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.

Smart Energy Code

SECMP0024

‘Enduring Approach to Communication Hub Firmware Management’

Modification Report

Version 0.4

18 January 202

Corporate member of Plain English Campaign
Committed to clearer communication
592

About this document

This document is a Modification Report. It currently sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views and conclusions. This document will be updated as this modification progresses.

Contents

1. Summary 3
2. Issue 3
3. Solution 5
4. Impacts 5
5. Costs 7
6. Implementation approach 8
7. Solution development 8
8. Assessment of the proposal 17

Appendix 1: Progression timetable 20

Appendix 2: Glossary 21

This document also has three 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 latest full Data Communications Company (DCC) Preliminary Assessment response.

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 Firmware Management Policy and make this available to the Smart Energy Code Administrator and Secretariat (SECAS) for publication on the SECAS website. The Firmware Management Policy is a DCC owned document and therefore this does not require a change to the SEC.

This modification's impacts will be limited to the DCC and Suppliers. It is expected to cost £151,000 – £350,000 up to the end of Pre-Integration Testing (PIT). The full implementation costs will be identified in the DCC Impact Assessment. SECAS recommends this be 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 SMETS2+ 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.

Other than for the DCC to validate the credentials of the firmware and its relevant entries in the Central Products List (CPL), there are no other obligations on the DCC to give notice to Users before and after the firmware updates are made.

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 consisting of two solution options, which has now been discarded, was modelled on the Hypercare approach.

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 CH firmware update pilots.
- 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 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 or 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 or be discovered at a later date. This would then require investigation to determine problems were as a result of a firmware upgrade. In addition, it would 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 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 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 Firmware Management Policy and make this available to SECAS for publication on the SECAS 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 policy being available. However, SECAS will continue to monitor its progression and make it available to Parties once it has been signed off 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 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 Smart Metering Inventory (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, publishing the DCC's Firmware Management Policy on the SECAS website will make it easily accessible and the process more transparent.

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. This Schema will need to be loaded into DSP's Data Power appliances across all DSP environments.

The full impacts on the DCC Systems and DCC's proposed testing approach can be found in the DCC Preliminary 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 SEC required to deliver the proposed solution can be found in Annex B.

Technical specification versions

We anticipate the new DCC Alert will likely only impact the next Principal Version of the DUIS at the time of implementation. However, this is yet to be determined and will be consulted up with the DCC and the Technical Architecture and Business Architecture Sub-Committee (TABASC).

Consumers

The new DCC Alert will make Suppliers aware of CH firmware updates and could help them be quicker to address any HAN and Wide Area Network (WAN) issues if they arise. 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 up to the end of Pre-Integration Testing (PIT) to implement this modification is £151,000 – £350,000[1]. The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	**Cost**
Design, Build and Pre-Integration Testing (PIT)	£151,000 – £350,000
Systems Integration Testing (SIT)	TBC
User Integration Testing (UIT)	TBC
Implement to Live	TBC
Application Support	TBC

More information can be found in the DCC Preliminary Assessment response in Annex C.

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

The new DCC Alert will need to be implemented in a new version of DUIS. Parties that choose to uplift to this new version will incur a cost, but this would include all modifications associated with this uplift.

This will be updated subject to any feedback received from this Refinement Consultation.

[1] This modification will only impact the DSP. At Preliminary Assessment stage the DSP is only able to provide a cost range indication of the costs.

6. Implementation approach

Recommended implementation approach

SECAS is recommending 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
- **3 November 2022** (November 2022 SEC Release) if a decision to approve is received after 30 August 2021 but on or before 30 January 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 DCC has advised that it will need a four-month lead time up to the end of PIT to implement this modification. The duration for SIT, UIT and Implement to Live will be assessed as part of the Impact Assessment and is assumed to be six months in the interim. This would provide enough lead time to implement this modification in the June 2022 SEC Release.

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 page 15).

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 version is introduced, User testing requirements shall be set out in the applicable modification.

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 are available and allow them to specify the date and time, within a period defined by the DCC, when these are 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 are deployed by the DCC to mitigate the Proposer's identified risks. These options were eventually discarded in favour of the current Proposed Solution (see page 15).

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 will 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 will 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 for which 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 needs 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 will be informed of CH firmware updates via release "road maps" and release notes. For core Releases, Release Notes will be published following SIT and UIT. Users would be notified of maintenance Releases once the Release is 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 and that such updates considered by

the SSC. However, the DCC advised that in the event of a security/emergency incident, a Release Note will be issued as early as possible.

The Working Group agreed that Users' priority is 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, are requirements of this modification. However, the ability to safe launch security/ emergency CH firmware updates is not a requirement of this modification. It was also agreed that the DCC needs 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 needs to be implemented urgently. SECAS confirmed this has 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 shall 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 will 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 will be required to deploy the firmware within a five-day Target Response Time (TRT). However, Suppliers will 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 is required for when problems occur 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 is 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" can 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 it 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. It was therefore agreed that no further requirements were needed in relation to incident management, and the DCC shall confirm via its future assessments.

