
ChangeOfSupplier	The trigger event indicates if an Update Security Credentials (CoS) has succeeded or has failed the CoS Party access control	sr:ChangeOfSupplier See 3.9.8	N26 and N27	None	N/A
DeviceLogRestored	The trigger event indicates that the CHF or GPF Device Log has been restored	sr:DeviceLogRestored (See clause 3.9.9)	N30, N31	None	N/A

DCC Alert Format / Data Item	Description / Allowable values	Type	Mandatory for Alert Codes	Default	Units
PPMIDAlert	The trigger event indicates an Alert has been generated by the PPMID Device	sr:PPMIDAlert (See clause 3.9.10)	N39	None	N/A
SecurityCredentialsUpdated	The trigger event indicates receipt of a success Response from Update Security Credentials where the Remote Party whose certificate has been placed on the Device is not the sender of the Service Request	sr:SecurityCredentials Updated (see clause 3.9.11)	N42	None	N/A
PPMID Removal	The trigger event is receipt of a successful Response from Update HAN Device Log (Removal) where the removed Device is a PPMID that was joined to both an ESME and the GSME	sr:PPMIDRemoval (See clause 3.9.12)	N43	None	N/A
QuarantinedRequest	The trigger event indicates that the Service Request has been quarantined, because an Anomaly Detection volume threshold or attribute limit has been breached	sr:QuarantinedRequest (See clause 3.9.17)	N46, N47, N48	None	N/A

FirmwareVersionMismatch	N49. The trigger event indicates there is a mismatch between the Device’s Firmware Version in SMI and that returned by the Read Firmware Version Service Request and that the version returned by the Device matches an entry on the CPL with a status of “Current” N50. The trigger event indicates there is a mismatch between the Device’s Firmware Version in SMI and that returned by the Read Firmware Version Service Request, the Activate Firmware Service Request or the Future Dated Firmware Activation Alert and that the version returned by the Device matches an entry on the CPL with a status of “Removed” N51. The trigger event indicates there is a mismatch between the Device’s Firmware Version in SMI and that returned by the Read Firmware Version Service Request, the Activate Firmware Service Request or the Future Dated Firmware Activation Alert and the version returned by the Device doesn’t match an entry on the CPL N52. The trigger event indicates there is a mismatch between the	sr:FirmwareVersionMismatch (See clause 3.9.13)	N49, N50, N51, N52.	None	N/A

DCC Alert Format / Data Item	Description / Allowable values	Type	Mandatory for Alert Codes	Default	Units
	GSME’s Firmware Version in SMI and that returned by the Read Firmware Version Service Request where the target Device is GPF				

DCC Alert Format / Data Item	Description / Allowable values	Type	Mandatory for Alert Codes	Default	Units
DualBandCHAlert	The trigger event indicates an Alert has been generated by the Dual Band CHF Device	sr:DualBandCHAlert (See clause 3.9.14)	N54	None	N/A
S1SPAlertDSP	Used for conveying an S1SP Alert N55: The trigger event indicates that a SMETS1 Service Provider reports a Service Request validation error or other notification. N56: The trigger event is the provision of a prepayment top-up UTRN in response to a Service Request where SRV is 2.2	sr:S1SPAlertDSP (See clause 3.9.15)	N55, N56	None	N/A
SMETS1CHFirmwareNotification	See Clauses 1.4.7.13 and 1.4.7.14.	sr: SMETS1CHFirmware Notification (See clause 3.9.18)	N57	None	N/A
ALCSHCALCSConfigurationChange	The trigger event indicates the ESME's ALCS/HCALCS/APC configuration has changed	sr:ALCSHCALCSConfigurationChange (See clause 3.9.19)	N58	None	N/A
CommsHubFirmwareActivation	The trigger event indicates that a new version of Firmware has been activated on a SMETS2+ Comms Hub.	sr:FirmwareVersionUpdate (See clause 3.9.20)	N64	None	N/A
DUISVersionMismatch	The trigger event indicates that the DCC Alert or Service Response to be sent to the User is not compatible with their DUIS XSD version	sr:DUISVersionMismatch (See clause 3.9.16)	N999	None	N/A

Table 262 : DCCAlert (sr:DCCAlert) data items

Add ‘CommsHub Firmware Activation’ section

Note, the section and table number below may change following the implementation of SECMP0007. This is due to SECM0007 adding sections that would consequently alter the numbering of this added section.

