MP203

'Security Assurance of Device Triage Facilities'

Modification Report

Version 1.0

10 October 2022

Corporate member of
Plain English Campaign
Committed to clearer
communication

592

MP203 Modification Report

Managed by
Gemserv

Page 1 of 12

This document has a Classification
of **White**

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

This document also has two annexes:

- **Annex A** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.

- **Annex B** contains the full responses received to the Refinement Consultation.

Contact

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

Mike Fenn

020 3314 1142

mike.fenn@gemserv.com

Gemserv

This document has a Classification of White

1. Summary

This proposal has been raised by Gordon Hextall on behalf of the Security Sub-Committee (SSC).

The Commercial Product Assurance (CPA) Security Characteristics (SCs) for Use Case 004 (Factory Reset) have recently been agreed and published on the National Cyber Security Centre (NCSC) website which will allow the triage and refurbishment of Devices in line with relevant use cases.

The SEC does not currently take account of the need for regulatory assurance of Triage Facilities, Triage Tools and Triage Interfaces to provide security assurance across the end-to-end smart metering system. Whilst most Meter Asset Providers (MAPs) are SEC Parties, it is not a requirement for them to be. Therefore, Triage Facilities could be operated by non-SEC Parties, such as MAPs or their contracted agents. However, there is currently no way for SEC Parties to be assured that those Facilities comply with the necessary controls to ensure the security of Devices to be installed or reinstalled in consumer premises.

The Proposed Solution will be to specify the exact requirements of all Triage Facilities and to detail the assurance activities that are needed for the SSC to approve them for use.

This modification will impact SEC Parties that wish to operate Triage Facilities. The costs to implement the modification are limited to Smart Energy Code Secretariat and Administrator (SECAS) time and effort to update the SEC. However, each SEC Party that wishes to operate a Triage Facility will incur the costs of undertaking the assurance process. The cost of the initial Full Security Assessment (FUSA) is unlikely to exceed £10,000, with subsequent assessments being a lower cost.

This modification is targeted for the November 2022 SEC Release and this will be a Self-Governance Modification.

2. Issue

What are the current arrangements?

Device triage and refurbishment

The SEC requires the SSC to work with the NCSC to develop and maintain CPA SCs for the end-to-end Smart Metering System. Ensuring compliance with these SCs helps to provide confidence to all SEC Parties that the Devices are appropriately secure, and CPA Certification is needed before a Device can be put onto the Central Products List (CPL).

Historically, these SCs have not supported Device triage and refurbishment. Therefore, once installed or partially installed, Devices were not able to be re-installed on the Data Communications Company (DCC) network, even if they were removed without defect.

Suppliers and MAPs have provided a business justification to the SSC and have proposed a series of use cases for Device triage and refurbishment. Use Cases 001 – 004 have all been agreed and approved, and there is scope for more use cases to be raised, such as triage and refurbishment of Communications Hubs which will provide an efficient solution to SECMP0010 'Introduction of triage arrangements for Communication Hubs'.

Security Characteristics update – April 2022

Previously, the NCSC, the Department for Business, Energy and Industrial Strategy (BEIS) and the SSC have confirmed that they were open to considering compelling use cases from industry that protect security controls whilst facilitating the triage and refurbishment of Devices.

In the June 2022 SEC Release, MP195 'Security Sub-Committee guidance on Device Assurance' was implemented, which placed an obligation on the SSC to develop and maintain guidance documents that cover these use cases.

There has been a period of uncertainty about the security arrangements to allow Device Triage under Use Case 004 (Factory Reset) without adversely impacting existing CPA SCs. However, the CPA SCs for have now been agreed and published on the NCSC website which will allow the triage and refurbishment of Devices that are the subject of Use Case 004.

Security Assurance

Use Cases 001 (HAN Reset via a Port), 002 (Identifying Installed SMKI Certs) and 003 (HAN Reset via the Device User Interface) do not need any regulatory assurance of the security arrangements. However, Use Case 004 (Factory Reset) involves processes that could pose a security risk if not carried out in line with certain SEC Section G security controls. This therefore requires independent assurance of the Triage Facilities, Triage Tools and Triage Interfaces.

The SSC has been considering the nature and details of triage assurance arrangements for these and the User Competent Independent Organisation (CIO) has worked with the SSC to agree proposals. These have also been shared with the SSC CPA Issue Resolution Sub-group (SCIRS). The SSC noted that Triage Facilities operated by Suppliers can be accommodated under SEC security obligations. However, Triage Facilities could be operated by other parties, such as MAPs or other Agents, that are not required to be SEC Parties.

