



MP078

‘Incorporation of multiple Issue Resolution Proposals into the SEC - Part 2’

Modification Report

Version 1.0

19 January 2022



About this document

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

Contents

1. Summary.....	3
2. Issue.....	3
3. Solution	6
4. Impacts.....	6
5. Costs.....	8
6. Implementation approach	8
7. Assessment of the proposal	9
Appendix 1: Progression timetable	12
Appendix 2: Glossary	13

This document also has four annexes:

- **Annex A** contains the business requirements for the solution.
- **Annex B** contains the full Data Communication Company (DCC) Impact Assessment response.
- **Annex C** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.
- **Annex D** contains the full responses received to the Refinement Consultation.

Contact

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

Kev Duddy

020 3574 8863

kev.duddy@gemserv.com

1. Summary

This Proposal has been raised by Simon Trivella from British Gas.

Issue Resolution Proposals (IRPs) identify and resolve issues in the Technical Specifications documents of the SEC. The IRPs contained in this document have been identified as DCC System impacting and have been requested to be progressed as a Modification Proposal for implementation into the SEC. Implementation of these IRPs ensures that Devices will operate as intended.

There are three IRPs included in this modification. Two (IRP 550 and IRP 604) are aimed at ensuring when the Gas Smart Metering Equipment (GSME) receives a message known as GCS20r (report event configuration) the GSME can respond. The third (IRP 603) is to ensure Devices such as the In-Home display (IHD), Prepayment meter Interface Device (PPMID) and Consumer Access Devices (CADs) cannot access the security logs on the GSME or Electricity Smart Metering Equipment (ESME).

The Proposed Solution is to incorporate these IRPs into the SEC.

This modification will cost £2,633,973 and require an estimated eight-month lead time for implementation. It will impact Large Suppliers, Small Suppliers, Other SEC Parties and the DCC. Implementation is targeted for the November 2022 SEC Release, if approved as a Self-Governance Modification.

2. Issue

What are the current arrangements?

IRP 550 and IRP 604

A 'GCS20' message is triggered by Service Request Variant (SRV) 6.2.10 'Read Device Configuration (Event and Alert behaviour)'. Currently, there are no instructions in the Technical Specification Great Britain Companion Specification (GBCS) on what response the GSME should provide in the instance it receives a message GCS20 from a Device. As it stands, when a GSME has no data to return, it is unable to provide a defined response to confirm this.

IRP 603

The Smart Metering Equipment Technical Specifications (SMETS) and the GBGS require that the Gas Proxy Function (GPF), Communication Hub Function (CHF), GSME and ESME Security Logs can be read by remote parties. The GSME provides changes of its Security Log to the GPF so that the GPF can maintain a copy of the GSME's Security Log. This copy can be read by remote parties. Both the ESME and GSME make their Security Logs available on a user interface level through meter display. There are no explicit prohibitions currently for sharing Security Logs with Home Area Network (HAN) Devices.

What is the issue?

The individual IRP details for this modification can be found on the Smart Energy Code Administrator and Secretariat (SECAS) website link [here](#) under document name 'MP078 - IRP documents'. These documents reflect the issue, background information and details of the solution that has been

discussed and agreed at Technical Specification Issues Resolution Sub-group (TSIRS). They are an integral part of the SEC modification.

These IRPs are inconsistencies within the Technical Specification. Manufacturers are dependent on these specification for using and developing their Devices. Without these corrections being implemented, Manufacturers are impacted as their Devices are unable to provide an accurate service to consumers. The TSIRS has agreed that these are issues and has agreed upon the solutions.

The IRPs included in this proposal, listed below, require changes to the GBCS with initial key impacts identified by SECAS in the table below.

IRPs included in MP078					
IRP No.	IRP Title	Impacted Technical Specification	Impacted Users	Impacted Devices	Notes
IRP550	GCS20r - Response when an error occurs	GBCS	<ul style="list-style-type: none"> Gas Suppliers Device (GSME) manufacturers 	<ul style="list-style-type: none"> GSME 	Limited / no impact on GS.
IRP603	Security Log display over HAN	SMETS & CHTS	<ul style="list-style-type: none"> Import Supplier Gas Suppliers 	<ul style="list-style-type: none"> CHF GPF GSME ESME 	Expected little impact on Users
IRP604	Query on IRP550 - Frame Control	GBCS	<ul style="list-style-type: none"> Gas Suppliers Device (GSME) manufacturers 	<ul style="list-style-type: none"> GSME 	Limited / no impact on GS

IRP 550

Currently when a GSME receives a message from the Communications Hub known as GCS20r it reports the event configuration back to the Communications Hub, which in turn sends a Service Response to the DCC User. However, there are no instructions in the technical specifications (GBCS) on what response the GSME should give if it cannot send the information (for instance if it does not have the data). This in turn means no Service Response will be received by the DCC User requesting the information.

IRP 604

This IRP has resulted from a typographical error in IRP 550. It has come to light there is an error in the alternate GCS20r response created for IRP 550. The Frame Control which has been set for this response has been defined as "profile -wide; not manufacturer specific; server-client; allow default response;". However, the direction should be 'client-server' and not 'server-client'. This is because the GSME is the client in the Device Management cluster and the response is sent from the client to the server.

IRP 603

Currently IHDs, PPMIDs and CADs on the HAN can request security log information from the GSME or ESME and can display this information to the consumer.

What is the impact this is having?

IRP 550

No response will be received by the DCC User if the GSME does not hold the data, leaving the User unsure where the problem is.

IRP 604

The IRP 550 solution has a typographical error which needs correcting for the response message to work accordingly. The incorrect direction of the Frame Control will cause inconsistency in the way the Device operates.

IRP 603

As things stand, the consumer could view the security log information, which could be a security risk.

Impact on consumers

IRP 603 impacts consumers as they can potentially view Security Log information.

3. Solution

Proposed Solution

IRP550

The Proposed Solution is to include instructions in the technical specifications for the case where the GSME does not have the necessary information.

IRP604

The Proposed Solution is to correct the GCS20r message template. The correction will be made to the direction of the Frame Control to display 'client-server', and not 'server-client'. By amending this in GBCS the specification will align with the ZigBee Smart Energy (ZSE) requirements.

IRP603

The Proposed Solution is to include instructions to ensure the security log information is not accessible by IHDs, PPMIDs and CADs.

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

Breakdown of Other SEC Party types impacted			
	Shared Resource Providers		Meter Installers
✓	Device Manufacturers		Flexibility Providers

Large Suppliers, Small Suppliers and Other SEC Parties, specifically Device Manufacturers, are impacted as they would require additional firmware for Devices. This would then require further testing from a User perspective. A new firmware version which would require testing would incur costs around testing, piloting, and deployment.

A Large Supplier responded to the Refinement Consultation supporting the solution put forward and advised there are gaps that need to be corrected to ensure robustness of the specification. It noted the changes to the SMETS and the GBCS would have to be understood and further work would be required with its meter providers to produce a firmware that adheres to the new specification.

