CPA Security Characteristic

Triage interface updates to GSME, ESME, SAPC & CH SCs and CPA Build Standard Extensions

Version 3.0

About this document

This document describes the changes to SC mitigations that apply when smart metering devices include a triage interface used for operations related to restoring a product to a state ready for installation and commissioning. The first part (section 1 to section 3) deals with Use Case 004 functionality in GSME, ESME and SAPC devices; the second part (section 4 to section 5) deals with Use Case 005 functionality to perform similar operations for Communications Hubs. It also describes extensions to the Build Standard validation required for Manufacturer systems that support the operation of Use Case 004 in a Triage Facility. Build Standard validation extensions are not defined for Use Case 005. This document is not required to address the requirements for Use Cases 001, 002 and 003, which are described in [j]. The changes described here for Use Case 004 are not intended to affect the use of the triage interface for In-Service Testing or Disputed Meter Testing. It is intended that this document will remain as a standalone addition to the Device SCs until such time that a different approach is required and agreed. Incorporation of the information included in this document may be added to future versions of the specific SCs.

Capitalised terms are defined in the Smart Energy Code (SEC) or the SSC Guidance for Device Security Assurance and Triage (published on the SEC website - https://smartenergycodecompany.co.uk/) or are consistent with other CPA documentation.

Changes to the introductory text and appendices in the relevant SC are given in section 1, and changes to requirements in section 2. The changes to requirements are of two types:

a) Existing mitigations that have changes applied
b) New mitigations for triage functionality.

Extensions to the Build Standard for Manufacturer Triage System (and Triage Tools) that support Use Case 004 are given in section 3.

Document history

The CPA Scheme Owner may review, amend, update, replace or issue new Scheme Documents as may be required from time to time.

Version	Date	Notes
1.0	05 Apr 2022	First formal release based on cross-industry input.
2.0	09 Dec 2022	Updated to include threat statements for Triage interface mitigations and Build Standard extensions for the Manufacturer's Triage System including Triage Tools and the Triage System Interface.
2.1	25 May 2023	Updated to clarify DEV.8.M<001> & DEV.4.M927 (section 2.1), and Q3 & A3 (section 3.2). Updated reference [j].
3.0	30 Apr 2025	Updated to reflect change in Scheme Operator and to add Use Case 005 content as sections 4 and 5.

Contents

1 Changes to the ESME, GSME & SAPC SC Overview and Appendices

1.1 Additional Variant

The following additional variant text is included (in addition to any other variants that the SC may already include):

This document covers an optional triage interface variant which is used for the authorised refurbishment of a device to a state ready for the Installation and Commissioning of Use Case 004 functionality only.

1.2 Changes to High level functional components

The following diagram[1] replaces the figure showing the functional components of the device. The example below is based on the SAPC, but the change can be described as the addition of a functional component named ‘Triage interface’ which is marked ‘Triage capability ONLY’ because it is only applicable to a variant which implements Use Case 004 triage capability.