What is the issue?

The SEC does not currently take account of the need for regulatory assurance of Triage Facilities, Triage Tools and Triage Interfaces to provide security assurance across the end-to-end smart metering system.

The SSC has noted that manufacturers' development facilities are covered by the CPA Build Standard and it may be possible to include Triage Facilities operated by Suppliers under the User Security Assessments conducted by the User CIO, which are covered under SEC Section G8 'User Security Assurance'. However, Triage Facilities could be operated by other parties (MAPs or other Agents) that are not required to be SEC Parties. Therefore, unless changes are made to the SEC, there will be no means of ensuring that remediation of any non-compliances arising from Triage Facilities operated other than by Suppliers can be enforced within the SEC.

Additionally, there may be more use cases in the future, such as Communications Hub refurbishment, that would also require similar assurance arrangements.

What is the impact this is having?

Without the necessary assurance, there is an inconsistency of security obligations, a potential for avoidable security vulnerabilities and a risk of uncertainty for continued CPA Certification.

There has been uncertainty relating to the CPA arrangements for Devices containing Use Case 004 functionality that is being resolved by the agreement of CPA Triage SCs. Suppliers and Device Manufacturers may now submit Devices for CPA evaluation. However, MAPs and other organisations need certainty about the assurance arrangements required for Triage Facilities, Triage Tools and Triage Interfaces as soon as possible to avoid unnecessary write-off of otherwise functional Devices.

Impact on consumers

Without the necessary assurance in place, there is an increased risk of scrapping re-usable devices resulting in costs which could be avoided.

3. Solution

The SSC considers that the greatest clarity will be provided by a new section under Section G 'Security' that will cover off the requirements for Triage Facilities. This will refer to the existing clauses within Section G that apply to Triage Facilities, as well as new additional clauses that are specific to Triage Activities.

The User CIO has produced analysis for the SSC of which sections of SEC Section G are applicable to Triage Facilities. The SSC intends to adopt this into the equivalent of the Security Controls Framework that will be Part 3 of the SSC Guidance on Device Security Assurance and Triage. That document will list the obligations that do and do not apply and what the User CIO will look for by way of evidence that the obligation is being met.

Parties that wish to operate Triage Facilities will be subject to an initial FUSA to determine whether that Facility can operate Triage Activities. These Assessment will either result in 'approval', 'rejection' or 'approval subject to additional steps'.

If approved, then the SSC will determine the category of all follow up assessments based on an assessment of the security risks. Follow up assessments will be either another FUSA, a Verification User Security Assessment or a User Security Self-Assessment.

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

Managed by

Gemserv

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

This modification will impact any party that wishes to become a Triage Facility Provider and operate a Triage Facility. It does not apply to Device Manufacturers that undertake Triage Activities at their own development workshop.

Device Manufacturers are not directly impacted. This modification does require Device Manufacturers to provide a Triage Tool and Triage System Interface to the Triage Facility but assurance of these components will be covered under the CPA Build Standard.

The DCC is not impacted by this modification currently; however, these assurance activities will be required should a use case for triaging Communications Hubs be approved. This is currently progressing under SECMP0010 'Introduction of triage arrangements for Communication Hubs'.

Suppliers and MAPs will be positively impacted by being able to have Devices triaged and available for re-use.

DCC System

There are no DCC system impacts from this modification.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section G 'Security'

The changes to the SEC required to deliver the proposed solution can be found in Annex A.

Technical specification versions

This modification does not impact the Technical Specifications.

Devices

Devices impacted			
✓	Electricity Smart Metering Equipment	✓	Gas Smart Metering Equipment
	Communications Hubs		Gas Proxy Functions
	In-Home Displays		Prepayment Meter Interface Devices
	Standalone Auxiliary Proportional Controllers		Home Area Network Connected Auxiliary Load Control Switches
	Consumer Access Devices		Alternative Home Area Network Devices

There will be no impacts to Device behaviour from this modification. However, Devices will need to have the appropriate functionality to support this activity in line with Use Case 004 and any additional Use Cases which may be introduced in future.

Consumers

Consumers will not be directly affected by the modification. However, this modification would indirectly impact Suppliers and MAPs who could re-use Devices once triaged and refurbished which should lead to lower costs that would otherwise be passed onto consumers.

Other industry Codes

This modification will not have an impact on any other Industry Codes.