DCC System

The implementation of these IRPs will impact both Communication Service Providers (CSPs) and the Data Service Provider (DSP). The DCC has highlighted the following anticipated areas of impact:

- Parse & Correlate application
 - SMITEn Lite
- GBCS Integration Testing For Industry (GFI) tool
 - SMITEn Lite
- CSP design and build activities
- Device Future Dated Command processing
- Transform Library
- Self Service Interface (SSI)

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

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Schedule 8 'Great Britain Companion Specifications' (GBCS)
- Schedule 9 'Smart Metering Equipment Technical Specifications 2' (SMETS2)
- Schedule 10 'Communications Hub Technical Specifications' (CHTS)
- Schedule 11 'Technical Specifications Applicability Tables' (TSAT)

The changes to the SEC required to deliver the Proposed Solution can be found in Annex C.

Technical specification versions

These changes will be applied to the next Sub-Version of the following Technical Specification series at the time the modification is implemented:

- GSME Technical Specification (GSMETS) v4.x
- ESME Technical Specification (ESMETS) v5.x
- CHTS v1.x
- GBCS v4.x

These changes will also be applied to any new Principal Versions of these documents that subsequently become effective on or before the MP078 implementation date.

Consumers

No impacts on Consumers have been identified.

Other industry Codes

No impacts on other industry Codes have been identified.

Greenhouse gas emissions

No impacts on Greenhouse gas emissions have been identified.

5. Costs

DCC costs

The DCC implementation costs to implement this modification is £2,633,973 if this was implemented as a standalone modification.

The breakdown of these costs are as follows:

Breakdown of DCC implementation costs	
Activity	Standalone cost
Design and Build	£580,643
Pre-Integration Testing (PIT)	£1,306,073
Systems Integration Testing (SIT)	£727,257
User Integration Testing (UIT)	£0
Implement to Live	£20,000

Application Support costs will also be applicable at a cost of £1,573 per annum.

More information can be found in the DCC Impact Assessment response in Annex B.

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.

Party costs

One respondent to the Refinement Consultation advised they would incur cost through testing of new firmware Devices, but no other information was provided.

6. Implementation approach

Agreed implementation approach

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

- **3 November 2022** (November 2022 SEC Release) if a decision is received on or before 28 February 2022; or

- **2 November 2023** (November 2023 SEC Release) if a decision to approve is received after 28 February 2022 but on or before 1 November 2022.

As the change impacts Technical Specifications, the modification should be implemented in a SEC Release that included an uplift to the Technical Specifications. The DCC Impact Assessment has stated that there is an anticipated lead time of eight months for its Service Providers up to implementation. Therefore, the earliest release this modification can be implemented in is the November 2022 SEC Release.

If this modification misses the cut-off date, it will then be implemented in the next Release which included a Technical Specification update. This is expected to be the November 2023 SEC Release.

7. Assessment of the proposal

Observations on the issue

The CSC recommended to the SEC Panel that the Draft Proposal be converted to a Modification Proposal and proceed to the Refinement Process.

The Working Group agreed the issue was clear and should progress further. The Working Group members were supportive of IRP603, IRP604 and IRP550 being included in MP078.

Solution Development

The issues and the solutions have been discussed and agreed upon by the TSIRS. Although the TSIRS is a Department of Business, Energy and Industrial Strategy (BEIS) led group, various SEC Parties are represented. The TSIRS agreed the solutions and agreed they should be implemented into the SEC. Please note, no business case analysis is performed by the TSIRS.

Discussions around the costs of this modification

Preliminary Assessment

SECAS presented the findings of the DCC Preliminary Assessment, which was received 31 December 2019, to the Working Group, which included the cost for delivering the changes and services required to implement this modification. This was originally expected to be £1,700,000 with a full DCC Impact Assessment costing £274,860, with an implementation lead time of three to six months for the DSP and six to 12 months for the CSPs. The Working Group members noted the DCC Preliminary Assessment findings and questioned the high cost. The DCC has been continuously challenging the cost with Service Providers since the first DCC Preliminary Assessment was presented to the Working Group.

SECAS subsequently presented the revised DCC Preliminary Assessment, which was received on 18 November 2020, to the Working Group. This included the revised cost, up to end of PIT, to be £705,680. SECAS highlighted the DCC's estimate of the cost to deliver MP078 would reduce by £240,000 if MP078 was released alongside [SECMP0015 'GPF timestamp for reading instantaneous Gas values'](#) and [SECMP0056 'IHD / PPMID Zigbee Attributes Available on the HAN'S'](#) in the June 2022 SEC Release. This would reduce the overall cost to £465,680 due to synergies across the testing phase.

Impact Assessment

The Proposer was concerned by the large costs contained within the Preliminary Assessment, both for the solution as well as carrying out the Impact Assessment. This caused a delay in requesting the Impact Assessment from the Change Board as further information on the high costs was requested from the DCC. The Technical Architecture and Business Architecture Sub-Committee (TABASC) acknowledged and noted the DCC cost to complete the Full Impact Assessment of £94,430 and was supportive of MP078 proceeding for a DCC Impact Assessment. Following this support, the Change Board approved the request.

The DCC Impact Assessment was received in November 2021. The costs for development, PIT, SIT and Implementation were increased to £2.6m. This increase is largely due to the increase in proposed testing by the CSP North, although the DCC also noted that it considered the Design, Build and PIT costs to be higher than expected too. The CSP Central & South's costs were far lower and it also noted that the functionality was either already introduced, or would be introduced as part of its upgrades to its Communications Hubs.

The Impact Assessment was also discussed with the TABASC. The TABASC queried whether a modification would be required at all given this is already being implemented by the CSP Central and South under its firmware development and if it should instead be made clear that it should not make the Security Log available on the HAN, without necessitating a change to the Technical Specifications.

The TABASC discussed whether it could be acceptable for the CSPs to have different functionality around the availability of the security log on the HAN, and whether having functionality on a single CSP would set any precedent for allowing changes only in one CSP region. The Chair challenged the need to make all regions the same in this case as, at a minimum, only the CSP Central and South making the change would mean that two-thirds of the SMETS2+ estate would benefit from this change. The Chair also noted that this functionality could be added as a requirement in the Network Evolution Communications Hub programme. If that could be included, then the costs would not be borne under this modification.

A TABASC member representing Other SEC Parties suggested this issue should be returned to the TSIRS to determine the actual scope of the problem. They noted that most Devices, if not all, did not share the Security Log with the HAN anyway. Therefore, any change to Technical Specifications could be added to prevent future instances, but without an impact on the Communications Hub. The TABASC Chair agreed, stating that would result in a new IRP and therefore would be managed separately to this modification.

The Impact Assessment was also presented to the Working Group. Working Group members queried why the CSP North required two cycles of PIT. The DCC confirmed it had continually pushed back on the CSP North on the testing level it deems necessary and associated costs. The CSP North has stated it requires two cycles of PIT in case an issue is missed during the first cycle. A Working Group member questioned whether SEC Parties should incur double the costs because the CSP North was not able to have confidence in its own testing through a single cycle.

Business case

These IRPs add clarity and corrections to the Technical Specifications documents. Device manufacturers are required to follow these Specifications when developing or maintaining their Devices. Therefore, any errors or miscommunication of these Specifications will mean the Device will not work as intended. Implementing MP078 will benefit the industry as Devices will be performing accurately. It will also add clarity and consistency across the Specification.

IRP603 has been determined by SSC as a low risk and is tolerable as a standalone risk.

During this modification SEC Parties have not confirmed that IRP550 presents an issue that affects them.

Support for Change

Working Group

The Working Group members were supportive of IRP603, IRP604 and IRP550 being included in MP078. However, they also acknowledged the high costs for this modification and the need for a business case to justify implementation.