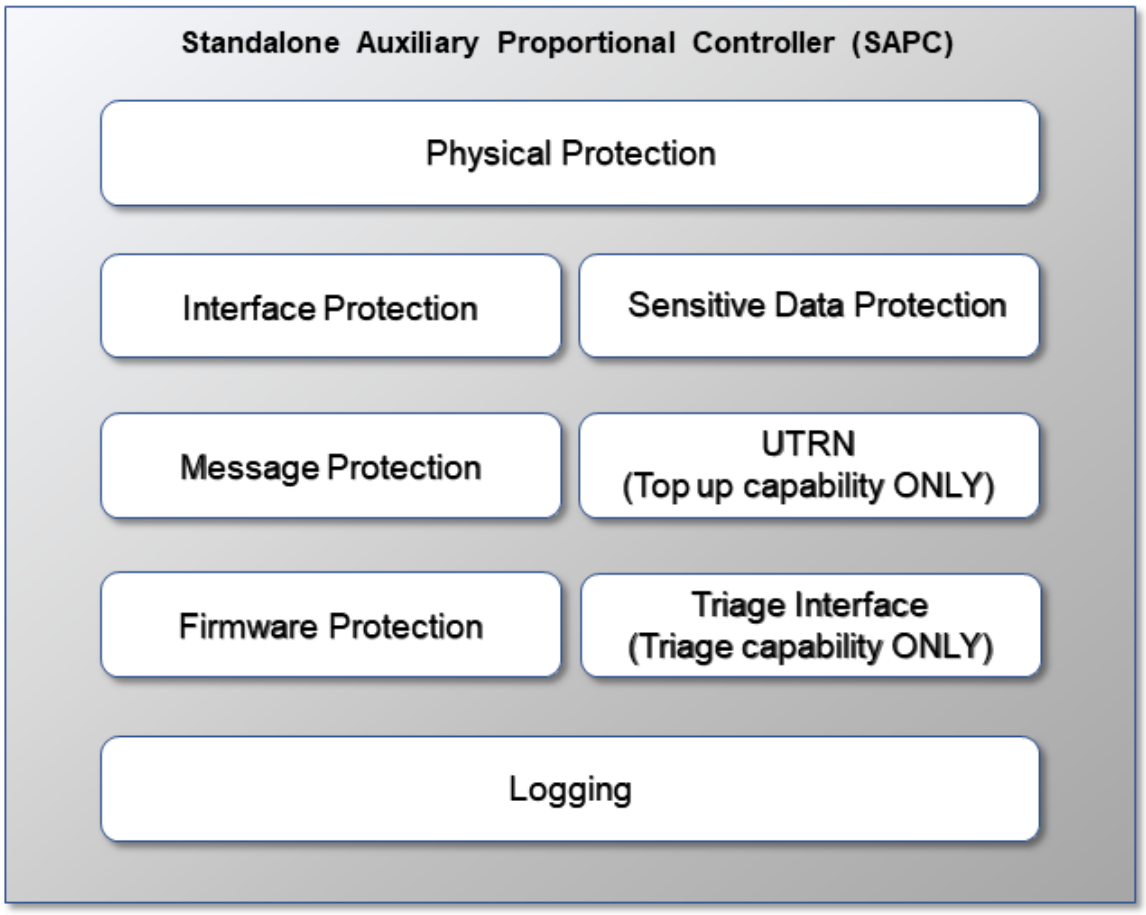

Figure 2: Functional components of an SAPC

[1] Note that numbering of replaced figures in this document reflects the numbering in the original SC to which the changes are being applied. Figure 3 in this document is additional and appears before figure 3 in the original SC.

The following text and figure are added to the description of the functional components figure, to describe the additional functional component.

- **Triage interface.** An optional interface that may be supported in order to allow execution of triage Use Case 004 on the Smart Metering Equipment as described in [j]. Triage Use Case 004 requires the tamper boundary to be breached, and authentication to be carried out based on a manufacturer key, before the triage interface can be activated and used. Messages that perform critical actions require further cryptographic authentication of individual messages. The use of triage mode and the triage interface for triage Use Case 004 is summarised in the figure below.

