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.

Document Control

Document Owner	Smart Energy Code Company Ltd
Version	1.1
Date	17 July 2019
Document Status	SSC Approved
Date of Next Review	TBD
Classification	White

Change Record

Date	Author	Version	Change Reference
21/02/2019	SECCo	0.01	Draft version created for review by NCSC prior to SSC approval
06/03/2019	SECCo	0.02	Amendments following comments from BEIS (TSIRs Chair) and from the CPA Industry Day on 28/02/19
13/03/2019	SECCo	0.03	Amendments following SSC comments on 13/03/19 and re-classified as 'White' to enable access by non-SEC Parties
27/03/19	SECCo	1.0	Final version approved by SSC on 27/03/19
17/07/19	SECCo	1.1	Updated to take account of use cases for device refurbishment for which SSC guidance can be issued.

Table of Contents

1. Introduction

Security has been at the heart of the design of the end-to-end Smart Metering System from the start of the Smart Metering Implementation Programme (SMIP). Considerable effort has been invested by the energy industry, with support from BEIS and NCSC, in designing security controls that protect the end-to-end 'trust-based' security architecture.

Due to the interconnected nature of the systems supporting smart metering, each SEC Party requires assurance that other parties are operating secure systems and are compliant with their SEC security obligations. Assurance arrangements have been developed to provide a mechanism for assessing security compliance to provide confidence to all SEC Parties that the systems and Devices supporting smart metering are appropriately secure. In having a connection to the DCC, all Users can become a source of security risk to the system as a whole. Independent assurance is provided across the endto-end smart metering system assuring:

a) the DCC's compliance with the appropriate Smart Energy Code (SEC) security obligations via an annual Statement of Organisation Controls (SOC2) audit by an independent qualified organisation;
b) the compliance of DCC Users with the appropriate SEC security obligations via an annual User Security Assessment by a User Competent Independent Organisation (CIO); and
c) the compliance of smart metering equipment with a set of NCSC Commercial Product Assurance (CPA) Security Characteristics (SCs) agreed by industry and NCSC against which smart metering equipment is evaluated by independent, NCSC accredited Test Laboratories before being CPA certified by NCSC. Only equipment that has been CPA Certified can be included on the Central Product List (CPL) which allows DCC Users to communicate with the equipment.

Role of the SEC Security Sub-Committee (SSC)

The SSC was established in line with the requirements set out in SEC Section G7. Membership is drawn from representatives of Large energy Suppliers, Small energy Suppliers, Gas and Electricity Network Operators, Shared Resource Providers and Other Users. SEC Section G7.16 (b) allows the SSC Chair to invite any other person to provide expert advice. The duties and powers of the SSC are set out in SEC Section G7.18 to G7.25. In respect of CPA, the SEC places the following obligations on the SSC:

"G7.20 (d) keep under review the NCSC CPA Certificate scheme in order to assess whether it continues to be fit for purpose in so far as it is relevant to the Code, and suggest modifications to the scheme provider to the extent to which it considers them appropriate;"

"G7.20 (i) provide advice and information to the Authority in relation to any actual or potential noncompliance with the CPA Security Characteristics of any Device or apparatus in respect of which a CPA Certificate is issued or required."

"G7.19 (f) liaise and work with the NCSC to develop and maintain CPA Security Characteristics that set out the levels of security required for Smart Meters, Communications Hubs and HCALCs that are proportionate and appropriate taking into consideration the security risks identified in the Security Risk Assessment."

The SEC Appendix Z (CPL Requirement Document) also contains obligations on the SSC relating to the removal of Devices from the CPL when a CPA Certificate expires or is withdrawn or cancelled by the Certification Body (NCSC).

2. Purpose

The purpose of this document is to clarify the arrangements for the development, maintenance, modification and governance of the CPA Security Characteristics (SCs) and the same process can be used for industry to propose use cases for Device refurbishment.

To meet the obligation in G7.19 (f), the SSC has developed and will maintain the methodology set out in this document to ensure that it:

a) explains the process and governance for the development and maintenance of CPA SCs;

b) follows the broad principles and processes of the SEC Modification process;

c) is able to be applied consistently and proportionately for all Devices that are subject to the CPA SCs; and

d) is readily available as guidance to all parties including Device Manufacturers, energy Suppliers, Meter Asset Providers – MAPs who purchase Devices, Test laboratories and any party that relies on the secure operation of smart metering equipment.

This document is intentionally technical in nature, and assumes the reader has a high degree of familiarity with the SEC and is knowledgeable on security matters. As such, the use of defined terms (where capitalised) have the same meaning as those defined in the Smart Energy Code and are not redefined within this document

Agreed Interpretations

This document should be read in conjunction with the Agreed Interpretations which have been developed by the SSC where a Party or the User CIO has asked the SSC for clarity on a specific SEC obligation. The purpose of that document is to provide SSC Agreed Interpretations of certain SEC definitions to enable these to be consistently applied by all SEC Parties.

3. CPA and the Role of NCSC

NCSC is the CPA Authority and Certification Body and oversees the CPA Scheme and provides the CPA Certificates based on evidence provided from evaluations of products by an accredited Test Laboratory (Evaluation Facility).

The CPA (Foundation) Scheme was selected by BEIS (then DECC) as the most appropriate assurance scheme from a range of options and after a public consultation in 2012.

The process for performing CPA (Foundation) grade evaluations is set out in documents available from the NCSC website: www.ncsc.gov.uk/document/cpa-scheme-library

The evaluations assess the compliance of a product with a set of Security Characteristics (SCs) that are published on the NCSC website: www.ncsc.gov.uk/document/security-characteristics-smartmeters

4. Security Characteristics (SCs)

The Smart Metering SCs were developed by a CPA Working Group consisting of industry security experts drawn from Device Manufacturers, energy Suppliers, BEIS (then DECC), NCSC (then CESG) with support from an accredited CPA Test Laboratory. The CPA Working Group met monthly over a two-year period and was disbanded when the SCs were published.

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 which are produced as part of the CPA evaluation.

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), the explicit requirement (or group of requirements) that must be carried out

5. Modifications to Security Characteristics (SCs)

Unlike the Smart Metering Technical Specifications (SMETS), the CPA SCs are not SEC documents since NCSC retain overall responsibility for sign-off and publishing the CPA Security Characteristics. The SEC Modification process is therefore not appropriate for the SCs. Following a BEIS consultation, the SEC places the responsibility for maintaining the SCs with the SSC. In considering any SC Modification Requests, the SSC will follow the broad principles and processes of the SEC Modification process but will also involve non-SEC Parties in the review and impact analysis. Proposals for modifications to the SCs may arise for a number of reasons including:

a) **New risk mitigations:** Modifications may be necessary in response to changes in threat and risk assessments that become known to NCSC and / or to the SSC;
b) **Changes to specifications:** Modifications may be necessary because of updated SMETS and CHTS specifications. Such changes may be cosmetic such as updates to paragraph numbers or cross-references but nevertheless need amendment;
c) **Changes to standards:** Modifications may be necessary as a result of changes to existing standards used in the SCs e.g. MISRA; or existing standards which are deprecated or new standards that are appropriate;
d) **Lessons learned:** Modifications and / or clarifications may be necessary as a result of lessons learned during the CPA evaluation and certification process; and from the operation of smart metering equipment;
e) **Business needs:** Modifications may be necessary as a result of new or changed business needs that could arise from the installation and operation of Communications Hubs, Electricity Smart Metering Equipment (ESME), Gas Smart Metering Equipment (GSME) and HCALCs;
f) **New equipment requirements:** New SCs may be required if there are new equipment proposals that need assurance or if there are changes to the risk profile of existing equipment that is not subject to CPA e.g. Pre-Payment Interface Devices (PPMIDs);
g) **SEC Modifications**: Modifications to SCs may be needed as a result of SEC Modifications that are accepted by the SEC Change Board. Such modifications could have Device security implications that require changes to the existing SCs.

The SEC Schedule 11 contains the Technical Specification Applicability Tables that indicate for each Technical Specification or GBCS where the Maintenance End Date or GBCS Applicability Period End Date has been applied and energy suppliers should have taken all reasonable steps to ensure that there are no Devices operating with that combination of Technical Specification and GBCS once the end date has passed.

Since multiple versions of hardware and software can be deployed and operating at the same time over the lifetime of Devices, Table 4 of SEC Schedule 11 maps the SCs to relevant versions of GBCS.

6. Process for achieving modifications to Security Characteristics (SCs)

In all cases an SC Modification Request will need to be raised for SSC consideration and liaison with NCSC using the template available from SECAS [here] (and also included at Appendix 2). The template seeks to clarify the origin, purpose and business need for the proposed change.

Any party such as a Device Manufacturer, test laboratory, Trade Body or SEC Party may propose a SC Modification Request. However, the SSC will expect such a Proposer to have obtained the support of one or more SEC Parties before progressing the SC Modification Request.

On receipt of a SC Modification Request supported by a SEC Party, the SSC will conduct a 'triage' review to establish whether the business need is clearly articulated. This could be an iterative process between the SSC and the Proposer (who can be invited to attend a SSC meeting) until a clear proposition is agreed. SSC will then liaise with NCSC to consider whether the proposed change is valid and in line with the CPA Scheme, security architecture and controls and SEC security obligations and merits further consideration. If it does, the SSC will initiate a refinement process by convening one or a series of CPA Working Groups (WGs) under SSC governance and invite attendance from Suppliers, Device Manufacturers, test laboratories, DCC (and its Service Providers as appropriate), NCSC, BEIS, any SEC Panel nominees and any other relevant parties (e.g. Subject Matter Experts) that may have an interest.

The SSC will notify the SEC Panel of SC Modification Requests for their awareness and to invite nomination or contribution from Panel members and/or for the Panel to request regular updates.

The CPA Working Group will be an Advisory Body without decision-making powers but will provide a valuable source of advice for the SSC and NCSC when coming to a conclusion on any modifications to the SCs. The Terms of Reference for the CPA Working Group are set out in Appendix 1.

Following a period of consultation during the refinement process and taking account of views and comments on the proposals provided by the CPA Working Group, which is likely to be an iterative process, the SSC will make a decision on the final outcome of the SC Modification Request. based on advice from the CPA Working Group and NCSC. The SSC will notify the SEC Panel of the outcome and provide a Modification Report.

Once a final version of the updated SCs has been approved, the SSC will notify the Proposer and the SEC Panel. The SSC will set an implementation date for the new SC version and notify industry. NCSC will publish the updated version on the NCSC website on the implementation date.

The SSC will consider with NCSC whether any changes are required e.g. to Assurance Maintenance Plans (AMP) or to the Technical Specification Applicability Tables in SEC Schedule 11, noting that the general rule is that:

- the most recent Sub-Version of the Principal Version (e.g. V1.3 or V2.1) of the CPA Security Characteristics published on the NCSC website at the time the relevant Device Model commences the CPA Certification or re-Certification process (as applicable) shall be used;

- changes to the Principle Version will be determined by changes to SMETS and / or GBCS and subject to SEC consultation.

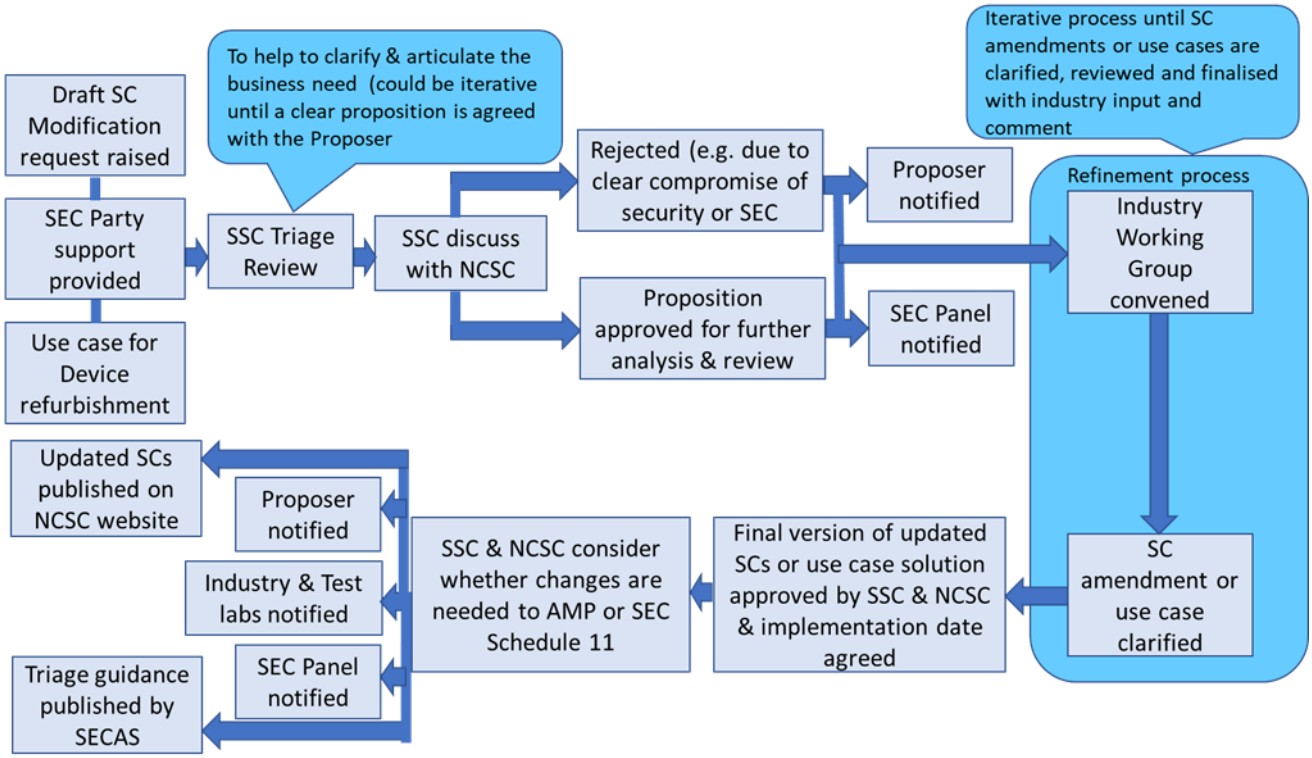
SECAS will notify all SEC Parties and the CPA Working Group when publication occurs to ensure that all relevant parties are aware of the updated version.

7. Proposing use cases for Device refurbishment

In the same way that any party may raise a SC modification proposal, any party may also provide a use case for Device refurbishment using the process described in the SEC website (and the form provided at Appendix 1 to this document): [https://smartenergycodecompany.co.uk/latest-news/howto-modify-the-cpa-security-characteristics/.](https://smartenergycodecompany.co.uk/latest-news/howto-modify-the-cpa-security-characteristics/)

The same process and template apply to raising a SC Modification Proposal and to proposing a use case for Device refurbishment. It provides a structured way of exploring the implications of changes to the CPA SCs or of exploring new use cases for guidance on Device refurbishment with industry involvement.

The typical process is set out in the diagram below.



Appendix 1 – CPA Working Group Terms of Reference

1. Purpose

These Terms of Reference for the CPA Working Group have been agreed by the SEC Security Sub-Committee (SSC). All CPA Working Group members must act in accordance with the agreed Terms of Reference and with the SSC governance arrangements and the SEC regulatory obligations.

The CPA Working Group is responsible for assisting the SSC with developing, assessing and commenting on SC Modification Requests to the CPA Security Characteristics (SCs) or use cases for Device triage and/or refurbishment,

The specific areas for assessment for each SC Modification Request or use case for Device triage and/or refurbishment being considered by the CPA Working Group will be agreed by the SSC in liaison with NCSC. The SSC will also agree any specific instructions or variations to these Terms of Reference when forming each CPA Working Group.

2. Duties of CPA Working Group Members

A CPA Working Group is expected to undertake the following tasks and activities as part of its assessment of each SC Modification Request or proposed use case for Device triage and/or refurbishment:

- to review the modification or use case proposals indicated by the SSC;
- to consult within the relevant industry sectors to assess the impact of the SC Modification Request or use case for Device triage and/or refurbishment;
- perform an estimate of any cost or other implications and the benefits of each SC Modification Request or use case for Device triage and/or refurbishment;
- propose amendments or alternative solutions if members believe there are other solutions that would deliver the intent of the SC Modification Request or use case for Device triage and/or refurbishment and provide an assessment of each solution raised;
-

The duties and responsibilities of CPA Working Group members are:

- to act in a fair and objective manner when considering SC Modification Requests or use cases for Device triage and/or refurbishment, whilst factoring in the complexity, potential impact and urgency of each SC Modification request;
- to act impartially while participating in a CPA Working Group;
- when joining the CPA Working Group, to confirm their availability for attending CPA Working Group meetings and undertaking any additional work that is required (including reviewing documentation produced by the SSC or NCSC;
- to inform SECAS if they do not wish to continue participating in the CPA Working Group.

A CPA Working Group may consider multiple SC Modification Requests or use cases for Device triage and/or refurbishment in parallel.

3. CPA Working Group Membership

Chairman: The CPA Working Group will be chaired by the SSC Chair.
Secretariat: The Secretariat will be provided by SECAS.
Industry Parties and participants: Attendance will be invited from a representative sample of Suppliers, Device Manufacturers, Test Laboratories, DCC (and its Service Providers as appropriate), NCSC, BEIS and any other parties that may have an interest e.g. Subject Matter Experts (SMEs).
Proposer: Membership will include the Proposer of each SC Modification Request or use case for Device triage and/or refurbishment being considered.
Quorum: The quorum shall be the quorum that applies to SSC meetings.
Withdrawal of membership: The SSC reserves the right to replace or remove a CPA Working Group member if in the SSC's opinion this member is unable to fulfil their duties as a CPA Working Group member and/or acts detrimentally to the work of the CPA Working Group.

4. CPA Working Group Meetings

CPA Working Group meetings will adhere to the following general requirements:

- meetings shall be held as required for the CPA Working Group to fulfil its objectives and to achieve the timetable agreed by the SSC for each relevant SC Modification Request or use case for Device triage and/or refurbishment;
- the secretary shall send notice to each CPA Working Group member with details of the time, date and location of the CPA Working Group meeting. Unless specified otherwise, meetings will be held at the SECAS Offices or nearby;
- the chairman may request a telephone conference to resolve clarifications that do not require a full meeting;
- the chairman may involve wider industry membership in any consultation on Working Group proposals;
- the chairman may choose to conduct certain business via correspondence e.g. commenting on a draft document that does not require a full meeting;
- an agenda and any additional supporting material for a CPA Working Group meeting will be distributed to the CPA Working Group members to allow consideration of these items prior to the CPA Working Group meeting.
- wherever possible, such materials should be provided at least five Working Days prior to the meeting;

5. Confidentiality and Disclosure

The CPA Working Group shall operate in accordance with the SEC Panel Information Policy. Prior to joining a CPA Working Group, each member will be asked to undertake in writing to abide by the confidentiality and disclosure provisions in relation to each information sharing level as described in the policy.

CPA Working Group members who breach the rules of the confidentiality and disclosure provisions under any information sharing level may have their CPA Working Group membership revoked.

Appendix 2: Template for:

I. a SC Modification Request or

II. a Use Case for Guidance on Device Refurbishment

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.

Appendix 2: Proposal for a Modification to the CPA Security Characteristics (SCs) or for a Use Case for Guidance on Device 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) liaise and work with the NCSC to develop and maintain CPA Security Characteristics that set out the levels of security required for Smart Meters, Communications Hubs and HCALCs that 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 SC Modifications that is explained https://smartenergycodecompany.co.uk/latest-news/how-to-modify-the-cpa-security-characteristics/.

The same process can be used to propose a Use case for Guidance on Device Refurbishment.

Any party can raise a draft 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 to ssc@gemserv.com

SC Modification Proposal (complete as appropriate)
Proposed SC Modification Title:
Use Case for Device 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 SC? If so, please explain the specific SC affected?	Yes/No
[ase insert the SC affected and explain why it needs to be changed e.g. not working/needs clarification etc]	

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

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