Views of Sub-Committees

The TABASC highlighted it was dependent on the DCC to reduce the high costs of this modification. Upon receipt of the DCC Impact Assessment the TABASC provided a strong recommendation to reject the modification as the costs to implement were not justified against a business case. The TABASC noted that the CSP South & Central was implementing this fix regardless of the modification outcome and that would deliver the outcome for two thirds of the country, albeit there would not be such in depth testing.

SECAS also presented MP078 to the Security Sub-Committee (SSC) regarding IRP603 which demonstrated security concerns. The SSC agreed and requested the DCC Security Team to conduct a risk assessment on IRP603. The findings of the assessment confirmed the level of risk associated with IRP603 is very low and tolerable as a standalone issue.

Views against the General SEC Objectives

Proposer's views

The Proposer believes that MP078 would better facilitate SEC Objective (a)¹, as these IRPs resolve issues with the Technical Specifications which are the minimum requirements for Device manufacturers.

Industry views

Two responses were received from the Refinement Consultation. A Network Party supported the modification as it was not impacted by any of the IRPs. A Large Supplier supported the solution put forward due to gaps which require correcting to ensure a robust specification. However, the Large Supplier did state it would be impacted if MP078 was implemented. It advised IRP603, IRP604 and IRP550 would require additional firmware for Devices which are not compliant to the current gaps. Changes to the GBCS and the SMETS would need to be understood and further discussions with meter providers would need to be conducted to produce firmware that adheres to the new specification. The Large Supplier did remain supportive of the MP078 and agreed the modification effectively better facilitates the SEC Objectives.

¹ Facilitate the efficient provision, installation, operation and interoperability of smart metering systems at energy consumers' premises within Great Britain.

Views against the consumer areas

Improved safety and reliability

The change is neutral against this area.

Lower bills than would otherwise be the case

The change is neutral against this area.

Reduced environmental damage

The change is neutral against this area.

Improved quality of service

This implementation will have a positive impact as manufacturers will have access to the most up to date Technical Specification which are accurate and consistent. This will enable manufacturers to develop or enhance their Devices using the guidance provided from these specifications. The quality of service their Device provides will benefit their customers.

Benefits for society as a whole

This implementation will benefit society as premises will have the most up to date Devices which operate as they should per the Technical Specification.

Appendix 1: Progression timetable

Following the Modification Report Consultation the modification will be presented to the Change Board for vote under Self-Governance on 23 February 2022.

Timetable	
Action	Date
Draft Proposal raised	10 Jul 2019
Presented to CSC for comment and recommendations	23 Jul 2019
Panel converts Draft Proposal to Modification Proposal	9 Aug 2019
First Preliminary Assessment requested	6 Sep 2019
First Preliminary Assessment returned	31 Dec 2019
Modification discussed with Working Group	5 Feb 2020
Refinement Consultation	17 Feb – 6 Mar 2020
Second Preliminary Assessment requested	16 Apr 20
Second Preliminary Assessment returned	3 Sep 2020
Updated Preliminary Assessment with cost information received	18 Nov 2020
Presented to Security Sub Committee	25 Nov 2020
Presented to TABASC	4 Feb 2021

Timetable	
Action	Date
Impact Assessment costs approved by Change Board	24 Mar 2021
Impact Assessment requested	10 May 2021
Impact Assessment returned	18 Nov 2021
Impact Assessment discussed with Working Group	1 Dec 2021
Impact Assessment discussed with TABASC	2 Dec 2021
Impact Assessment discussed with TABASC	6 Jan 2022
Modification Report approved by CSC	18 Jan 2022
Modification Report Consultation	19 Jan – 8 Feb 2022
Change Board vote	23 Feb 2022

Appendix 2: Glossary

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

Glossary	
Acronym	Full term
BEIS	Department of Business, Energy and Industrial Strategy
CAD	Consumer Access Device
CHF	Communications Hub Function
CHTS	Communications Hub Technical Specifications'
CSC	Change Sub-Committee
CSP	Communication Service Provider
DCC	Data Communications Company
DSP	Data Service Provider
ESME	Electricity Smart Meter Equipment
ESMETS	ESME Technical Specification
GBCS	Great Britain Companion Specification
GFI	GBCS Integration Testing For Industry
GPF	Gas Proxy Function
GSME	Gas Smart Meter Equipment
GSMETS	GSME Technical Specification
HAN	Home Area Network
IHD	In Home Device
IRP	Issue Resolution Proposal
PIT	Pre-Integration Testing
PPMID	Prepayment meter Interface Device
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SMETS	Smart Metering Equipment Technical Specifications

Glossary	
Acronym	Full term
SRV	Service Request Variant
SSC	Security Sub Committee
SSI	Self Service Interface
TABASC	Technical Architecture and Business Architecture Sub-Committee
TSAT	Technical Specifications Applicability Tables
TSIRS	Technical Specifications Issue Resolution Sub-group
UIT	User Integration Testing
ZSE	ZigBee Smart Energy

MP078 ‘Incorporation of multiple Issue Resolution Proposals into the SEC - Part 2’

Annex A

Business requirements – version 0.4

About this document

This document contains the business requirements 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) and Sub-Committees. It also provides the considerations and assumptions for each business requirement with respect to this Modification Proposal.

1. Business requirements

This section contains the functional business requirements needed for each Issue Resolution Proposal (IRP) contained within MP078 that the DCC have indicated could be DCC System impacting. Based on these requirements a full solution will be developed.

Business Requirements	
Ref.	Requirement
1	DCC System changes for IRP550 'GCS20r - Response when an error occurs'
2	DCC System changes for IRP603 'Security Log display over HAN'

2. Considerations and assumptions

2.1 General

This section contains the considerations and assumptions for each business requirement. These are excerpts from each of the IRPs and it is expected that the DCC will develop solution(s) to the consequential changes these IRPs will have on the DCC Systems. The document text changes are contained within each of the IRPs.

2.2 Requirement 1¹: DCC System changes for IRP550 ‘GCS20r - Response when an error occurs’

Errors cannot be signalled via the ZSE Report Event Configuration command which is currently required as the only option in the GCS20r Response. However, errors could occur in Device processing and so the GCS20r Response needs to allow for such situations.

In common with other Use Cases where this situation applies, the proposed change is to allow the GCS20r Response to contain a ZigBee Default Response (as an Alternate Response) to signal any failures.

2.3 Requirement 2: DCC System changes for IRP603 ‘Security Log display over HAN’

SMETS / GBCS require that:

- the GPF, CHF, GSME and ESME Security Logs can be read by remote parties (and so with access controlled by the DCC);
- the GSME provides changes to its Security Log to the GPF, so that the GPF can maintain a copy of the GSME’s Security Log. This copy can be read by remote parties; and
- both the GSME and ESME make their Security Logs available on the user interface (e.g. the meter display) ‘following physical access through the Secure Perimeter’.

The design intention was that these would be the only ways to access Security Logs, so the Logs should not be made available to HAN devices (e.g. PPMIDs, IHDs or CADs), by either the CH or the ESME (GSME do not communicate with HAN Devices, except for the CH).

Further, GSME and ESME should not make Security Logs available on the User Interface, unless there has been ‘physical access through the Secure Perimeter’.