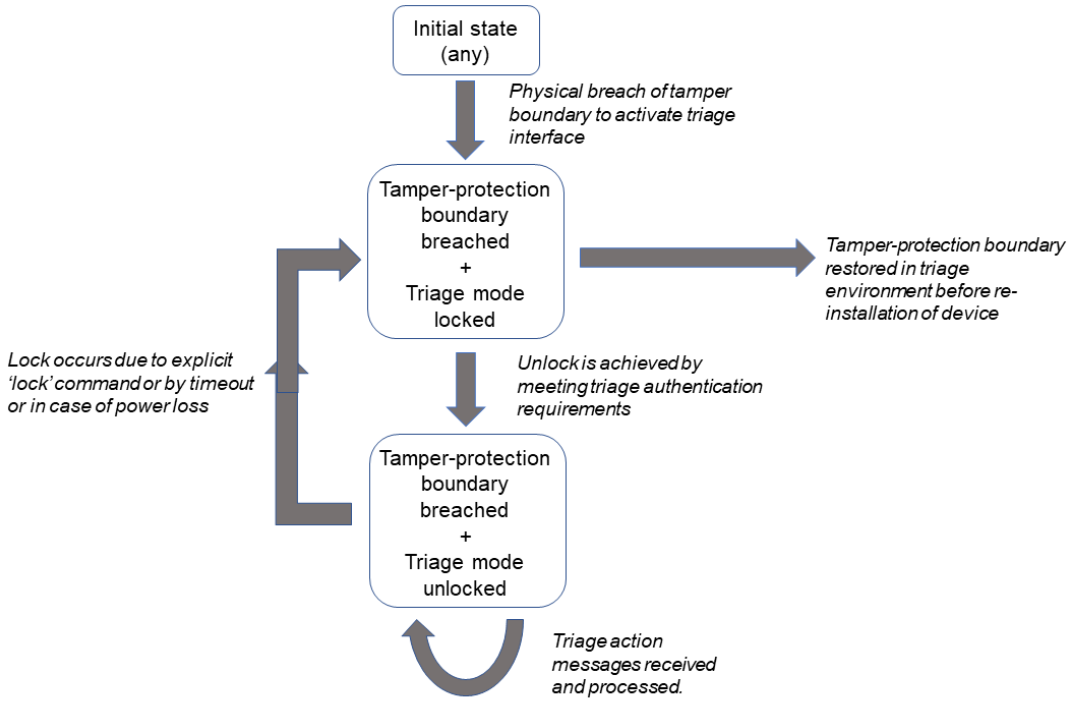

Figure 3: Use of triage mode and triage interface for triage use case 004

1.3 Changes to SC Appendix A (References)

The following references are added:

Label	Title	Location	Notes
[j]	SSC Guidance for Device Security Assurance & Triage Part 2: Security Requirements & Guidance for Approved Use Cases	https://smartenergycodecompany.co.uk/ssc-guidance-on-device-security-assurance-and-triage/	Provides surrounding system context for the device refurbishment process based on using a device's (optional) triage interface.

Label	Title	Location	Notes
[k]	HMAC-based Extract-and-Expand Key Derivation Function (HKDF)	https://datatracker.ietf.org/doc/html/rfc5869	The HKDF defined in RFC 5869 is used in the keyed hash implementation of triage message authorisation, which applies to devices with the optional triage capability

1.4 Changes to SC Appendix B (Glossary)

The following glossary entry is added:

Term	Definition
Triage interface	An interface that is optionally present on the device, meeting the requirements for the ‘triage interface’ functional component in this SC, and used for operations related to diagnosing the state of a product and restoring a product to a state ready for installation and commissioning. It is distinguished from a ‘non-operational interface’ and from an ‘additional interface’ by its integration with the refurbishment system described in [j] for performing critical actions.

1.5 Additional Appendix (Triage capability details)

The following appendix text is added:

<Appendix>.1 Symmetric and asymmetric cryptographic alternatives for triage use case 004

The triage interface functional component for the 'Triage capability' variant uses a common approach to unlocking triage mode, as described in DEV.8.M<003>, but allows alternative cryptographic methods for authorisation of commands performing critical refurbishment actions as described in DEV.8.M<004>. These alternatives are shown diagrammatically in the figures below.

The 'triage system' referred to in the figures is described in [j]. The symmetric alternative in figure 4 is explained further in section <Appendix>.2 below.