Greenhouse gas emissions

There will be no direct impact on greenhouse gas emissions from this modification. However, this would lead to a reduction in Devices being scrapped and a positive impact.

5. Costs

DCC costs

There are no DCC costs associated with this modification.

SECAS costs

The estimated SECAS implementation cost to implement this as a stand-alone modification is one day of effort, amounting to approximately £600. This cost will be reassessed when combining this modification in a scheduled SEC Release. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.
- Additional administration effort to arrange and process the assessments.

SEC Party costs

This modification assures the requirements that the SSC has developed to operate Triage Facilities. Parties will incur costs from developing the Triage Facility and going through the assurance process. Respondents to the Refinement Consultation noted that their costs would depend on whether they subcontracted out triage activities or provided the service themselves. Respondents did not envisage high costs in either scenario The SSC is mindful of the need for proportionality to avoid negating the business case for refurbishment. The costs of the initial FUSA is unlikely to exceed £10,000, with subsequent assessments being a lower cost.

6. Implementation approach

Recommended implementation approach

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

- **3 November 2022** (November 2022 SEC Release) if a decision to approve is received on or before 26 October 2022; or

- **10 Working Days following approval** (ad-hoc SEC Release) if a decision to approve is received after 26 October 2022.

The Assurance activities are needed in advance of SEC Parties being able to operate Triage Facilities. SEC Parties have advised that this needs to be implemented as soon as possible as the numbers of Devices that are awaiting triage for re-use is growing daily.

Should a decision not be reached in time for the November 2022 SEC Release then SECAS is recommending an ad-hoc SEC Release ten Working Days after the Change Board decision. This approach was supported by respondents to the Refinement Consultation. Only one respondent objected on the basis it could impact their other triage activities. SECAS notes this modification should not impact current triage processes.

7. Assessment of the proposal

Observations on the issue

The SSC noted that these assurance activities are required before any Triage Facility can undertake Triage Activities. The User CIO has produced a report for SSC detailing what activities are covered under the existing provisions and what requirements are missing from the SEC that need to be captured.

Solution development

Futureproofing

SECAS noted under the current guidance, Use Case 004 (Factory Reset) is predominantly aimed at Electricity Smart Metering Equipment (ESMEs) and Gas Smart Metering Equipment (GSMEs) and there is a need to futureproof these requirements for other use cases that would need the same assurance. SECMP0010 'Introduction of triage arrangements for Communication Hubs' aims to introduce a further use case to manage the triage of Communications Hubs and the Proposed Solution has been developed so that would also follow the same assurances that are required under this modification.

Should triage be attempted if the tamper-protection boundary has been breached?

The SSC has worked together with the NCSC, BEIS and SCIRS to develop the specific requirements for the Proposed Solution. During the development of the requirements at the SCIRS, a MAP noted that triage shouldn't be undertaken on a Device that arrives at the Triage Facility with the tamper

boundary already breached. However, SSC Supplier members countered that it is sometimes necessary to breach the outer tamper boundary during installation and maybe the restriction should be on breaching any internal tamper seals.

The Working Group discussed this issue and noted that there was ambiguity around tamper protection. One member noted they can sometimes receive tamper Alerts when a battery is replaced, and this fault should not exclude that Device from eligibility for triage. Another Working Group member suggested referencing the CPA Security Characteristics within the legal text as each manufacturer may have applied the standard differently and therefore it would be very complex to have a clear definition otherwise.

Feedback from the Refinement Consultation noted a variety of acceptable instances where the tamper protection boundary may have been breached in a legitimate scenario. The Proposer is satisfied that the revised legal text incorporates these scenarios.

Do the new proposed clauses add enough clarity for Parties?

The User Assessment processes are already set out within SEC Section G8. The new clauses were originally drafted only referencing the earlier section of SEC Section G8 that applied. However, respondents to the Refinement Consultation noted that further detail should be provided within the new clauses. SECAS has discussed this with the Proposer and the SEC Lawyer. It was determined that referencing the sections as done in proposed new SEC Section G12.4(i) was sufficient and prevents duplication within the SEC. The new clauses have been updated to include the specification that the User Assessments will be conducted on an annual basis.

Will this modification impact existing Triage arrangements?

This modification aims to provide assessments for Triage Facility Providers (parties such as MAPs, MOPs and MAMs) who wish to undertake triage under Use Case 004 (Factory Reset). It is not intended to impact existing triage arrangements under Use Cases 001, 002 or 003 that have already been agreed and approved.

Will there be guidance for Parties that wish to operate Triage Facilities?

