

SEC Modification Proposal, MP169

DCC CR5157

Managing SEC Obligations and the Consumers Right to refuse a Smart Meter Full Impact Assessment (FIA)

Version:	1.0
Date:	10th May 2024
Author:	DCC
Classification:	DCC Public

Contents

1	Executive Summary	4
2	Document History	5
2.1	Revision History	5
2.2	Associated Documents	5
2.3	Document Information.....	5
3	Context and Requirements	6
3.1	Problem Statement	6
3.2	Business Requirements	7
4	Description of Solution	9
4.1	DSP Functional and Technical Solution Changes.....	9
4.1.1	Configuration.....	9
4.1.2	SSMI	10
4.1.3	SSI	10
4.1.4	DUIS/DUGIDS	10
4.1.5	Security.....	10
4.1.6	Request Management.....	10
4.1.7	Data Management.....	10
4.1.8	Reporting	10
4.1.9	Logging	10
4.1.10	Other Impacted Components	11
5	Testing Considerations.....	12
5.1	Pre-Integration Testing (PIT).....	12
5.2	Performance Testing	12
5.3	System Integration Testing (SIT)	12
5.4	User Integration Testing (UIT).....	13
6	Implementation Timescales and Releases.....	14
6.1	Change Lead Times and Timelines	14
6.2	SEC Release Allocation and Other Code Impacts	14
6.3	Costs and Charges	15
6.4	Changes to the Contract	15
7	RAID.....	17
	Risks 17	
	Assumptions	17
	Issues 17	

Dependencies.....	17
Appendix A: Glossary	18

1 Executive Summary

The Change Board are asked to approve the following:

- Total cost to implement SECMP0169 of £383,388, which includes Design, Build and Pre-Integration Testing (PIT);
- Post-PIT costs for solution testing in SIT and UIT (apportioned to this SEC Modification as part of a subsequent Release CR, which will also include other Release costs such as regression testing) of £348,114; and
- A timescale to complete implementation of six (6) months.

Problem Statement

MP169 proposes a set of arrangements to cater for consumers who wish to refuse to have a Smart Meter installed, or who have a Smart Meter but wish to prevent their Energy Supplier from collecting consumption data remotely.

Due to the dwindling number of heritage meters in the supply chain, and Energy Suppliers' obligations relating to the installation and operation of Smart Meters, it is generally not an option to install a heritage meter at these consumers' premises.

MP169 will implement a flag in the DSP system to identify where a Smart Meter is to be restricted from operating in a fully smart mode, meaning that Service Requests to retrieve consumption data will be rejected: only Critical, Security and Safety Alerts and Firmware updates will be allowed.

Benefit Summary

The benefits of implementing this Modification will be:

- consistent and clear advice to consumers who wish to refuse a Smart Meter – remote retrieval of consumption data can be prevented;
- clarity for Energy Suppliers when dealing with consumers who wish to refuse a Smart Meter – no need to evaluate each case;
- continuity of arrangements for the consumer following Change of Supplier (CoS) – the flag in the DSP system is not reset automatically on CoS.

2 Document History

2.1 Revision History

Revision Date	Revision	Summary of Changes
10/05/2024	1.0	Issued to SECAS

2.2 Associated Documents

This document is associated with the following documents:

Ref	Title and Originator's Reference	Source	Issue Date
1	MP169 Business Requirements v0.4	SECAS	29/08/2023
2	MP169 Modification Report v0.7	SECAS	14/02/2024

References are shown in this format, [1].

2.3 Document Information

The Proposer for this Modification is Emslie Law from the OVO.

The Full Impact Assessment was requested of DCC on 11 March 2024.

3 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.

3.1 Problem Statement

Suppliers are unable to comply with consumer requests to install a smart meter in 'dumb' mode. The SEC does not allow for the Devices on the Smart Metering Inventory to be either installed and not commissioned (this is a transient state and not an enduring one) or to fit the meters without also fitting the DCC provided Communications Hub (as reference above in Gas and Electricity Supply Licence Condition 54.9). There is no concept, by design, of fitting a smart meter in 'dumb' mode.¹

Suppliers are currently either installing heritage meters or installing the smart meter in ways that are or will cause problems elsewhere.