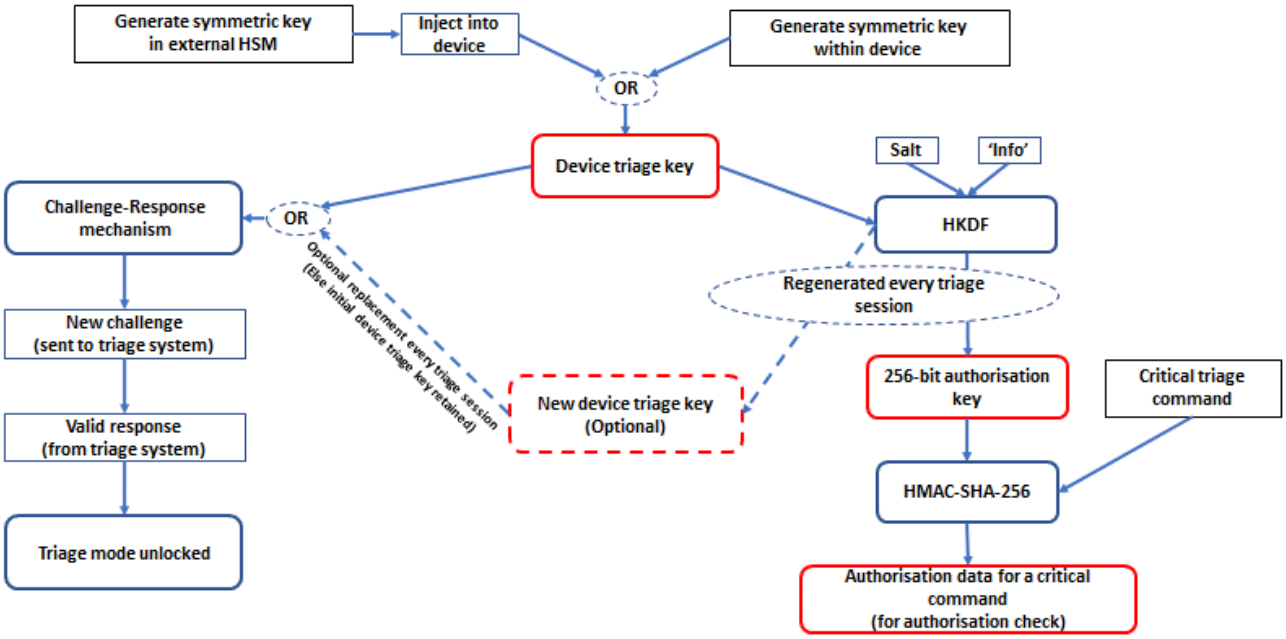

Figure 4: Triage mode unlock and critical refurbishment action authorisation – symmetric alternative

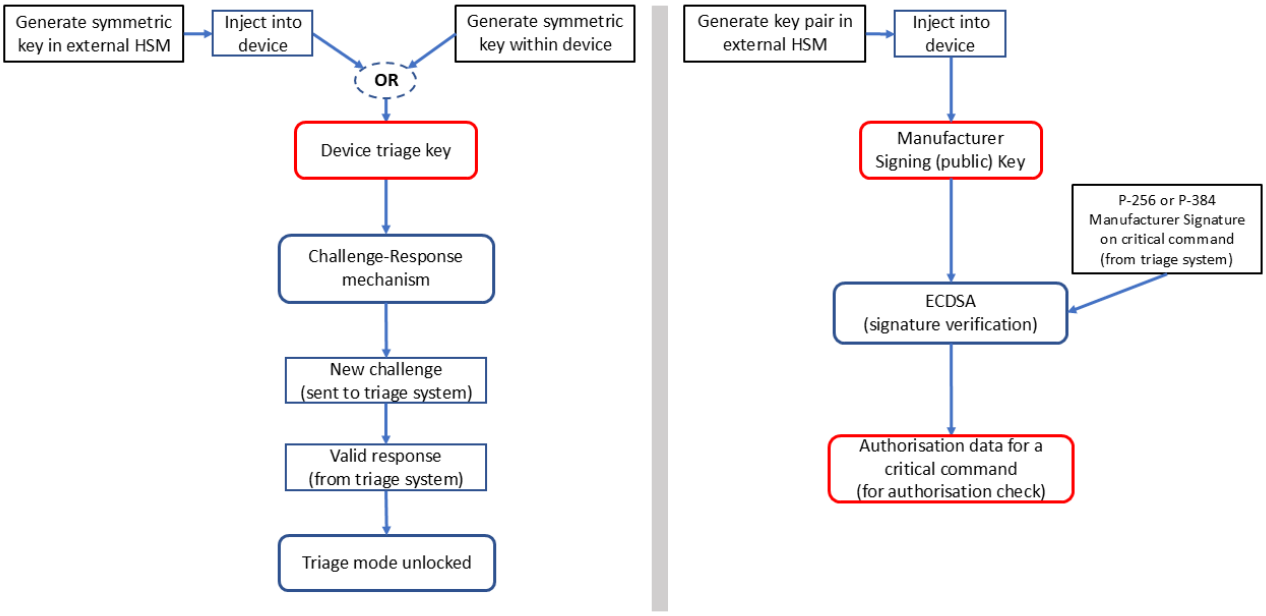

Figure 5: Triage mode unlock and critical refurbishment action authorisation – asymmetric alternative

<Appendix>.2 Using HKDF and HMAC-SHA256 to create authorisation data for a critical refurbishment action

This section uses notation and function names described in RFC 5869 [k].