However, there are no explicit prohibitions currently for:

- sharing Security Logs with HAN devices; or
- only displaying security logs without access through the Secure Perimeter. The proposed position is to amend SMETS (for ESME and GSME) and CHTS (for CH) to add explicit prohibitions.

¹ Please note, IRP604 can only be implemented at the same time, or following the implementation of IRP550. IRP604 has been identified as a GBCS text only change and will be implemented in MP078, applying text changes on top of those implemented by IRP550.

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
ALCS	Auxiliary Load Control Switch
CAD	Consumer Access Device
CH	Communications Hub
CHTS	CH Technical Specifications
DCC	Data Communications Company
ESME	Electronic Smart Metering Equipment
GBCS	Great Britain Companion Specifications
GPF	Gas Proxy Function
GSME	Gas Smart Metering Equipment
HAN	Home Area Network
HCALCS	Han Connected Auxiliary Load Control Switch
IHD	In-Home Display
IRP	Issue Resolution Proposal
PPMID	Pre-Payment Meter Interface Device
SECAS	Smart Energy Code Administrators and Secretariat
SMETS	Smart Metering Equipment Technical Specifications

SEC Modification Proposal, SECMP0078

DCC Change Requests 1233, 1342, 4294

Incorporation of Multiple Issue Resolution Proposals Into the SEC - Part 2

Full Impact Assessment (FIA)

Version:

0.3

Date:

3rd November, 2021

Author:

DCC

Classification:

DCC Public

Contents

2	Executive Summary	4
3	Revision History	5
3.1	Associated Documents	5
3.2	Document Information.....	5
4	Solution Requirements and Overview	6
4.1	Context	6
4.2	Issue.....	6
4.3	Business Requirements	6
4.3.1	Requirement 1, IRP550 GCS20r - Response when an error occurs	6
4.3.2	Requirement 2, IRP603 Security Log display over HAN	7
4.3.3	Requirement 3, IRP604 Query on IRP550 - Frame Control	7
4.4	Business Benefits	7
5	Solution Overview	9
5.1	DSP Solution	9
5.1.1	IRP550 - GCS20r Response when an error occurs	9
5.1.2	IRP604	9
5.1.3	GBCS Versioning and Other Components.....	9
5.2	Critical Software.....	10
5.2.1	GFI Core.....	10
5.2.2	SMITEn Lite.....	10
5.3	CSP South and Central.....	11
5.4	CSP North Solution.....	12
6	Testing Considerations.....	13
6.1	PIT Testing	13
6.1.1	DSP Testing	13
6.1.2	CSP South and Central Testing	14
6.1.3	CSP North Testing.....	14
6.2	System Integration Testing	16
6.2.1	DSP SIT	16
6.2.2	CSP South and Central SIT	16
6.2.3	CSP North SIT.....	17
6.2.4	System Integrator Effort.....	17
6.3	UIT Testing	17
7	Implementation Timescales and Releases	18
7.1	Change Lead Times and Timelines.....	18

7.2	Costs and Charges	18
7.3	Application Support.....	19
7.4	Impact on Contracts and Schedules	19
Appendix A: Risks, Assumptions, Issues, and Dependencies		20
	Risks	20
	Assumptions	20
	Issues	21
	Dependencies.....	21
Appendix B: Glossary		22
Appendix C: Source Documents with IRP Details		23

2 Executive Summary

The Change Board are asked to approve the following:

- Total cost to implement SECMP0078 of £2,633,973 as a standalone release
- The timescales to complete the implementation of eight (8) months
- Include SECMP0078 as part of the November 2022 SEC Systems Release

Problem Statement

Three Issue Resolution Proposals (IRPs) have been identified, IRP550, 'GCS20r - Response when an error occurs', IRP603, 'Security Log display over HAN' and IRP604, 'Query on IRP550 - Frame Control'. The solution for these IRPs have been identified and fixes proposed.

Benefit Summary

These IRPs add clarity and corrections to the Technical Specifications documents. Device manufacturers are required to follow these Specifications when developing or maintaining their Devices. Therefore, any errors or miscommunication of these Specifications will mean the Device will not work as intended. Implementing SECMP078 will benefit the industry as Devices will be performing accurately. It will also add clarity and consistency across the Specification.

3 Revision History

Revision Date	Revision	Summary of Changes
09/07/2021	0.1	Initial compilation from Service Providers
03/11/2021	0.3	Challenged and reviewed submissions

3.1 Associated Documents

This document is associated with the following documents:

#	Title and Originator's Reference	Source	Issue Date
1	MP078-Business-Requirements-v0.4-Updated-2IRPs	SECAS	17/04/2020
3	SECMP0078 CR1233 – PIA – IRPs v0.85	DCC	27/11/2020

3.2 Document Information

The Proposer for this Modification is Simon Trivella of British Gas. The original proposal was submitted in July 2019.

The first PIA was requested of DCC on 30th September 2019. DCC submitted an initial PIA on 31st December, 2019, and the total ROM was £1.9million. The scope of the Modification was changed, and a further request for a PIA was received on 17th April, 2020. Service Providers submitted a response to DCC with the total costs of the PIA was a ROM of £1.2million. After discussions with SECAS, DCC rejected the ROM, requesting that SPs revise their submission. There have been two further iterations and the final ROM is presented within this PIA.

The Full Impact Assessment was requested on the 1st April 2021. Initial responses from the Service Providers were challenged on the basis of costs and content and resulted in the further releases of the FIA responses by both CSP North as well as CSP South and Central.

The FIA for the Modification contained costs broken down by application phase only. Costs for each Service Provider with Release Cost calculations are shown in a separate Code Red Annex.

4 Solution Requirements and Overview

In this section, the context of the Modification, assumptions, and the requirements are stated.

The SEC Definitions, issue statement, and requirements following have been provided by SECAS, the Technical Specification Issue Resolution Sub-Group (TSIRS), and the Proposer.

4.1 Context

This SEC Modification handles incorporation of a set of IRPs into the SEC. Issue Resolution Proposals (IRPs) identify issues within the SEC Technical Specification documents and put forward a solution to the identified problem. In the early stages of the Smart Metering Implementation Program, BEIS took the lead in developing the Technical Specifications that sit under the SEC. As part of this, BEIS also took responsibility for receiving and responding to issues raised internally, by the DCC, and by other interested industry parties. Since its inception, several hundred issues have been raised in relation to technical specifications under the SEC through the Technical Specification Issue Resolution Sub-Group (TSIRS). In some cases, these queries have been resolved by providing an explanation of the specifications, whilst others have resulted in proposed amendments to the specifications in the form of IRPs.

BEIS has previously implemented the required IRPs via BEIS-led designations; however, this process has now been handed over to SECAS for changes to be implemented through the Modifications Process. To improve efficiency, it was agreed these changes should be progressed under a single proposal at regular intervals. This will be the second batch of these changes.

4.2 Issue

In general, IRPs add clarity and corrections to the Technical Specification documents. Device manufacturers are required to follow these documents for the specifications of their Devices. Therefore, any errors or miscommunication of these specifications will mean the Device will not work as intended. TSIRS have agreed that these are issues and have agreed upon the solutions. Not implementing these solutions would mean that these problems would not be resolved.

4.3 Business Requirements

This section contains the considerations and assumptions for each business requirement. Excerpts from each of the IRPs and it is expected that the DCC will develop solution(s) to the consequential changes these IRPs will have on the DCC Systems. The document text changes are contained within each of the IRPs.

The IRPs provided for the PIA are included in "Appendix C: Source Documents with IRP Details" at the end of this document. The following sections contains supporting information about each IRP as well as the IRP title.

4.3.1 Requirement 1, IRP550 GCS20r - Response when an error occurs

Errors cannot be signalled via the Zigbee Smart Energy (ZSE) Report Event Configuration command which is currently required as the only option in the GCS20r Response. However, errors could occur in Device processing and so the GCS20r Response needs to allow for such situations.

In common with other Use Cases where this situation applies, the proposed change is to allow the GCS20r Response to contain a ZigBee Default Response (as an Alternate Response) to signal any failures.

This addresses cases where a failure occurs while a Device executes GCS20r and errors occur in Device processing.

4.3.2 Requirement 2, IRP603 Security Log display over HAN

The Smart Metering Equipment Technical Specification (SMETS) and Great Britain Companion Specification (GBCS) require that the:

- Gas Proxy Function (GPF), Communications Hub Function (CHF), Gas Smart Metering Equipment (GSME) and Electricity Smart Metering Equipment (ESME) Security Logs can be read by remote parties (with access controlled by the DCC).
- GSME provides changes to its Security Log to the GPF, so that the GPF can maintain a copy of the GSME's Security Log. This copy can be read by remote parties.
- GSME and ESME make their Security Logs available on the user interface (e.g. the meter display) 'following physical access through the Secure Perimeter'.

The design intention was that these would be the only ways to access Security Logs, so the Logs should not be made available to Home Area Network (HAN) devices (e.g. PPMIDs, IHDs or CADs), by either the Communications Hub or the ESME. Note GSMEs do not communicate with HAN Devices, except for the Comms Hub.

Further, GSME and ESME should not make Security Logs available on the User Interface, unless there has been 'physical access through the Secure Perimeter'.

However, there are no explicit prohibitions currently for:

- sharing Security Logs with HAN devices
- only displaying security logs without access through the Secure Perimeter

The proposed solution is to amend SMETS (for ESME and GSME) and CHTS (for Comms Hubs) to add explicit prohibitions.

This change would ensure security logs are not available to PPMID, IHD, or CAD devices or readable through non-secured access which might otherwise compromise the security of the Smart Metering System.

4.3.3 Requirement 3, IRP604 Query on IRP550 - Frame Control

IRP604 has been identified as a GBCS text only change and will be implemented in SECMP0078, applying text changes on top of those implemented by IRP550. IRP604 can only be implemented at the same time as, or following, the implementation of IRP550.

4.4 Business Benefits

The IRPs included in this Modification add clarity and corrections to the Technical Specifications documents. Device manufacturers are required to follow these Specifications when developing or maintaining their Devices. Therefore, any errors or miscommunication of these Specifications will mean the Device will not work as intended. Implementing

SECMP078 will benefit the industry as Devices will be performing accurately. It will also add clarity and consistency across the Specification.

The Security Sub-Committee (SSC) noted that the security concern identified in IRP603 presents a low risk, but that the modification should still progress to resolve the issue.

5 Solution Overview

Elements of changes to the solution are identified in the following sections. The following table identifies impacts to each Service Provider.

Ref.	Requirement	DSP	Critical	CSP North	CSP South and Central
1	IRP550, 'GCS20r - Response when an error occurs'	✓	✗	✓	✓
2	IRP603, 'Security Log display over HAN'	✗	✓	✓	✓
3	IRP604, Query on IRP550 - Frame Control	✗	✗	✓	✓

Table 1: IRP Impacts for Each Service Provider

It should be noted that this solution is only applicable to SMETS2 devices.

5.1 DSP Solution

5.1.1 IRP550 - GCS20r Response when an error occurs

Currently, there is no way of signalling an error if a failure occurs while a Device executes GCS20r (Read non-critical event and alert behaviours - GSME-Supplier).

However, errors could occur in Device processing and so the GCS20r Response needs to allow for such situations. In common with other Use Cases where this situation applies, the GCS20r Response will be allowed to contain a ZigBee Default Response (as an Alternate Response) to signal any failures. This will be an additional element in the Response.

The Zigbee Cluster Library (ZCL) payload of the Default Response will contain 0x05 as the value of the Command identifier if the GCS20r command does not succeed. DCC Data Systems will need to amend the corresponding Transform Library to support the new element in the GCS20r Response. In the absence of the Default Response, the processing shall be carried out as it is today.

Although a Default Response has been added to GCS20r, this does not change the existing functional behaviour of the Service Request Variant 6.2.10 (Read Device Configuration (Event And Alert Behaviours)) and as such, no changes are expected to DUIS.

5.1.2 IRP604

IRP604 is a correction to a sub-field that indicates the direction of message (client-server) of the Frame Control field within the new Default Response added to GCS20r. This has no impact on the DSP, as the correction will be made alongside IRP550.

5.1.3 GBCS Versioning and Other Components

A new GBCS version will be introduced in order to support IRP550 and IRP604. The version of GBCS that will include these IRPs are not finalised yet, but is most likely to be part of the GBCS 4.x version.

DSP is required to make data updates to support the new version of GBCS. It is possible that the effort involved in adding support for new version of GBCS is absorbed by a wider Release CR, and any other Modifications or Change Requests in this SEC Release will share the GBCS development costs across multiple activities. Based on that assumption, DSP have provided the effort involved in adding support for GBCS version as a separately identifiable item.

The Transform component will need to parse the Default Response for the Use Case GCS20r.

For the Data Management component, the DSP will need to update reference data to add support for the new version of GBCS.

5.2 Critical Software

Notice that Critical did not supply an FIA, but the following information is included for completeness.

5.2.1 GFI Core

To meet the requirements specified in **IRP550**, the GBCS Integration Testing For Industry (GFI) tool will need to implement full support of GCS20r as follows:

- Enhance the GFI Testing Tool to support GCS20r on GFI Testing Tool
- Implement support for GCS20r on the Reference Test Data Set (RTDS)
- Update GMST with GCS20r
- Enhance the Triage Tool to support GCS20r

To meet the requirements specified in **IRP603**, GFI will need to update the Comms Hub to restrict the access of Security Logs to HAN devices.

- Restrict access to CHF Security Log to Type1 and Type2 devices
- Restrict access to GPF Security Log to Type1 and Type2 devices

5.2.2 SMITEn Lite

The changes required to implement this Modification will affect the SMITEn parse service requiring an upgrade to a new version of the Parse and Correlate application.

For the IRPs, SMITEn Lite changes are:

- IRP550 Add integration and system tests for use case GCS20r and review tests.
- IRP603 No effort required – this only affects the availability of the Security Logs for HAN devices.

As a whole, these changes will require the release of a new version of SMITEn Lite.

5.3 CSP South and Central

For CSP South and Central, there is no Comms Hub firmware release required to implement this Modification.

IRP #	Description	Impacts CH ?	Comments
550	DCC System changes for IRP550 'GCS20r - Response when an error occurs	No	No change to the Communication Hub required to implement this IRP.
603	Security Log display over HAN	Yes	WNC as a result of the IRP581 implementation, requires no further changes to implement IRP603. For Toshiba, IRP603 requires a configuration change which is being included as part of the current quarterly FMP release 13.x.
604	Query on IRP550 - Frame Control raised by Flonidan	No	No change to the Communication Hub required to implement this IRP.