Major Incidents and Major Security Incidents

The Proposer advised that the intention of the modification is to manage CH firmware deployment for all types of CH releases. This is 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 rest 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 is collaboration between Suppliers. The Proposer opted to progress a business requirement whereby in a split Supplier scenario, both the Import and Gas Suppliers need to coordinate CH firmware deployments. The solution shall 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. More information can be found under business requirement 5 'any solution shall be able to accommodate split Supplier scenarios' in the business requirements in Annex A.

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)[2]. 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.

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 can 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, noting that the SSI and internal systems were not yet merged. 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/second Preliminary Assessment response.

[2] 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.

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 Change of Supplier (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 upgrade 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 have requested.

With Hypercare, Suppliers also noted that they were not receiving Alerts from the CSPs once an upgrade was carried out, meaning that they were 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 can 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 is done now, 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 being scaled to millions of CHs, which could quickly become unfeasible. Ultimately though, the solution comes down to 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 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: £2.7 – £3.7 million**

  The general principle behind Option 1 is 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 could be communicated back to the Service Users via either DCC Alerts or emails.

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

  Option 2 is the Web Portal based solution and will be built using the existing SSI and Self-Service Management Interface (SSMI) suite. The SSI and SSMI will be updated to provide new interfaces to manage all stages of the CH firmware update process. The solution will 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 page 15).

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 agreed that the DCC's solution deliver 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 Smart Metering Inventory (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 will make Suppliers aware of CH firmware updates and therefore would be able to address any HAN issues quicker if they arise. This would have an indirect consumer benefit as it should reduce the risk of HAN instability issues.

One Supplier Party noted that there have 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, the Proposer and other Suppliers in the Working Group believed the new Alert should be implemented as soon as possible.

DCC Firmware Management Policy

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 is already in place and that it works with Parties to make sure they are aware of such scenarios.

The DCC acknowledged that its Firmware Management Policy requires an update and made a commitment to do this by January 2021. SECAS suggested that once updated, the Firmware Management Policy 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.

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

8. Assessment of the proposal

Support for Change

Working Group views

Considering the costs up to the end of PIT, the Proposer and the Working Group agreed with the following benefits highlighted in the DCC's Preliminary 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 Smart Metering Inventory (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 and the Working Group also agreed with SECAS' view that publishing the DCC's Firmware Management Policy on the SECAS website will make it easily accessible and the process more transparent.

TABASC views

The TABASC (61_0701) reviewed the latest DCC Preliminary Assessment and believed the solution developed is cost effective. They were supportive of the costs having significantly decreased from the high costs of the previous solution noted in the first Preliminary Assessment. However, a member

considered the current solution to be relatively simple compared to most other DCC System impacting modifications and believed the costs to be high, but was still supportive of the modification.

Views against the General SEC Objectives

Proposer's views

Objective (a)[3]

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.

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 provide input into the scheduling of CH firmware updates would:

1. Reduce the risk of large-scale corrective action and remediation following inappropriate deployment and activation of firmware to significant numbers of CHs;
2. Reduce the risk of impact to consumers through issues related to CH firmware performance issues;
3. Reduce the risk of large-scale interoperability issues;
4. Allow DCC and suppliers to monitor and provide feedback on successes and failures;
5. Reduce financial expenditure on meter technician visits to resolve interoperability issues;
6. Assist the journey to technical excellence in the SMIP program; and
7. 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.

Objective (b)[4]

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*

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

[4] To 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

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. 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.

Industry views

Industry views will be gathered through the Refinement Consultation.

Views against the consumer areas

Improved safety and reliability

This modification will be neutral against this consumer benefit area.

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

Views on the business case will be sought during this Refinement Consultation.

Appendix 1: Progression timetable

Following this Refinement Consultation, we will seek Change Board approval of the Impact Assessment costs on 24 February 2021. If approved we will subsequently request a DCC Impact Assessment.

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
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 Feb 2021

Timetable	
Event/Action	**Date**
Impact Assessment requested	25 Feb 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**
CoS	Change of Supplier
CRM	Customer Relationship Management
CSP	Communication Services Provider
DCC	Data Communications Company
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
IVP	Installation Validity Period
MVP	Maintenance Validity Period
RSA	Registered Supplier Agent
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SMI	Smart Metering Inventory
SMIP	Smart Metering Implementation Programme
SSI	Self-Service Interface
TABASC	Technical Architecture and Business Architecture Sub-Committee
TRT	Target Response Time

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'

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'

Legal text – version 0.1

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 N63 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+
N63	Comms Hub Firmware Activation	Successful Comms Hub Firmware Activation	Response from Comms Hub to the Activate Firmware request (CS06) sent by the CSP via CSP Management Gateway. Response indicates new active firmware version.	IS GS	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 N63 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
N63	I0
N999	I0

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

Add DCC Alert N63 to Table 262 'DCCAlert (sr:DCCAlert) data items'

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.