The Manufacturer Keyed Hash method of authorisation in DEV.8.M<004> (Require message authorisation for critical refurbishment actions) uses the Hashed Key Derivation Function (HKDF) as defined in RFC 5869 [k]. The hash function to be used with HKDF must be HMAC-SHA256.

The variable length OKM output by HKDF-Expand can be used to produce either just the single 256-bit authorisation key required for DEV.8.M<004> (Require message authorisation for critical refurbishment actions), or both the device triage key for DEV.8.M<003> (Unlocking triage mode) and the authorisation key (for DEV.8.M<004>).

The authorisation key (for DEV.8.M<004>) must be different in every ‘triage session’ where such a key is required (where a ‘triage session’ starts with an unlock as in DEV.8.M<003> and ends with one of the locking events described in DEV.8.M<005>) and the HKDF must be used to generate it.

It is allowed (but not required) to generate a new device triage key (for DEV.8.M<003>) for every triage session. This means that the device triage key (for DEV.8.M<003>) may be the one loaded into a device during manufacture, one generated using HKDF during a previous triage session or one generated using HKDF during the current triage session.

The IKM input to HKDF-Extract needs to be unique to the device. This will avoid the compromise of one device enabling the compromise of another. The device triage key (for DEV.8.M<003>) loaded into a device during manufacture may be used as the IKM, or the IKM may use a different secret value provided it is of the same or greater cryptographic strength.

The salt input to HKDF-Extract could be a timestamp or could be based on the meter identifier and a counter, provided that the counter is guaranteed to increment for each use (e.g., if it is stored in the device then it must not be reset by other actions - including any that can be carried out during a triage session).

Authorisation data for a critical refurbishment action message is then generated as the output of an HMAC-SHA256 function that uses the HKDF generated 256-bit authorisation key as the key input, and the relevant message data as the text input.

1.6 Evaluating triage interfaces based on older SC versions

The changes specified in section 2 are defined using the mitigation text from the latest versions of the SCs (ESME & GSME SC v1.4 and SAPC SC v1.3). If there is a need to evaluate triage interfaces based on earlier versions of the SCs, then the entire updated versions of DEV & VER requirements in section 2 must be used (e.g. the version of DEV.2.M44 in section 2 below replaces any earlier version of DEV.2.M44 in an earlier SC version).

1.7 Assurance Maintenance of a meter with a triage interface

When a meter has been evaluated against the triage requirements in this document, then any future security impact assessments and Assurance Maintenance activities shall use the mitigation text from this document (including the updated versions of existing mitigations).

2 Changes to the ESME, GSME & SAPC Requirements

This section uses mitigation text from the SAPC SC to describe the changes applicable for triage capability: ESME & GSME SCs use the same text for the affected requirements except as follows (all of which can be seen in DEV.6.M944 (Privacy PIN Protection)):

- where a specific device name is used
- where a reference to an external document (e.g. [b]) may be different for each type of device
- where the SAPC may include the functionality as a variant (e.g. 'PIN capability'), whereas for ESME and GSME it is mandatory functionality.

For the avoidance of doubt: in any of these cases, the triage updates shown in this document must be applied to the text from the SC for the relevant device.

2.1 Changes to Development mitigations

The changes below describe updates to existing DEV mitigations. Where a DEV mitigation is not listed in the changes then it is included unchanged (i.e. absence of the mitigation below does not imply that it is deleted). The changes are specified by stating the entire new mitigation.

DEV.1.M863: Check authentic activation message required

This mitigation is required to counter causing unauthorised activation of authentic firmware

At Foundation Grade the product **is required to** activate downloaded firmware only on receipt of an authentic activation command.

(Firmware updates carried out over a triage interface are covered separately by the triage interface requirements in this Security Characteristic and are not subject to the requirements in this mitigation.)

At Foundation Grade the product **is required to** activate only the version of the firmware identified in the activation command.

At Foundation Grade the product **is required to** record the version of its current executing firmware and of any firmware updates currently stored.

DEV.1.M866: Check firmware update signature

This mitigation is required to counter unauthorised modification to a firmware update in transit

At Foundation Grade the product **is required to** check a secure signature over downloaded firmware on receipt of the firmware update.

If the signature check defined in [d, 11] fails then the firmware update shall be rejected. The failure shall be recorded in the Security Log as identified in [d, 16], and an alert shall be sent as identified in [d, 16] to the recipients specified in [d, 16].