Also, the Table numbers in the remainder of the document will also need updating upon implementation.

3.9.20 CommsHub Firmware Activation

3.9.20.1Specific Data Items for this DCC Alert

FirmwareVersionUpdate Data Items Definition

Data Type / Data Item	Description / Allowable values	Type	Mandatory	Default	Units
DeviceID	The Device ID of the Device for which a new Firmware Image has been activated.	sr:EUI (see Section 3.10.1.3 EUI)	Yes	None	N/A
FirmwareVersion	The version of the Firmware Image activated on the Device.	sr:FirmwareVersion (Restriction of xs:string)	Yes	None	N/A

Table 298: CommsHubFirmwareActivation (sr:FirmwareVersionUpdate) data items

SEC Modification Proposal, SECMP0024

Enduring Approach to Firmware Management

Full Impact Assessment (FIA), DCC CR4032

Version:	**0.4**
Date:	**7th June 2021**
Author:	**Robin Seaby**
Classification:	**DCC Public**

Contents

1 Executive Summary

The Change Board are asked to approve the following:

- Total cost to implement SECMP0024 of £512,003, which comprises:
  - £202,395 in Design, Build and PIT costs; and
  - £309,608 in release costs (SIT, UIT and Systems Integrator costs)
- The timescale to complete the implementation of eleven (11) months
- Include SECMP0024 as part of the June 2022 SEC Systems Release

Problem Statement

Currently, there is no system generated notification to Responsible Suppliers to confirm successful activation of Communications Hub firmware.

This Modification solution proposes that:

- the DCC is to generate an Alert to the Service User upon successful activation of Communications Hub firmware, containing the firmware version of the newly activated firmware.

Without the proposed changes:

i. a Service User receives no targeted notification from DCC that it can use as a trigger to update the firmware on the Meter(s) for which it is the Responsible Supplier in order to maintain the Smart Metering System to a reasonable level; and

ii. Service Users are reliant on repeatedly querying the Smart Metering Inventory to establish the current firmware version on each Communications Hub for which they are a Responsible Supplier, resulting in sub-optimal asset management processes.

Benefit Summary

The benefits of delivering this change include enabling Suppliers to:

- track progress of Communications Hub firmware update pilots;
- update back office systems to record the active firmware version on each Communications Hub, avoiding the need to query the Inventory periodically to obtain this information; and
- plan the deployment of firmware updates to other HAN Devices following activation of the new Communications Hub firmware.

2 Revision History

Revision Date	Revision	Summary of Changes
25/05/2021	0.1	Initial compilation from Service Provider
07/06/2021	0.2	DCC internal review completed
07/06/2021	0.3	Further DCC internal review completed

2.1 Associated Documents

This document is associated with the following documents:

#	Title and Originator's Reference	Source	Issue Date
1	Business Requirements v2.0	SECAS	19/02/2020
2	SECMP0024 CR4032 PIA CH Firmware Management v0.2	DCC	22/10/2020

2.2 Document Information

The Proposer for this Modification is Rob Williams of E.ON. The original proposal was submitted on the 27th October 2016.

Preliminary Impact Assessments (PIA) were requested of DCC on 1st May 2019 and 23rd September 2020, and the latest submitted on 22nd October 2020.

The Full Impact Assessment was requested on the 12th April 2021.

This document should be treated as a Confidential document and must be treated as a RED basis for SECAS distribution.

3 Solution Requirements and Overview

3.1 Context and Benefits

Currently, there is no system generated notification to Responsible Suppliers to confirm successful activation of Communications Hub firmware.

In previous iterations of this Modification, it was conceived that Responsible Suppliers would have some level of control over the target list of Communications Hubs that would receive firmware updates as part of a pilot phase and over the schedule for deployment of firmware to Communications Hubs during both pilot and mass deployment phases. A DCC Alert notifying successful activation was also proposed, to enable Suppliers to:

- track progress of Communications Hub firmware update pilots;
- update back office systems to record the active firmware version on each Communications Hub, avoiding the need to query the Inventory periodically to obtain this information; and
- plan the deployment of firmware updates to other HAN Devices following activation of the new Communications Hub firmware.