ALCSHCALCSConfiguration Change	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	Response from Comms Hub to the Activate Firmware request (CS06) sent by the CSP via CSP Management Gateway. Response indicates new active firmware version.	sr:CommsHubFirmwareActivation (See clause 3.9.20)	N63	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 'Comms Hub 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 Comms Hub Firmware Activation

3.9.20.1 Specific Data Items for this DCC Alert

CommsHubFirmwareActivation Data Items Definition

Data Type / Data Item	Description / Allowable values	Type	Mandatory	Default	Units
CommsHubDeviceID	The Device ID of the Comms Hub that has successfully activated the firmware	sr:EUI (See clause 3.10.1.3)	Yes	None	N/A
TimeStamp	The time at which the Comms hub sent the firmware update response	xs:dateTime	Yes	None	N/A
FirmwareVersion	The current firmware version of the Comms Hub	sr:FirmwareVersion (Restriction of xs:string)	Yes	None	N/A

Table 298 : CommsHubFirmwareActivation (sr: CommsHubFirmwareActivation) data items

Data Communications Company

SEC Modification Proposal, SECMP0024

Enduring Approach to Firmware Management

Preliminary Impact Assessment (PIA), DCC CR 4032

Version:	**0.2**
Date:	**22nd October 2020**
Author:	**DCC**
Classification:	**DCC PUBLIC**

Contents

1 Document History 2
1.1 Revision History 2
1.2 Associated Documents 2
1.3 Document Purpose 2
1.4 Previous Document Information 2
2 Introduction 3
2.1 Context and Benefits 3
2.2 High Level Business Requirements 3
3 Proposed Solution 4
3.1 Solution Description 4
3.2 DSP Impacted Components 4
4 Impact on DCC's Systems, Processes and People 5
4.1 Security Impact 5
4.2 Infrastructure Impact 5
4.3 Integration Impact 5
4.4 Service Impact 5
5 Implementation Timescales 6
5.1 Implementation Approach 6
5.2 Testing and Acceptance 6
6 Costs and Charges 7
6.1 Design, Build, and Testing Cost Impact 7
7 Risks, Assumptions, Issues, and Dependencies 9
7.1 Risks 9
7.2 Assumptions 9
7.3 Issues 9
7.4 Dependencies 9
Appendix A: Glossary 10

1 Document History

1.1 Revision History

Revision Date	Revision	Summary of Changes
20/10/2020	0.1	Initial draft based on Service Provider PIA

1.2 Associated Documents

This document is associated with the following documents:

Ref	Title	Source	Issue Date
1	Business Requirements v2.0	SECAS	

1.3 Document Purpose

The purpose of this Preliminary Impact Assessment (PIA) is to provide the relevant Working Group with an assessment of the business requirements and solution that were put forward by the Working Group.

1.4 Previous Document Information

The original Proposer for this Modification was Rob Wilson.

The Preliminary Impact Assessment was requested of DCC in September 2020.

2 Introduction

This Modification seeks to amend the Smart Energy Code (SEC) and DCC's systems to provide an Alert that notifies each Responsible Supplier for a Communications Hub of the successful activation of a firmware image on that Communications Hub.

It should be noted that the functionality described for this Modification is also part of the scope of SECMP0122B, CR1423. The changes under this Modification and CR4032 are DSP only in nature, whereas the changes under CR1423 cover a wider scope and have a dependency on the CSPs. The dependency will be investigated if and when the changes are progressed to a Full Impact Assessment.

For the purposes of this Preliminary Impact Assessment, it is assumed that the SECMP0024 required changes will be delivered standalone – i.e independently of SECMP0122B.

2.1 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.

2.2 High Level Business Requirements

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

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.

3 Proposed Solution

3.1 Solution Description

DCC Data Systems will introduce a new DCC Alert to notify the Service Users of the successful activation of a Comms Hub firmware version. DCC Alert N63 will be used for this and will include the version of the activated firmware on the Device.

The scenario under which this DCC Alert is generated and the applicable recipients are summarised in the table below.

Notification Scenario	Trigger	Condition	DCC Alert ID	Recipients
Successful Comms Hub Firmware Activation	Response from Comms Hub to the Activate Firmware request (CS06) sent by the CSP via CSP Management Gateway.	Response indicates new active firmware version.	N63	All Responsible Suppliers

Table 1 Criteria for N63

The definition of the new DCC Alert will need to be included in DUIS. The required changes to DUIS are minor.

3.2 DSP Impacted Components

The following components will be impacted:

- 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.

- 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.

4 Impact on DCC's Systems, Processes and People

This section describes the impact of SECMP0024 on the DCC Total System services and interfaces that impact Users and/or Parties.

4.1 Security Impact

The new DUIS schema will need to be loaded into DSP's Data Power appliances across all DSP environments.

The change does not impact the DSP resilience or its DR implementation.

4.2 Infrastructure Impact

The new DUIS schema will need to be loaded into DSP's Data Power appliances across all DSP environments.

Additional processing and storage will be required, however, they are not sufficiently large to warrant the procurement of additional compute power or storage.

The change does not impact the DSP resilience or its DR implementation.

4.3 Integration Impact

The new DCC Alert will need to be tested in both SIT and UIT.

4.4 Service Impact

There is not expected to be a material service impact but a more detailed service impact will be carried out as part of the Full Impact Assessment.

5 Implementation Timescales

A minimum of four months should be allowed from commercial cover being provided to the change being declared PIT Complete.

A more detailed timeline for the implementation of the change will be determined via the Full Impact Assessment.

5.1 Implementation Approach

Implementation of this change is assumed to follow a waterfall methodology. The release lifecycle duration will be confirmed as part of the FIA.

5.2 Testing and Acceptance

This change includes the standard test phases as documented in schedule 6.2 and it is assumed that the change will be implemented and tested as part of a major release and will include release-based regression testing in SIT and UIT.

6 Costs and Charges

The table below details the cost of delivering the changes and Services required to implement this Modification Proposal.

The scope of supply under this PIA includes design, development (build), system testing, and unit testing within the PIT environments.

The Rough Order of Magnitude cost (ROM) shown below describes indicative costs to implement the functional requirements as assumed above. The price is not an offer open to acceptance. It should be noted that the change has not been subject to the same level of analysis that would be performed as part of a Full Impact Assessment and as such there may be elements missing from the solution or the solution may be subject to a material change during discussions with the DCC. As a result, the final offer price may result in a variation.

6.1 Design, Build, and Testing Cost Impact

The table below details the cost of delivering the changes and Services required to implement this Modification. For a PIA, only the Design, Build and PIT indicative costs are supplied.

Design, Build and PIT	SIT	UIT	TTO	App. Support	SP Total
£151,000 – £350,000	n/a	n/a	n/a	n/a	£151,000 – £350,000

Design	The production of detailed System and Service designs to deliver all new 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. It includes Unit Testing (also referred to as System Testing), Performance Testing and Factory Acceptance Testing by the Service Provider or supplier.
Pre-Integration Testing (PIT)	Each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. This is assured by DCC. This phase also includes regression testing across all Comms Hub products
Systems Integration Testing (SIT)	All the Service Providers PIT-complete solutions are brought together and tested as an integrated solution, ensuring all SP solutions align and operate as an end-to-end solution. The System Integrator is responsible for leading this phase with the Service Providers offering testing support services.
User Integration Testing (UIT)	Users are provided with an opportunity to run a range of pre-specified tests in relation to the relevant change. The DCC is responsible for leading this phase with the Service Providers offering testing support services.
Implementation to Live (TTO)	The solution is implemented into production environments and ready for use by Users as part of a live service. The Transition to Operations (TTO) service is subject to implementation costs.
Application Support	Any costs associated with supporting the new functionality.

The fixed price cost for a Full Impact Assessment is:

£11,702.01

and would be expected to be completed in 30 days.

7 Risks, Assumptions, Issues, and Dependencies

In the following sections, Risks, Assumptions, Issues, and Dependencies have been identified.

It is possible that further RAID will be established as part of the Working Group reviews and the FIA.

7.1 Risks

None at this time.

7.2 Assumptions

Ref.	Area	Description	Accept
MP24-AD01	Testing	Testing for this Modification will be delivered via the B stream of test environments.	
MP24-AD02	Deployment	This Modification will be delivered as part of a release that includes other Modifications with greater impacts to DUIS. The DUIS uplift is expected to be handled as part of those other Modifications and is, therefore, excluded from the scope of this PIA and the accompanying estimates.	
MP24-AD03	Service Levels	There will be no additional Performance Measures or Service Levels as part of this Modification.	
MP24-AD03	Capacity	This Modification will result in additional load on the DSP Systems, however it is assumed that this will not materially impact the available processing headroom to the extent that performance is affected. An estimate of the additional DCC Alert traffic will be provided as part of the Full Impact Assessment.	
MP24-AD04	Deployment	The changes required under this SECMP0024 will be delivered standalone – i.e independently of SECMP0122B.	

7.3 Issues

None at this time.

7.4 Dependencies

None at this time.

Appendix A: 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
UIT	User Integration Testing