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.

MP203

'Security Assurance of Device Triage Facilities'

Modification Report

Version 0.3

8 September 2022

Corporate member of Plain English Campaign
Committed to clearer communication
592

Managed by Gemserv

About this document

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

Contents

This document also has one annex:

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

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 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 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 the Smart Energy Code Secretariat and Administrator (SECAS) time and effort. However, each SEC Party that wishes to operate a Triage Facility will incur the costs of undertaking the assurance process. The costs of the initial Full Security Assessment (FUSA) is unlikely to exceed £10k 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' will be implemented which will place 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 and 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 who are not obligated to be SEC Parties 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. Manufacturers may now submit Devices for CPA evaluation. However, Suppliers and MAPs 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 avoidable security vulnerabilities being found in Devices at consumer premises. There is also the potential for increased costs if some Parties are unable to reuse the Devices in their stores as there is no assurance over their processes.

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 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

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

This modification will impact any SEC Party that wishes to operate a Triage Facility. Device manufacturers are impacted as they will be involved in the triage of any of their Devices at a Triage Facility.

The DCC are 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'.

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 be able to be triaged in line with Use Case 004 (Factory Reset) should Parties wish to do so.

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, indirectly 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 have developed to operate Triage Facilities. Parties will incur costs from developing the Triage Facility and going through the assurance process. Further details will be sought from SEC Parties via the Refinement Consultation. The SSC is mindful of the need for proportionality to avoid negating the business case for refurbishment and the costs of the initial FUSA is unlikely to exceed £10k with subsequent assessments being a lower cost.

6. Implementation approach

Recommended implementation approach

SECAS is recommending 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 10 working days after the Change Board decision.

7. Assessment of the proposal

Areas for assessment

Sub-Committee input

As part of the modification assessment, SECAS has engaged with the Chairs from the Operations Group (OPSG), the Technical Architecture and Business Architecture Sub-Committee (TABASC), the SSC and the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) to confirm what input is required from these forums.

SECAS believes the following Sub-Committees will need to input to this modification:

Sub-Committee input	
Sub-Committee	**Input sought**
OPSG	None
SMKI PMA	None
SSC	Input on legal text and Proposed Solution
TABASC	None

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 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.

Views on this element will be sought in the Refinement Consultation.

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 also incur 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 £10k 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 Devices that have been installed, removed and no fault identified.

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

This will be updated following the Refinement Consultation.

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.

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.

Improved quality of service

This change is neutral in this area.

Benefits for society as a whole

This change is neutral in this area.

[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

Appendix 1: Progression timetable

This modification will be discussed with the September Working Group before being issued for Refinement Consultation.

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 – Jul 2022
Modification discussed with Working Group	7 Sep 2022
Refinement Consultation	8 – 28 Sep 2022
Modification Report approved by CSC (ex-committee)	*Early Oct 2022*
Modification Report Consultation	*10 – 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
MAP	Meter Asset Providers
NCSC	National Cyber Security Centre
OPSG	Operations Group
SC	Security Characteristics
SCIRS	SSC CPA Issue Resolution Sub-group
SEC	Smart Energy Code

Glossary	
Acronym	**Full term**
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

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.

MP203 ‘Security Assurance of Device Triage Facilities’

Annex A

Legal text – version 0.3

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

Section G 'Security'

These changes have been redlined against Section G version 16.0.

Add Section G12 as follows:

G12 Security Assurance of Device Triage Facilities

G12.1 Some of the expressions used in this Section G12 are defined in Section G12.9

G12.2 Where the SSC Guidance for Device Security Assurance and Triage specifies that independent assurance of Triage Facility Providers is required to achieve appropriate levels of security assurance in accordance with the requirements of this Code, this Section G12 shall apply.

Triage Facility Provider Obligations

G12.3 In order to become a Triage Facility Provider, an entity must either be an existing Party or accede to this Code and become a Party. A Triage Service Provider is not required to be a User.

G12.4 Each Triage Facility Provider shall:

(a) not attempt to undertake Triage Activities on any Device where the tamper-protection boundary required by the CPA Security Characteristics has already been breached before reaching the Triage Facility (taking into account any allowable breaches necessary as part of essential Device maintenance and/or the de-commissioning process);

(b) only use the Triage Tool and Triage Interface provided by a Device's Manufacturer to access the Manufacturer's Triage System and not use any other electronic devices, interfaces or IT systems for carrying out Triage Activities;

(c) ensure multi-factor authentication and role-based access controls are used within its Triage Facility to control access to the graphical user interface (GUI) of the Triage Tool, and to control access to the Triage Interface;

(d) at all times prevent unauthorised use of the Triage Tool and Triage Interface, and ensure the physical security of the Triage Tool and any Devices that are subject to Triage Activities;

(e) ensure that all the required tamper-protection seals are fitted to Devices on completing the Triage Activities;

(f) maintain an asset management system to record Triage Activities undertaken at the Triage Provider's Triage Facility, including details of:

(i) the Requestor of any change to the configuration of a Device;
(ii) the Device Model and serial number of each Device where the tamper-protection boundary is breached in order to undertake (or attempt to undertake) Triage Activities;
(iii) details of Triage Activities successfully undertaken;
(iv) details of any failed attempts to complete Triage Activities; and
(v) confirmation that any seals and tamper-protection required by the CPA Security Characteristics have been applied before returning a Device to a Requestor;

(g) when requested by the Security Sub-Committee, provide the Security Sub-Committee with an up-to-date copy of the records maintained pursuant to Section G12.3(f);

(h) provide all reasonable assistance that may be requested by the Security Sub-Committee or the User Independent Security Assurance Service Provider for the purposes of conducting a User Security Assessment;

(i) subject to G12.5, comply with the requirements of Sections G1, G3 to G5, G7 and G8;

(j) comply with the requirements of Sections G12.6 to G12.8; and

(k) act in accordance with Good Industry Practice.