One of the CSP North Comms Hub vendors (WNC) has already made the changes for IRP603 fix as part of its GBCS 3.2 firmware release, while the other vendor (Toshiba) will be implementing IRP603 configuration changes as part of its currently planned quarterly FMP release 13.x.

The impact on the device emulators are as follows.

IRP	Emulator Impacted	Description of Change
550	GSME	On reception of GCS20r command, the GSME Emulator always provides "Normal response" as default configuration of Event is available in it. There will be test support in GSME Emulator UI to generate "alternate response" for GCS20r command.
603	PPMID and IHD	PPMID/IHD Emulator does not support "GetEventLog" command generation over HAN. Also, Event cluster is not present in ZSE Device requirements as per GBCS v3.2. For GPF/ESME Testing purpose, this command can be added to support PPMID/IHD Emulator UI if required for negative testing
603	ESME and GSME	1. Add support to see Security Logs in ESME/GSME Emulator UI (Password protection). 2. ESME Emulator does not send "PublishEvent" command with LogId="Security Event Log" to type1/type2 devices. GSME Emulator does not send "PublishEvent" command to type1/type2 devices.
IRP604	GSME	On reception of GCS20r command, the GSME Emulator always provides "Normal response" as default configuration of Event is available in it. As part of this CR, there will be test support in GSME Emulator UI to generate "alternate response" for GCS20r command.

5.4 CSP North Solution

IRP 550 has no effect on development for the CSP North.

For IRP603, the Comms Hub shall reject any `getEventLog` command received for log id 0x04 (Security Log) with a ZigBee status of 0x7E – NOT_AUTHORIZED. When the GSME publishes an event to the GPF, it uses the event control bits within the command to denote whether the event should be published to all bound HAN devices. Where a `publishEvent` command is received from the GSME containing an event with log id of 0x04 (Security Log), the Communications Hub will now disregard the setting of event control bit 0 and will not publish the event to bound devices.

For Unit Testing, CSP North have indicated the need to develop an IHD stub, and request the security log from the Comms Hub. Unit Testing with IHD and PPMID devices joined and bound on the events cluster will also be required. The existing IHD and GSME stubs will need to be modified to support testing because real devices will not send the commands required to test these firmware changes.

6 Testing Considerations

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

DCC-L provided assumptions for PIT testing are as follows:

Area	Assumption
PIT Environment	Assume a PIT environment will be made available for this testing to be carried out.
Communication Hub	Any change testing will be limited to PIT testing of the new functionality outlined in the Modification as well as PIT regression testing. PIT System testing will consist of one cycle of testing of the new functionality delivered by this Change Request, plus one cycle of targeted regression testing.
Repeat Testing	A subset of PIT System test cases will be conducted for DCC Test Assurance witnessing
Non-Functional / Performance Testing	Will be carried out at this stage

Table 2: DCC Supplied PIT Testing Assumptions

Testing costs for SIT and UIT will be built on the following assumptions provided by DCC and agreed with the Service Providers

Area	Assumption
Standalone Release	As required by SECMP0049, with costs calculated as if no other Modifications or CRs are in this release Note that CSP South and Central may include testing as part of their Firmware Management Policy (FMP).
SIT Testing	8 weeks
UIT Testing	8 weeks
Test Sets	10 Test Sets per Communication Hub type (20 for Telefónica, same split per band but two manufacturers). A device set will be agreed.
Regression Testing	Risk based regression testing.

Table 3: SIT and UIT Testing Assumptions

Note that SIT Testing duration has been reduced by the CSPs on their recommendations, and that no UIT testing is required.

6.1 PIT Testing

6.1.1 DSP Testing

Pre-Integration Testing (PIT) will be required to align DSP functionality and the functionality described above. The development team will carry out unit testing and the

build will be subject to continuous build and automated testing to identify build issues at the earliest opportunity. The implementation team will carry out system testing consisting of positive and negative path testing.

6.1.2 CSP South and Central Testing

CSP South and Central have indicated a need to design, build and system test changes to the HAN Device Emulator (SLS) required to implement the IRPs.

During PIT, CSP South and Central will design, build and system test changes to test tooling required to assure the solution in the PIT environment. By using the FMP delivery approach, no additional Comms Hubs, test hardware or software needs to be procured. PIT Functional / Regression testing with RTL and ITCH variants is out of scope for this Modification. As the IRP changes are limited to HAN specific changes, CSP South and Central will carry out the PIT Functional and Regression testing with only Production codebase Comms Hub variants as follows:

1. Toshiba Single Band Comms Hubs (SBCH)
2. WNC SBCH
3. Toshiba SBCH Mesh
4. Toshiba DBCH
5. WNC DBCH
6. Toshiba DBCH Mesh

CSP South and Central will carry out limited regression testing for this Modification with only the above listed Production codebase variants, with the scope of the PIT regression testing being more focussed to only cover the basic testing on GPF, GSME, ESME - read security logs as follows:

- Functional testing in PIT with the Production codebase variant and HAN device emulator changes. The functional testing will be limited to one cycle of testing in PIT with both Toshiba and WNC SBCH and DBCH operating on GBCS 3.2 and 4.x firmware.
- Regression Testing in PIT
- Triage, Defect Management and Release management support during PIT functional and regression testing.

Note that no savings would be generated by grouping these into a Release. The nature of the Firmware Management Policy has already resulted in savings to the charges.

6.1.3 CSP North Testing

PIT will be performed with:

- real (physical) meters
- PPMIDs

- HCALCS

Comms Hub variants along with Debug and Non-Debug test variants. These will be tested in a near parallel approach. The governance will be developed and published in an agreed DCC Test Approach and will provide daily and end of PIT phase completion reports as well as attend all relevant calls and facilitate DCC witness testing. The following testing will be carried out in PIT:

Comms Hub Variant Test Scope	EDMI Single Band Standard 420	EDMI Dual Band Standard 420	EDMI Dual Band Variant 450
GPF should not share the GSME security log to Type 1 Device	X	X	X
GPF should not share the GSME security log to Type 2 Device	X	X	
GPF should respond with NOT_AUTHORIZED to Type 1 device when requested for GSME security log	X	X	X
GPF should respond with NOT_AUTHORIZED to Type 2 device when requested for GSME security log	X	X	
GPF should share GSME event log to type 1 device	X	X	X
GPF should share GSME event log to type 2 device	X	X	
GSME security Log can be read from GPF via SR 6.13	X	X	
GPF can store all GSME security event in its GPF GSME proxy log	X	X	

Table 4: Test Cases and Comms Hub Variants for CSP North PIT Testing

The test approach for PIT will be as follows:

- Consumption data will be set up during preparation for PIT phase
- Testing in PIT will be performed with real devices for regression testing, with emulators used to validate the specific IRP603 fix functionality
- New functionality testing with primarily with SBCH and DBCH; other variants will be covered targeting new functionality testing and targeted regression testing
- • PIT will take a risk-based approach for regression testing, where DBCH will be tested primarily compared to SBCH
- • • PIT for DBCH will cover testing with both SubGHz and 2.4GHz band functionality

- Two cycles of PIT testing - four weeks¹ for each test cycle with each Comms Hub variant (SBCH, DBCH/DBCH-F), excluding test preparation, ITCH, W-ITCH execution, test completion report and work-off.
- All functional sets will be planned in combination of ne ESME, one GSME and one PPMID or IHD.

