Data
Communications
Company

SEC Modification Proposal, SECMP 0038

Sending Commands via PPMIDs

DCC Preliminary Impact Assessment (PIA), DCC CR 280

Version:	1.2
Date:	8 August 2018
Author:	DCC
Classification:	DCC PUBLIC

Contents

1 Document History

1.1 Revision History

Revision Date	Revision	Summary of Changes
21/05/2018	0.1	Initial compilation from Service Providers
24/06/2018	0.3	Internal DCC Review
26/07/2018	1.1	Included all DCC internal review comments, and requests for clarifications
18/8/2018	1.2	Review with Gemserv

1.2 Associated Documents

This document is associated with the following documents:

Title and Originator's Reference	Source	Issue Date
SECMP0038 - Solution Design Document	https://smartenergycodecompany.co.uk/download/601	3/10/2016
SECMP0038 - Modification-Proposal-Form	https://smartenergycodecompany.co.uk/download/592	1/6/2017

1.3 Reviews and Approvals

This document requires the following DCC internal reviews and approvals:

Name	Title & Company	Issue Date	Revision
Nicola Roteglia	Head of Architecture, DCC	29/6/2018	0.3
Chalam Neelan	Solution Architect, DCC	29/6/2018	0.3
Frederick Wamala	Lead Security Architect, DCC	29/6/2018	0.2
Amanda Rooney	Regulation Manager, DCC	29/6/2018	0.3

2 Introduction

2.1 Document Purpose

The purpose of this DCC Preliminary Impact Assessment (PIA) is to provide the relevant Working Group with the information requested in accordance with SEC Section D6.9 and D6.10.

2.2 Previous Information Provided by DCC

This DCC Preliminary Assessment was requested of DCC on 09/11/2017.

2.3 DCC Contact Details

Please raise any queries regarding this DCC PIA using the contact details provided below.

Name	DCC - SEC Modification queries
Contact email	mods@smartdcc.co.uk

2.4 Proposer's Modification Description

The following text was provided by the Modification Proposer.

Smart Metering Equipment Technical Specification 1 (SMETS1) meters use GB mobile telephone networks for their Wide Area Network (WAN) connections. SMETS2 meters have not yet been deployed in significant numbers, but those in two out of three Communication Service Provider (CSP) regions will also use the GB mobile telephone networks for WAN connections. Thus, WAN performance in SMETS1 deployments gives the best current indication of the likely SMETS2 WAN performance in two out of three CSP regions.

The Proposer (Utilita) has over 90% success with WAN, however they have found that over 9% of their SMETS1 meters continue to have an unpredictable quality of WAN coverage following installation, even using roaming SIM technology which will link into the strongest mobile phone network signal. This means that the meter has intermittent WAN connection, to material numbers of Premises, which is not sufficiently reliable to deliver configuration Commands in a sufficiently timely manner. SECMP0038 is one of a pair of modifications that would replace SECMP0031 to better support customers when faced with intermittent or no WAN situations.

This modification seeks to allow for alternative ways to deliver Commands to SMETS2 Devices, to cater for situations where the WAN connection is not of sufficient quality to deliver them in a timely manner. It is expected that the Commands would usually be routed from the Supplier to the PPMID via Wi-Fi connectivity.

2.5 Context

Each Great Britain Companion Specification (GBCS) Remote Party Command ("Command") is a large number[1] which can be sent via a range of mechanisms to the target Device. Each Command instructs the target Device to take specific actions. All GBCS Remote Party Commands must have

[1] When represented as binary, the number which is a Command is typically in the range from a few hundred to a few thousand bytes.

been validated by the DCC (and a cryptographic DCC check added that the target Devices validate) before they can be communicated to target Devices. Nothing in this modification affects that requirement for DCC validation before the issue of GBCS Remote Party Commands.

A Command is typically delivered to the Consumer's premises via the Communication Service Provider's (CSP's) network to the Communications Hub (CH), but can also be delivered to the CH using a Hand Held Terminal (HHT). Regardless of the route, the CH then sends the Command on to the target Device specified in the Command. The target Device is unaware of the delivery route to the CH and applies the same security checks in all cases. The reason for extending the range of delivery mechanisms is to allow for alternatives when there are issues with the CSP's WAN connection to the CH (e.g. interference).

2.5.1 In Scope

The following activities and changes are in scope for the SEC Modification.

- Uplift of Communications Hub software to support the receipt and forwarding of correctly formatted and authenticated GBCS commands and responses between a Supplier provided PPMID and any HAN connected devices
- Uplift to the Pre-Integration Testing (PIT) PPMID emulator to test the new functionality in the Communications Hubs
- PIT testing
- Uplift to the following documentation:
    - CH02 – Communication Hub Design Specification
    - TS03 – PIT Test Approach.

