Data Communications Company

SEC Modification Proposal, SECMP0078, DCC CR1233, CR1342

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

Preliminary Impact Assessment (PIA)

Version:	**0.5**
Date:	**1st September, 2020**
Author:	**DCC**
Classification:	**DCC PUBLIC**

Contents

1 Document History 4
1.1 Revision History 4
1.2 Associated Documents 4
1.3 Document Information 4
2 Context and Requirements 5
2.1 Problem Statement 5
2.2 Business Requirements 5
2.2.1 Requirement 1, IRP550 'GCS20r - Response when an error occurs' 5
2.2.2 Requirement 2, IRP603 'Security Log display over HAN' 5
2.2.3 Requirement 3, IRP 604, Query on IRP550 - Frame Control 6
3 Description of Solution 7
3.1 DSP Solution 7
3.1.1 IRP550 7
3.1.2 IRP604 7
3.2 Critical Software Solution 7
3.2.1 GFI Core 8
3.2.2 SMITEn Lite 8
3.3 Communication Service Provider (CSP) Changes 8
4 Impact on DCC Systems, Processes and People 9
4.1 Security Impact 9
4.2 Request Management 9
4.3 Data Management 9
4.4 Transform 9
4.5 Self Service Interface (SSI) 9
4.6 Integration Impact 9
4.7 Infrastructure Impact 9
4.8 Application Support 10
4.9 Service Impact 10
4.10 Safety Impact 10
4.11 Contract Schedules 10
5 Implementation Timescales and Approach 11
5.1 Implementation Approach 11
5.2 Testing and Acceptance 11
6 Costs and Charges 12
6.1 Design, Build, and Testing Cost Impact 12

Appendix A: Glossary 13

1 Document History

1.1 Revision History

Revision Date	Revision	Summary of Changes
27/12/2019	0.25	Initial version
02/01/2019	0.27	Updated Table 1 with CSP impacts
01/09/2020	0.5	Changed requirements, new PIA document

1.2 Associated Documents

This document is associated with the following documents:

Ref	Title and Originator's Reference	Source	Issue Date
1	MP078-Business-Requirements-v0.4-Updated-2IRPs	SECAS	17/04/2020

References are shown in this format, [1].

1.3 Document Information

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

The Preliminary Impact Assessment was requested of DCC on 30th September 2019. DCC submitted an initial PIA on 31st December, 2019. However the scope of the Modification was changed, and a further requested for a PIA was received on 17th April, 2020.

2 Context and Requirements

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

The requirements have been provided by SECAS, the Proposer, and the Working Group.

2.1 Problem Statement

This SEC Modification handles incorporation of a set of IRPs into the SEC.

2.2 Business Requirements

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.

Req.	Requirement
1	IRP550, 'GCS20r - Response when an error occurs'
2	IRP603, 'Security Log display over HAN'
3	IRP 604, 'Query on IRP550 - Frame Control'

Table 1: Business Requirements for SECMP0078, CR1342

2.2.1 Requirement 1, 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.

These points are fully explained in Annex A of IRP582.

2.2.2 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).
- 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.
- 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 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 position is to amend SMETS (for ESME and GSME) and CHTS (for Comms Hub) to add explicit prohibitions.

2.2.3 Requirement 3, IRP 604, 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, or following the implementation of IRP550.

3 Description of Solution

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	IRP 604, Query on IRP550 - Frame Control	×	×	✓	✓

Table 2: IRP Impacts for Each Service Provider

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

3.1 DSP Solution

3.1.1 IRP550

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.

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.

3.1.2 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 theDSP, as the correction will be done alongside IRP550.

3.2 Critical Software Solution

Changes to Critical Software applications will be required to implement this Modification.

3.2.1 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

3.2.2 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/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.

3.3 Communication Service Provider (CSP) Changes

Design and build activities to support the following will be required for both CSPs:

- Comms Hub; Assessing the impact to the Communication Hub, update and up-issue any new versions of Technical Specifications including CHTS and CHDS
- CHM; Assessing the impact to CHM of changes to CHF Security Log

There will be a requirement for further Zigbee certifications and CPA Certification which is not included in the PIA estimates.

4 Impact on DCC Systems, Processes and People

This section describes the impact of SECMP0078 on DCC Services and Interfaces that impact Users and/or Parties.

4.1 Security Impact

The implementation will be security assured during the implementation phase. This includes reviewing designs, test artefacts and providing consultancy to the implementation and test teams.

There are no material changes to interfaces or the security solution as part of this Modification and therefore a penetration test is not required. There will not be any changes to the DSP protective monitoring solution as result of this Modification.

CSP Security impacts will require assessing the impact to the network and security vulnerabilities.

A more detailed Security impact will be carried out as part of the Full Impact Assessment.

4.2 Request Management

Request Management will need to add support for the revised Device Future Dated Command processing.

4.3 Data Management

Data Management will require updates to support the revised Device Future Dated Command processing.

4.4 Transform

Transform will be updated to parse the Default Response for the GBCS Use Case GCS20r.

4.5 Self Service Interface (SSI)

SSI will need to be updated such that it ignores the SAT Log entries related to the Response received after the final Execution Alert when determining the final status.

