

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.



DP203

‘Security Assurance of Device Triage Facilities’

Modification Report

Version 0.1

10 May 2022

Corporate member of
Plain English Campaign
Committed to clearer
communication

592



Managed by



About this document

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

Contents

1. Summary.....	3
2. Issue.....	3
3. Assessment of the proposal	5
Appendix 1: Progression timetable	6
Appendix 2: Glossary	6

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 Smart Energy Code (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. Triage Facilities operated by Supplier Parties may be covered under the security obligations in SEC Section G 'Security' and Device Manufacturers may be covered under the existing CPA Build Standard, although this is not confirmed. However, Triage Facilities could be operated by non-SEC Parties, such as Meter Asset Providers (MAPs) or their contracted agents.

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.

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 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 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. Assessment of the proposal

Areas for assessment

Sub-Committee input

As part of the modification assessment, the Smart Energy Code Secretariat and Administrator (SECAS) will engage 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

SECAS has identified the following areas and questions that will need to be further considered before a suitable solution will be able to be implemented:

When should a solution be targeted for?

It is understood that MAPs and Suppliers will want the Triage Facilities to be prepared to implement Factory Reset as soon as it becomes available. Until the assurance requirements are defined within this modification then assessing compliance of a facility will not be possible. SEC Parties will be asked for estimates on when Devices will be available that can facilitate Factory Reset.

Is a new section of Section G 'Security' needed?

A solution could be developed by expanding the current exclusions under SEC Section G1.7, or a new section could be added, like that for Shared Resource Providers under SEC Section G10. The SSC considers that the greatest clarity will be provided by a new SEC section for Triage Facilities. SEC Parties will be asked if they agree with this approach.

What is the best way to introduce this obligation on Triage Facilities?

If a definition is introduced specifically for Triage Facilities this will need to be futureproofed for other new use cases.

Appendix 1: Progression timetable

This proposal was raised 10 May 2022. SECAS will present this Draft Proposal to the Change Sub-Committee (CSC) to be converted to a Modification Proposal and enter the Refinement Process. It will then be discussed at the 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
Modification discussed with Working Group	6 Jul 2022
Refinement Consultation	11 – 29 Jul 2022
Modification discussed with Working Group	7 Sep 2022
Modification Report approved by CSC	20 Sep 2022
Modification Report Consultation	21 Sep – 11 Oct 2022
Change Board Vote	26 Oct 2022

Appendix 2: Glossary

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

Glossary	
Acronym	Full term
BEIS	Department for Business, Energy and Industrial Strategy
CIO	Competent Independent Organisation
CPA	Commercial Product Assurance
CPL	Central Products List
CSC	Change Sub-Committee
HAN	Home Area Network
MAP	Meter Asset Providers
NCSC	National Cyber Security Centre
OPSG	Operations Group
SC	Security Characteristics

Glossary	
Acronym	Full term
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