2.5.2 Out of Scope

The following specific points are excluded and considered out of scope for this document:

- Modification to, procurement of, and delivery of, Communications Hub hardware. There will be no hardware delivered to Service Users via this Modification.
- Provision, and CPA certification, of PPMIDs supporting this Modification
- Any activities including beyond PIT exit required to further assure the functionality delivered by this Modification or promote the functionality into the Production environment.
- Changes to the specifications for the PPMID emulator beyond those specifically required to assure the Communications Hub functionality in PIT.

2.6 Requirements

The requirements for this Modification have been developed by the Working Group during the Refinement phase. The impact on DCC has been assessed against the Business Requirements and the corresponding draft legal text set out in the SECMP0038 Solution Design Document v1.0.

The business requirements are to:

- Require that a CH delivers any GBCS Command received from a PPMID to the target Device identified in the Command. This extends the range of GBCS Commands from the PPMID that the CH is required to deliver;
- Implement this facility in all new and already installed Comms Hubs. This would require firmware upgrades on installed Comms Hubs. Thus, this change is to be included in the next available release which already contains requirements to update firmware on all installed Comms Hubs.

Use of this facility would also require that the Supplier in question provides the Consumer with an ‘enhanced PPMID, i.e., one that has additional capability beyond that in SMETS (PPMIDs are Supplier Devices and so cannot be bought by the Consumer or provided by any other DCC User). There would be no requirement on any Supplier to provide such ‘enhanced PPMIDs’, and so no change to SMETS (which details the minimum PPMID specification).

Rather, Suppliers may elect to provide such Devices to those Consumers where ‘enhanced PPMIDs’ may be needed to provide required services (e.g. those where a CSP WAN connection is of intermittent reliability). Where Suppliers so elect, they would need to have in place some mechanisms in the ‘enhanced PPMIDs’ to receive Commands (e.g. internet connection via WiFi; mobile network connection, etc.). It would be for the Supplier to decide on such provision, which is outside the scope of SEC technical standards.[2]

Such ‘enhanced PPMIDs’ would not be able to use the functionality in the modification until the CH to which it is attached has been updated.

The change to the CH does not affect interoperability with other types of types or with PPMIDs supporting SMETS mandated functionality.

Based on the discussions at the Working Group and the Business Requirements as set out in the Solution Design Document, DCC consider the requirements for SECMP 0038 to be **STABLE**. Where the requirements or SEC obligations set out in the Solution Design Document change, DCC will be required to carry out further impact assessment.

2.6.1 GBCS Specific Changes, 10.8.2

To the version of GBCS in which this change is to be implemented[3], add the underlined and italicised bullet to specify the additional CH requirement::

10.8.2 CH Routing of Remote Party Commands, SME.C.PPMID-GSME and Alerts

Whenever a CH receives any of the following:

- a Remote Party Message via its WAN interface; or
- a Remote Party Message in the Data parameter payload of a Transfer Data command which is from an HHT; or
- *a Remote Party Command in the Data parameter payload of a Transfer Data command which is from a PPMID; or*
- an SME.C.PPMID-GSME Message in the Data parameter payload of a Transfer Data command from a Device, which is in its CHF Device Log,

The CH shall:

- Process the Message Header Structure(s) in that Message sufficiently to identify the target Device’s Entity Identifier; and
- Where the identified Device is in the CHF Device log and is not an HHT, GPF or CHF, attempt to deliver that Message to the identified Device.

[2] SEC Technical Standards relate to Zigbee Home Area Network (HAN) interactions, and do not extend to other network in the premises

[3] This section of GBCS is to be introduced by BEIS IRP521

2.7 High Level DCC Assessment

This modification is to extend the range of mechanisms used to deliver Commands to the CH in Consumers' premises to include delivery via an 'enhanced PPMID'. The modification would not affect the mechanisms the CH uses to forward on the Command to the target Device, nor does the modification affect any processing undertaken by the target Device.

Note that PPMID must already be capable of delivering two types of GBCS Commands via the CH. This modification extends the range of such Commands from the PPMID delivered via the CH, but uses the same PPMID to CH mechanism as the existing two Commands.

Note that HHT cannot be used either to distribute firmware to Smart Meters or to carry Commands resulting from the 'Commission Device' Service Request (SR). The same limitations would apply to a delivery via PPMID.

The Modification Proposal is technically feasible. However there are multiple concerns regarding the potential implementation that are listed in the following sections and in section 8, Clarifications and RAID, following. In addition the CSP for South and Central disputes the predicted failure rate quoted in the Modification will be applicable for the SMETS2 solution, with a significant impact on the business case for this Modification.

3 Impact on DCC's Systems, Processes and People

This section describes the impact of SECMP 0038 on the DCC Total System services and interfaces that impact Users and/or Parties.

3.1 Solution Design

A high level conceptual architecture has been defined to show a potential solution and to identify the magnitude of changes required, as shown below.