4.6 Integration Impact

The functionality will need to be validated in both the Systems Integration Testing (SIT) and User Integration Testing (UIT) environments and will require integration tests that involve both DSP and the CSPs as a minimum. It is assumed that it will be integrated as part of the November 2021 release. An initial estimate of the costs for integration (PIT) testing of the Modification are included in this PIA. The costs exclude release based regression testing in SIT and UIT.

4.7 Infrastructure Impact

There will be no change to the infrastructure design as a result of this change. Additional processing and storage will be required; however, they are not sufficiently large to warrant the procurement of additional compute power or storage as part of this Modification. Note that the aggregated impact of many such changes to the DSP solution will ultimately result in a reduction of the available processing headroom assumed as part of the original DSP agreement. As such, DSP may need to raise a Change Request (CR) for the provision of

additional infrastructure should the DCC Data System experience performance problems that are the direct result of such changes.

The change does not impact the DSP resilience or Disaster Recovery implementation.

4.8 Application Support

No changes to Application Support are expected.

4.9 Service Impact

This change updates behaviour of existing functionality. It is not expected that this will have a material impact on service desk activity, however, the change in behaviour will require updated service desk procedures to document expected new processing patterns. The change will also require knowledge transfer from the implementation team to the service desk team ahead of its release to supported environments. A more thorough assessment of the service impact will be carried out as part of the Full Impact Assessment.

4.10 Safety Impact

No impact is expected, but a full Safety Impact Assessment will be carried out as part of the production of the Full Impact Assessment (FIA).

4.11 Contract Schedules

Schedules will require modification to reflect the changes necessitated under this Modification. Contract schedules will be updated as part of a Contract Amendment Note (CAN) which combines schedule updates from other relevant Modifications.

No impact to any DSP contracts are expected.

The following contract Schedules may require amendment in terms of CSP-driven changes:

- Schedule 1 - Definitions
- Schedule 2.1 – DCC Requirements
- Schedule 4.1 - Contractor Solution
- Schedule 6.1 – Implementation Planning (to reflect any delivery milestones)
- Schedule 7.1 – Charges and Payment
- Schedule 11 – Communication Hub (to reflect an uplift to the CH specifications)

5 Implementation Timescales and Approach

Notwithstanding in which release this change is implemented, based on the currently stated requirements, the elapsed time for DSP implementation will be between 3 and 6 months following the provision of full commercial cover. Communication Service Provider (CSP) implementation will be between 6 – 8 months following the provision of full commercial cover.

The release lifecycle duration will be confirmed as part of the FIA. As currently planned, the standard ongoing major release model will provide drops to the production environment in November 2021.

5.1 Implementation Approach

Implementation of this change is assumed to follow a waterfall methodology. The release lifecycle duration will be confirmed as part of the full impact assessment. The standard ongoing major release model will provide drops to the production environment in June and November each year.

5.2 Testing and Acceptance

It is assumed that the change will be implemented and tested as part of a major release, and will include release based regression testing in SIT and UIT.

CSP North platform test and build changes will be as follows:

- Platform Test; Assessing the testing of CH for the implementation of IRPs
- Platform Build; Assessing impact on Platform Build requirements
- Retest against IRP550

CSP South and Central have identified the following testing tasks:

- Creation of additional PIT test scenarios to cover IRP550 and IRP603
- Regression testing on firmware for all 16 Communication Hub (CH) variants. DCC recommends a review on the number of test variants required for the FIA.
- Deployment and testing of the changes within this CR within Telefónica's PIT environment in accordance with the existing PIT Approach document.
- Deployment of this firmware to the PIT environment.

6 Costs and Charges

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

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

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

6.1 Design, Build, and Testing Cost Impact

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

£	Design, Build and PIT	SP Total
Phase ROM	680,000	680,000

Note a substantial part of both the above cost and the FIA development cost given below are associated with one Service Provider. DCC believe that the quoted cost is not appropriate and will be reviewing the provided figures.

Design	The production of detailed System and Service designs to deliver all new requirements.
Build	The development of the designed Systems and Services to create a solution (e.g. code, systems, or products) that can be tested and implemented. It includes Unit Testing (also referred to as System Testing), Performance Testing and Factory Acceptance Testing by the Service Provider or supplier.
Pre-Integration Testing (PIT)	Each Service Provider tests its own solution to agreed standards in isolation of other Service Providers. This is assured by DCC. This phase also includes regression testing across all Comms Hub products

Based on the existing requirements, the fixed price cost for a Full Impact Assessment is **£118,487** and would be expected to be completed by most of the Service Providers in 30 days. CSP North have requested a period of 50 days.

Appendix A: Glossary

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

.Acronym	Definition
CAD	Consumer Access Device
CAN	Contract Amendment Note
CHF	Communications Hub Function
CHM	Communications Hub Management
CHTS	Communications Hub Technical Specification
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
ESME	Electricity Smart Metering Equipment
FIA	Full Impact Assessment
GBCS	Great Britain Companion Specification
GFI	GBCS Integration Testing For Industry
GSME	Gas Smart Metering Equipment
HAN	Home Area Network
IRP	Issue Resolution Proposal
PIA	Preliminary Impact Assessment
PIT	Pre-Integration Testing
ROM	Rough Order of Magnitude (cost)
RTDS	Reference Test Data Set
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SMETS	Smart Metering Equipment Technical Specification
SMITEn Lite	Smart Metering Integrated Test Environment Lite
SP	Service Provider
SSI	Self Service Interface
TTO	Transition to Operations
UIT	User Integration Testing