Whilst it was agreed by the Working Group that the planning and scheduling aspects of the previous iteration of the Modification are largely in place within the process described in the DCC Firmware Management Policy, and were hence removed from the scope of the Modification, the benefits associated with the additional DCC Alert remain valid.

3.2 Business Requirements for this Modification

The high-level business requirements for this Modification are as follows.

Req.	Requirement
1	The DCC is to generate an Alert to the Service User upon successful activation of Communications Hub firmware, containing the firmware version of the newly activated firmware.

Table 1: Business Requirements for SECMP0024, DCC CR4032

4 Solution Overview

This modification only impacts the DSP component of the DCC Total System.

4.1 DSP Solution Overview

DCC Data Systems will introduce a new DCC Alert to notify the Service Users of the successful activation of a Communications Hub (CH) firmware version. A new DCC Alert called Comms Hub Firmware Activation (N64) will be used. It will include the version of the active firmware on the Device. If the Service User uses a version of DUIS that does not support the newly introduced DCC Alert, then the DCC Alert N999 will be used to notify the firmware activation, including the firmware version.

The scenario in which the new DCC Alert is generated, including the recipients, is summarised in the table below.

Notification Scenario	Trigger	Condition	DCC Alert ID	Recipients
Successful Comms Hub Firmware Activation	Response from CH to the Activate Firmware request (CS06) sent by the CSP via CSP Management Gateway.	Response indicates new active firmware version.	N64	All Responsible Suppliers

Table 2: Criteria for DCC Alert N64

The definition of the new DCC Alert will be added to DUIS and the cost of DUIS uplift is provided in this FIA. There are no delivery dependencies on other DCC Service Providers in completing this change.

Note: The functionality within SECMP0024 (CR4032) is also part of the scope of SECMP0122B (CR1423). The changes under CR4032 are **DSP only** in nature, whereas the changes under CR1423 have dependencies on the CSPs. If approval is gained for CR1423 to go ahead, the overlap of functionality will be accounted for in the FIA for CR1423.

4.1.1 Impacted DSP Components and Designs

Request Management

Request Management will handle the DCC Alert generation.

Data Management

There will be minor changes such as reference data updates within Data Management.

DUIS/DUGIDS

DUIS and DUGIDS documentation will be updated to describe the behaviour of the new DCC Alert. The DUIS XML Schema will be updated to include the definition of the new DCC Alert. The DUIS extract is embedded here for reference. The DUGIDS changes will be provided to SECAS for inclusion in the June 2022 SEC Release.

DUIS Legal Text
Draft CR4032.docx

4.2 Deliverables

The deliverables of this Modification are described in the table below. These deliverables are split into two parts covering the implementation up to and including PIT, and the Post PIT activities required to deploy the changes into production (i.e. SIT, UIT and Transition To Operations).

This Modification is expected to be included in the June 2022 SEC Release, in which case the Post PIT deliverables will be rolled into the SEC Release.

Reference	Deliverable / Artefact	Changes Required (for artefact)
PIT DELIVERABLES		
Design and Solution Documentation		
SD2.1.1	Functional Specification – Instant Energy	Update
SD4.1	DCC User Gateway Interface Design Specification (DUGIDS)	Update
SD2.2.1.2	Component Design Spec - Request Manager	Update
SD2.2.1.4	Component Design Spec - Data Management	Update
SD2.2.1.4.3	Reference Data Definition (DS.0584)	Update
SD2.2.13	Component Model Diagram	Update
DUIS-related		
	DUIS XML Schema	Update to include definition of new DCC Alert
	DUIS documentation	Update
POST-PIT DELIVERABLES		
SIT		
TBC	Functional HeatMap	Create
DT.0034	System Integration Test Scenarios	Create/Update
In ALM	New & Updated Test Scripts	Create/Update
In ALM	Test Traceability Matrix mapped for SECMP0024	Update
TBC	Test Completion Report	Create
UIT		
	Run UIT Service Request regression test packs to prove existing functionality is still working as expected. Test packs will be run twice - on existing DUIS version and on new DUIS version introduced to accommodate SECMP0024.	
	Test reporting, including Test Completion Report	Create

5 Impact on DCC Systems, Processes, and People

This section describes the impact of SECMP0024 on DCC Services and Interfaces that impact Users and/or Parties.