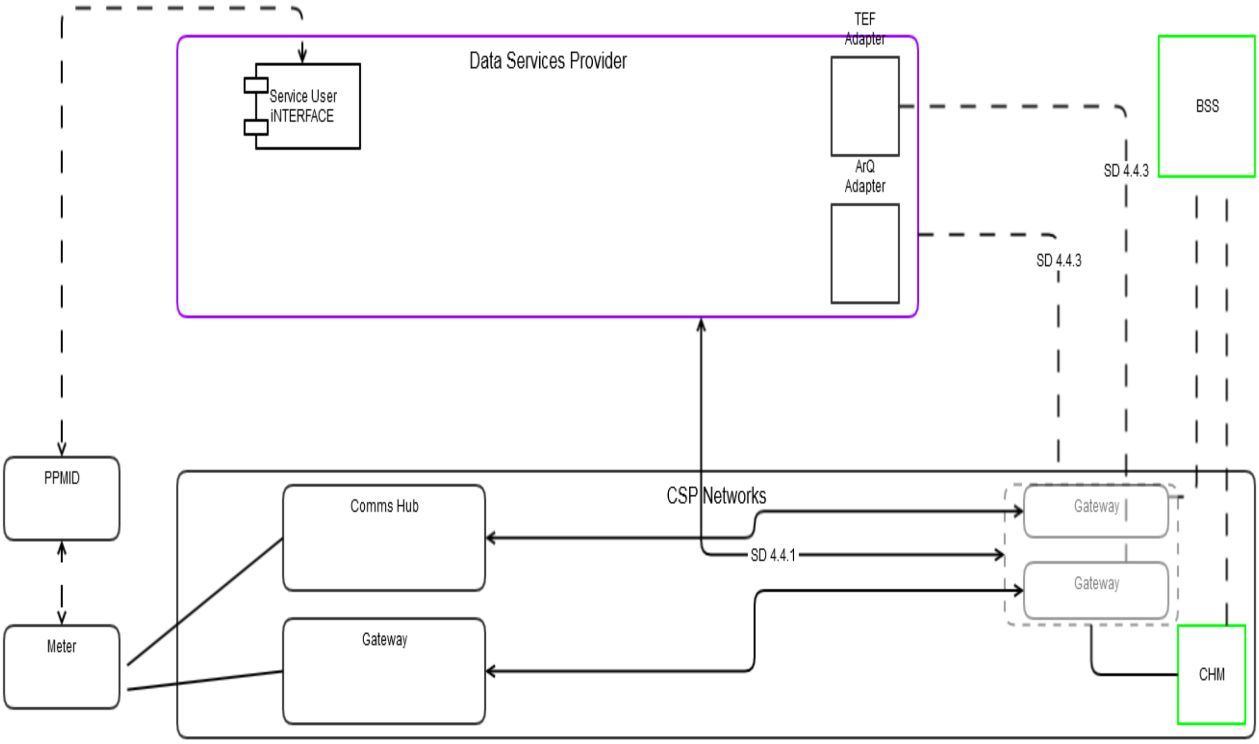

Figure 1: Potential Conceptual Architecture for This Modification

In the currently defined Service User Service Request flow, the Data Service Provider sends a Service Request (SR) through the SM WAN Gateway and the same is sent to the Communications Hub across the CSP network. This Modification is focused on a situation where the SM WAN is deemed not responsive or intermittent, and in this case the Service Request will be passed through the PPMID so that it will bypass the SM WAN Gateway.

However, any responses from a meter related to the Service Request are expected to travel through the current Communications Hub and then the SM WAN route. This Modification and the change to response routing will have an impact on the current CSP business support processes for billing and performance reporting. To use the current reporting framework, it is proposed that the DSP will pass the log files periodically to the CSP for the Service Requests that passed through PPMID connected with the respective CSP Communications Hubs.

3.1.1 DUGIDS, DUIS

When a DCC User submits a non-critical Service Request (SR) or a Signed Pre-Command to the DCC, the DCC User can request that a copy of the resulting GBCS Command is returned; for non-critical Service Requests, these are DUIS Command Variants 2 and 3; for Signed Pre-Commands, they are Command Variants 6 and 7.

This command currently uses the HHT tunnelling cluster to route this message to the HAN. This modification requests the same ability from a PPMID. The pre-formatted message could be passed to the PPMID via Wi-Fi or similar.

The Commission Device SR is currently not available for local delivery. This means that smart meter systems without WAN cannot be set up for communication with the DCC Total System even for local command delivery only. However for the case of no WAN the "Commission Device" SR must be enabled for local delivery. This is a prerequisite for setting up the HAN and prepare it for local delivery of commands and the return of responses.

Without a connection to the WAN the meters will have the time status set to Unreliable. This impacts all date items where a UTC time stamp is required and will need to be resolved in order to enable local delivery of commands.