Some of the factors that will need consideration as part of any solution are:

Additional Issues with non-communicating meters	
Issue for consideration	Details
Any form of Load (Heating / Hot Water / Electric Vehicle)	Any consumer on an Economy 7 tariff (or similar) arrangement relies completely on the Smart Meter communicating.
Change of Mode (Credit to Prepayment and vice versa)	This explicit part of Smart Metering; Prepayment will not work on a meter in dumb mode (or when not communicating)
Eligibility and non-eligibility	Potential Network Managed sites with No Wide Area Network (WAN) and those on specific Radio TeleSwitched regimes must have communications.
'Dumb' meters will need manual reads	It is likely Suppliers will no longer have meter reading agents, especially for a Smart Meter, so may need the customer to provide reads themselves. Smart Meter displays contain more screens and information and the potential for the customer reading the wrong data is therefore increased. There are billing implications Smart is designed to address
DCC / Distribution Network Operator (DNO) flagging the meter as non-communicating	These will be 'invisible' to the DCC. The DNO currently raise these with the Supplier to 'fix'.
Supplier taking on a meter not recorded in the Smart Metering Inventory (SMI) as Smart	May require meters to be replaced and incur Premature Replacement Charges.
Industry standard	A new way to manage these installs must be standardised across the industry so that Change of Supplier (CoS) is not impacted, and the new gaining Supplier is aware of the customer

¹ Elsewhere in this document, such meters are referred to as Smart Meters that are operating in 'restricted' mode.

	preference and situation. There is currently no flag or state to highlight this.
Availability of Heritage Meters	They are no longer being made in some circumstances. Stocks are running low.
Supplier Licence Requirements	Supplier Licence requires the Installing Supplier to configure and maintain a tariff on the system
Security and Safety Alerts.	The Smart Metering Solution is designed for these to be provided and sent out. This is part of the Benefits case and solution in place for DNOs.
Critical Alerts	SEC Parties are required to take action on specific critical or mandated Alerts.

3.2 Business Requirements

Requirement 1: Suppliers will be able to notify the DCC of the consumer's preference for Smart functionality.

At the Working Group meeting in November 2021 the Ofgem representative expressed the view that using Service Reference Variants (SRVs) to notify the DCC could undermine Supplier Licence obligations. The solution was subsequently developed to state that Suppliers should only offer a 'reduction' in Smart functionality once all reasonable steps to install and commission a fully communicative Smart meter have been exhausted. Existing Install and Commissioning processes will be unaffected by the solution; the MP169 solution will simply add an additional, optional step to be taken in the event that a consumer wishes to not have their consumption data retrieved remotely.

Exceptions to this requirement are to be considered through the solution development process. For instance, any consumer on an Economy 7 tariff (or similar) arrangement relies on the Smart meter communicating. Potential Network Managed sites with no Wide Area Network (WAN) and those on specific Radio TeleSwitched regimes must also have communications. In such exceptional cases, where a Smart meter is refused, this needs to be communicated to the customer and the option of reducing communications removed.

Notification of consumer preference should only be sent after the Smart Meter and Communications Hub have been installed and commissioned. It should also be possible to send them if there is a Change of Tenancy (CoT) and the incoming tenant has different preferences to the outgoing tenant.

The DCC will need to amend its reporting on Supplier obligations to install Smart meters to allow for the scenario where a Supplier has installed and commissioned a SMETS2+ Device which subsequently has reduced communications due to consumer preference.

Requirement 2: A DCC System flag will be created to indicate if communications with a Device have been reduced due to consumer choice.

The presence of a flag in the DCC System would prevent consumer preference being lost in a Change of Supplier (CoS). It will also prevent the new Supplier from wasting time and resource investigating the reason for lack of communication.

This flag could be held in the DCC System and its presence have the function of suppressing certain Smart functionality. It could also be held outside of the DCC System, for instance in

the Priority Service Register. During solution development it was agreed that the most effective option would be for the flag to be applied within the DSP System at Device level.

Requirement 3: The responsible Supplier will be able to request the addition and removal of the DCC System flag, subject to its adherence with all reasonable steps for Smart installations.

Suppliers are able to appoint Other SEC Parties to collect consumption data on their behalf or to offer data services to consumers. While this Modification will not impact these commercial arrangements, it must be ensured that consumers' data privacy is not undermined by allowing Other SEC Parties to remove the DCC System flag. It is therefore a requirement that only the responsible Supplier can request the addition or removal of the DCC System flag, and its addition can only be requested once the Supplier has completed all reasonable steps to install the Device in a fully communicative state.

Requirement 4: Critical, Security and Safety Alerts and Firmware updates will still be sent when communication with a Device has been reduced due to consumer choice.

The Smart Metering solution is designed for Security and Safety Alerts to be provided and sent out. This is part of the benefits case and solution in place for Distribution Network Operators (DNOs). Smart Energy Code (SEC) Parties are also required to act on specific critical or mandated Alerts. Which Alerts require exceptions and the mechanism for allowing them to be sent will be agreed during the solution development process.

Critical Alerts, such as those relating to Certificate updates, are necessary to ensure the security of the DCC System. Firmware updates will also still need to be possible to prevent issues with Device firmware version compatibility, which may result in the need to replace otherwise healthy Devices.

During solution development, it was agreed that the only messages which should be prevented from sending are those which relate directly to the consumer's consumption.

Requirement 5: The DCC to amend any reporting for which the success/failure of Service Requests relating to energy consumption is a metric to allow for exceptions where communications have been reduced due to consumer choice.

A full list of the affected reporting will be investigated as part of the DCC's Preliminary Assessment and developed during the Refinement Process. This requirement will need to consider whether the reporting in question requires exceptions for specific Service Requests, related business processes or for the Devices themselves.

4 Description of Solution

The solution for this Modification will introduce the following functionality:

A new 'Restricted' attribute (True/False) will be added to the data held for each device in the Smart Metering Inventory. By default the 'Restricted' attribute will be False for all existing devices at the point this change is applied and will be False for any new devices subsequently added to the Inventory.

A new screen will be provided on the Self-Service Management Interface (SSMI) to allow DCC, when instructed by the Responsible Supplier, to set (or clear) the 'Restricted' attribute for a device.

The value of the 'Restricted' attribute will be displayed on the SSI Read Inventory screen and included in the response to SRV8.2 Read Inventory requests. It will also be included in Device Extracts delivered to the DCC via the Enterprise Systems Interface.

When processing Service Requests there will be a check to determine whether the 'Restricted' attribute is set to True for that device (referred to hereafter as the device being in 'Restricted' mode).

If the device is in 'Restricted' mode then only a specific set of Service Reference Variants (SRVs) shall be allowed to be sent to the device. The list of allowed SRVs shall be a configurable item, agreed with the DCC and subject to an appropriate governance process.

The DCC User Interface Specification (DUIS) interface will be amended to return a new Error Response Code when an SRV is rejected due to the device being in Restricted mode. There will also be a new Warning Response Code returned when a Supplier executes an SR6.23 Change of Supplier request and becomes responsible for a device that is in 'Restricted' mode.

Similar to SRVs, if the device is in 'Restricted' mode then only a specific set of Alerts shall be allowed to be forwarded from the device to the relevant Service User. The list of allowed Alerts shall be a configurable item, agreed with the DCC and subject to an appropriate governance process.

Any Alerts not delivered due to the device being in 'Restricted' mode will not be recorded in the SAT log, but will be recorded in a new Discarded Alert log for triage and diagnostic purposes.

This Change will require a DUIS uplift, a change to the DUIS schema, and a change to DCC User Gateway Interface Design Specification (DUGIDS).

Change under this Modification will form part of a SEC System Release; DCC has provided, alongside the FIA price to PIT Complete, a price including post-PIT, in line with responses to other Modifications.

4.1 DSP Functional and Technical Solution Changes

The solution for this Modification requires changes to the following components:

4.1.1 Configuration

- a list of SRVs allowed to be sent to devices in Restricted mode; and
- a list of Device Alerts allowed to be delivered from devices in Restricted mode.

4.1.2 SSMI

- amended to allow maintenance of Restricted attribute.

4.1.3 SSI

- display 'Restricted' attribute for the following device types: ESME, GSME, GPF

4.1.4 DUIS/DUGIDS

- new generic E72 Response Code for rejection of SRV because device is in 'Restricted' mode and SRV is therefore not allowed;
- new W062301 code for successful submission of SRV 6.23 (Change of Supplier) where device is in 'Restricted' mode; and
- new 'Restricted' attribute added to SRV 8.2 (Read Inventory) response.

The proposed changes to DUIS are included in the extracts below.



DUIS Legal Text
changes for SECMP01

4.1.5 Security

- extend Authorisation component to include a check for 'Restricted' mode and if device is restricted then check if the SRV of a message is in 'allowed' list; and
- extend Device Alert authorisation to check for 'Restricted' mode and if device is restricted then check Alert Code is in 'allowed' list.

4.1.6 Request Management

- where Authorisation responds that a Service Request is not allowed because device is restricted then respond with new DUIS error code; and
- call northbound authorisation for Device Alerts; where not allowed then write to Discarded Alert log and discard the Alert.

4.1.7 Data Management

- add 'Restricted' attribute to logical and physical data models;
- new API (called by SSMI) to maintain restricted attribute for devices, including maintenance of the attribute in the motorway cache;
- change to GPF device log transfer post processing to copy Restricted attribute; and
- include 'Restricted' attribute in device object (getDevice and read Inventory).

4.1.8 Reporting

- device extract to include 'Restricted' attribute (subject to "Restricted mode reporting" feature being enabled).

4.1.9 Logging

- a new Discarded Alert log. Note that the Discarded Alert log is not provided externally.

4.1.10 Other Impacted Components

There will be no impacts to:

- Performance
- Infrastructure
- Disaster Recovery

5 Testing Considerations

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

5.1 Pre-Integration Testing (PIT)

The consumer can use SMETS2 meters in a restricted manner if they choose not to have a Smart Meter. The concept of 'Restricted mode' attribute to applicable device types is introduced as part of this change.

The DSP PIT Test team will verify new use cases in SSMI to Set/Clear restricted mode for applicable devices when the 'Restricted' attribute feature switch is ON. The PIT Test Team will also validate the SSI inventory displays Restricted mode.

The PIT Test Team will also run set of tests to test the following:

- only supported SRVs and Device Alerts are processed;
- unsupported SRVs are rejected, and Device Alerts are not delivered; and
- ESI report will also be tested to confirm new field is displayed when Restricted reporting feature switches is ON.

A series of regression tests will also be run. Automated testing will be used where possible.

5.2 Performance Testing

These changes are not anticipated to have a performance impact, therefore no performance assurance activities have been included in this FIA.

5.3 System Integration Testing (SIT)

The full scope of Solution Testing for this Modification will consist only of SIT functional testing, executed in the SIT-B environment and baseline uplift testing, executed in SIT-A. CR5157 is to be delivered in alignment with a SEC System Release (expected to be June 2025). In accordance with all previous SEC releases, a separate Release CR or PR will provide cover for release level testing, e.g. Functional Regression, End of Cycle (EOC) and System Regression testing.

Testing will be executed on SMETS2 device sets only. This change does not apply for SMETS1.

The scope of testing this Modification comprises:

- verifying that devices can be flagged as 'Restricted' or 'Not Restricted' via SSMI;
- checking that an SSI user is able to view the 'Restricted' attribute against a device;
- swapping devices between 'Restricted' / 'Not Restricted' state;
- verifying the SRV 8.2 response returns the new 'Restricted' attribute;
- verifying the Device Extract ESI Report includes the new Restricted attribute;
- testing that if a Comms Hub is replaced, the 'Restricted' attribute mode remains the same on the new GPF;
- ensuring Device Alerts that are unsupported for 'Restricted' mode are rejected and written to the Restricted Alert Log;
- processing the supported SRVs for devices in 'Restricted' mode;

- processing unsupported SRVs to verify an error is returned to the Service User; and
- ensuring that Service Audit Trail is updated with validation errors when an SRV is rejected due to a 'Restricted' device as the target.

5.4 User Integration Testing (UIT)

The UIT Projects team will conduct testing to confirm that the functionality for SMETS2 devices operating in 'Restricted mode' are working as expected in each UIT test environment.

The Pre-UTS test execution scope for this Modification will cover running the following testing on two SMETS2 meter sets, with one meter set for each of the CSPs. All SRVs tested will use the updated DUIS version (schema version 5.4 to be implemented under the SEC System Release expected to be in June 2025) associated with the change.

The UIT testing for each meter set will comprise:

- Customer Journey 1 - Install and Commission the meter set;
- a selected sample of SRV testing to prove that the sending of relevant SRVs is not 'Restricted';
- update devices to 'Restricted' via SSML;
- a selected sample of SRV testing to validate that the device behaviour is now being treated as 'Restricted';
- for SRV 6.23 (CoS), check for a W062301 response;
- Over-the-Air (OTA) firmware updates to the 'Restricted' ESME and GSME to check the upgrades are successful;
- check Alerts from devices which are Restricted are limited as specified;
- check rejected Alerts are recorded in a new log (not the SAT log)
- update devices to not be 'Restricted' via SSML;
- re-run a selected sample of SRVs to validate that the device behaviour is no longer being treated as 'Restricted'; and
- decommission the meter set.

The above testing will be conducted in both the UIT-A and UIT-B test environments and will be undertaken by the UIT Projects team.

6 Implementation Timescales and Releases

This Modification is expected to be included in a SEC Release in June 2025. Implementation timescales will be finalised as part of the relevant SEC Release.

6.1 Change Lead Times and Timelines

From the date of approval (in accordance with Section D9 of the SEC), to implement Design, Build and PIT requires a lead time of approximately **six months**.

This Modification would be scheduled alongside other Modifications and CRs, and there might be a period of no activity for this Modification.

6.2 SEC Release Allocation and Other Code Impacts

This Modification is expected to be implemented as part of the June 2024 SEC Release, however the allocation to a release may be dependent on other Modification timings and the suitability of a release. No functionality overlap with other Modifications has been identified at the time of undertaking this FIA.

6.3 Costs and Charges

This section indicates the quote for all phases of application development stage for this Modification. Note these costs assume a release of just this SEC Modification without any other Modifications or Change Requests in the release, which is not truly reflective of what the post-PIT test costs or programme duration will look like. A calculation of those costs will be carried out when the contents of the future Release are finalised, and the post-PIT costs determined through a "Release CR" also referred to as a "Post-PIT CR".

£	Design, Build, PIT, including DUIS uplift	Integration Testing, SIT and UIT	Total
SECMP0169	£383,388	£348,114	£731,502

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.
Pre-Integration Testing (PIT)	Each Service Provider tests their 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 for a Release 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.

6.4 Changes to the Contract

The DSP contract updates will be detailed within the CAN and will impact the following schedules:

- Schedule 2.1 (DCC Requirements): addition of new requirements for this change
- Schedule 3 (DCC Responsibilities): addition of new DCC Responsibilities to enable achievement of the activities and / or deliverables under this Change
- Schedule 4.1 (Contractor Solution): solution design documents
- Schedule 6.1 (Implementation Planning): addition of new milestones
- Schedule 7.1 (Charges and Payment): revisions to incorporate charges and payment

7 RAID

The risks, assumptions, issues and dependencies below are applicable to both solution options.

Risks

Ref.	Risk Description	Status
MP169-R-001	There is a risk that customers who opt out of smart metering functionality will attempt to block any signals into the CHs which will result in key updates such as firmware updates not occurring. This represents a security risk as the meters and CHs require latest firmware updates to address any security limitations. Firmware versions on 'Restricted' devices should be monitored so that this can be addressed with the customer should there be persistent failures in firmware updates.	Open

Assumptions

Ref.	Description	Status
MP169-A-002	It is assumed that this will form part of the June 2025 release.	Open
MP169-A-003	It is assumed that there is no requirement for DCC to suppress the transmission of messages inbound via the SMWAN from 'Restricted' Devices. The controls applied to 'Restricted' Devices will be solely in the form of rejection of specific Service Reference Variants and discarding of specific Device Alerts by DSP.	Open
MP169-A-004	There is no workflow for the changing of the 'Restricted' attribute. A suitable authorised DCC user can change the flag for a device.	Open
MP169-A-005	Setting devices as 'Restricted' will be done on a one-by-one basis. There is no bulk update mechanism.	Open

Issues

None identified at this time.

Dependencies

None identified at this time.

Appendix A: Glossary

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

Acronym	Definition
BAU, BaU	Business As Usual
CPL	Central Products List
CSP	Communication Service Provider
CSV	Comma Separated Variable
DCC	Data Communications Company
DNO	Distribution Network Operator
DSP	Data Service Provider
DUGIDS	DCC User Gateway Interface Design Specification
DUIS	DCC User Interface Specification
ESME	Electricity Smart Metering Equipment
FIA	Full Impact Assessment
FTE	Full Time Employees
GBCS	Great Britain Companion Specification
GSME	Gas Smart Metering Equipment
I&C	Installation and Configuration
IHD	In Home Display
KPI	Key Performance Indicators
MVP	Minimum Viable Product
OMR	Operational Metrics Review
PIA	Preliminary Impact Assessment
PIT	Pre-Integration Testing
PMR	Performance Measurement Report
PPMID	Payment Meter Interface Device
ROM	Rough Order of Magnitude (cost)
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SLA	Service Level Agreement
SMETS	Smart Metering Equipment Technical Specification
SMS	Smart Metering System
SRV	Service Request Variant
SVP	Speed, Volume, Payload
S1SP	SMETS1 Service Provider
TOC	Technical Operations Centre
UIT	User Integration Testing