The proposed test set requirement for PIT is as follows:

CH Variant/Env PIT	SBCH (Standard 420 CH)	DBCH (Standard 420 DB CH)	DBCH-F (Variant 450DN CH)
Functional and regression	4	6	4
Soak Tests	1	2	1
ITCH	3	3	n/a
W-ITCH	1	1	1

It should be noted that the regression testing proposed by CSP North is more extensive than would be expected for a change of this magnitude. It is expected that when combined with other Modifications and Change Requests in a SEC Release, the effort and cost for CSP North PIT testing in this Modification will be reduced.

6.2 System Integration Testing

6.2.1 DSP SIT

The scope of Systems Integration Testing (SIT) within the Modification will consist of:

1. Generation of the error a device emulator will use;
2. Execute SRV 6.2.10 (Read Device Configuration (Event and Alert Behaviours))
3. Generation of Use Cases for both ESME and GSME, Use Case GCS20r is for the GSME to verify this not impacted by the change.

SRV6.2.10 will be executed against an emulator and against any one of the CHF types for a current SMETS2 and GBCS configuration that is selected by the DCC. The emulator will be required to generate a device error that is incorporated into the SRV response.

The following changes for SIT activities are required:

6.2.2 CSP South and Central SIT

The CSP South and Central SIT assumptions are:

- A total of 4 device sets (Comms Hubs, meters or emulators) and 4 contingency Comms Hubs has been considered for SIT test preparation and readiness.
- There are no new devices/ emulators which are introduced in SIT and the devices/emulators already exists in the Test Lab.

¹ This is an exceptional level of testing four weeks to carry out eight test cases per device type. This has been challenged by the DCC. IN addition testing the Wireless ITCH variant does not seem necessary

CSP South and Central have costed for three(3) weeks of SIT Test execution support for assuring the changes for this Modification.

6.2.3 CSP North SIT

CSP North SIT testing will follow the same format as that in PIT.

6.2.4 System Integrator Effort

There will be a requirement for System Integrator Release Management to coordinate deployment of the CSP functionality to the SIT environment and finally into Production.

6.3 UIT Testing

There is no perceived need to specifically test this change separately in the UIT environment. Regression testing is assumed to be covered under the release within which this change is implemented.

7 Implementation Timescales and Releases

This Modification was expected to be included in a SEC release in November 2022.

Implementation timescales will be finalised as part of the relevant SEC Release Change Request.

7.1 Change Lead Times and Timelines

From the date of approval (in accordance with Section D9 of the SEC), to implement the changes proposed DCC requires a lead time of approximately **8 months**.

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

Phase	Duration
SECAS agreement on scope of release	
CAN signature, CSP South and Central Mobilisation starts	D + 1 Month
Design, Build and PIT Phase	D + 5 Months
SIT and UIT Phases Complete	D +8 Months
Transition to Operations and Go Live	D + 8 Months

7.2 Costs and Charges

This section indicates the quote per application phase for this Modification.

£	Design and Build	PIT	SIT	UIT	TTO	SP Total
Phase Total	580,643	1,306,073	727,257	0	20,000	2,633,973

Design and Build

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

Pre-Integration Testing (PIT)

Each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. This is assured by DCC.

Systems Integration Testing (SIT)

All the Service Provider's PIT-complete solutions are brought together and tested as an integrated solution, ensuring all SP solutions align and operate as an end-to-end solution.

User Integration Testing (UIT)

Users are provided with an opportunity to run a range of pre-specified tests in relation to the relevant change.

Implementation to Live (TTO)

The solution is implemented into production environments and made ready for use by Users as part of a live service.

The development costs include an element for a GBCS change. If the SEC Release contains other GBCS changes, these costs will be shared amongst the other Modifications and Change Requests leading to a drop in DSP development costs.

It should be noted that the regression testing proposed by CSP North is more extensive than would be expected for a change of this magnitude. It is expected that when combined with other Modifications and Change Requests in a SEC Release, the effort and cost for this Modification will be reduced.

However CSP South and Central noted that no savings would be generated by grouping this Modification and other CRs into a SEC Release. The nature of the Firmware Management Policy has already resulted in savings to the charges above.

7.3 Application Support

The Application Management Support team is responsible for the provision of application level support for the DCC Data System application. This change provides additional functionality that will be subject to support to the end of the DSP contract.

The new functionality could result in approximately one call per month on an ongoing basis. As a result, DSP has made a conservative estimate that the change will result in one low-medium complexity call that needs to be assimilated, investigated, resolved and monitored per month over the life of the contract.

The team will need to be prepared to support the change from the day it goes into live operation. As such the team must review the functional solution and its technical implementation. The team must understand any configurable options and develop procedures to enable its support. This information must be absorbed across the team.

For the DSP an one-off Application Support charge of £1,573 is anticipated for this Modification.

7.4 Impact on Contracts and Schedules

At a minimum, the following DSP schedules will be updated as a result of the changes introduced by this Modification:

- Schedule 6.1 - to reflect delivery milestones
- Schedule 7.1 - to reflect payment milestones under this Modification
- Schedule 11 - to reflect an uplift to the CH specifications
- Schedule 12 - to reflect the uplifted technical specification versions

CSP contract schedules to be amended include:

- Schedule 6.1 – to reflect any delivery milestones under this Change Request.
- Schedule 7.1 – to reflect any payments under this Change Request.

Appendix A: Risks, Assumptions, Issues, and Dependencies

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

Risks

Ref	Description	Status/Mitigation
CSC-R3	Risk that this Change Request is seen to be poor value for money given the expectation that all Test Comms Hub variants have been included in scope. The Test Comms Hub variants in operation today have significant overlapping scope and use cases. CSP South and Central recommend considering reducing the scope and complexity of this Modification by simplifying the Test Comms Hub product line.	Accept
CSC-R8	As additional CRs are included in FMP scheduled releases, there may be a priority call on which defects can be fixed within the available slots in FMP. There is a risk that defect fixes may be delayed to accommodate CRs to be in scope for FMP release candidates. Prioritising and scheduling of CR and defects within the FMP will be agreed within the Firmware Management Forum.	Open, but management will also involve DCC In Life Change Delivery team

Assumptions

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

Ref	Description	Status/Mitigation
CSC-A3	Assume that when the associated GBCS/SMETS/CHTS specifications to support the changes for this Modification are defined, there will be no material changes from the documentation beyond those specified in this document.	Accepted, but noted that there are no changes in SMETS or CHTS, and that CSP South and Central will update CH02
	Further, CSP S and C assumes that the DCC-L will raise a separate CR once the baselined approved industry specification is made available (GBCS 4.x, CHTS 1.x) prior to Telefónica Communication Hubs being able to declare compliance to the associated CHTS version.	Accepted, but note no CHTS version change
CSC-A12	Assumes that the functional changes to CH firmware can be delivered with the application layer and do not require stack developments from the ZigBee chip provider, or the WAN modem providers. Should a new stack be needed, besides additional development time, experience has shown a lengthy CPA accreditation is also needed.	Accepted

Issues

None at this time.

Dependencies

Ref.	Dependency	Implication if not met	Status
CSC-D1	Dependency on DCC to provide and confirm the GBCS/SMETS/CHTS specifications to support the changes in this Modification	Work cannot start and a further FIA may be required	Accepted but noted that there are no changes in SMETS or CHTS, and that CSP South and Central will update CH02
CSC-D2	Dependency on updating the Parse and Correlate application		Rejected; no changes in Parse and Correlate are required.

Appendix B: Glossary

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

Acronym	Definition
ACB	Access Control Broker
BEIS	Department for Business, Energy & Industrial Strategy
CH, Comms Hub	Communications Hub
CoT	Change of Tenancy
CHF	Communications Hub Function
CPA	Commercial Product Assurance
CR	(DCC) Change Request
CSP	Communication Service Provider
DCC	Data Communications Company
DSP	Data Service Provider
DUIS	DCC User Interface Specification
ESI	Enterprise Systems Interface
ESME	Electricity Smart Metering Equipment
FIA	Full Impact Assessment
FMP	Firmware Management Policy
FOC	Final Operating Capability
GBCS	Great Britain Companion Specification
GFI	GBCS Integration Testing For Industry
GPF	Gas Proxy Function
GSME	Gas Smart Metering Equipment
HAN	Home Area Network
IHD	In Home Display
IRP	Issue Resolution Proposal
PIA	Preliminary Impact Assessment
PIT	Pre-Integration Testing
PPMID	PrePayment Meter user Interface Device
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SMETS	Smart Metering Equipment Technical Specification
SM WAN	Wide Area Network
SP	Service Provider
SRV	Service Request Variant
TSIRS	Technical Specification Issue Resolution Sub-Group
TTO	Transition to Operations
UIT	User Integration Testing

Appendix C: Source Documents with IRP Details



IRP550
GCS20r-Responsewl



IRP603 Security Log
display over HANv0_

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.

MP078 ‘Incorporation of multiple Issue Resolution Proposals into the SEC - Part 2’

Annex D

Refinement Consultation responses

About this document

This document contains the full collated responses received to the MP078 Refinement Consultation.

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

Question 1				
Respondent	Category	Response	Rationale	SECAS Response
Western Power Distribution	Network Party	N/A	We have not reviewed IRP 550, IRP 306 or IRP 604 as they have no impact on us so are neutral to this.	-
OVO	Large Supplier	Yes, in principle.	These gaps need to be corrected to ensure robustness of the specification.	-

Question 2: Will there be any impact on your organisation to implement MP078?

Question 2				
Respondent	Category	Response	Rationale	SECAS Response
Western Power Distribution	Network Party	No	IRP 550, IRP 306 or IRP 604 have no impact on Electricity Distributors.	-
OVO	Large Supplier	Yes	<p>Potentially- IRP603 and IRP604/550 may require additional firmware for Devices where they are not compliant to these current gaps. This could necessitate further testing from a User perspective. Impact is most concerning with IRP603, as if CHs are not currently compliant to this then our testing volume rises exponentially.</p> <p>Changes to SMETS and GBCS would have to be understood and further work with our meter providers would be required to produce firmware that adheres to the new specifications.</p>	-

Question 3: Will your organisation incur any costs in implementing MP078?

Question 3				
Respondent	Category	Response	Rationale	SECAS Response
Western Power Distribution	Network Party	No		-
OVO	Large Supplier	Yes	Yes we will incur costs as a result of the testing mentioned in Q2. Furthermore, we note that new firmware will incur costs around testing, piloting and deployment.	-

Question 4: Do you believe that MP078 would better facilitate the General SEC Objectives?

Question 4				
Respondent	Category	Response	Rationale	SECAS Response
Western Power Distribution	Network Party	N/A	See response to Question 1.	-
OVO	Large Supplier	Yes	Facilitates objectives and effectively.	-

Question 5: Noting the costs and benefits of this modification, do you believe MP078 should be approved?

Question 5				
Respondent	Category	Response	Rationale	SECAS Response
Western Power Distribution	Network Party	N/A	See response to Question 1.	-
OVO	Large Supplier	Costs require further review	<p>The costs quoted are not clear as to whether these include IRPs 554 and 582, which this consultation has sought to move into MP098. The DCC document states IRPs 550, 554, 582 and 603 as being included in the costing, and the consultation still quotes this figure despite seeking to remove 554 and 582- which we note have the largest impact for DCC.</p> <p>As noted by Telefonica in Section 7.3 of Annex B to this SECMP, the quoted costs would be significantly lowered if implemented with a major release incorporating these IRPs. Since MP078 would now only include IRP550 and IRP603- both which we are currently living with and neither of which have significantly detrimental impacts- we may make more efficient use of resources if the DCC-requirements of these IRPs are also rolled into MP098</p>	-

Question 6: How long from the point of approval would your organisation need to implement MP078?

Question 6				
Respondent	Category	Response	Rationale	SECAS Response
Western Power Distribution	Network Party	N/A	See response to Question 1.	-
OVO	Large Supplier	No comment	This is dependent on firmware changes required, which would then require testing from our perspective. It would also depend on how long our manufacturers will take to develop compliant firmware.	-

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

Question 7				
Respondent	Category	Response	Rationale	SECAS Response
Western Power Distribution	Network Party	N/A	See response to Question 1.	-
OVO	Large Supplier	Yes but timing needs to be addressed.	The implementation is sound, however the timing of when this is implemented could be better improved to minimise on cost.	-

Question 8: Do you agree that the legal text will deliver MP078?

Question 8				
Respondent	Category	Response	Rationale	SECAS Response
Western Power Distribution	Network Party	N/A	See response to Question 1.	-
OVO	Large Supplier	No comment	This will only deliver MP078 provided all manufacturers are currently adhering to the behaviour described in MP078, which we cannot fully comment on.	-

Question 9: Do you agree with removing IRP554 and IRP582 from MP078 and incorporating them into MP098?

Question 9				
Respondent	Category	Response	Rationale	SECAS Response
Western Power Distribution	Network Party	Yes	<p>Whilst we agree with the proposal to remove IRP554 and IRP582, we cannot see them detailed anywhere in MP098. We are concerned that because they are not detailed within MP098 that they might get omitted, either in their entirety or parts of the solution.</p> <p>Please can MP098 be updated and republished to include these IRPs, or if they are now referred to as something else can this be clarified?</p>	<p>IRP554 has been added to the scope of MP098 and is included in the Modification Report.</p> <p>IRP582 has been withdrawn by BEIS and has been superseded by IRP623</p>
OVO	Large Supplier	Yes	No comment.	

Question 10: Do you agree with implementing the legal text drafting from MP078 to the current Principal Versions of the Technical Specifications as a Sub-Version, and as a Sub-Version to the next Principal Version?

Question 10				
Respondent	Category	Response	Rationale	SECAS Response
Western Power Distribution	Network Party	N/A	See response to Question 1.	-
OVO	Large Supplier	Yes	No comment.	-

Question 11: Do you agree with including IRP604 in MP078?

Question 11			
Respondent	Category	Rationale	SECAS Response
Western Power Distribution	Network Party	See response to Question 1.	-
OVO	Large Supplier	Yes- IRP604 should be implemented in conjunction with IRP550.	-

Question 12: Please provide any further comments you may have

Question 12			
Respondent	Category	Comments	SECAS Response
Western Power Distribution	Network Party		-
OVO	Large Supplier	We would encourage caution in the implementation of IRP582 to ensure it does not conflict or become nullified by changes brought in by the introduction of Proportional Load Control devices, and the proposed changes to existing ALCS/HCALCS devices as part of this.	-