G12.5 For the purposes of Sections G1, G3 to G5, G7 and G8, unless the SSC Guidance for Device Security Assurance and Triage states otherwise, a Triage Facility Provider shall be treated as if it is a User and:

(a) any reference to a 'User' shall be deemed to include a reference to a 'Triage Facility Provider';

(b) except for where the SSC Guidance for Device Security Assurance and Triage states otherwise, obligations in those Sections which are expressed to apply to a User shall apply to a Triage Facility Provider;

(c) references in those obligations to 'User Systems' shall be deemed, for the purpose of their application to the Triage Facility Provider, to be references to the- Triage Activities undertaken at the Triage Facility, and

(d) the Security Sub-Committee shall provide Triage Facility Providers and other Parties with guidance on interpretation of Sections G1, G3 to G5, G7 and G8 in respect of their application to Triage Facility Providers and Triage Activities.

User Security Assessments of Triage Facilities

G12.6 Prior to undertaking any Triage Activities, each Triage Facility Provider shall be subject to an initial Full User Security Assessment by a User Independent Security Assurance Service Provider following the process in Sections G8.22 to G8.30.

Approval

G12.7 On receipt of the initial Full User Security Assessment Report and the User Security Assessment Response, the assurance status shall be set in accordance with Sections G8.35 to G8.36 and:

(a) where the assurance status is set to ‘approved’ under Section G8.36(a) then the Triage Facility Provider may undertake Triage Activities as set out in the SSC Guidance for Device Security Assurance and Triage;

(b) where the assurance status is set to ‘approved' subject to conditions (as set under Section G8.36(b)) then the Triage Facility Provider will require explicit approval from the Security Sub-Committee before undertaking Triage Activities; and

(c) where the assurance status is ‘deferred’ or ‘rejected’ under Section G8.36(c) or (d), respectively, then the Triage Facility Provider is not approved to undertake Triage Activities.

Second and subsequent User Security Assessments

G12.8 Following completion of the initial and each subsequent User Security Assessment of the Triage Facility Provider, the Security Sub-Committee shall determine the category of the next User Security Assessment to be carried out and, in doing so shall:

(a) consider any security risks identified during or since the previous User Security Assessment;

(b) take account of the volume of Devices for which Triage Activities are carried out;

(c) reach a determination based on a proportionate assessment of the security risks as to whether the next User Security Assessment should be:

(i) a Full User Security Assessment;
(ii) a Verification User Security Assessment; or
(iii) a User Security Self-Assessment.

Definitions

G12.9 For the purpose of this Section G12:

Requestor	means an entity (such as a Party or a meter asset provider) that requests that Triage Activities are undertaken by a Triage Facility Provider.
SSC Guidance for Device Security Assurance and Triage	means the document published by the Security Sub-Committee under Section G7.19(g), which sets out guidance on the requirements and processes (including security controls and security assurance) to be followed by Triage Facility Providers undertaking Triage Activities.
Triage	means the diagnosis, upgrading or resetting of a Device.
Triage Activities	means any Triage-related activity carried out in circumstances where the SSC Guidance for Device Security Assurance and Triage requires independent assurance, including in such circumstances: a) the breach of the tamper-protection boundary; b) any unlocking of internal non-operational ports; c) any changes to the configuration of the Device Data; d) confirmation of the firmware version on the Device when Triage has been completed; and e) completion of Triage by replacing all internal non-operational port seals required pursuant to the CPA Security Characteristics and all tamper-protection boundary seals.
Triage Facility	means a premise where Triage Activities are undertaken.
Triage Facility Provider	means a Party which operates a Triage Facility for the purpose of carrying out Triage Activities.
Triage Interface	means a secure IPsec VPN site to site encrypted link provided by a Manufacturer in order to connect its Triage System to a Triage Tool at a Triage Facility, which provides confidentiality and integrity of communications.

Triage System	means a secure IT system established for the purposes of Triage and operated by a Manufacturer, as part of its Device manufacturing capability, which the Triage Facility Provider connects to using the Triage Tool and Triage Interface, and which is compliant with the requirements of the NCSC Commercial Product Assurance (CPA) Scheme and the associated CPA Security Characteristics.
Triage Tool	means an electronic device provided by a Manufacturer, which is used to Triage Devices in accordance with SSC Guidance for Device Security Assurance and Triage, and~~,~~ which is cryptographically authorised such that it can only be used for Triage Activities and cannot be given additional capabilities by an operator in a Triage Facility.