3.1.2 GBCS

New commands will include.

- GBCS Alert
- New GBCS command to enable “Block Buffer Feed” command
- New GBCS command to disable “Block Buffer Feed” command

There could be further text changes to GBCS to expand both the HHT and CHF communication references to PPMID. The existing HHT functionality cannot be used for this Modification since HHT joining requires re-starting of the CH. This would work on initial install with an installer present but not in cases where the PPMID lost the connection.

The required changes have not been defined in this PIA as full design information has not yet been defined. This will be assessed at the Impact Assessment (IA) phase.

3.1.3 Communications Hub Manager Change

CH Manager (CHM) will receive a new alert from the CHF, i.e. receive the alert, decode and process it, so that it can be displayed in the Alerts Dashboard and appropriate reports (both on the GUI and downloadable reports). The new alert is generated by the CHF when the PPMID connects to a meter.

CHM is required to support functionality to be able to temporarily ‘Block Buffer Feed’ in CHF, when identified or suspected as compromised. These Communications Hubs shall be treated as in standalone mode. CHM will create the capability to unblock the buffer feed. The enabling and disabling of the ‘Block Buffer Feed’ is expected to be achieved via two new commands from CHM to CHF. CHM will report on the Communications Hubs which are in standalone mode.

3.1.4 Data Service Provider

DSP will pass the log files periodically to the CSPs for the Service Requests that passed through any PPMIDs directly connected with the corresponding CSP Communications Hubs.

It is likely there will be a need to change the DSP systems and or processes in line with remote command delivery through the PPMID. The DSP commands for local delivery would have to be provide to the Service User ahead of an install, or the local supplier would have to connect their device at the time of an install. It is possible this would incur charging for local delivery messaging.

In addition, there may be an impact on the ESI interface and the DCC BI MI system, as BI MI may require supplementary information for reporting on these cases. All these potential changes will need to be considered as part of the IA, DSP costs have not been added to the current PIA estimates.

3.1.5 Data Management

A new data feed will be introduced to the solution, although no change to the data model is expected.

3.1.6 Infrastructure Impact

Additional interfaces to DSP will be required. Changes to physical architecture are likely but these changes have not been evaluated for the PIA; they will be assessed in the IA.

3.1.7 Device Emulators

HAN Device Emulators (HDEs) are used in the Systems Integration Testing (SIT) and User Integration Testing (UIT) test phases to enable parties to efficiently exercise the HAN and end to end environments without using real HAN devices. This testing checks the various components of the system, and most importantly, performs a Quality Assurance function upon the Communications Hubs.

The new expected behaviours of the PPMID would require the ability to simulate the delivery of GBCS messages from an emulated PPMID device to a Communication Hub (CH) and thus test the CH's ability to properly receive and respond to GBCS commands. This would require a change to the PPMID HDE Device Type and a means to control the GBCS message in the Emulator control software, requiring changes to both the Emulator firmware and the Emulator PC control software. Note that if at the time of the implementation of this Modification any Virtual HDEs based on a ZigBee dongle, were available then the change would also need to be applied to this solution.

3.1.8 Service Management

This Modification will introduce a number of new scenarios for the Service Management Team to consider in terms of service support, operation and maintenance. For the IA for this Modification, Service Management will be required to review several existing processes including CH Certificate Rotation and Refresh, CH In Life Returns, CH Firmware Management, CH Diagnostics, CH estate monitoring (proactive), Event Management, Incident Management as well as the knock-on impact on Performance Measures. A more detailed review will take place as part of the Impact Assessment.

3.1.9 Contract Schedules

DCC believes that this Modification will have an impact on at least twelve Contract Schedules, including but not limited to design documents, Communications Hubs specifications and pricing. Each change will require CSP, DSP, and DCC resource to implement, with commensurate Compensation for the changes.

Costs associated with these changes have not been included in the estimates following, except for some limited effort associated with supporting any funding changes. The costs associated with Contract Schedules changes have not been included in the PIA. The complete list of contract schedules that will require modification will be provided in the IA.

4 Impact on Security

The proposed Modification significantly changes the Security landscape introducing the possibility of injecting commands from Service User provided devices while still directing such commands through the SM WAN. This will have a direct impact on the CSPs.

As a pre-formatted message could be passed to the PPMID via Wi-Fi or similar, the host code will need to generate an alert when the PPMID connects to CHF, which will be used to monitor the Communications Hubs. In the event of a perceived security threat, the CSP network management team will initiate a command to block the buffer feed which, will block any messages passing to the CSP network. Similarly, CHF will support the unblock buffer feed request. Security measures would be required to isolate any CHs that are perceived to be compromised.

The PPMID device would have the ability to connect to both the households' internet capability as well as connect to the HAN and inject commands. This is regarded as a considerable risk to the HAN and connected systems. Devices being connected to the HAN that are not controlled by the CSPs will impact the service agreement of the HAN and its operational service agreement. The proposed solution goes someway to attempting to prevent unauthorised commands propagating from the CH inbound to the CSP core infrastructure but this capability would require thorough testing to ensure CHM can isolate the HAN and place the HAN in Standalone mode within a timely manner. While the use of HHTs to pass commands is a limited, because the HHTs are only available to trusted individuals, and the connections are of a limited time, connections through a PPMID would remain in place as long as the PPMID is in place. In addition there is currently no message checking in place for the PPMID, and this functionality would most likely have to be introduced. The new message checking would need additional regulation in SMETS for checking by the PPMID.

The PPMID will receive commands from the DCC Total System via a new route outside the smart meter infrastructure and potentially using public networks. The Modification proposes that the verification of a message is done by the CH using its device log and then ultimately by the intended receiver of the command; it doesn't specify whether the PPMID receiving the message/commands should carry out checks prior to forwarding messages to the CH. Without preliminary checks by the PPMID it may be possible for other potentially harmful messages to be sent to the CH which originate from sources other than the DCC Total System. This could result in a Denial-of-Service attack over the HAN and the throttling or disabling of data communications on the HAN. It may also result in alerts raised in high numbers which then might get sent back to the DSP.

The CSPs would seek non-liability responsibility for any unlawful activity originating from within the HAN or a non-CSP managed devices (PPMID, etc.) connected to the HAN, to either the meters, or any subsequent consumer devices attached to the HAN. Any unauthorised commands originating from the PPMID to the HAN should be logged and alerted immediately.

It should be noted that the PPMIDs are currently not CPA security assessed and this would need to be in place before implementing this Modification. This requires the PPMID manufacturers to undertake the CPA process for any new PPMID SMETS2-compliant meters.

A more detailed review of the security implications will be required during the IA.

5 Testing Considerations

This section describes the testing phases required to support the implementation of SECMP 0038. Note that only Pre-Integration Testing costs are included in the cost estimates following.

5.1 Summary

Following initial assessment and responses from impacted workstreams, this will require PIT regression testing and PIT System testing of the new functionality brought in by this Modification, including:

- Communications Hub new functionality to enable GBCS messages via PPMID, and parallel SM WAN to PPMID message delivery
- Two cycles of CH regression testing (PIT only), via SM WAN
- CHM new functionality testing
- CH new functionality testing: full set of regression tests via PPMID
- New functionality testing: message transaction billing, verification that CHs sent SRs via PPMID are excluded for performance measures reports
- Repeat of a subset of PIT test cases for DCC Test Assurance witnessing.

In addition, this CR will require development of the Automation test tool (ATPS) to add API interface capability with a PPMID emulator. Effort required for the integration of an updated ATPS with the PIT test environment and test tools and is included in the costs.

- DCC will be required to carry out PIT and SIT.
- Users will require UIT to support their implementation of SECMP 0038. DCC asks that the Working Group considers and compiles the User testing requirements with DCC support, to ensure an optimal approach is taken for UIT.
- Testing with real devices is likely to require some Data Service Provider involvement as part of wider end to end scenarios. Any associated costs of resourcing will be supplied once an outline of the scenarios has been developed.

5.2 Pre-Integration Testing

Pre-Integration Testing comprises the tests that each Service Provider performs on its respective System changes, prior to the integration of all Service Provider systems. DCC has factored the cost of PIT, including DCC assurance, into this PIA. Suggested PIT scope would include:

- Production, review and agreement of a design to enable development;
- Low level design production, development, unit test and any rework to achieve PIT complete status
- Data generation and loading into the Test environment
- Execution of System Tests through sufficient iterations to enable PIT complete
- Design, implementation and execution of scripts in accordance with assurance procedures used for Release 1.2
- Achieving PIT complete status and subsequent reporting

5.3 Systems Integration Testing

Systems Integration Testing (SIT) is the testing of DCC's Total System, which brings together the components, e.g., DSP and CSP Systems, to allow testing of the end-to-end solution by DCC. SIT is carried out for every DCC System release and incorporates the test and integration of multiple changes. As such the costs of SIT are not included in this assessment.

Additional SIT is recommended by DCC for a modification of this type. It should however be noted that the scope of SIT is likely to be more focused on regression testing to confirm that the changes applied as part of this modification have not had an impact on the wider DCC Total Systems.

Suggested SIT scope would at a high level typically include:

- System Test script and data design
- Data generation and loading into a co-ordinated System Test environment
- Execution of System Tests through sufficient iterations to enable SIT complete

5.4 User Integration Testing

User Integration Testing enables Users to run specific tests to support their implementation of a change. DCC expects that UIT will be required to support User implementation of this modification.

Individual changes are collected into a DCC release. In order to achieve more efficient User Integration Testing for all parties, the DCC will coordinate specific testing requirements for all changes that comprise a release and issue a testing release approach document. As such the costs of UIT are not included in this assessment.

6 Implementation Timescales and Releases

6.1 Change Lead Times

From the date of approval, (in accordance with Section D9 of the SEC), in order to implement the changes proposed, DCC requires a lead time of **12 months.**

As this change introduces a new DUIS schema it should be implemented as part of a wider DCC Release.

7 DCC Costs and Charges

7.1 Design, Build, and Testing Cost Impact

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

Implementation costs							
Implementation Phase	**Design**	**Build**	**Pre-Integration Testing**	**System Integration Testing**	**User Testing**	**Implement to Live**	**Total**
SECMP 0038	*Between £1.37 and £1.86 million*			*Not included*	*Not included*	*Not included*	**£1.37 million - £1.86 million**

Implementation costs – supplementary information	
Implementation cost assumptions	A. *Costs are exclusive of VAT and any applicable finance charges* B. *Majority of the costs above represent labour costs.* C. *Costs provided for Design, Build and Pre-Integration Testing are quotes provided by the Service Providers with specific exclusions of costs as identified above and in section 8,* Clarifications and RAID *following. DCC have reviewed and challenged the costs from the Service Providers to ensure this reflects best price to date.* D. *Costs will be refined during future assessments.*
Explanation of Implementation Phases	*DCC's implementation costs are provided by implementation phases. The following describes the purpose of each phase:* • *Design: The production of detailed System and Service design 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.* • *Pre-integration Testing: Each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. This is assured by DCC.* • *System Integration Testing: All Service Providers' PIT-complete solutions are brought together and tested as DCC's Total Solution, ensuring all Service Provider solutions align and operate as an end to end solution.* • *User Integration Testing: Users are provided with an opportunity to run a range of pre-specified tests in relation to the relevant change.*

	- *Implementation to Live Costs: The solution is implemented into production environments and ready for use by Users as part of a live service. This service is subject to implementation costs.*

The fixed price cost for a Full Impact Assessment is **£162,690**.

7.2 Impact on Charges

This section describes the potential impact on Charges levied by DCC in accordance with the SEC.

DCC notes that SECMP 0038 does not propose any changes to the charging arrangements set out in SEC Section K. DCC has made the assumption that, in the absence of an agreed alternative arrangement by the Working Group, the costs associated with the implementation of SECMP 0038 will be allocated to DCC's fixed cost based and passed through to Parties via Fixed Charges.

Subject to the commercial arrangements put in place to support the relevant Release, DCC expects the increase in Charges associated with the implementation of SECMP 0038 to commence in the month following the Modification implementation.

8 Clarifications and RAID

Note that at the time of the first release of this document, the Service Providers have asked for several clarifications about the proposed design. Responses to these clarifications could significantly impact this PIA.

In the following sections, Risks, Assumptions, Issues, and Dependencies have been identified as part of this Preliminary Analysis. It is very likely that more RAID items will be identified, and existing entries updated, at the time of a full Impact Analysis (IA).

8.1 Clarifications

Ref.	Area	Clarification Requested	Assumption	Status
MP38_C1	PPMID	Whether there is any mechanism or timeout to enable or disable PPMID for routing GBCS message.	UIT test approach and therefore associated test and lab support services in support of R2.0 will be the same as R1.3. Any variations to the support services provided will be by covered by discussions around User Integration Test Service charges	Open
MP38_C2	PPMID	Whether PPMID is required to send the GBCS response/alert from HAN devices or CHF/GPF to remote party via PPMID.	Assume it is not required and the responses will be sent via WAN.	Open
MP38_C3	Identify WAN Capable PPMID	How will a Comms Hub identify which PPMIDs are capable for WAN connection if there is more than one PPMID?		Open
MP38_C4	Band Support	Is it required that the solution supports PPMID in ZigBee 2.4GHz band only or for both 2.4GHz and Sub GHz bands.	Assume only ZigBee 2.4 GHz is required.	Open
MP38_C5	Comms Hub Buffer and Process	The requirements on the Communication Hub to buffer and process commands, responses, and alerts relating to messages originating via the HAN connected PPMID have not been defined as part of this Modification. Confirm the requirements in relation to buffering and processing commands that originate via the PPMID.	Assume there are no additional requirements as part of Modification and therefore existing buffers and processing capacity are judged to be suitable.	Open

MP38_C6	Business Case	In order for a clearer picture of the validity of this modification, we would request the working group to verify that the fault rate for PPMID SMETS 1 and 2 meters is, or is likely to be, of a similar nature across multiple vendors, and for an assessment of the scale of the problem. We understand there is a concern that no SMETS2 PPMID meters are available at this time.		Open
MP38_C7	WAN Status	Will the judgement regarding whether a likely PPMID site is in a state of "Intermittent" or "No WAN" be made prior to a site visit or at the time of installation? What is the basis of a status of "Intermittent"?		Open
MP38_C8	Updated SR	Does the Commission Device SR support the requirement for whenever a CH receives a Remote Party Command in the Data parameter payload of a Transfer Data command which is from a PPMID to deliver it'? If not, does the requirement need to change to enable this restriction?		

