This document is classified as **CLEAR** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.

SSC Guidance for Device Security Assurance and Triage

Part 1: Methodology to Raise a Change to CPA SCs or to Raise a Use Case

Document Control

Document Owner	Smart Energy Code Company Ltd
Version	1.3
Date	11 February 2026
Document Status	SSC Approved
Date of Next Review	TBD
Classification	Clear

Change Record

Date	Author	Version	Change Reference
18/05/2022	SECCo	0.01	Draft version created for review by SSC for comment
31/05/2022	SECCo	0.02	Updated draft version created for review by SSC, BEIS, NCSC and SCIRS for comment
23/11/2022	SECCo	1.0	Aligned with Parts 2 and 3 and approved by SSC
22/03/2023	SECCo	1.1	Updated with current SEC website URL and reference to SSC clarifications in the Glossary.
28/05/2025	SECCo	1.2	Updated following transfer of CPA Scheme from NCSC to SSC; updated references to DESNZ; inclusion of Use case 005.
11/02 2026	SECCo	1.3	Updated to include references to Part 4 (Use Case 005 TSCF) and to update references.

Contents

1. Regulatory Context

The security controls and assurance arrangements for the end-to-end Smart Metering System are defined in the Smart Energy Code (SEC) and aim to provide confidence to all SEC Parties that the systems and Devices supporting smart metering are appropriately secure.

The SEC Section G7.19 places an obligation on the Security Sub-Committee (SSC): *"The Security Sub-Committee shall: …….*

(j) develop and maintain documents to be known as "SSC Guidance for Device Security Assurance and Triage" which shall set out the SSC's guidance on the requirements and processes to be followed in respect of Devices (including in relation to their Triage and refurbishment) in order to:

(i) achieve appropriate levels of security assurance in accordance with the requirement of this Code; and

(ii) obtain and maintain CPA Certification."

The SSC Guidance for Device Security Assurance and Triage is in three parts:

- Part 1 provides the methodology, a process and a template for any party to raise a change to the Commercial Product Assurance (CPA) Security Characteristics (SCs) or to raise a Use Case for Device Triage.
- Part 2 provides details of the arrangements and the Security Requirements and Guidance to be applied to Use Cases that have been approved by the SSC.
- Part 3 provides details of the assurance arrangements for Use Case 004 (ESME & GSME Factory Reset) Triage Facilities in the form of a Triage Security Controls Framework (TSCF):
    - Section 1 of the TSCF describes the purpose and what the TSCF aims to achieve; the different types of Security Assessment and their frequency; and the role of the User CIO;
    - Section 2 of the TSCF provides greater detail at a practical level for the User Assessment lifecycle with information and logistical requirements for how a User should engage with the User CIO; the timeline for User Assessments; and the detailed questions the User CIO might ask, and the evidence it might expect to see from a User to support its assessment.
- Part 4 provides details of the of the assurance arrangements for Use Case 005 (4G CH & Later Factory Reset) Triage arrangements in the form of a Triage Security Controls Framework (4G CH TSCF) and provides detailed questions the DCC CIO might ask, and the evidence it might expect to see from the DCC and its Service Providers to support its assessment.

[Note that for Use case 004, the Manufacturer's Triage Systems, Triage Tools and Triage System Interfaces are assured via an extension to the CPA Build Standard, as defined in *"CPA Security Characteristic Triage interface updates to GSME, ESME, SAPC and CH SCs and CPA Build Standard Extensions"*.]

The SSC Guidance for Device Security Assurance and Triage forms part of the SEC Materials defined in SEC Section M5.1, and the document is regularly reviewed and updated by the SSC.

As CPA Scheme Owner, the SSC uses an SSC CPA Issue Resolution Sub-Group (SCIRS) to provide a working level industry engagement forum through which SSC, DCC, DESNZ, and the CPA Scheme Operator can work together with key industry partners to consider any CPA-related matters. The SCIRS operates under the governance of the SEC Security Sub-Committee and recommendations from the SCIRS are then submitted to the SSC for approval.

The Smart Metering Equipment Technical Specifications (SMETS2+), Communication Hub Technical Specifications (CHTS) and Great Britain Companion Specifications (GBCS) are Schedules to the SEC that contain a minimum set of functional, technical and security requirements to enable SMETS2+ Devices to be installed and to operate efficiently and securely in consumer premises. The

SSC Guidance for Device Security Assurance and Triage has been created to support Device Triage since the SMETS, CHTS and GBCS do not contain requirements when the Device has been removed from the consumer premises.