(Firmware updates carried out over a triage interface are covered separately by the triage interface requirements in this Security Characteristic and are not subject to the requirements in this mitigation.)

DEV.2.M44: Data validation on untrusted input

This mitigation is required to counter exploitation of a non-operational interface through crafted input
This mitigation is required to counter exploitation of an additional interface through crafted input
This mitigation is required to counter exploitation of an operational interface through crafted input
This mitigation is required to counter exploitation of a triage interface through crafted input

At Foundation Grade the product **is required to** validate all inputs before attempting to process them.

For example, malformed and random inputs must not cause insecure behaviour.

In normal operation, when a message specified in [d] is delivered via any interface, data validation, as specified by [d] for the type of message in question, must be applied.

When a message not specified in [d] is delivered via any interface (in particular on the other types of interface as identified in DEV.*.M847 'Minimise interfaces'), data validation, as specified by the manufacturer for the type of message in question, must be applied. Where the device is capable of processing messages not specified in [d] the manufacturer must demonstrate the measures in place to ensure these cannot be used to undermine device security.

DEV.2.M847: Minimise interfaces

This mitigation is required to counter exploitation of a non-operational interface through crafted input
This mitigation is required to counter exploitation of an additional interface through crafted input
This mitigation is required to counter exploitation of an operational interface through crafted input
This mitigation is required to counter exploitation of a triage interface through crafted input

At Foundation Grade the product **is required to** ensure that only necessary protocols and services are available on the device.

The developer shall provide a list of all types of interface ('operational', 'non-operational', 'additional', and 'triage') present on the device. Where a device provides additional functionality, beyond that required to meet the functional requirements detailed in [b], [d] and [e], via additional protocols and services, the developer shall provide details of the functionality with an associated analysis that clearly indicates where security impacting functionality can occur. Requirements for protecting triage interfaces against unauthorised use are covered separately by the triage interface requirements in this Security Characteristic, but if the product provides a triage interface then the developer shall describe the messages that are sent and received over that interface. For other interface types, where 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 [d] that protect against unauthorised use of critical commands, using the same RBAC model. As a guide, "security impacting functionality" here is that functionality that would have the same material impact as a GBCS "critical command" (e.g. with the SME.C.C categorisation).

DEV.2.M950: Protect configuration

This mitigation is required to counter exploitation of insecure internal or external interfaces

At Foundation Grade the product **is required to** ensure that operational configuration changes can only be made using operational and triage interfaces.

Design information shall describe how the device prevents unauthorised changes to the configuration data. In particular it shall describe how configuration data is protected from unauthorised changes via any additional interfaces as identified in DEV.*.M847 'Minimise interfaces'.

DEV.3.M941: Security logging

This mitigation is required to counter making attack actions that leave no trace on the device

At Foundation Grade the product **is required to** ensure Sensitive Events, security failures and other security events are recorded in the Security Log.

The device shall record entries in the Security Log as identified in [d, 16]. Where the entry relates to a command, the command and outcome details shall be recorded in the entry. All entries shall include the UTC date and time of the event.
(For clarity it is noted that this requirement does not imply that all commands must be logged, only that relevant details must be included in all cases where a log entry is made).

At Foundation Grade the product **is required to** prevent modification or deletion of entries in the Security Log.

The device shall not allow entries in the Security Log to be modified, nor deleted other than by the normal overwriting action of the circular log buffer.

(Deletion of security logs carried out over a triage interface, after unlocking triage mode, is not subject to the requirements in this mitigation, but see also DEV.8.M<005> & VER.8.M<005>.)

At Foundation Grade the product **is required to** provide capacity for at least 100 entries in the Security Log.

If the developer is logging events in the Security Log beyond those identified in [d, 16], they shall provide a rationale that the size of the Security Log is sufficient for normal operation, to reduce the risk of entries being overwritten before they have been retrieved.

DEV.4.M140: Smooth output of Entropy Source with approved PRNG

This mitigation is required to counter prediction of randomly generated values due to insufficient raw entropy reaching the PRNG

At Foundation Grade the product **is required to** ensure that all random data used originate from a PRNG that is seeded by an approved entropy source.

The device design information shall include a description of how the output from all Entropy Sources and their associated PRNG can generate sufficient entropy for all keys and random numbers used in the product's regular operation (and triage functionality, if supported) including, where applicable, demonstrations of conformance to relevant standards such as the NIST SP800-90 series.