The SSC has developed a Triage Security Controls Framework. This will form part of the 'SSC Guidance on Device Security Assurance and Triage' which was introduced as a SEC required document through MP195 'Security Sub-Committee guidance on Device Assurance'. This will detail the exact clauses that will apply and provide examples of how Triage Facility Providers should comply with them.

8.   Case for change

Business case

The modification provides assurance for Triage Activities and is a requirement before a Triage Facility can operate. It can be delivered into the SEC as a legal text change and therefore the costs are

limited to SECAS implementation. SEC Parties that wish to operate a Triage Facility will incur the costs of developing their own Triage Facility and to cover the costs of the assurance assessment by the User CIO. These are expected to be in the region of £10,000 per FUSA.

MAPs and Device Manufacturers have indicated support for the modification and are keen to find a solution to the ever-growing numbers of off-the-wall Devices that have been installed, removed and no fault identified. Refinement Consultation respondents noted this modification would be beneficial to the environment by not necessitating the replacement and scrapping of Devices. They also noted it could potentially lead to lower operating costs for the supplier through reduction in stock purchasing requirements and reduced scrappage. This in turn could have an impact on consumer bills.

Views against the General SEC Objectives

Proposer's views

The Proposer believes the modification better facilitates SEC Objectives (a)[1] and (f)[2] as it would enable SEC Parties to better develop processes and functionality that align with the security principles, as well as re-use of existing Devices.

Industry views

Respondents to the Refinement Consultation agreed that the modification would better facilitate SEC Objectives (a) and (f) for the reasons stated above.

Views against the consumer areas

Improved safety and reliability

This change is neutral against this area.

Lower bills than would otherwise be the case

Indirectly this change would provide a benefit in this area as SEC Parties would have more confidence in designing processes and functionality to refurbish Devices. This would result in lower costs which could be passed onto consumers. This view was supported by some respondents to the Refinement Consultation.

Reduced environmental damage

Indirectly this change would provide a benefit in this area as SEC Parties would have more confidence in designing processes and functionality that would result in Devices being reused and not scrapped. A respondent to the Refinement Consultation agreed with this and believed the impacts are undersold within the Modification Report.

---

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

[2] to ensure the protection of Data and the security of Data and Systems in the operation of this Code

Improved quality of service

This change is neutral in this area.

Benefits for society as a whole

This change is neutral in this area.

Final conclusions

Respondents to the Refinement Consultation all supported the implementation of this modification and believed it resolved the identified issue. Respondents support an expedited implementation plan to ensure the Assessments can be conducted as soon as possible. The SSC is keen to support the re-use of assets and would like this modification implemented as soon as possible.

The SSC is developing further guidance, the Triage Security Controls Framework, which will be added to the 'SSC Guidance for Device Security Assurance and Triage'. This has been developed and shared with the members of SSC and SCIRS and will be implemented outside of this modification once comments received have been incorporated.

Appendix 1: Progression timetable

The final Modification Report will be presented to the CSC ex-Committee for approval by 7 October 2022. If approved, a five Working Day Modification Report Consultation will be issued, to enable the Change Board vote to be held on 26 October 2022 under Self-Governance.

Timetable	
Event/Action	**Date**
Draft Proposal raised	10 May 2022
Presented to CSC for comment and conversion to Modification Proposal	17 May 2022
SSC develop the Proposed Solution	May 2022 – Jul 2022
Modification discussed with Working Group	7 Sep 2022
Refinement Consultation	8 Sep 2022 – 28 Sep 2022
Modification Report approved by CSC (ex-committee)	7 Oct 2022
Modification Report Consultation	10 Oct 2022 – 17 Oct 2022
Change Board Vote	*26 Oct 2022*

Italics denote planned events that could be subject to change

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 for Business, Energy and Industrial Strategy
CIO	Competent Independent Organisation
CPA	Commercial Product Assurance
CPL	Central Products List
CSC	Change Sub-Committee
DCC	Data Communications Company
ESME	Electricity Smart Metering Equipment
FUSA	Full User Security Assessment
GSME	Gas Smart Metering Equipment
HAN	Home Area Network
MAM	Meter Asset Manager
MAP	Meter Asset Providers
MOP	Meter Operator
NCSC	National Cyber Security Centre
OPSG	Operations Group
SC	Security Characteristics
SCIRS	SSC CPA Issue Resolution Sub-group
SEC	Smart Energy Code
SECAS	The Smart Energy Code Administrator and Secretariat
SMKI	Smart Metering Key Infrastructure
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee