This document is classified as **GREEN**. Limited disclosure, recipients can distribute this information to SEC Parties and SMIP stakeholders but not made publicly available.

SSC Guidance for Device Security Assurance and Triage

Part 2: Security Requirements & Guidance for Approved Use Cases

Document Control

Document Owner	Smart Energy Code Company Ltd
Version	1.5
Date	11 February 2026
Document Status	SSC Approved
Date of Next Review	TBD
Classification	Green

Change Record

Date	Author	Version	Change Reference
06/06/2022	SECCo	0.01	Draft version created for review of format by SSC prior to issuing to SCIRS
20/06/2022	SECCo	0.02	Updated draft following comments from a SCIRS member.
13/07/2022	SECCo	0.03	Updated draft following SSC comments.
01/11/2022	SECCo	0.04	Updated to include Use Cases 001, 002, 003 and 004.
21/11/2022	SECCo	0.05	Updated to include comments from SSC and SCIRS members.
23/11/2022	SECCo	1.0	Updated and approved by SSC
22/03/2023	SECCo	1.1	Updated to clarify Device Logs should be deleted for Use Cases 001 and 003.

Date	Author	Version	Change Reference
12/07/2023	SECCo	1.1.1	Updated to clarify the need for a Letter from the Test Lab to the Manufacturer for SSC to confirm compliance with the Triage Build Standard extensions for Use Case 004 and to provide a template Letter and an SSC Certificate
10/04/2024	SECCo	1.2	Updated to advise Manufacturers on Device credentials to change and not change during Use Case 004 Triage Activities and to add the TLS option to the Triage System Interface.
04/09/2024	SECCo/CyTAL	1.3	Updated to include Use Case 003A to allow Change of Mode following Use Case 003; and to allow deletion of security logs in Use Case 004. This document has also been classified TLP **GREEN** (previously **CLEAR**)
28/05/2025	SECCo	1.4	Updated following transfer of CPA Scheme from NCSC to SSC; updated references to DESNZ; inclusion of Use Case 005.
11/02 2026	SECCo	1.5	Updated to align with other parts of the SSC Guidance and to include Part 4 (Use Case 005)

Table of 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 NCSC Commercial Product Assurance (CPA) Security Characteristics (SCs) or to raise a Use Case for Device Triage;

- Part 2 provides details of the Security Requirements for Device Triage described in Use Cases that have been approved by the SSC in consultation with industry;

- Part 3 provides details of the assurance arrangements for Use Case 004 Triage Facility Providers in the form of a Triage Security Controls Framework (TSCF) – note that 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"*.

- 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.

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+), the Communication Hub Technical Specification (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 specifications or Security Requirements for Triage when the Device has been removed from the consumer premises but has no defects.

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.

Responsible Suppliers have SEC obligations to ensure the security of Smart Metering Systems which includes ESME, GSME and SAPC 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 and compliance with SEC security obligations is assessed by the annual DCC CIO Security Assessments.

2. Introduction

For the avoidance of doubt, there is no requirement in SEC regulations, including SMETS, CHTS and GBCS, for Devices to implement the functionality described in the Use Cases described in this document. Such functionality is optional.

This document describes the Security Requirements to be applied to Use Cases that have been approved by SSC to enable the Triage of Devices to be undertaken securely and consistently to support business requirements and in line with CPA SCs.

Triage is only permitted to be carried out in compliance with the Security Requirements described for the explicit Use Cases described in this document.

Additional Use Cases may be submitted to the SSC using the process outlined in Part 1 'Methodology to Raise a Change to CPA SCs or to Raise a Use Case' of the SSC Guidance for Device Security Assurance and Triage.

The Security Requirements contained within this document should not be considered a replacement for the security controls defined in the SEC and CPA SCs. It is expected that there are multiple ways of meeting the requirements of the SEC and the SCs and this document lists the Use Cases where the SSC has agreed methods which are considered to be consistent with the mandated security controls.

The Use Cases described in this document are each standalone in their own right.

3. CPA Security Characteristics (SCs)

The CPA Security Characteristics (SCs) contain a list of Development, Verification and Deployment mitigations that describe the specific security controls required to prevent or hinder attacks.

Unless indicated and explained otherwise, the Use Cases described in this document are expected to comply with relevant CPA SCs. In respect of Device Triage involving Use Case 004, a separate set of requirements apply to all Devices that support that Use Case and these are described in the separate document *"CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions"* issued by NCSC and SSC [Note that, in future, these requirements may be integrated into the GSME, ESME, SAPC and CH SCs (although support for Use Cases 004 and 005 will remain optional)].

Use Case 001 & Use Case 003 are subject to the SC Requirements for non-operational interfaces and, in particular, the SCs require that any non-operational interfaces must be behind a tamper-protection boundary, must be protected against unauthorised use, and must not bypass GBCS controls. These Use Cases are subject to confirmation during CPA evaluation that they do not create a 'negative impact' on the security of the

Device. This may require the application of Assurance Maintenance (AM) arrangements to confirm the 'no negative impact' aspects (and future changes to that functionality would likely be considered SC-impacting for the same reasons).

This might involve the CPA Test Lab checking the design against the DEV.2.M44 (Data validation of untrusted input) requirement. Where the Device is capable of processing messages not specified in GBCS the Manufacturer must demonstrate the measures in place to ensure these cannot be used to undermine device security. Also, in DEV.2.M847 (Minimise interfaces): "Where such additional functionality is present and has the potential to be security impacting, its unauthorised use shall be protected against using security mechanisms at least as strong as those in GBCS that protect against unauthorised use of critical commands, using the same RBAC model."

In addition, DEV.2.M873 (Disable non-operational logical and physical interfaces) may be applicable if the interfaces used for the Use Case need to be re-enabled. Depending on what the tests against the DEV requirements show, that might also mean some of the protections on the Triage Interface have to be tested under related VERs (e.g. VER.2.M80, VER.2.M903, VER.4.M927) and also the related DEPs (e.g. DEP.4.M925 relating to tamper evident seals on the perimeter.

4. Security Requirements – Use Case 001 (HAN Reset via a Port)

[Note: This Use Case is drafted as a standalone Use Case. It is accepted that multiple Use Cases could be triaged at the same time and Use Case 004 (Factory Reset) achieves the same business objectives as Use Case 001.]

This Use Case is applicable to GSME, ESME and SAPCs only.

4.1 Business Requirement

This Use Case is to enable a meter to be disassociated from a HAN it has already joined having been connected to a live Comms Hub. The business requirement arises from a number of aborted installations of meters that have not completed the Commissioning process. For this Use Case, 'not completed Commissioning' means that the Devices are not listed on the Smart Metering Inventory (SMI) as 'Commissioned' by the DCC. This could be caused by system outage/ consumer issues/delays during or shortly after installation. See Section 4.2 for the responsibility to ensure that the Device is correctly listed on the SMI.

Suppliers and MAPS who have invested cost and effort in procuring and installing meters wish to be able to re-install such meters which are capable of reuse to avoid unnecessary costs. It is for Responsible Suppliers to make arrangements with Triage Facilities to be able to identify which Devices meet the criteria of 'not completed Commissioning'.

Meters do not have the means to reset HAN information and will not join to a new HAN which, unless Triage takes place, will prevent the meter from being installed or having firmware upgraded via the normal DCC Service Request route.

The outcome from the Triage described in this Use Case is to achieve an appropriately authorised command (or set of commands) which is delivered locally through a non-operational port. The commands will reset the HAN (disassociate the meter from its existing HAN and return it to a state whereby it can join a new HAN).

This Use Case explains the Security Requirements by different parties to enable the Device to undertake a HAN Reset via a Port.

4.2 Responsibilities of Suppliers

4.2.1 Decommissioning Devices prior to Triage:

There is no SMETS or GBCS requirement for a Device to know what status is listed for the Device on the DCC's SMI. The SMI status can show any of the following:
'P' = Pending; 'INC' = Installed Not Commissioned; 'C' = Commissioned; 'D' = Decommissioned; 'S' = Suspended; 'WLT' = Whitelisted; 'Recovery' = SMKI Recovery Event – User comms disabled; 'Recovered' = SMKI Recovery Event successful credential update.

It is a SEC obligation (see below) for the Responsible Supplier to ensure that the correct status is recorded on the SMI and this is not a matter for a CPA Test Lab to assess.

Smart Energy Code (SEC)
"H6. DECOMMISSIONING AND SUSPENSION OF DEVICES
Decommissioning
H6.1 Where a Device other than a Type 2 Device is no longer to form part of a Smart Metering System, then that Device should be Decommissioned. A Device may be Decommissioned because it has been uninstalled and/or is no longer operating (whether or not it has been replaced, and including where the Device has been lost, stolen or destroyed).

H6.2 Only the Responsible Supplier(s) for a Communications Hub Function, Smart Meter, Gas Proxy Function, Standalone Auxiliary Proportional Controller or Type 1 Device may Decommission such a Device; provided that only the Lead Supplier may Decommission a SMETS1 CHF.

H6.3 Where a Responsible Supplier (or, in the case of a SMETS1 CHF, the Lead Supplier) becomes aware that a Device has been uninstalled and/or is no longer operating, that User shall send a Service Request requesting that it is Decommissioned."

Suppliers will need to process any firmware upgrades required once the meter has been installed and commissioned in the new premises. For this to work, the version of the firmware in the meter to be pre-notified and reinstalled must not have been suspended.

It is for the Responsible Supplier to satisfy themselves that the Security Requirements have been met including tight control of relevant tamper protection arrangements during Triage.

4.2.2 Triage Facilities:

The Triage defined in this Use Case may only be undertaken in a Supplier or Manufacturer's or Triage Facility Provider's Triage Facility, not at a consumer site. [Note: the assurance required for Use Case 004 Triage Facilities i.e., SEC Section G 12 and additional Triage Build Standard requirements does not apply to Use Case 001]

Suppliers, MAPs or their Agents and Manufacturers must ensure that any Triage Facilities used for this Use Case are included within the scope of and are subject to proportionate but appropriate security controls and in line with general good industry security practice. For this Use Case, the minimum level of security control is compliance with ISO27001 and having access controls to the premises, being undertaken only by authorised personnel and with records kept of all actions taken.

It is for Responsible Suppliers to ensure that Triage for this Use Case is either carried out at Triage Facilities and with processes that are compliant with the security controls defined and assured through the Supplier's or Triage Facility Provider's User Security Assessment or are carried out at a Manufacturer's premises and with processes that are compliant with the CPA Build Standard.

4.2.3 Security Assurance:

The Responsible Supplier has SEC obligations to ensure the security of Devices it installs and operates.

4.2.4 Re-installation:

Under this Use Case, Responsible Suppliers will be permitted to reinstall meters but only if the meter's own key material and the SMKI Organisation Certificates retained in the meter memory have not been modified following removal from the consumer premises due to aborted or failed installations (as opposed to faulty behaviour identified in the meter). It is also assumed that the SMKI ACB certificates have not yet been replaced on the meter via DCC/DSP (a daily DCC process).

Re-installation under this Use Case will only be possible if the Triaged meter is returned to the originating Supplier for installation in the original Network Operator area with the original Supplier SMKI Organisation Certificates and Network Operators (or ACB) Certificates in the meter.

4.3 Responsibilities of Manufacturers

The Manufacturer is responsible for ensuring that the Device complies with the relevant CPA SCs and for providing documentation to the CPA Test Lab to clarify that any Triage capability outside the CPA SCs also meets the requirements set out below.

The additional requirements defined for this Use Case are to ensure that Responsible Suppliers are able to meet their SEC security obligations. The Manufacturer will therefore need to ensure that their arrangements with the CPA Test Lab enables the Test Lab to confirm compliance with the Use Case 001 requirements set out below and to provide the Manufacturer and the SSC with confirmation.

These arrangements will enable Manufacturers and the SSC to provide assurance to Suppliers that the security requirements for Use Case 001 are met.

The Manufacturer will need to ensure that the Device incorporates a mechanism that enables the Supplier or Manufacturer (on behalf of the Supplier), to set it into a state that allows installation, following an aborted or failed installation.

Requirements to be demonstrated to the CPA Test Lab

It is likely that one or more persistent data items in the meter will need to be modified (e.g. reset) to achieve this. The CPA Test Lab should review documentation that demonstrates that the following requirements have been met or demonstrated to be not applicable to the implementation:

R1. any modified data items must not include the Device's current SMKI Private Keys, SMKI Organisation Certificates or firmware version.
To achieve this there could be one or more non-GBCS commands (Note: other approaches may be possible too but will require a separate, compelling Use Case to be reviewed and approved through SSC).

R2. where a non-GBCS command is used, it will be delivered through (in the terminology of the CPA SCs) a logical non-operational interface, which may or may not use the physical interface used for GBCS commands but will have some sort of physical restriction to limit its use to local access only (and will require a breach of the tamper-protection boundary);

R3. where a non-GBCS command is used it will require, as a first step, some form of access control check to have been successfully performed to protect against unauthorised use of the command.

R4. subsequent analysis of the Device by the CPA Test Lab will review documentation that demonstrates that the following requirements have been met or demonstrated to be not applicable to the implementation:

- **a.** the level of protection is in line with general good industry security practice, with a documented rationale by the Manufacturer to justify why this is the case and why, for instance, the access control mechanism, and associated procedural controls, cannot be trivially defeated or bypassed (which a CPA Test Lab can assess and, if satisfied with the rationale, accept). Where Manufacturers are unclear as to whether their planned solution meets the guidance in this document, this can be discussed with a CPA Test Lab;
- **b.** the "authentication value" used to authenticate the command either with the command or shortly prior to the command being provided, (see Note: below) must vary from meter to meter i.e. it must not be possible to re-use the authentication value for one meter in other meters or modify the value in a trivial manner to enable the same outcome (such as by changing part of the value that relates to a unique identifier value that is printed on the Device). However, this does not necessarily mean the meter has to have its own unique key material.
- **c.** possible approaches for such an access control mechanism may include use of Manufacturer key material (asymmetric or symmetric) with existing GBCS-defined

cryptographic mechanisms. Other approaches may be possible too and could for instance include the use of non-GBCS defined cryptography. In all cases, the CPA Test Lab will need to be satisfied that the properties of the access control mechanism meet the general requirements of this Use Case.

Note: It may be acceptable for the access control mechanism described to be performed via a separate command received beforehand (some type of "unlock" command) that then allows the "Reset HAN" command and other non-security impacting commands (e.g. requesting diagnostic information) to then be performed over the interface without any need for access control protection to be performed on each of these subsequent commands. If such an "unlock" approach is used, the meter must implement a mechanism that automatically ensures that it reverts back to a normal "locked" state (i.e. requiring access control to then be re-performed via the "unlock" command before the "Reset HAN" command can be accepted again), prior to leaving the Triage Facility.

R5. if the access control checks above are successful, the meter can then proceed to perform the "Reset HAN" functionality with the following result:

- **a.** the meter is left in a condition whereby any 'join network' functionality in the meter application will be re-enabled or allows the normal join procedures to be activated. Either way its resultant state will be compliant with GBCS expectations, in which one such state could be that defined by the ZigBee Stack Specification "05-3474" (e.g. revision 22), section 3.6.1.4.1 or any subsequent updated Stack Specification; and
- **b.** the Device Log is deleted to enable re-installation to join a new In Home Display (IHD) and Pre-Payment Interface Device (PPMID).

  Note: The meter must only modify a minimal amount of its data to release any previous HAN association and to delete the Device Log. This is to avoid unexpected side-effects on other CPA SC-compliant functionality. If the Manufacturer is unclear about the impacts made to their specific implementation to accommodate such functionality, they should discuss the impact of the changes with the CPA Test Lab.

R6. Regardless of whether the above process succeeds, the attempt to perform a "Reset HAN" operation shall be treated by the Device as a tamper breach, with a security log entry being written and an alert must be generated.

R7. No other critical refurbishment actions are carried out as part of the functionality for this Use Case. (Critical refurbishment actions are defined as part of the requirements for Use Case 004 as follows: "A critical refurbishment action is one that has (or includes) the effect of a command in [GBCS] that is critical".)

4.4 Responsibilities of CPA Test Labs

CPA Test Labs are responsible for establishing that the Device is compliant with the relevant CPA SCs and for providing a report to the CPA Scheme Operator (SOp) in line with normal CPA practice set out in the CPA Policies and Procedures. There is no requirement to provide the CPA Scheme Operator with a report of compliance against the Triage Security Requirements set out for this Use Case that are outside the CPA SCs.

CPA Test Labs should examine whether the requirements set out in Section 4.3 have been met and allow the Manufacturer to resolve any concerns about compliance.

In line with the arrangements between the Manufacturer and the CPA Test Lab, the Test Lab will provide the Manufacturer and the SSC with a letter, at a reasonable and proportionate cost, to confirm compliance or to explain any non-compliances with the requirements in 4.3. This will enable the SSC to provide assurance to Suppliers that the security requirements for Use Case 001 are met.

4.5 Impact for the SEC and CPA SCs

If the Use Case outlined in this guidance is implemented in line with the requirements set out above, it is not considered by the SSC that a change is required to the SEC or to the CPA SCs.

5. Security Requirements – Use Case 002 (Identifying Installed SMKI Certificates)

[Note: This Use Case is drafted as a standalone Use Case. It is accepted that multiple Use Cases could be triaged at the same time.]

This Use Case is applicable to GSME, ESME & SAPCs only.

5.1 Business requirement

Use Case 002 allows the Responsible Supplier to be identified by reference to the Public SMKI Organisation Certificate on the Device. This will, subject to commercial arrangements, allow the MAP to arrange the return of a Triaged Device to the Responsible Supplier for installation.

As with other Use Cases, the requirement arises from a number of aborted installations or where commissioning has not completed i.e. the Device is not yet registered on the DCC Smart Meter Inventory (SMI), or where commissioning has completed but other factors have resulted in the Device being returned e.g. following Change of Supplier.

Once a Device has been joined to the HAN and either partially or fully installed, the Device cannot be re-installed elsewhere without being reset to their former un-joined state. The disassociation from the HAN is addressed by Use Cases 001 and 003 (other Use Cases with a variation on the solution may also be considered in future). However, Use Cases 001 and 003 leaves the SMKI Organisation and Device Certificates unchanged but doesn't give the Triage Facility visibility of the Supplier to whom the Device should be returned.

A Triage Facility may be undertaking Triage of Devices on behalf of multiple Suppliers. Once the procedure to disassociate the Device from the HAN has been satisfactorily completed, the Triage Facility will need to return the Device to the Supplier whose SMKI Organisation Certificate is on the Device. At present, the Triage Facility has no means of identifying the relevant Supplier.

Suppliers and MAPS who have invested cost and effort in procuring and installing meters wish to be able to re-install such Devices which are capable of reuse to avoid unnecessary cost and wastage.

This Use Case explains the Security Requirements by different parties to enable the Responsible Supplier to be identified through the Public SMKI Organisation Certificate.

5.2 Security Constraints

The SSC has confirmed that, allowing Public information identifying the relevant SMKI Organisation Certificates from within the Public SMKI Organisation Certificate stored on the Device to be accessed and viewed, does not pose a security risk.

5.3 Requirements relating to DCC interaction

None. There is no interaction with the DCC for this Use Case.

5.4 Requirements for this use case

The information to identify the Supplier and relevant SMKI Organisation Certificates could be visible on the Device e.g. via a menu or could be machine readable by a factory system during Triage or could be accessible by the energy supplier.

5.5 Impact for SEC and CPA SCs

If the Use Case outlined in this guidance is implemented in line with the requirements set out above, it is not considered by the SSC that a change is required to the SEC or to the CPA SCs.

6. Security Requirements – Use Case 003 (HAN Reset via a User Interface)

This Use Case is applicable to GSME, ESME & SAPCs only.

6.1 Business Requirement

This Use Case has the same business requirement as Use case 001 (to enable a meter to be disassociated from a HAN) but allows a different solution to enable a meter to be disassociated from a HAN via a User Interface.

The business requirement arises from a number of aborted installations of meters that have not completed the Commissioning process. For this Use Case, 'not completed Commissioning' means that the Devices are not listed on the Smart Metering Inventory (SMI) as 'Commissioned' by the DCC. This could be caused by system outage/ consumer issues/delays during or shortly after installation. See Section 6.2 for the responsibility to ensure that the Device is correctly listed on the SMI.

Suppliers and MAPS who have invested cost and effort in procuring and installing meters wish to be able to re-install such meters which are capable of reuse to avoid unnecessary costs. It is for Responsible Suppliers to make arrangements with Triage Facilities to be able to identify which Devices meet the criteria of 'not completed Commissioning'.

Meters do not have the means to reset HAN information and will not join to a new HAN which, unless Triage takes place, the meter is prevented from being installed or having firmware upgraded via the normal DCC Service Request route.

The outcome from the Triage described in this Use Case is to achieve an appropriately authorised command (or set of commands) which is delivered locally through a User Interface. The commands will reset the HAN (disassociate the meter from its existing HAN and return it to a state whereby it can join a new HAN).

Use Case 003 provides an alternative method by utilising an already existing User Interface which does not require any further non-operational interfaces to be reactivated, nor would it require the potentially significant level of Device damage needed to reactivate such interfaces. Whilst there may be an outlay in both development and test of a User Interface based solution, no further tools should need to be developed and supported and the security controls required for the Triage Facility will be proportionately reduced.

6.2 Responsibilities of Suppliers

6.2.1 Decommissioning Devices prior to Triage:

There is no SMETS or GBCS requirement for a Device to know what status is listed for the Device on the DCC's SMI. The SMI status can show any of the following:
'P' = Pending; 'INC' = Installed Not Commissioned; 'C' = Commissioned; 'D' = Decommissioned; 'S' = Suspended; 'WLT' = Whitelisted; 'Recovery' = SMKI Recovery Event – User comms disabled; 'Recovered' = SMKI Recovery Event successful credential update.

It is a SEC obligation (see below) for the Responsible Supplier to ensure that the correct status is recorded on the SMI and this is not a matter for a CPA Test Lab to assess.

Smart Energy Code (SEC)
"H6. DECOMMISSIONING AND SUSPENSION OF DEVICES
Decommissioning
H6.1 Where a Device other than a Type 2 Device is no longer to form part of a Smart Metering System, then that Device should be Decommissioned. A Device may be Decommissioned because it has been uninstalled and/or is no longer operating (whether or not it has been replaced, and including where the Device has been lost, stolen or destroyed).

H6.2 Only the Responsible Supplier(s) for a Communications Hub Function, Smart Meter, Gas Proxy Function, Standalone Auxiliary Proportional Controller or Type 1 Device may Decommission such a Device; provided that only the Lead Supplier may Decommission a SMETS1 CHF.

H6.3 Where a Responsible Supplier (or, in the case of a SMETS1 CHF, the Lead Supplier) becomes aware that a Device has been uninstalled and/or is no longer operating, that User shall send a Service Request requesting that it is Decommissioned."

Suppliers will need to process any firmware upgrades required once the meter has been installed and commissioned in the new premises. For this to work, the version of the firmware in the meter to be pre-notified and reinstalled must not have been suspended.

It is for the Responsible Supplier to satisfy themselves that the Security Requirements have been met including tight control of relevant tamper protection arrangements during Triage.

6.2.2 Triage Facilities:

The Triage defined in this Use Case may only be undertaken in a Supplier or Manufacturer's Triage Facility, not at a consumer site. Where third party installers are involved, it is for the Responsible Supplier to satisfy themselves that the Security Requirements have been met. Access through the secure perimeter must conform with the requirements set out in SMETS2+ and will be different for ESME and GSME. [Note: the assurance required for Use Case 004 Triage Facilities i.e. SEC Section G 12 and additional Triage Build Standard requirements does not apply to Use Case 003]

Suppliers, MAPs or their Agents and Manufacturers must ensure that any Triage Facilities used for this Use Case are included within the scope of and are subject to proportionate but appropriate security controls and in line with general good industry security practice. For this Use Case, the minimum level of security control is compliance with ISO27001 and having access controls to the premises, being undertaken only by authorised personnel and with records kept of all actions taken.

It is for Responsible Suppliers to ensure that Triage for this Use Case is either carried out at Triage Facilities and with processes that are compliant with the security controls defined and assured through the Supplier's User Security Assessment or are carried out at a Manufacturer's premises and with processes that are compliant with the CPA Build Standard.

The Devices must be returned to either the Responsible Supplier whose SMKI Organisation Certificate is on the Device or to the MAP or to the MOP who is installing on behalf of the Supplier in line with the specific arrangements made for triage and refurbishment.

6.2.3 Security Assurance:

The Responsible Supplier has SEC obligations to ensure the security of Devices it installs and operates.

6.2.4 Re-installation:

This Use Case applies where the meter incorporates a mechanism via a User Interface that enables the Supplier, MAP or their Agent or the Manufacturer, to set the Device into a state that allows re-installation following an aborted or failed installation.

Responsible Suppliers will be permitted to reinstall meters but only if the meter's own key material and the SMKI Organisation Certificates retained in the meter memory have not been modified following removal from the consumer premises due to aborted or failed installations (as opposed to faulty behaviour identified in the meter). It is also assumed that the SMKI ACB certificates have not yet been replaced on the meter via DCC/DSP (a daily DCC process).

Re-installation under this Use Case will only be possible if the 'reset' meter is returned to the originating Supplier for installation in the original Network Operator area with the original Supplier SMKI Organisation Certificates and Network Operators Certificates in the meter.

Suppliers will need to process any firmware upgrades required once the meter has been re-installed and commissioned to the new premises. For this to work, the version of the firmware in the meter to be pre-notified and reinstalled must not have been suspended.

6.3 Responsibilities of Manufacturers

The Manufacturer is responsible for ensuring that the Device complies with the relevant CPA SCs and for providing documentation to the CPA Test Lab to clarify that any Triage capability outside the CPA SCs also meets the requirements set out below.

The additional requirements defined for this Use Case are to ensure that Responsible Suppliers are able to meet their SEC security obligations. The Manufacturer will therefore need to ensure that their arrangements with the CPA Test Lab enables the Test Lab to confirm compliance with the Use Case 003 requirements set out below and to provide the Manufacturer and the SSC with confirmation. This will enable Manufacturers and the SSC to provide assurance to Suppliers that the security requirements for Use Case 003 are met.

The Manufacturer will need to ensure that the Device incorporates a mechanism that enables the Supplier or Manufacturer (on behalf of the Supplier), to set it into a state that allows installation, following an aborted or failed installation.

Requirements to be demonstrated to the CPA Test Lab

It is likely that one or more persistent data items in the meter will need to be modified (e.g. reset) to achieve this. The Test Lab should review documentation that demonstrates that the following requirements have been met or demonstrated to be not applicable to the implementation

- **R1.** the User Interface does not allow for the removal of consumption data or any changes to the Device's current Private Keys, SMKI Organisation Certificates or firmware. Any modified data items must not include the Device's current SMKI Private Keys, SMKI Organisation Certificates or firmware version.
- **R2.** the command to reset the Device is only available on the Device's User Interface following physical access through the Secure Perimeter of the Device itself. Access through the secure perimeter must conform with the requirements set out in SMETS2+ and will be different for ESME and GSME.
- **R3.** this Use Case uses the same methodology currently used to allow Devices to display Security Logs, change batteries and test valve functionality (where applicable).

R4. the User Interface has the capability to issue a command for the Device to leave the ZigBee SEP Smart Metering HAN it has been operating on and then:

a. revert the Device to its original installation code; and
b. delete the Device Log to enable re-installation to join a new In-Home Display (IHD) and Pre-Payment Interface Device (PPMID);

and where applicable and reasonably practicable:

c. cause the Device to remove previous ZigBee network parameters; and
d. cause the Device to remove previous ZigBee application parameters.

R5. successful completion of the preceding points enables the meter to change its state from the HAN connected state to a ready to reinstall to a HAN state and any 'join network' functionality in the meter application is re-enabled or allow the normal join procedures to be activated.

Note: The meter must only modify a minimal amount of its data to release any previous HAN association and to delete the Device Log. This is to avoid unexpected side-effects on other SC-compliant functionality. If the Manufacturer is unclear about the impacts made to their specific implementation to accommodate such functionality, they should discuss the impact of the changes with the CPA Test Lab.

R6. the resultant state is compliant with GBCS expectations such as that defined by the ZigBee Stack Specification "05-3474" (e.g. revision 22), section 3.6.1.4.1 or any subsequent updated Stack Specification.

R7. regardless of whether the above process succeeds, the attempt to perform a "Reset HAN" operation shall be treated by the Device as a tamper breach, with a security log entry being written and an alert must be generated.

R8. With the exception of Use Case 003A (if implemented as part of Use Case 003), no other critical refurbishment actions are carried out as part of the functionality for this Use Case. (Critical refurbishment actions are defined as part of the requirements for Use Case 004 as follows: "A critical refurbishment action is one that has (or includes) the effect of a command in [GBCS] that is critical".)

6.4 Responsibilities of CPA Test Labs

CPA Test Labs are responsible for establishing that the Device is compliant with the relevant CPA SCs and for providing a report to the CPA Scheme Operator (SOp) in line with normal CPA practice set out in the CPA Policies and Procedures. There is no requirement to provide the CPA SOp with a report of compliance against the Triage Security Requirements set out for this Use Case that are outside the CPA SCs.

CPA Test Labs should examine whether the requirements set out in Section 6.3 have been met and allow the Manufacturer to resolve any concerns about compliance.

In line with the arrangements between the Manufacturer and the CPA Test Lab, the Test Lab will provide the Manufacturer and the SSC with a letter, at a reasonable and proportionate cost, to confirm compliance or to explain any non-compliances with the requirements in 6.3. This will enable the SSC to provide assurance to Suppliers that the security requirements for Use Case 003 are met.

6.5 Impact for SEC and CPA SCs

If the Use case outlined in this guidance is implemented in line with the requirements set out above, it is not considered by the SSC that a change is required to the SEC or to the CPA SCs.

6A. Security Requirements – Use Case 003A (Change of Mode after HAN Reset via a User Interface)

This Use Case is applicable to GSME, ESME & SAPCs only.

6A.1 Business Requirement

This Use Case supports and follows on from Use Case 003 only (HAN Reset via a User Interface).

The business requirement arises from the need to re-install Devices that were in Prepayment Mode when removed from premises and have subsequently been successfully Triaged under Case 003 to reset the HAN.

Whilst there is no SEC or GBCS requirement to change the mode to Credit prior to re-installation, the SSC has established and accepted that common operational processes used by energy Suppliers prevents installation in Prepayment Mode. The commissioning sequence typically requires a meter to be installed in Credit Mode and subsequently changed to Prepayment mode.

The Triage action described in this Use Case 003A is an additional, optional, part of Use Case 003 and is invoked as part of selecting the same User Interface option as Use Case 003. It adds a change of Payment Mode from Prepayment to Credit where the Device supports these functions.

Since this Use Case follows on from Use Case 003, the Device will already have been decommissioned

6A.2.1 Triage Facilities:

The Triage defined in this Use Case may only be undertaken in a Supplier or Manufacturer's Triage Facility, not at a consumer site. Where third party installers are involved, it is for the Responsible Supplier to satisfy themselves that the Security Requirements have been met. Access through the secure perimeter must conform with the requirements set out in SMETS2+ and will be different for ESME and GSME. [Note: the assurance required for Use Case 004 Triage Facilities i.e. SEC Section G 12 and additional Triage Build Standard requirements does not apply to Use Case 003]

Suppliers, MAPs or their Agents and Manufacturers must ensure that any Triage Facilities used for this Use Case are included within the scope of and are subject to proportionate but appropriate security controls and in line with general good industry security practice. For this Use Case, the minimum level of security control is compliance with ISO27001 and having access controls to the premises, being undertaken only by authorised personnel and with records kept of all actions taken.

It is for Responsible Suppliers to ensure that Triage for this Use Case is either carried out at Triage Facilities and with processes that are compliant with the security controls defined and assured through the Supplier's User Security Assessment or are carried out at a Manufacturer's premises and with processes that are compliant with the CPA Build Standard.

The Devices must be returned to either the Responsible Supplier whose SMKI Organisation Certificate is on the Device or to the MAP or to the MOP who is installing on behalf of the Supplier in line with the specific arrangements made for triage and refurbishment.

6A.2.2 Security Assurance:

The Responsible Supplier has SEC obligations to ensure the security of Devices it installs and operates.

The SSC advises Responsible Suppliers that this Use Case carries some risks for Suppliers in the event that the facility to Change Mode via a local interface becomes known to consumers operating

a meter in prepayment mode and who make use of debt facilities. In these circumstances, there is potential for a financial fraud risk to be realised and this risk is carried by Responsible Suppliers who should pay attention to alerts that then tamper-boundary has been breached.

6A.2.3 Re-installation:

This Use Case applies where the meter incorporates a mechanism via a User Interface that enables the Supplier, MAP or their Agent or the Manufacturer, to set the Device into a state that allows re-installation following an aborted or failed installation.

Responsible Suppliers will be permitted to reinstall meters but only if the meter's own key material and the SMKI Organisation Certificates retained in the meter memory have not been modified following removal from the consumer premises due to aborted or failed installations (as opposed to faulty behaviour identified in the meter). It is also assumed that the SMKI ACB certificates have not yet been replaced on the meter via DCC/DSP (a daily DCC process).

Re-installation under this Use Case will only be possible if the 'reset' meter is returned to the originating Supplier for installation in the original Network Operator area with the original Supplier SMKI Organisation Certificates and Network Operators Certificates in the meter.

Suppliers will need to process any firmware upgrades required once the meter has been re-installed and commissioned to the new premises. For this to work, the version of the firmware in the meter to be pre-notified and reinstalled must not have been suspended.

6A.3 Responsibilities of Manufacturers

The Manufacturer is responsible for ensuring that the Device complies with the relevant CPA SCs and for providing documentation to the CPA Test Lab to clarify that any Triage capability outside the CPA SCs also meets the requirements set out below.

The additional requirements defined for this Use Case are to ensure that Responsible Suppliers are able to meet their SEC security obligations. The Manufacturer will therefore need to ensure that their arrangements with the CPA Test Lab enables the Test Lab to confirm compliance with the Use Case 003 and Use Case 003A requirements set out below and to provide the Manufacturer and the SSC with confirmation. This will enable Manufacturers and the SSC to provide assurance to Suppliers that the security requirements for Use Case 003 and Use Case 003A are met.

The Manufacturer will need to ensure that the Device incorporates a mechanism that enables the Supplier or Manufacturer (on behalf of the Supplier), to set it into a state, including Change of Mode to Credit that allows installation, following an aborted or failed installation.

Requirements to be demonstrated to the CPA Test Lab

The CPA Test Lab should review documentation that demonstrates that the following requirements have been met or demonstrated to be not applicable to the implementation. This is in addition to confirming the requirements for Use Case 003 (section 6.3 above)

R1. The change of payment mode preserves the data identified in Use Case 003 R1.
R2. The change of payment mode preserves the Billing Data Log.
R3. Error cases handled by the device must include failure to change the payment mode during UC003A (whether detected at the time of the change or on restart of the device), and the handling must identify the failure as part of the UC003 result. Such errors should be logged.
R4. The change of payment mode as part of Use Case 003 is not available as a separately selectable action and cannot be carried out separately from the other Use Case 003 actions.

R5. No other critical refurbishment actions are carried out as part of the functionality for this Use Case. (Critical refurbishment actions are defined as part of the requirements for Use Case 004 as follows: “A critical refurbishment action is one that has (or includes) the effect of a command in [GBCS] that is critical”.)

6A.4 Responsibilities of CPA Test Labs

The CPA Test Lab responsibilities described in section 6.4 above also apply to Use Case 003A. Where Use Case 003A functionality is included in a report to the CPA Scheme Operator (e.g. an ESR or Assurance Maintenance Report), then the implementation of a payment mode change should be noted in the report.

CPA Test Labs should examine whether the requirements set out in Section 6.3 and Section 6A.3 have been met and allow the Manufacturer to resolve any concerns about compliance.

It is noted that changing the payment mode of a meter to credit is a critical refurbishment action in the sense of DEV.8.M<004> (Require message authorisation for critical refurbishment actions) in *“CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions”*: “A critical refurbishment action is one that has (or includes) the effect of a command in [GBCS] that is critical”. Setting a payment mode to credit is a critical command (SME.C.C) for both ESME (ECS02) and GSME (GCS02). For clarity: the Use Case 003A change of payment mode as part of UC003 is treated as an exception to the rule in DEV.8.M<004> that critical refurbishment actions require message authorisation and that such actions can only be done using the mechanisms in Use Case 004. The exception applies only when the change is included as part of Use Case 003, and does *not* apply to any change of payment mode carried out using a separate command as part of Use Case 004.

6A.5 Impact for SEC and CPA SCs

If the Use case outlined in this guidance is implemented in line with the requirements set out above, it is not considered by the SSC that a change is required to the SEC or to the CPA SCs.

7. Security Guidance – Use Case 004 (ESME, GSME, SAPC Factory Reset)

This Use Case is applicable to GSME, ESME & SAPCs only.

7.1 Business Requirement

This Use Case was originally raised by MAPs to address the situation where ESME, GSME and SAPC Devices (excluding CH that are dealt with in Use Case 005), that may or may not have completed Commissioning, have been returned to the MAP or to the Supplier, and are not found to have any defects and need to be reset for re-installation. In these situations, 'have completed Commissioning' means that the Devices have been listed on the Smart Metering Inventory (SMI) as 'Commissioned' and 'not completed Commissioning' means that the Devices have not been listed on the SMI as 'Commissioned'.

Having reached this state, the Device must have established HAN communications, and so will no longer be using its factory set Install Code for communications. This means it is unable to join any other HAN.

In turn, this means that some or all of the following changes may have been applied to the Device's initial configuration, as applied during manufacturing:

- Changes to one or more of the Supplier, Network Operator or Access Control Broker Organisation Certificates (and, to the Transitional CoS Certificate);
- Generation of new Device private keys for one or both of the SMKI required key usages (Digital Signature, Key Agreement), and so issuance by the Device of corresponding Certification Requests;
- Provision back to the Device of the resulting SMKI Device Certificates, meaning that they are stored on the Device and the corresponding new private keys are in use;
- Updates to firmware;
- Joins to other Devices on the same HAN, so entries added to the Device Log; and
- Wider changes to SMETS required configuration data.

Additionally, the Device would have captured SMETS operational data from the period when it was operating, including consumption related information.

The business requirement arises from scenarios that could result from aborted installations of meters due to system outage/ consumer issues/ delays during or shortly after installation or when a Device has been returned to a MAP by a Supplier or returned to a MAP or Supplier by a meter installer e.g. Meter Operator (MOP) or Meter Asset Manager (MAM). Suppliers and MAPS who have invested cost and effort in meters wish to be able to re-install such meters which are capable of reuse to avoid unnecessary cost and waste.

Without Triage intervention, there is no means to reset HAN information or to remove or replace SMKI Certificates and / or daily or half-hourly consumption data to enable a Device to be un-joined from a previous HAN and joined to a new HAN by a Supplier willing to install such Triaged Devices. **Note:** The Measuring Instruments Directive (MID) requires meters to retain the cumulative consumption data and for this to be visible on the Device – see advice from the Information Commissioner's Office in Section 7.6 below.

The industry requirement is for the Factory Reset to be achieved without physically returning the Device to the Manufacturer, to avoid the costs incurred in the process and to avoid the complex logistics this often involves.

7.1.1 Current Constraint applying to Business Requirements

At present, the DCC is unable to recognise Device credentials if the Device Private Keys or DCC ACB Certificates have been changed during Use Case 004 Triage. For this reason, Manufacturers are asked to restrict changes of Device credentials as set out on Section 7.5.1 until further notice.

7.2 Background

The main differences from Use Cases 001 and 003 are that the Devices in Use Case 004:

- may have been Commissioned for varying lengths of time whereas Use Cases 001 and 003 have not completed Commissioning and therefore have relatively little information stored;
- will require independent assurance of the Triage Facility Provider as required by SEC Section G12 (unless the Triage is carried out by the Manufacturer in their development environment). **Note:** Manufacturers undertaking Triage of Use Case 004 Devices outside the development environment will also be subject to independent assurance required by SEC Section G12;
- will need to have SMKI Organisation Certificates replaced which requires additional security protection (changing SMKI Certificates are Critical commands in GBCS);
- will have variable amounts of consumption data and security log data recorded on the Device; and, as a result
- incurs higher security risks that require additional security controls and risk mitigations.

Whilst it is possible for Use Case 004 to be performed by a Manufacturer, the main industry requirement is for the Factory Reset to be achieved without returning the Device to the Manufacturer due to costs and complex logistics. However, there are higher security risks involved in replacing SMKI Organisation Certificates together with actions behind the tamper-protection boundary which leads to the requirement for appropriate security controls and assurance. These are needed to prevent a Compromise of the Device that could have an adverse impact on the wider smart metering system.

7.3 Security Characteristics

Recognising the potential impact on security, the NCSC has published specific CPA mitigations that apply to Use Case 004: *"CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions"*

It is essential that Devices with Use Case 004 functionality are assessed against those SCs by a CPA Test Lab approved by the SSC.

Note: an exception to the requirement for protection of messages causing critical refurbishment actions, as described in the Use Case 004 CPA SC updates, is defined for a change of payment mode to credit as part of Use Case 003A – see section 6A.4.

7.3.1 CPA Build Standard Extensions

The Manufacturer's Triage Tool and Triage System Interface are required to be compliant with the CPA Build Standard extensions set out in section 3.1 of the *"CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions".*

It has been clarified in Q3 and A3 of that document that CPA Certification of a Device containing Use Case 004 functionality can be evaluated at a different time to the evaluation of compliance of the Triage Tool and Triage System Interface with the CPA Build Standard extensions.

For this reason, Manufacturers must ensure that the CPA Test Lab provides a letter to enable the SSC to confirm compliance of the Triage Tool; and Triage System Interface. A template of the Letter required is provided in Appendix 1. This will enable the SSC to confirm compliance as part of the User Security Assessment of the Triage Facility Provided required by SEC Section G 12.

7.3.2 SSC Certificate confirming compliance with CPA Build Standard

To enable Triage Facility Providers to readily verify whether specific Triage Tools and Triage System Interfaces have received confirmation of compliance with the CPA Build Standard Extensions set out in the *"CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions"*, the SSC will publish a Certificate on the SEC website. A draft copy of the Certificate is provided in Appendix 2.

Note that the expiry of the Build Standard Extensions will align with the existing CPA Build Standard.

7.4 Components for Use Case 004 Triage

Where Device Triage is to be carried out in the Manufacturer's development premises that have already been assessed under the CPA Build Standard, the Triage Facility is required to be assessed against the 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 Manufacturer's Triage System is trusted to be a secure system operated by the Manufacturer, as part of its manufacturing capacity.

Where a Manufacturer undertakes Triage of Use Case 004 Devices in a facility/site that is not covered by the CPA Build Standard, then the SEC Section G12 assurance requirements will be necessary.

Where Device triage and refurbishment is to be carried out in the premises of a Supplier, a MAP or an Agent, the SEC Section G12 requires independent assurance that the SEC security controls in SEC Sections G1, G3 to G6, G7 and G8 are being met.

The components of Use Case 4 Triage include:

Manufacturer's Triage System: a secure IT system established and operated by the Manufacturer, as part of its Device manufacturing capability, which the Triage Facility Provider connects to using a Triage Tool and a Triage System Interface. The Triage System must be compliant with the requirements of the Commercial Product Assurance (CPA) Scheme Build Standard including the Triage extensions as defined in *"CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions"*.

Manufacturer's Triage Tool: 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. The Triage Tool must be compliant with the requirements of the Triage extensions to the NCSC CPA Scheme Build Standard as defined in *"CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions"*.

The Triage Tool must communicate with the Triage System at least at the start of every Triage session (see section 1.5 of *"CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions"* for the definition of a Triage session), during which the continued authorisation of the Triage Tool by the Triage System is established.

Manufacturer's Triage System Interface: a secure IPsec or TLS (as defined in SEC Section G12.9 and the SSC Guidance on Standards, Procedures and Guidance) Virtual Private Network (VPN) encrypted link provided by a Manufacturer in order to connect its Triage System to a Triage Tool at a remote Triage Facility, which provides authentication, confidentiality and integrity of communications. The Triage System Interface must be compliant with the requirements of the Triage extensions to the

CPA Scheme Build Standard as defined in *"CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions"*. **Note:** Manufacturers undertaking Triage of Use Case 004 Devices outside the development environment will also be required to use the Manufacturer's Triage System Interface and be subject to independent assurance required by SEC Section G12.

Triage Facility: secure premises operated by a Supplier, a MAP or their Agent, or a Manufacturer where Triage Activities are undertaken and subject to independent assurance required by SEC Section G12 (for Suppliers, MAPs and their Agents, or a Manufacturer operating a Triage Facility outside the facility/site covered by the CPA Build Standard), or the Triage extensions to the CPA Scheme Build Standard as defined in *"CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions"* (for Manufacturers operating a Triage Facility within the facility/site covered by the CPA Build Standard). The details of the assurance required by SEC Section G12 are explained in detail in Part 3 of the *"SSC Guidance for Device Security Assurance and Triage" – the Triage Security Controls Framework (TSCF).*

Device Triage Key: a symmetric cryptographic key used to unlock the triage mode on a Device, and optionally (as an alternative to using a Manufacturer Signing Key) to authorise Use Case 004 Triage commands, requirements for which are set out in *"CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions".*

Device Triage Interface: an interface within the Device, requirements for which are set out in *"CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions".*

Manufacturer Signing Key: an asymmetric cryptographic key optionally used as an alternative to the Device Triage Key for authorising Use Case 004 Triage commands, requirements for which are set out in *"CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions".*

7.5 Triaging a Device using Use Case 004

Once the configuration functions on the Device Triage Interface are unlocked, the Triage Systems can take the steps:

- that are equivalent to those in the manufacturing configuration process (except that the Device ID, ZigBee CBKE and Install Codes are not expected to be capable of re-configuration in this way)
- that are needed to allow it to join a new HAN; and
- that are permissible in relation to removing SMETS Configuration and Operational data relating to its prior installation, including in light of the prior ICO input.

Thus, the steps are those required to return the Device to a state where it can be re-installed.

Note: Any such steps must only be possible if properly authorised by the Manufacturer's Triage System and authenticated by the Device as being authentically from the Manufacturer's Triage System, as described in *"CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions"*.

The available Triage actions will always include removing any HAN specific details (such as the ZigBee PAN ID and TC Link Keys / associated Device IDs), so that the Device can join a new HAN. The resultant state must be compliant with GBCS expectations such as that defined by the ZigBee Stack Specification "05-3474" (e.g. revision 22), section 3.6.1.4.1 or any subsequent updated Stack Specification.

The Triage steps may also include some or all of the following, dependent on what is required to make the Device re-usable (see also section 7.5.1 for changes denoted by *):

- *Replacement of SMKI Organisation Certificates – there would appear to be no reason to constrain those which can be used, since post installation obligations on Suppliers mean that invalid certificates would require replacement of the Device (if correct certificates cannot be installed using normal installation processes).
- Installation of new Firmware, subject to the Manufacturer's Triage System only being capable of installing firmware that is currently on the CPL and which its manufacturing systems are capable of installing.
- Reversion to factory settings for SMETS Configuration Data items, including for Device Logs (so that details of Devices from a prior installation are not retained).
- *Regeneration of the Device key agreement and digital signature private keys, and so generation of new SMKI Certificate Signing Requests.
- Setting of the supply state required for re-installation.
- starting "It is noted that firmware installation during Triage may be…":
- During Triage, the existing security log and event log may be deleted. However, the CPA SC requires the tamper event from activation of Triage to be preserved: DEV.8.<M005> 'Locking triage mode' says that *"the product is required to preserve the tamper event representing breach of the tamper-protection boundary to use the triage interface… the device shall not delete this event from logs when re-locking triage mode".*
  ***see section 7.5.1 relating to guidance on changing Device credentials.**

It is noted that firmware installation during Triage may be significantly different from the OTA mechanism used in GBCS. In particular, it is not required (although it is allowed) to use a separate message type for activation of a firmware image downloaded during Triage. This is the reason for a difference in the definition of a critical Triage action in the CPA SC, compared to the critical commands defined in GBCS. In the GBCS OTA mechanism, there is no need for the firmware download itself to be treated as a critical action, because the activation is a critical command and the Device will only activate the stored firmware if that firmware has a hash value that is the same as the hash value in the activation command. However, if the firmware image replacement method in Triage does not use an activation message that is strongly (cryptographically) bound to the firmware image, then the image download itself must be treated as a critical action, which requires use of the Authorisation Key to authorise the action. If an image is downloaded in multiple messages, then authorisation may not be needed on every download message (e.g. the manufacturer hash of the reassembled image might be included only in the last message of a download), provided that the reassembled image is subject to an integrity and authenticity check by the device before it becomes active on the Device. The mechanism will be checked during the CPA evaluation to ensure valid authorisation is always required.

If the Devices are Triaged by or on behalf of the MAP, the Devices may be returned by the MAP for installation by any Supplier or MOP acting on behalf of a Supplier who is willing to accept and install the Triaged Devices. If the Devices are Triaged by or on behalf of a Supplier, they may be re-installed as appropriate.

7.5.1 Guidance on changing Device credentials

The DCC is currently unable to recognise certain Device credentials if the Device Private Keys or the DCC (ACB) Certificates have been changed during Use Case 004 Triage. Changing the Device Private Keys will mean the Device cannot be re-installed and changing the DCC ACB Certificates will lengthen the installation process for UC004 Triaged Devices. For this reason, Manufacturers are asked to follow the guidance below for Use Case 004 Triage until further notice.

Device Private Keys

Manufacturers MUST NOT change the Device Private Keys until further notice.

ACB Certificate:

The ACB Certificates in Trust Anchor cells 8 and 9 in the diagram below MUST NOT change until further notice:

TCoS or ECoS Certificate:

The Change of Supplier Certificate in Trust Anchor cell 10 can be changed without any impact on Use Case 004 Triage. However, for good practice, it is recommended to update the COS Certificate from the latest available DCC Manufacturing Pack.

Supplier Certificates:

The Supplier Certificates in Trust Anchor cells 3, 4 and 5 can be changed without any impact on Use Case 004 Triage but this will be a choice for Suppliers as is the case during manufacture. Some Suppliers may request no change or their own SMKI Certificates to be installed and others may request a current ACB Certificate. The Triage Facility Provider will need to agree the requirement with the Supplier.

Network Operator Certificates:

The Network Operator Certificates in Trust Anchor cells 6 and 7 can be changed without any impact on Use Case 004. However, for good practice and to avoid re-installation of the Device being restricted to the original Network Operator, it is advised to replace the Network Operator Certificates with an ACB Certificate from the latest available DCC Manufacturing Pack.

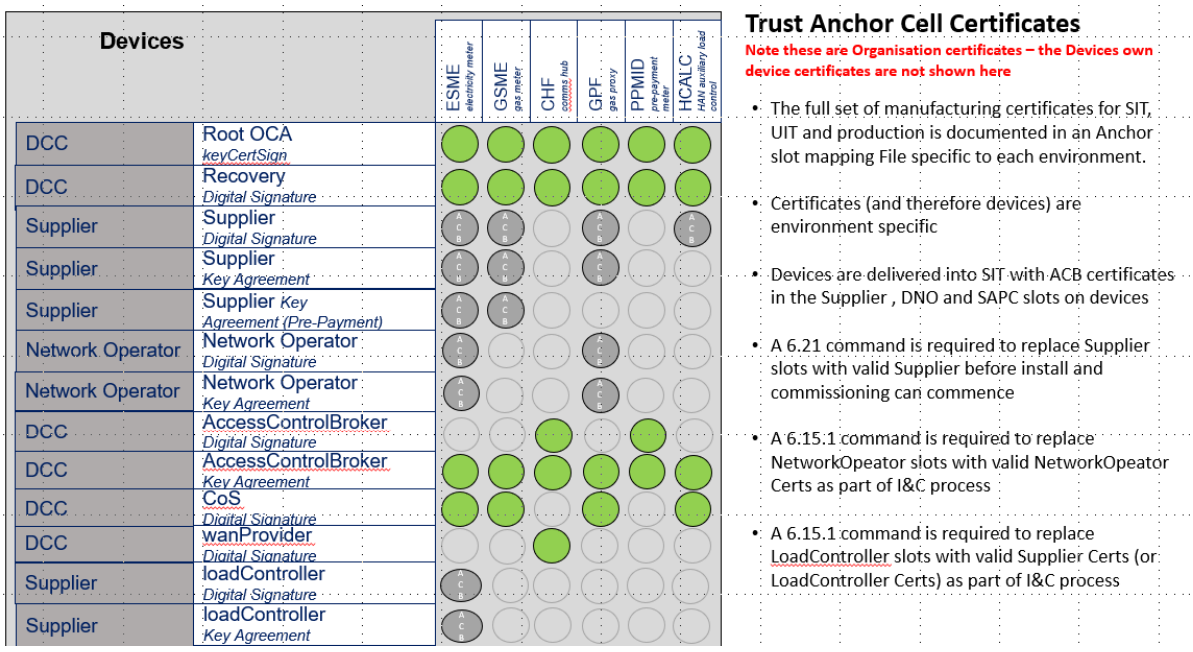
Summary: The Trust Anchor cell Certificates set out in GBCS section 4.3.2.5 should be applied during Use Case 004 Triage as shown in the right hand column of this diagram. Note that this diagram shows only Organisation Certificates; the Device Private Keys that MUST NOT be changed are not shown.

				Type of Device (✓= is required; empty = is not required)						
				ESME	GSME	CH (CHF)	CH (GPF[1])	HCALCS	PPMID	Use Case 004 Triage
	deviceType value(s)			1	0	2	3	4	5	
	TrustAnchorCellIdentifier									
No	**remotePartyRole**	**keyUsage**	**cellUsage**							
1	root	keyCertSign	management	✓	✓	✓	✓	✓	✓	
2	recovery	digitalSignature	management	✓	✓	✓	✓	✓	✓	
3	supplier	digitalSignature	management	✓	✓		✓	✓		SUPPLIER CHOICE
4	supplier	keyAgreement	management	✓	✓		✓			SUPPLIER CHOICE
5	supplier	keyAgreement	prePaymentTopUp	✓	✓					SUPPLIER CHOICE

[1] Supplier and Network Operator credentials on the Communications Hub (Gas Proxy Function) relate to the supply of gas only. These Trust Anchor Cells on a Communications Hub are still required and valid where there is no GSME connected to the SMHAN, but the stores should be populated with Access Control Broker certificates (so ensuring the Gas Proxy Function functionality, apart from Update Security Credentials, is inoperable)

6	networkOperator	digitalSignature	management	✓			✓			LATEST MANUFACTURING PACK ACB CERT
7	networkOperator	keyAgreement	management	✓			✓			LATEST MANUFACTURING PACK ACB CERT
8	accessControlBroker	digitalSignature	management			✓			✓	NO CHANGE
9	accessControlBroker	keyAgreement	management	✓	✓	✓	✓	✓	✓	NO CHANGE
10	transitionalCoS	digitalSignature	management	✓	✓		✓	✓		LATEST MANUFACTURING PACK COS CERT
11	wanProvider	digitalSignature	management			✓				

Summary (continued): Another representation of the Certificates to be populated in the Trust Anchor cells together with the Service Request Variants needed is shown below. Note that this diagram shows only Organisation Certificates; the Device Private Keys that MUST NOT be changed are not shown.



7.6 Consumption Data requirements (reproducing ICO advice)

The Measuring Instruments Directive (MID) requires meters to retain the cumulative consumption data and for this to be visible on the Device. However, meters undergoing a Factory Reset will have variable amounts of consumption data stored and the Triage Facility may choose to delete e.g. half hourly data from the storage.

The Information Commissioner's Office (ICO) have previously advised that consumption data should be treated as personal data. GDPR defines information to be considered to be personal data where a natural person can be identified, directly or indirectly. In connection with this Use Case, the ICO

has confirmed that consumption data continues to be considered by the ICO as personal data, due to the fact that it could be linked with other information to identify an individual.

The ICO draws attention to Recital 26 of the GDPR that explains that the GDPR should not apply to information that has been anonymised. Anonymous information is defined as data where the data subject is not or no longer identifiable. If, following Triage, there is no means of linking the meter to the original premises or consumer, then the MAP or Supplier should consider if the data that continues to be held within the meter is still classed as personal data or if it is now classed as truly anonymised.

If the data is anonymised, then as per Recital 26, the GDPR would not need to be considered in the context of repurposing the meters. However, if the data is still considered to be personal data, there would need to be consideration of the legislation.

The ICO also points out that Article 5(1)(e) of the GDPR explains that personal data should be kept in a form that permits identification of data subjects for no longer than is necessary, for the purposes for which the personal data are processed. This is the storage limitation principle.

In this context, the MAP or Supplier would need to demonstrate why retaining smart meter data, relating to a previous customer, is relevant when repurposing the meter if the information contained within is still considered to be personal data. In this context, the Measuring Instruments Directive (MID) will have a bearing.

The ICO points out that it would be good practice to document the consideration and this could be done in the form of a Data Protection Impact Assessment (DPIA).

Ultimately, it is for the Data Controller to assess the necessity and proportionality of the processing and to demonstrate that any risk involved is mitigated to an appropriate level but, producing a document such as DPIA would present a good opportunity to clarify the interaction between the MID and the GDPR.

7.7 Requirements relating to DCC interactions

Suppliers will need to be able to send appropriate “decommission” Service Requests (SRs) to the DCC once the meter has been removed from an installation at a consumer premises.

7.8 Impact for SEC and CPA SCs

This Use Case 004 has required changes to:

a) **The CPA SCs:** These have been updated to include: *“CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions”;*
b) **The CPA Build Standard:** This has been updated to include extensions to the CPA Build Standard Requirements, adding requirements for the Manufacturer’s Triage System, the Manufacturer’s Triage Tool and the Manufacturer’s Triage System Interface as set out in the *“CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions”*; and
c) **The Smart Energy Code (SEC):** has been modified to include Section G12 which sets out the arrangements for independent security assurance of Triage Facility Providers.

8. Security Requirement – Use Case 005 (4G) (4G and later generations) CH Factory Reset

This Use Case is applicable to CH (4G & later) only.

8.1 Business Requirement

This Use Case updates earlier guidance issued by the Department for Environment and Climate Change (now DESNZ) in 2015, covering the unlocking of a Triage interface on a Communications Hub (CH), under the title 'Messaging over non-operational interfaces under the Commercial Product Assurance (CPA) scheme'. This update covers **the Factory Reset of 4G and later generation Communications Hubs**, and references to '4G' here should be taken also to refer to later generations.

Where 4G CH Manufacturers include a Triage Interface as part of their Device to enable maintenance, diagnostics and refurbishment (and to reduce waste) where economically viable. This reflects a similar business requirement to that for Triage of meters in Use Cases 001-004 above and is based on providing an ability to deal with scenarios in which a CH has been removed from its installed premises (or has failed during the installation process, or requires other refurbishment action to make is suitable for installation) but may be suitable for reinstallation in different premises after the Device has been suitably refurbished. Any such refurbishment activity requires removal from the premises to the premises of a CH Triage Facility Provider (CHTFP) selected by the DCC and approved by the SSC where diagnostics, sanitisation of sensitive data, firmware overwrite, and regenerating key material can then be performed. The security assurance of the CHTFP will be provided by the DCC CIO operating in accordance with the DCC Security Controls Framework required by SEC Section G7.19(a) and G9.2(d)(iv).

8.2 Background

Triage activity on a CH is to be carried out only at the CHTFP's premises and uses an 'Unlock' command, which is delivered to the CH over a local physical interface which requires an 'activation' action[2] to make the interface usable for triage, and requires a tamper event if the CH is connected to a host ESME[3]. The CHTFP premises are required to implement physical, procedural and IT security measures to protect the integrity of the Triage process and its elements (including firmware images, keys and certificates, Unlock message generation, and data collected from Devices before sanitisation and overwriting). The Unlock command is specified in a 'DCC Use Case 005 Triage Specification Document', and is formatted in a similar way to a GBCS critical command, including a MAC created by the ACB and a signature by the wanProvider role. Applying the signature to the command will require that it is sent to the Data Service Provider (DSP) for anomaly detection/message validation as appropriate to ensure integrity.

The Unlock command must be replay-protected and cannot be future-dated.

[2] This could be, for example, settings of pins on the ICHI that are different from the normal operational settings (and different from the unpowered state).
[3] The tamper event may not arise if the CH has not been connected to an ESME (meaning that the local physical interface is already accessible). Logging of the tamper event will only take place if the CH has power at the time of the event.

After the CH has been unlocked, then a limited set of diagnostic commands are made available along with a data sanitisation command that removes any residual data from any previous installation of the CH, and a Triage command that will result in a complete overwrite of the CH memory. The diagnostic commands (which must not result in critical refurbishment actions) are used by the CHTFP to decide whether to proceed to the refurbishment step, based on determining whether the refurbishment is sufficiently likely to result in a Device that will then be suitable for reinstallation (e.g. whether it appears to be free of other underlying hardware faults).

If it is determined that the Factory Reset step is appropriate, then the refurbishment sequence is started. The refurbishment sequence consists of one or more messages to the 4G CH that can only be applied while Triage mode is unlocked, and which result in a complete overwrite of the Device firmware and configuration. Once the refurbishment sequence has started, the Device cannot function as a CH at any point before the successful completion of the refurbishment sequence. The complete overwrite will ensure that any data related to the previous installation of the Device is removed. If the refurbishment sequence fails then the Device must be securely destroyed (i.e. in a manner that prevents any risk of compromise of residual data). If the refurbishment sequence succeeds then all firmware and configuration data will have been replaced, resulting in a Device that is equivalent to a newly manufactured CH.

8.3 Security Characteristics

Recognising the potential impact on security, the SSC has published specific CPA mitigations that apply to Use Case 005: *"CPA Security Characteristic Triage interface updates to GSME, ESME, SAPC & CH SCs and CPA Build Standard Extensions".*

It is essential that Devices with Use Case 005 (4G) functionality are assessed against those SC mitigations by an approved CPA Test Lab.

8.4 Components for Use Case 005 Triage

CH Triage is to be carried out only in the Communications Hub Triage Provider's (CHTFPs) premises.

The components of Use Case 005 Triage include:

Comms Hub Triage Provider's Triage System: a secure IT system established and operated by the CHTFP, typically as part of a designated reverse logistics handling function, and which connects to other systems to perform functions including at least:

- gather the correct inputs necessary for refurbishment (e.g. firmware and certificates to be used), and validate their integrity and authenticity
- communicate with the target CH to obtain its identity details
- request Unlock messages (including MAC and signature) from the DCC
- deliver Unlock messages to a target CH
- generate and deliver diagnostic and refurbishment sequence messages to a target CH
- confirm the final state of the refurbished CH.

Communication with the DCC system for Triage activities must use a secure Virtual Private Network connection (or suitable private connection) that includes mutual authentication and appropriate confidentiality, integrity and authenticity protection of the communications.

The Triage process makes use of existing DCC processes to obtain ACB MAC and wanProvider signature on Unlock messages and will require the CH to have the current ACB credentials and the current wanProvider credentials (but does not require keys or certificates additional to those in Trust Anchor Cells defined in GBCS)[4]. This requires a connection from the CHTFP to the DCC which can only be used for Comms Hub Triage. When a request for an Unlock message is received then the DCC must make a check that the target CH is recorded as being in a suitable state for Triage (i.e. not installed in consumer premises) – if the target CH is not in a suitable state then the MAC and signature for an Unlock message then the request for an Unlock message will be rejected by the DCC and no Unlock message will be provided to the CHTFP. The CHTFP shall not use Unlock messages received via any means other than the defined request functionality in the CHTFP System.

The connection to the target CH for Triage must use a local physical interface (i.e. one that requires the connecting entity to be locally, physically present within the CHTFP site approved for Use Case 005 Triage – this would include an optical interface or contact/wired interface but not an RF-based interface). Unlock messages received by the CH on any other interface must be discarded without processing.

The Unlock message for 4G CH Triage must be similar to a GBCS critical (SME.C.C) message with protection against replay, and must be subject to validation of the relevant properties as specified in the SC mitigations for unlocking triage mode on a 4G CH. The message code used must be distinct from all other message codes.

Processing of an Unlock message must generate an associated event that records the result of validating the message. This event must record the result of the validation (i.e. successful or unsuccessful) and must be distinct from other events used to record receipt and validation of other commands (i.e. it must be clear that they relate to unlocking Triage mode and not to any other event). It is permissible for this event to be recorded in a log other than those defined in GBCS, and in that case to be defined in the DCC Use Case 005 Triage Specification Document instead of GBCS.

8.5 Responsibilities of the DCC

Note that in addition to the specific items below, the DCC is responsible for supporting its role and actions in the triage and refurbishment process described in section 8.6 below.

[4] It is noted that the DCC will also need to have the current public key for the target CH in order to create a valid ACB MAC.

8.5.1 Decommissioning Devices prior to Triage

The DCC is responsible for the process to ensure that the notification of removal of the CH from its installation site (or other location) to the CHTFP site is recorded and to ensure that the CH status in the DCC's SMI is correctly updated to show that the Device is not installed and is in a de-commissioned state.

8.5.2 Responding to Unlock requests

The DCC is responsible for validating the request for an Unlock message (using a statement of target CH identity that has been signed by the target CH), including confirming that the target CH is recorded as being in a suitable state for refurbishment by the CHTFP, and supplying a valid Unlock message if (and only if) the validation checks are successful.

8.5.3 Supplying inputs for refurbished device

The DCC is responsible for supplying the CHTFP with the correct firmware and other content to be put onto the target CH during the refurbishment sequence.

8.5.4 Updating Device records after Triage

The DCC is responsible for updating their records for the target CH to reflect the notification from the CHTFP of the new Keys generated for the triaged Device (and any other updates to technical parameters associated with the target CH, removing any associations with a previous installed location), and for confirming the other Certificates present on the triaged Device.

8.5.5 Receiving and preserving downloaded logs

The DCC is responsible for receiving and preserving the logs that the CHFTP has downloaded from a target CH before the refurbishment sequence is executed.

8.5.6 Assuring the Triage and refurbishment process

The DCC is responsible for producing a 'Use Case 005 Triage Specification Document', and the DCC CIO is responsible for providing assurance in the Triage and refurbishment process via the DCC CIO annual assessment of DCC Service Providers (in accordance with the DCC Security Controls Framework required by SEC Section G7.19(a) and G9.2(d)(iv)).

8.6 Triage and refurbishment of a 4G CH using Use Case 005

8.6.1 Triage and refurbishment process

The Triage and refurbishment process is carried out by the Comms Hub Triage Facility Provider (CHTFP) as follows:

- The CHTFP prepares the target 4G CH for Triage, gathering the correct firmware image and configuration data to be applied (according to specification by the DCC);

- The CHTFP downloads and preserves the security and event logs from the target CH (and any other logs that may contain records of triage mode Unlock commands) and sends them to the DCC for storage, in accordance with SSC-approved policy;
- An Unlock message is requested from the DCC for the target CH, including MAC and signature as for a GCBS critical (SME.C.C) message;
- The Unlock message is sent to the target CH, leaving it in an unlocked state (if the CH rejects the Unlock message then CHTFP policy will define the approach to retrying and/or when a decision would be reached to securely destroy the target CH);
- Diagnostic commands are sent to the target CH to determine whether it is suitable for refurbishment;
- If the target CH is not suitable for refurbishment then it is securely destroyed by the CHTFP and records kept;
- If the target CH is suitable for refurbishment then the CHTFP applies the refurbishment sequence (using the new firmware image and configuration data), which also ensures the deletion of any sensitive data on the target CH (including consumption data as appropriate in section 8.7 below);
- If the refurbishment sequence is not successful then the target CH is securely destroyed by the CHTFP and the CHTFP notifies the DCC to update their status record for the target CH to reflect the destruction (and to prevent reuse of the device identifier);
- If the refurbishment sequence is successful then the CHTFP notifies the DCC to update their status record and configuration records for the target CH, and releases it for re-installation.

8.6.2 Additional rules

None of the commands used in Triage may be capable of future-dated invocation.
Any diagnostic commands available after unlocking must not perform any critical refurbishment actions.

Triage mode on the target CH is required to lock on any of the actions specified in the SC mitigations for locking triage mode on a 4G CH (see DEV.5.M<105> 'Locking Triage mode' in Section 5.1 of *"CPA Security Characteristic Triage interface updates to GSME, ESME, SAPC & CH SCs and CPA Build Standard Extensions"*). It must not be possible to install a 4G CH while Triage mode is unlocked: CH design must confirm that Triage mode can never be unlocked when a CH is subject of Install and Commission or Operational use.

The CHTFP is required to record the actions performed on the target CH (and to preserve a record of the connection between the old and new CH identities).

8.7 Consumption Data requirements (reproducing ICO advice)

See section 7.6 above for the ICO advice relating to the treatment of consumption data as personal data, and its relationship to GDPR. This advice applies to any consumption data on a CH.

8.8 Requirements relating to DCC interactions

The DCC is responsible for an efficient and well-defined Comms Hub Returns Process that ensures that only Decommissioned Devices are submitted for Triage and to update the SMI once the CH has been removed from an installation at a consumer premises and marked as decommissioned..
The DCC will ensure secure communications with the CHTFP to (including, but not limited to):

- enable the CHTFP to obtain the Unlock messages for a target CH that the DCC confirms is in an appropriate, non-installed state (including MAC and signature);
- enable the DCC to authorise the CHTFP to perform refurbishment when appropriate;
- enable the DCC to specify the appropriate firmware and configuration data to be used in refurbishment;
- enable the CHTFP to request signing of new device credentials, and enable the DCC to respond with signed credentials;
- enable the CHTFP to notify the DCC of the refurbished CH identity and configuration details (and of other results such as secure destruction of a target CH).

8.9 Impact for SEC and CPA SCs

This Use Case 005 (4G) has required changes to:

a) **The CPA SCs:** These have been updated to include CH refurbishment updates in *"CPA Security Characteristic Triage interface updates to GSME, ESME, SAPC & CH SCs and CPA Build Standard Extensions".*

d) **The Smart Energy Code (SEC):** No SEC changes are necessary but the DCC Security Controls Framework (DCC SCF) [see SEC Section G 7.19(a)] will include a requirement for the DCC CIO Security Assessment scope (approved by the SSC) [SEC Section G9] to ensure compliance with the processes for Use Case 005 set out in this SSC Guidance on Device Security Assurance and Triage.

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.
CHTS	Means the Communication Hub Technical Specification published in the SEC,

Term	Definition
CPA Device Certificate	An Assurance Certificate issued for the purposes of the CPA Scheme, which is issued by the CPA Scheme Owner based on a recommendation by the CPA 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 to be capable of CPA evaluations by the SSC, operating under the requirements of the CPA Policies and Procedures and with a 'CPA Test Lab Framework Agreement' with the CPA 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.
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

Term	Definition
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.
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 or TLS (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.

Term	Definition
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.

Appendix 1: Template Letter for a Test Laboratory to confirm Compliance with the CPA Build Standard of the Manufacturer's Triage System including Triage Tool and the Triage System Interface

[Insert Test Laboratory letterhead]

Note: This template is classified as 'Clear' until it is completed when it becomes 'Amber - Strict' as below:

This document is classified as **Amber-Strict**. Limited disclosure, recipients can only share this document on a strict need-to-know basis to the Device Manufacturer, the Device Manufacturer customers and/or partners, CPA Test Laboratories, NCSC and SSC to protect and prevent harm. The SSC will communicate a successful outcome to Triage Facilities Providers.

[Use CPA Test Lab Letterheaded paper] *[insert date of letter]*

To [*insert Manufacturer name],*

This letter confirms the outcome of the evaluation of the Device Manufacturer *[Insert the Device Manufacturer]* Manufacturer's Triage System, including Triage Tool and Triage System Interface against the CPA Build Standard Validation Requirements set out in section 3 of the "Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions".

Compliance was assessed for Triage of:
[state the relevant Device name(s) and type(s) – Note: This is not the internal CPA ID reference but the Device Model versions that can be identified on the CPL. Note separate Triage Tool assurance is not needed for individual Devices with Use Case 004 functionality but please state the specific Device Name(s) and Type(s) with relevant CPL entries that the Triage System supports covered in this Build Standard assessment]
using Triage System *[state name/identifier of the Triage System – this must be sufficient to distinguish it from any other triage system in use by the Manufacturer, e.g. if separate systems are used for ESME and GSME; version numbers are not required to be given*]
and Triage Tool *[state name/identifier of the Triage Tool – this must be sufficient to distinguish it from any other Triage Tool in use by the Manufacturer, e.g. if separate Triage Systems are used for ESME and GSME; version numbers are not required to be given*].

Compliance of the Manufacturer's Triage System has been assessed against CPA Build Standard [*insert version number*] with Requirements 1, 3, 4, 6, 7 and 10 based on the requirement extensions defined in "Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions" [*insert version number*] sections 3.1.1-3.1.6. The following table provides confirmation of the outcome of the assessment with any relevant comments (e.g. 'acceptable' or 'observation'). The table below is for specific outcome comments on the Triage Tool and Triage System Interface to reflect the requirements in Section 3.1.5:

CPA Build Standard Validation Requirement*	**Comments****
Requirement 1	

General extension of configuration items	
Requirement 3 General extension of configuration items	
Requirement 4 General extension of configuration items	
Requirement 6 General extension of configuration items Secure transfer of items to Triage System environment Secure transfer of items to Triage Tool Secure transfer of items to Triage Facility	
Requirement 7 General extension of configuration items Secure transfer of items to Triage System environment Secure transfer of items to Triage Tool Secure transfer of items to Triage Facility	
Requirement 10 Extension of testing to Triage Tool	

* [Note 1: the test evidence in the extension to Requirement 10 is intended to be provided by the Manufacturer rather than from testing by the test laboratory]
[Note 2: the extension of Requirement 10 requires additional explanation as below]

** [Note 3: the test laboratory may simply state 'requirements met' as the comment, unless there is some additional point to be noted. Examples of additional points might be: a variation in the Manufacturer's method of meeting one or more of the requirements in "Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions"; an additional obligation or action needed from other parties involved in the triage process; or an additional assumption made.]

Triage System Interface (Requirement 10) Additional explanation
Evidence has been provided to confirm that the Triage System Interface is a secure IPsec or TLS Virtual Private Network (VPN) encrypted link provided by the Manufacturer to connect its Triage System to a Triage Tool at a Triage Facility and provides authentication, confidentiality and integrity of communications.

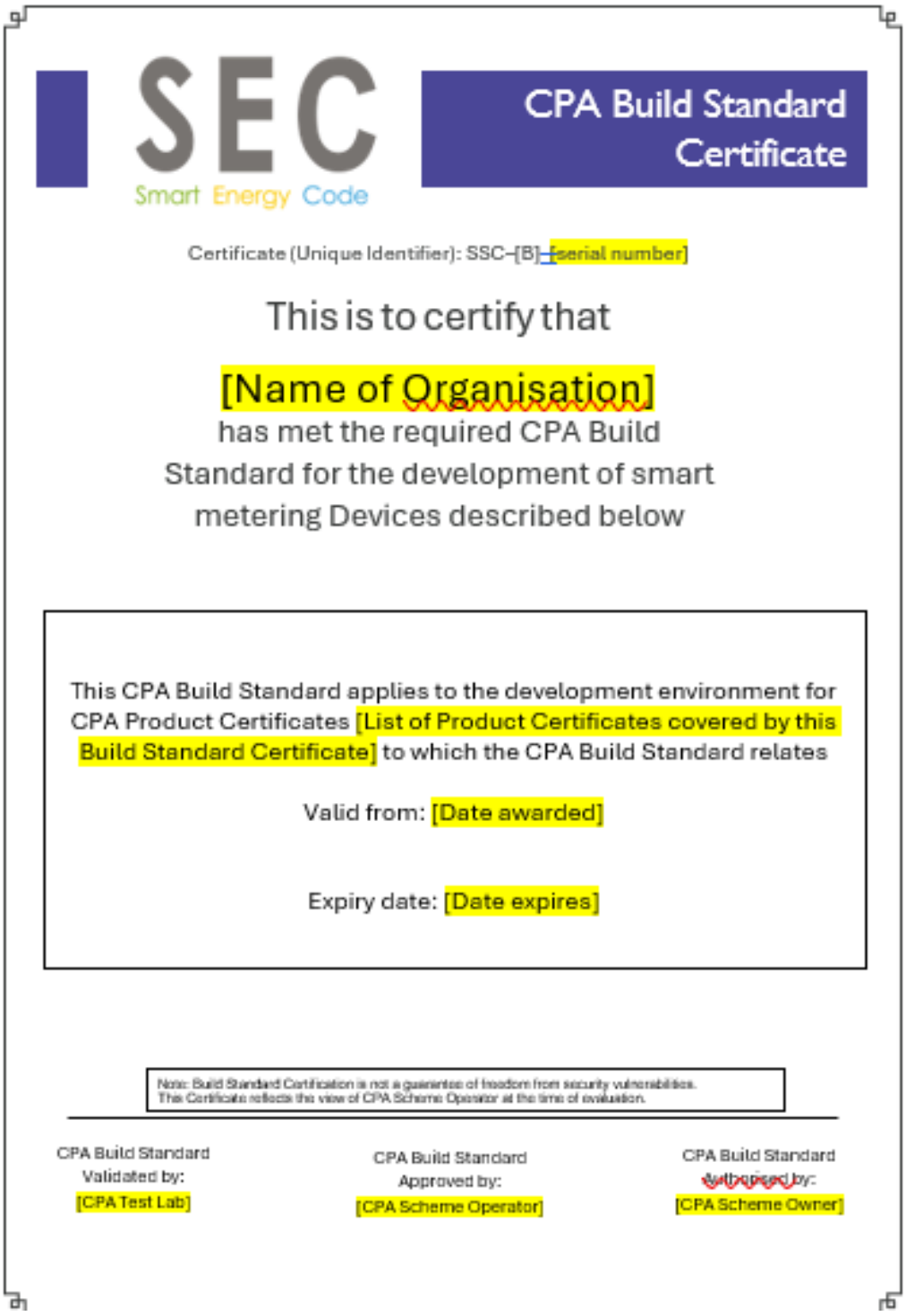
[*Note: Please provide an explanation, and any comments on findings, if an equivalent, alternative secure transport mechanism is used e.g. a secure, closed Factory network extended to the Triage Facility].*

Summary
Satisfactory evidence has been provided of compliance with the relevant CPA Build Standard Validation Requirements set out in section 3 of the "Triage interface updates to GSME, ESME, & SAPC and CH SCs and CPA Build Standard Extensions".

Yours

[Signed]
Authorised to sign on behalf of xx CPA Test Laboratory

Appendix 2: Certificate for SSC to publicise Build Standard Compliance



SEC
Smart Energy Code

CPA Build Standard Certificate

Certificate (Unique Identifier): SSC-[B]-[serial number]

This is to certify that

[Name of Organisation]
has met the required CPA Build Standard for the development of smart metering Devices described below

This CPA Build Standard applies to the development environment for CPA Product Certificates [List of Product Certificates covered by this Build Standard Certificate] to which the CPA Build Standard relates

Valid from: [Date awarded]

Expiry date: [Date expires]

Note: Build Standard Certification is not a guarantee of freedom from security vulnerabilities.
This Certificate reflects the view of CPA Scheme Operator at the time of evaluation.

CPA Build Standard Validated by:
[CPA Test Lab]

CPA Build Standard Approved by:
[CPA Scheme Operator]

CPA Build Standard Authorised by:
[CPA Scheme Owner]