The documents comprising SSC Guidance for Device Security Assurance and Triage assume the reader has a high degree of familiarity with the SEC and the CPA SCs and is knowledgeable on security matters. As such, the use of defined terms (where capitalised) have the same meaning as those defined in the SEC and CPA SCs and other capitalised terms are defined in this document.

For the avoidance of doubt, there is no requirement in regulations for meters to implement the functionality described in the Use Cases. Such functionality is optional.

Responsible Suppliers have SEC obligations to ensure the security of Smart Metering Systems which includes Devices that have been subject to Triage. A Supplier's compliance with SEC security obligations is assessed by annual User Security Assessments. Similarly, the DCC has SEC obligations to ensure the security of the DCC Total System which includes SMETS2+ Communication Hubs.

2. Introduction

Security assurance for Devices to be included on the Central Product List (CPL) is provided by ensuring the compliance of smart metering equipment against the CPA SCs. The SCs are agreed and updated from time to time in line with SEC Section G 7.19(f) following discussion with industry, DESNZ and the SSC.

Smart metering equipment is evaluated by independent CPA Test Labs and the resulting report and evidence is reviewed by the CPA Scheme Operator before being CPA certified. Only equipment that has been CPA Certified with a current CPA Build Standard can be included on the Central Product List (CPL) which allows DCC Users to communicate with the equipment.

Changes to CPA SCs: The SCs have been developed to mitigate security risks identified in threat mapping exercises with industry involvement and the SSC will periodically refresh the threat mapping. Changes to the SCs may be required to take account of the threat landscape for smart metering; or on completion of the SSC annual risk assessment of the end-to-end Smart Metering System; or to address any known security incidents or vulnerabilities. Changes may also be requested by participants in Device manufacture, asset provision or installation and operation of Devices. The SSC Guidance for Device Security Assurance and Triage Part 1 provides a methodology, a process and a template to manage changes to the published CPA SCs.

Use Cases for Device Triage: Experience of live smart metering operations identified a business justification for secure processes to enable the Triage of Devices that may or may not have completed Commissioning and have been returned to the Meter Asset Provider (MAP) or to the Supplier or, in the case of Communication Hubs, to the DCC but have no operational defects and just need to have certain functions reset to enable re-installation. This avoids wasteful and unnecessary scrapping of Devices and helps to minimise costs to consumers.

The SSC, with support from DESNZ have confirmed that they are open to considering compelling Use Cases from industry that protect security controls whilst facilitating the Triage of Devices for re-installation. The SSC Guidance for Device Security Assurance and Triage Part 1 provides a methodology, a process and a template to raise new Use Cases for Device Triage.

3. CPA Security Characteristics (SCs)

All CPA Security Characteristics contain a list of mitigations that describe the specific measures required to prevent or hinder attacks. The mitigations are grouped into three requirement categories:

a) **Development mitigations (indicated by the DEV prefix):** are measures integrated into the development of the product during its implementation. Development mitigations are checked by an evaluation team during a CPA evaluation.
b) **Verification mitigations (indicated by the VER prefix):** are specific measures that an evaluator must test (or observe) during a CPA evaluation.
c) **Deployment mitigations (indicated by the DEP prefix):** are specific measures that describe the deployment and operational control of the product. These are used by system administrators and users to ensure the product is securely deployed and used in practice and form the basis of the Security Operating Procedures.

Each of the mitigations contain the name of the mitigation. This will include a mitigation prefix (DEV, VER or DEP) and a unique reference number. a description of the threat (or threats) that the mitigation is designed to prevent or hinder (threats are formatted in italic text) and the explicit requirement (or group of requirements) that must be carried out.

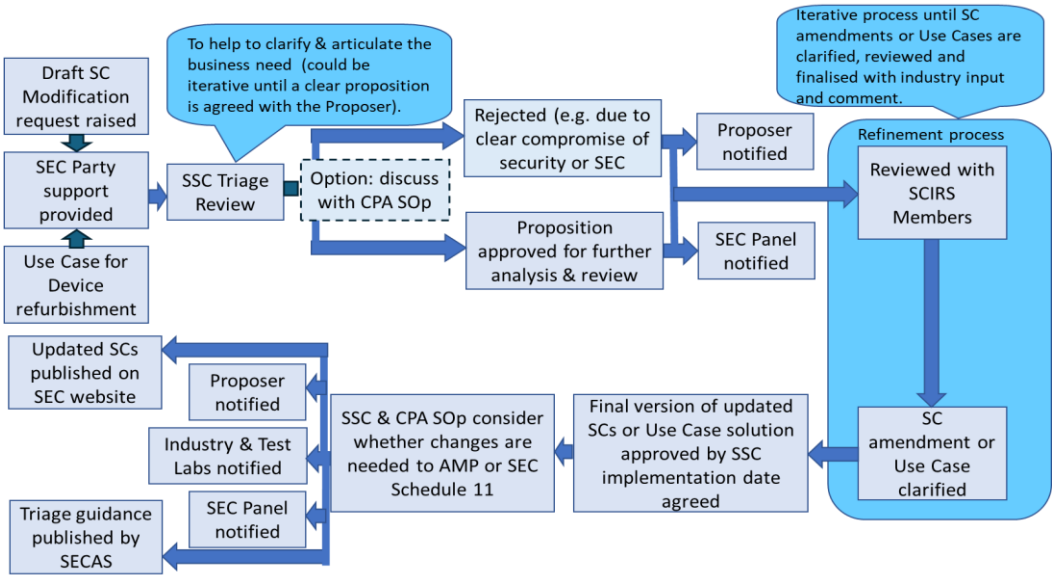
In respect of Device Triage, the SCs require that any non-operational interfaces must be behind a tamper-protection boundary and must not bypass GBCS controls. The Triage Interface for Use Cases 004 and 005 are separately defined as part of the requirements for the optional Triage Interface variant defined for the Device Security Characteristics (see *"CPA Security Characteristic Triage interface updates to GSME, ESME, SAPC and CH SCs and CPA Build Standard Extensions"* published by the SSC). In future these requirements may be integrated into the GSME, ESME, SAPC and CH SCs (although support for Use Case 004 and Use Case 005 will remain optional)).

4. Raising a Request for a CPA SC Modification or proposing a Use Case for Device Triage and Refurbishment

Any party may raise a request for a CPA SC modification or to provide a Use Case for Device Triage and Refurbishment using the process described in this document which is published on the SEC website (and using the form provided at Appendix 1 to this document):

https://smartenergycodecompany.co.uk/ssc-guidance-on-device-security-assurance-and-triage/

The process provides a structured way of exploring the implications of changes to the CPA SCs or of exploring new Use Cases for Device Triage and refurbishment with industry involvement.



It is possible that some Use Cases could require changes either to the SEC or to the CPA SCs or to both, which will elongate the timescales. Where a Use Case does not require any changes to the SEC or CPA SCs, the SSC will update the SSC Guidance for Device Security Assurance and Triage as soon as possible after conclusion of the process.

Appendix 1 – Template to propose a CPA SC Modification Request or a Use Case for Guidance on Device Triage and Refurbishment

This document is classified as **CLEAR** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

Proposal for a Modification to the CPA Security Characteristics (SCs) or for a Use Case for Device Triage Refurbishment

The SEC Security Sub-Committee (SSC) is responsible for maintaining the CPA Security Characteristics and for providing advice on security matters:

"SEC G7.19 (f) with respect to the CPA Security Characteristics:

(i) maintain CPA Security Characteristics that set out the levels of security required for Smart Meters, Communications Hubs, SAPCs and HCALCs; and

(ii) where it considers it appropriate from time to time, develop the CPA Security Characteristics so as additionally to set out levels of security required for any other Device, in each case so as to ensure that the required levels of security are proportionate and appropriate taking into consideration the security risks identified in the Security Risk Assessment;"

The SSC has established a process for considering proposals for CPA SC Modifications that is explained. The latest form should be used, as published on the SEC website:

https://smartenergycodecompany.co.uk/ssc-guidance-on-device-security-assurance-and-triage/

The same process can be used to propose a Use Case for Device Triage and Refurbishment. Any party can raise a draft CPA SC Modification Proposal but must also have the support of a SEC Party. This form should be completed and submitted to the SSC for consideration by e-mailing the form tossc@talan.com

CPA SC Modification Proposal (complete as appropriate)	
Proposed CPA SC Modification Title:	
Use Case for Device Triage and Refurbishment (complete as appropriate)	
Proposed Use Case Title:	
Name:	
Organisation:	
Contact Number:	
Email Address:	
Submission date:	

Details of SEC Party support	
Name:	
SEC Party:	
Contact Number:	
Email Address:	

1. What issue are you looking to address?

2. Why does this issue need to be addressed? *(i.e. Why is doing nothing not an option?)*

3. What is your Proposed Solution?

4. Does this affect an existing CPA SC? If so, please explain the specific SC affected?	Yes/No
[Please insert the CPA SC affected and explain why it needs to be changed e.g. not working/needs clarification etc]	

5. Does this require a new CPA SC? If so, please explain.	Yes/No

6. Is this Proposal considered to be an urgent business need? If so, please explain.	**Yes/No**

Appendix 2 – Glossary

This document also uses the terms defined in the Smart Energy Code (SEC) and the CPA Policies and Procedures and the smart metering CPA Security Characteristics. Relevant definitions are repeated here.

Term	Definition
Central Products List (CPL)	The list of Devices that are approved to communicate with the DCC, which requires that the Device has met the requirements as set out in SEC Appendix Z – The CPL Requirements Document, including the requirement for the version to have a CPA certificate associated with it.
Commercial Product Assurance (CPA)	The CPA Scheme owned by the SSC that is used to assure the security of smart metering Devices to a baseline of published security requirements.
CPA Device Certificate	An Assurance Certificate issued for the purposes of the CPA Scheme, which is issued by the Scheme Owner based on a recommendation by the Scheme Operator and published on the SEC website to confirm that a Device has been successfully evaluated against the relevant CPA Security Characteristics. A CPA Device Certificate is only valid if the Manufacturer of the Device also holds a currently valid CPA Build Standard Certificate relating to that Device Model.
CPA Build Standard Certificate	An Assurance Certificate issued for the purposes of the CPA Scheme, which is issued by the Scheme Owner, based on a recommendation by the Scheme Operator, and published on the SEC website. A CPA Build Standard Certificate: confirms that the Manufacturer of a Device meets the requirements of the CPA Build Standard for one or more Device Models. For a CPA Device Certificate to be valid for a Device, the Manufacturer of that Device must hold a currently valid CPA Build Standard Certificate relating to that Device Model.
CPA Policies and Procedures	Documents required by SEC Section G7.19 (g) setting out the governance and processes to obtain a CPA Device Certificate; to meet Assurance Maintenance requirements; to obtain a CPA Build Standard Certificate; and to undertake a periodic CPA Risk Review.
CPA Scheme Operator (SOp)	The expert organisation appointed by the SSC to make decisions on CPA Certification based on findings reported by CPA Test Labs for CPA Device Certification, Assurance Maintenance, Risk Reviews and CPA Build Standard validations.
CPA Security Characteristics (SCs)	The baseline of security requirements against which smart metering Devices are evaluated
CPA Test Lab	A Test Lab that is considered capable of conducting Cyber Resilient testing activities by the NCSC and additionally considered to be capable of CPA evaluations by the SSC, operating under the CPA Test Lab Operational Requirements and a 'CPA Test Lab Framework Agreement' with the SOp to create, implement and report tests and analysis that address each mitigation requirement in the CPA SCs and the requirements of the CPA Build Standard.
CHTS	Means the Communication Hub Technical Specification published in the SEC,
Data Communications Company (DCC)	The entity that manages the smart metering data and communications infrastructure, as described in the Smart Energy Code.
GBCS	Means the Great Britain Companion Specification published in the SEC
NCSC	Means the National Centre for Cyber Security
SC-impacting	The hardware, software, and/or firmware parts of a product that directly implement all or part of any mitigation in the SC against which the product is evaluated. Note1: directly implementing an SC mitigation means that the relevant part of the product (hardware, software, and/or firmware) is responsible for the specific decisions and behaviour that implement the mitigation. Note2: a new product version that contains SC-impacting changes requires an SIE Assurance Maintenance evaluation (or else it may be submitted for a full re-evaluation) to maintain its certified status.

Term	Definition
SEC	Means the Smart Energy Code that is published on the SEC website https://smartenergycodecompany.co.uk/
Security Sub-Committee (SSC)	The entity described in section G7 of the Smart Energy Code, with responsibilities including the maintenance and monitoring of assurance in various aspects of the smart metering system including the CPA Scheme..
SMETS 2+	Means the Smart Metering Technical Specification published in the SEC
SSC Guidance for Device Security Assurance and Triage	means the document published by the Security Sub-Committee under Section G7.19(j), 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 [Note the SSC clarification in Part 3 Section 2 of the SSC Guidance that explains which tamper-protection seals are relevant]; 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
Triage Facility	means a premises where Triage Activities are undertaken [Note the SSC clarification in Part 3 Section 2 of the SSC Guidance that explains the scope of assurance in a facility that undertakes Triage of non-Use Case 004 and non-Use Case 005 Devices].
Triage Facility Provider	means a Party which operates a Triage Facility for the purpose of carrying out Triage Activities.
Triage System Interface	means a secure IPsec (as defined in SEC Section G12.9 and the SSC Guidance on Standards, Procedures and Guidance) virtual private network, 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 authentication, 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 System Interface, and which is compliant with the requirements of the Commercial Product Assurance (CPA) Scheme Build Standard.
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.