5.1 DSP Team Impact

To implement the scope of supply as described in this Full Impact Assessment, DSP will supply the following services:

- Pre-integration (PIT) activities to align DSP functionality with the solution described in section 4.1;
- Preparation and Support for Solution Test and User Acceptance Testing;
- SIT support functions including support for issue investigation, resolution and deployment to SIT-B;
- Knowledge transfer from the PIT team to the Application Management Support team to enable support for the revised functionality in live operation; and
- A subset of the Programme Leadership and Operations team will be required to support the SECMP0024 resources.

5.1.1 Implementation Team

The design, implementation, System Testing and Factory Acceptance Testing (FAT) phase will operate as a single phase of activity with a single drop. FAT will consist of a defined subset of system tests being observed by DCC within the final two weeks of system test. The Schedule 6.2 exit criteria and defect mask will apply for the Pre-Integration Process.

5.1.2 Systems Integration Test (SIT) Team

The Systems Integration Test (SIT) team will be involved in the preparation and execution of Solution Tests and User Acceptance Testing in the SIT-B environment. This is activity is specific to the functional change introduced by SECMP0024 and excludes any wider release regression testing or uplift of A-Stream Environments.

5.1.3 User Integration Test (UIT) Team

The UIT Projects team will be involved in the preparation and Support for User Integration Testing on the UIT-B environment. This activity is specific to the functional change introduced by SECMP0024 and excludes any wider release regression testing or uplift of A-Stream Environments.

5.2 Support for Integration Testing

Effort will be required from the DSP PIT and Triage teams to support the additional testing. This consists of issue investigation, resolution and deployments to the SIT-B environment.

5.3 Operational Support

The Application Management Support team are responsible for the provision of application level support for the DSP System. This CR changes some core functionality of the DCC Data System and slightly increases system complexity. DSP has allowed three months Early Life Support, following Go Live, to cover any initial support issues.

6 Testing Considerations

This Full Impact Assessment includes the cost to develop, fully test and deliver this SEC Modification.

6.1 Pre-Integration Testing

The DSP PIT development team carries out unit testing and automated behaviour driven tests as part of DSP's continuous integration build and automated testing pipeline. The Early Automated System Testing (EAST) approach builds on this CI pipeline, helping to identify build issues and defects at the earliest opportunity. Any tests not run via EAST will be executed by the PIT System Test team manually. A Test Completion Report will be issued following the successful completion of PIT testing.

Acceptance will be defined by:

1. Completion of associated System Tests and achievement of the Schedule 6.2 defined defect mask for PIT exit, and
2. Approval from DCC Test Assurance of FAT completion and acceptance of PIT Exit.

6.2 Post PIT

The SIT and UIT phases of testing will be aligned with other Modifications and Change Requests in the target SEC release. System integration testing will be carried out on the B Stream environment i.e. SIT-B. There will be no separate testing on the A stream environments.

It should be noted that it is a requirement of the Testing Advisory Group (TAG) and Test Assurance Board (TAB) that a DUIS change of any nature should undergo full regression testing, which is the basis on which the Post PIT costs have been estimated. If the SEC Release in which this Modification is deployed contains no other DUIS changes and if the TAG and TAB were to relax the requirement for full regression testing in relation to this Modification, since the DUIS change is restricted to the addition of a single DCC Alert Code to the existing enumerated list in the DUIS XML Schema, then there would be a corresponding reduction in the Post PIT testing costs for the Release.

7 Implementation Timescales and Releases

This Modification is expected to be included in a SEC Release in June 2022. For the purposes of this FIA, timescales are shown for the development and PIT phase, and for the Post PIT activities that will be required as part of the release.

7.1 Change Lead Times and Timelines

The change will be implemented using a waterfall methodology such that a pre-integration implementation phase, consisting of design, development and system testing will precede a formal Systems Integration Test phase.

The pre-integration phase is expected to take approximately four months and the Systems Integration execution Testing phase is expected to last approximately five months and User Integration Testing a further month. Therefore, the change will be ready to schedule to a production release approximately ten months after full commercial cover has been provided by DCC to the Service Provider in the form of a CAN, which follows formal approval by SECAS of the release scope.

The broad breakdown of the testing regime is shown in the following table in months after an approval decision date (D).

Phase	Duration
SECAS agreement on scope of release	
CAN signature	D + 1 Month
Design, Build and PIT Phase	4 Months
SIT and UIT Phase (functional changes only), aligned with Release SIT and UIT dates	6 Months
Transition to Operations and Go Live	D + 11 Months

7.2 Costs and Charges

This section indicates the costs per application development stage for this Modification. Note that the implementation costs shown include the portion of the release costs (Post PIT) that are attributable to this Modification.

If, as DCC anticipates, the Modification is deployed as part of the June ‘22 release, the Post PIT costs shown below will be rolled into the SEC Release and associated CR.

£	Design, Build & PIT	Post PIT	Total
Phase Total	£202,395	£309,608	£512,003

Table 3: Cost Analysis

Design — The production of detailed System and Service designs to deliver the Modification requirements.

Build — The development of the designed Systems and Services to create a solution (e.g. code, systems, or products) that can be tested and implemented.

Pre-Integration Testing (PIT) — DSP tests its own solution to agreed standards in isolation of other Service Providers. This is assured by DCC.

Systems Integration Testing (SIT) — All the Service Provider's PIT-complete solutions are brought together and tested as an integrated solution, ensuring all solutions align and operate as an end-to-end solution.

User Integration Testing (UIT) — Users are provided with an opportunity to run a range of pre-specified tests in relation to the relevant change.

Implementation to Live (TTO) — The solution is implemented into production environments and ready for use by Users as part of a live service.

7.2.1 Application Support Costs

Application Support costs are any costs associated with supporting the new functionality and may include additional staff or infrastructure.

£	Application Support	Total
Phase Total	£20,963	£20,963

7.3 Impact on Contracts and Schedules

Contract updates will be required for this change. The detailed updates will be determined as part of the resulting Contract Amendment Note (CAN). Updates will be required to the following schedules:

- Schedule 4.1: Solution Design documents will need to be updated as per section 4.2 Deliverables.

There will be no change to Schedule 2.2 SLAs due to this Modification.

Appendix A: Risks, Assumptions, Issues, and Dependencies

The tables below provide a summary of the Risks, Assumptions, Issues, and Dependencies (RAID) observed during the production of the Full Impact Assessment. DCC requests that the Working Group considers this section and considers any material matters that have been identified. Changes may impact the proposed solution, implementation costs and/or implementation timescales.

Risks

Ref	Description	Status/Mitigation
R1	This change is to be implemented after the end of the initial term of the DSP Agreement. If any extended Agreement contains amended terms which affect DSP costs for change delivery, then the price for this Modification could be subject to variation.	Open

Assumptions

These assumptions have been used in the creation of this Full Impact Assessment. Any changes to the assumptions may require DCC to undertake further assessment, prior to the contracting and implementation of this change**.**

Ref	Description	Status/Mitigation
A1	Firmware used to upgrade the CHF will be firmware that has been tested previously.	Accepted
A2	It is assumed that this SECMP0024 will be delivered as part of an overall release, i.e. as part of June 2022 Release	Accepted

Issues

None at this time.

Ref	Description	Status/Mitigation

Dependencies

None at this time.

Reference	Dependency	Implication if dependency not met	Status
D1	In order for this Modification to be delivered as part of a yet to be defined SEC release, DCC will require commercial cover for that SEC release a minimum of	It may not be possible for this Modification to be included in the target SEC release.	To be

	ten months prior to the SEC release date.		

Appendix B: Glossary

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

Acronym	Definition
CH	Communications Hub, Comms Hub
CPL	Certified Products List
CR	(DCC) Change Request
CSP	Communication Service Provider
DCC	Data Communications Company
DCC-L	DCC Total System, DCC Licensing
FIA	Full Impact Assessment
GUID	Globally Unique IDentifier
PIA	Preliminary Impact Assessment
SEC	Smart Energy Code
SIT	System Integration Testing
SMIP	Smart Metering Implementation Programme
TAB	Test Assurance Board
TAG	Testing Advisory Group
UIT	User Integration Testing

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.

SECMP0024 ‘Enduring Approach to Communication Hub Firmware Management’

Annex D

Refinement Consultation responses

About this document

This document contains the full collated responses received to the SECMP0024 Refinement Consultation.

Question 1: Do you agree with the solution put forward?

Question 1			
Respondent	**Category**	**Response**	**Rationale**
OVO Energy	Large Supplier	Yes	On the basis that this is a similar solution to that offered under the SMETS1 E&A programme. Suppliers can already ascertain the current version of the comms Hubs using the SMI extract, however the alert being proposed in SECMP0024 means that Supplier could have real time view of the assets as the alert is received - rather than downloading a report periodically.
EDF Energy	Large Supplier	Yes	We are generally Supportive of the proposed changes for a new DCC N63 alert when the Comms Hub firmware has been successfully upgraded. It is unclear from the Modification report whether Suppliers also will get an alert when the firmware OTA is initiated / attempted. This has been identified as an issue in the circumstances of a simultaneous attempt to upgrade meter firmware OTA and at the same time when the associated Comms Hub firmware is downloading. This can impact the success of the meter OTA. The issue could have been avoided if we had been aware of the Comms Hub upgrade. We could have delayed the meter OTA and reduced meter OTA failure rates as a consequence. We consider that the introduction of a Comms hub OTA notification would be beneficial to the end-to-end process.
E.ON	Large Supplier	Yes	The solution provides the Suppliers with visibility of new comms hub firmware deployment, in its governance before production release and also as the firmware is deployed by the DCC/CSPs.

Question 2: Will there be any impact on your organisation to implement SECMP0024?

Question 2			
Respondent	**Category**	**Response**	**Rationale**
OVO Energy	Large Supplier	Yes	System changes will be needed to factor the new alert and process it accordingly. The benefits for this outweigh the costs that will be incurred.
EDF Energy	Large Supplier	Yes	The solution proposes a new DCC N63 alert when the Comms Hub firmware has been successfully upgraded. This will help us to understand when new firmware has been updated and allow us to maintain devices details appropriately.
E.ON	Large Supplier	Yes	To reap the benefits of the SEC Mod, effort would be required to process the new alert and update backend asset databases with the information from those alerts.

Question 3: Will your organisation incur any costs in implementing SECMP0024?

Question 3			
Respondent	**Category**	**Response**	**Rationale**
OVO Energy	Large Supplier	Yes	See question 2.
EDF Energy	Large Supplier	Yes	EDF will need to update our systems and business process to utilise the DCC alert generated for each firmware activation and automatically update the firmware versions of Comms Hub's in our systems. We will be able to process the alert but require changes will be required as the new firmware version would be included in the payload of the alert. There would be a cost to us to automatically process this info from the alert payload to update our back office systems to record the active firmware version on each Comms Hub. This cost has not yet been fully assessed.
E.ON	Large Supplier	Yes	Effort and costs are not available at this time, however they are thought to be relatively small compared to overall budgets. Cost savings are difficult to calculate. However, the alternative of not having accurate and quick access to a customer's comms hub firmware version can lead to poor customer service, longer customer contact times and inefficient asset deployment planning.

Question 4: Do you believe that SECMP0024 would better facilitate the General SEC Objectives?

Question 4			
Respondent	**Category**	**Response**	**Rationale**
OVO Energy	Large Supplier	Yes	As set out in the Modification Report.
EDF Energy	Large Supplier	Yes	The proposed change will better facilitate SEC Objective (a). The provision of a Comms Hub firmware update framework that is coordinated, controlled and transparent to the relevant parties will facilitate the efficient provision, installation, and operation and interoperability of Smart Metering Systems at Energy Consumers' premises within Great Britain.
E.ON	Large Supplier	Yes	The SEC Mod will facilitate the efficient operation and interoperability of Smart Metering Systems at Consumer's premises by providing Suppliers up to date information on the firmware version within the comms hub at the customer's premise. It will also allow the DCC to efficiently discharge their obligations imposed upon it by the DCC Licence which states: 5.9 The First Enduring General Objective of the Licensee is to carry on the Mandatory Business in the manner that is most likely to ensure the development, operation, and maintenance of an efficient, economical, co-ordinated, and secure system for the provision of Mandatory Business Services under the Smart Energy Code.

Question 5: Noting the costs and benefits of this modification, do you believe SECMP0024 should be approved?

Question 5			
Respondent	**Category**	**Response**	**Rationale**
OVO Energy	Large Supplier	Yes	Yes although we are still waiting to see the Policy document from the DCC that is required for the whole solution to work.
EDF Energy	Large Supplier	Yes	The proposed changes for a new DCC N63 alert when the Comms Hub firmware has been successfully upgraded will improve Suppliers ability to manage and record the accurate firmware version of comms hubs at premises they supply.
E.ON	Large Supplier	Yes	Costs of DCC/CSP implementation are relatively small (as per the DCC PIA document). Individual costs to the Supplier are not compulsory. Costs will be incurred only if the Supplier wishes to take advantage of the new alert to better serve customers.

Question 6: How long from the point of approval would your organisation need to implement SECMP0024?

Question 6			
Respondent	**Category**	**Response**	**Rationale**
OVO Energy	Large Supplier	6 months	We'd need to update our system to accept and recognise the new alert. We cannot give a view on any changes that may be revealed from understanding the Policy view from the DCC and any changes that may bring.
EDF Energy	Large Supplier	6 months	We would require a minimum of 6 months to update our back office systems for this change.
E.ON	Large Supplier	Estimated 6-12 months from SEC Mod approval to factor into the IT program of work.	Processing of the new alert and storage into back end databases may require an IT architecture work.

Question 7: Do you agree with the proposed implementation approach?

Question 7			
Respondent	**Category**	**Response**	**Rationale**
OVO Energy	Large Supplier	Yes	-
EDF Energy	Large Supplier	Yes	We agree with the proposed implementation approach
E.ON	Large Supplier	Yes	The proposed solution is straight forward and relatively inexpensive compared to the provided benefits.

Question 8: Do you agree that the legal text will deliver SECMP0024?

Question 8			
Respondent	**Category**	**Response**	**Rationale**
OVO Energy	Large Supplier	Yes	-
EDF Energy	Large Supplier	Yes	We have no comments on the legal text.
E.ON	Large Supplier	Yes	There are no obvious errors

Question 9: Do you believe there will be any impacts on or benefits to consumers if SECMP0024 is implemented?

Question 9			
Respondent	**Category**	**Response**	**Rationale**
OVO Energy	Large Supplier	Yes	SECMP0024 will enable the Responsible Supplier to update the CH in the overall metering systems to reflect the latest firmware version on the asset in a timely manner and not have to rely on periodically downloading SMI. This should support more effective asset management and firmware updates, where these updates are reliant on the corresponding CH firmware. The estate being on the latest compliant firmware will benefit consumers being able to enjoy full functionality.
EDF Energy	Large Supplier	Yes	Consumers could benefit from the implementation of this modification as the firmware of their connected comms hubs is more successfully managed and kept up to date. This may be important to overcome any security or technical issues found. It could improve the performance of their smart metering system.
E.ON	Large Supplier	Yes	On customer contact, the call agent would have instant access to the comms hub firmware version to check against known issues. From within a consumer's home, a Meter Technician contact with the Supplier's Technical Help Desk would have instant access to the comms hub firmware version to check against known issues and incompatibilities. A Supplier can better plan a customer's asset upgrade program of work knowing the exact Comms Hub firmware version within its IT databases.

Question 10: Please provide any further comments you may have

Question 10		
Respondent	**Category**	**Comments**
OVO Energy	Large Supplier	-
EDF Energy	Large Supplier	No further comments
E.ON	Large Supplier	Cost savings should be possible by integrating this SEC Mod implementation with other changes.