8.2 Risks

Ref.	Area	Risk Description	Risk Impact
MP38_R1	Comms Hub	The requirements on the Communication Hub to buffer and process commands, along with response and alerts that relate to messages originating via the HAN connected PPMID has not been defined as part of this Modification. As a result, there is a risk that a hardware uplift is required to increase the buffering and processing capacity of the CH. Should this be the case, then the functionality will differ for pre-Modification and post-Modification Communication Hubs. Note, this relates to clarification MP38_C5	High
MP38_R2	Security	There is a risk that legacy devices cannot be prevented from acting as new devices and to distinguish between legacy and new devices. This could lead to a security threat in the form of functionality impersonation.	Medium

MP38_R3	Security	There is a risk of data loss and device compromise due to the existence of a new interface into HAN which is connected to insecure HANs with internet connection, and limited visibility of CSP or SU. To mitigate this risk, we recommend that obligations are placed upon the users of any HAN device capable of forming connections with devices outside of the HAN	H
MP38_R4	Service Management	There is a risk of total loss of HAN communication and of an inability to send normal messages. This could lead to increased support tickets volumes provoked by the HAN flooding via PPMID entry into HAN. This risk should be mitigated by: • Additional obligations on Service Users to confirm correct behaviour of any installed PPMID prior to raising any tickets in relation to HAN connectivity (This is also logged as a Dependency below) • Additional obligations on Service Management to confirm correct operation of PPMID devices prior to assignment of tickets to CSP	M
MP38_R5	Benefit	There is a risk that this Modification is perceived as poor value for money given the rationale of SMETS1 meters and coverage does not match the SMETS 2 planned solution. The business case will be severely impact if this rationale is not accurate.[4]	H
MP38_R6	Contract Schedules	Costs associated with Contract Schedules changes have not been included in this PIA and are very likely to add to the total cost.	M
MP38_R7	Security	The proposed solution may not be security compliant. This will be reviewed further at the IA, including each Service Provider.	H
MP38_R8	Security	PPMID will become a targeted device for hackers with the potential to impact CHs.	M
MP38_R9	Security	There is a risk that the integrity of HAN devices and HAN communications can be compromised through the ability of the PPMID to inject firmware images into the HAN. This risks HAN communications and the integrity of the HAN via the transmission of potentially large and potentially corrupt images across the HAN. Within the SMWAN based distribution approach that is currently available for HAN devices, the DSP CPL and file size checks would serve to mitigate this risk. It is recommended the firmware image transfer is not permitted using messages injected via a HAN connected PPMID.	H
MP38_R18	DSP Costs	There could be a need to change the DSP systems and processes in line with remote command delivery. As the solution design has been defined to a deep enough level, this will be assessed at the IA stage. It is likely to add significant costs to the Modification costs overall.	H

[4] Smart Energy GB have published this information on planned network coverage: "The new wireless smart meter network, operated by the Data and Communications Company (DCC), will cover more homes than are currently covered by 4G . In Ofcom's latest Connected Nations report, just 88 per cent of premises receive data from mobile networks. The new national communications network will cover more than 99.25 per cent."

MP38_R19	Costs	New interfaces for this Modification have not been defined at a level to enable accurate estimates to be included in the development cost. In addition an assessment of any changes to infrastructure have not been included. These will be added in the IA.	M

8.3 Assumptions

Ref.	Area	Description	Accepted
MP38_A1	Scope	The Communications Hub will only route the GBCS commands from PPMID to target devices whitelisted in CHF device logs. Therefore the CH will discard the GBCS commands from PPMID to CHF, GPF, HHT, remote parties and any target GUIDs not added in those logs.	
MP38_A2	Scope	Additional routing complexity within the CHF to route responses and alerts back to the PPMID for any PPMID HAN-originating commands will not be required. The Communication Hub will therefore route all responses and alert from HAN devices or CHF/GPF to the remote party via WAN or HHT, rather than PPMID.	
MP38_A3	Scope	The PPMID join will follow “CCS01 device join to CHF”, rather than inter-PAN join.	
MP38_A4	Scope	A change request will be raised by DCC to cover the SIT, UIT and Go Live phases of this functionality.	Yes
MP38_A5	Scope	The scope of the Communications Hub is to process correctly formed messages and there is no expectation of additional capability within the CH to monitor HAN usage given the additional entry point into the HAN.	
MP38_A6	Scope	When connected in Sub GHz mode, the PPMID will not deliver GBCS commands while under critical duty cycle action.	
MP38_A7	PIT Test	PIT Testing will not be conducted with real meters or other HAN devices, but with test stubs or emulators	
MP38_A11	GBCS	New GBCS commands will include: • GBCS Alert • New GBCS command to enable “Block Buffer Feed” command • New GBCS command to disable “Block Buffer Feed” command	
MP38_A13	GBCS	The new GBCS commands will be processed and delivered using remote command delivery through HHT in the same way as existing commands.	
MP38_A14	Connectivity	Commands would usually be routed from the Supplier to the PPMID via Wi-Fi connectivity at the installed meter location.	

MP38_A16	CH	Comms Hub will be required to alert on fields that are not yet be defined, such as forced key rotation.	
MP38_A17	CH and Security	Communication between PPMID and Comms Hub must be encrypted.	
MP38_A20	CH and Security	There will be a new process or business logic in place that will allow an 'isolated' CH to re-join the CSP WAN after security concerns are addressed. Once the 'isolated' CH has re-joined the CSP WAN, it is Business As Usual (BAU) for all the existing CH's processes and functionality.	
MP38_A21	Reporting	Isolated CHs will be excluded from all Performance Measures.	
MP38_A22	Support	On the CH Returns Process, Service Management will have an automated solution to communicate to Meter Providers the CH being returned has been operated in ‘Isolated’ mode and its fault reason will default to ‘DCC Fault’. We have assumed as ‘no impact to Returns’, but may require to re-visit during the IA.	

8.4 Issues

Ref.	Area	Description
MP38_I1	Security	This solution introduces a new method for delivering GBCS messages from a non-CPA certified device and is expected to require additional security assessment.
MP38_I2	Schedule Changes	DCC believes that this Modification will have an impact on at least twelve schedules, including but not limited to design documents, Communications Hubs specifications and pricing, and the main schedule. Each contract change will require CSP, DSP, and DCC resource to implement, with commensurate Compensation for the changes. Note any costs associated with Contract Schedules changes have not been included in this PIA. The complete list of contract schedules that will require modification will be provided in the Impact Assessment.

8.5 Dependencies

Ref.	Dependency	Impact
MP38_D1	Updated version of technical specifications to support the changes within this Modification. This will include: • CHTS • GBCS • SMETS	Service Providers will be unable to deliver this Change Request
MP38_D2	This development would be based on GBCS 2.0.	
MP38_D3	There is a dependency to modify the CHIMSM to oblige Service Users to confirm correct operation of the PPMID amd that the PPMID is not reducing the HAN capacity prior to raising any tickets into Service Management.	If the dependency is incorporated but not met, then the SPs will incur additional costs in managing SRs and shall be entitled to recharge these on a time and materials basis.
MP38_D5	CH testing with a PPMID emulator will require a PPMID Application Programming Interface (API) to be provided in updated emulator firmware.	
MP38_D6	API documentation or any other material supplied by the DCC is fixed, agreed upon and made available to Service Providers for analysis and investigation prior to project start.	
MP38_D7	There is a dependency on this Modification for the development, build, and test of PPMIDs, which will result in new-PIAs and IAs for those devices.	
MP38_D8	The existing responsibility for Communications Hub firmware upgrade applies to devices that are dedicated in Service Users' QA warehouses. This includes the scheduling of firmware distribution and activation activates and in accordance with Hypercare processes which is not yet agreed. Therefore these is a dependency to instigate the required changes under SECMP 0013 (CR256).	

MP38_D9	Any new PPMIDs must be CPA compliant. Manufacturers must obtain this certification with associated costs.	

Appendix: Glossary

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

Acronym	Definition
API	Application Programming Interface
ATPS	Automation test tool
BEIS	Department for Business, Energy and Industrial Strategy
CH	Communications Hub, Comms Hub
CHF	Communications Hub Function
CHIMSM	Communication Hub Installation Maintenance Support Materials
CHM	Communications Hub Manager
CPA	Commercial Product Assurance
CSP	Communication Service Provider
DCC	Data Communications Company
DSP	Data Service Provider
ESI	Enterprise System Interface
GBCS	Great Britain Companion Specification
GPF	Gas Proxy Function
GSME	Gas Smart Metering Equipment
HAN	Home Area Network
HDE	HAN Device Emulators
HHT	Hand Held Terminal
IA	Impact Analysis
PIA	Preliminary Impact Analysis
PIT	Pre-Integration Testing
PPMID	Pre Payment Meter Interface Device
SEC	Smart Energy Code
SIT	Systems Integration Testing
SMETS	Smart Metering Equipment Technical Specifications
SMWAN, SM WAN	Smart Metering Wide Area Network
SP	Service Provider
SR	Service Request
SU	Service User
UIT	User Integration Testing
WAN	Wide Area Network