Note: The PRNG implementation may be based on standards other than the NIST SP800-90 series if it is believed they provide an equivalent level of security; if so, the rationale for this will need to have been agreed with the CPA Authority beforehand.

Device design information shall also describe how the entropy in PRNG's state will persist for any power-loss / device restart scenarios.

For more details about which key pairs need to be generated by the product, see [d, 4].

DEV.4.M853: Prevent unauthorised changes to future-dated actions

This mitigation is required to counter future-dated actions not being carried out at the specified time
This mitigation is required to counter unauthorised addition, modification or removal of a future action

At Foundation Grade the product **is required to** carry out relevant future-dated actions at the time specified.

The device design information will describe why a future-dated command will execute at the future time, according to [d, 9], regardless of other events that the device is expected to encounter that could conceivably impact when a future-dated action may occur (such as the device rebooting or a clock change taking place).

When the device clock is updated it shall neither miss nor repeat actions previously stored for future action nor miss calendar-based events.

At Foundation Grade the product **is required to** ensure that only authentic messages can cause a future-dated command to be added.

The device shall ensure that a future-dated message can only be added by receipt of a message from a source that is authorised to send that message type.

At Foundation Grade the product **is required to** ensure that only authentic messages can cause a future-dated command to be deleted, replaced or modified.

The device shall ensure that a future-dated message can only be modified, replaced or cancelled by receipt of another message of the same type from a source that is authorised to send that message type, or on change of control of the device.

(Future-dated events may also be deleted as a result of triage, if triage capability is supported by the device.)

DEV.4.M855: Receiver replay check

This mitigation is required to counter interception and replay of messages

At Foundation Grade the product **is required to** check that messages are not actioned more than once.

The device shall protect against replayed messages causing the same action to be carried out more than once.

The mechanism for protection against replay is defined in [d, 4.3]. Only certain messages require the protection, as specified in the Use Cases in [d, 19], summarised in [d, Table 20]. However, a different anti-replay mechanism is used for Security Credential commands as defined in [d, 13], and for Pre-Payment Top-Ups as defined in [d, 14].

(Messages sent and received over a triage interface are covered separately by the triage interface requirements in this Security Characteristic and are not subject to the requirements from [d] in this mitigation.)

DEV.4.M913: Command, response and alert integrity protection

This mitigation is required to counter interception and modification of commands, responses or alerts

At Foundation Grade the product **is required to** protect authenticity of security credentials.

The device shall not allow unauthorised replacement or modification of stored security credentials.

(Messages sent and received over a triage interface are covered separately by the triage interface requirements in this Security Characteristic.)

At Foundation Grade the product **is required to** protect integrity of commands, responses and alerts.

Critical messages shall be protected by digital signature of the sender; critical and non-critical messages shall be protected by MAC using a key shared with the broker. If the MAC or signature on a message is not valid then that message shall be rejected by the recipient without executing the actions requested by the message, and without sending a response.

The device shall implement the detailed integrity protection requirements specified in [d, 4.3.3].

(Messages sent and received over a triage interface are covered separately by the triage interface requirements in this Security Characteristic and are not subject to the requirements in this mitigation.)

DEV.4.M927: Check only valid messages accepted

This mitigation is required to counter circumventing message signature protection by entering messages via other interfaces including user interface
This mitigation is required to counter creation of unauthorised commands
This mitigation is required to counter modification of stored data in the device

At Foundation Grade the product **is required to** validate user interface commands.

The device shall validate user interface commands to ensure the use of only well-defined command values and robustness against crafted user input.

Any command that fails a validity check shall be discarded without execution.

At Foundation Grade the product **is required to** verify that any message received on an additional interface is a valid message for that device from an authentic source that is authorised to perform the operation.

If there is any additional functionality provided in the device beyond that required to meet the functional requirements detailed in [b], [d] and [e], the developer must provide the evaluators with design documentation and a rationale to demonstrate that messages received are validated, authenticated and authorised using mechanism(s) that the evaluators determine to be suitably robust, and that the functionality available does not impact the security requirements in this Security Characteristic. In particular this shall address all additional interfaces identified in DEV.*.M847 'Minimise interfaces'.

In particular, the evaluators must ensure that any interface between an APC and the load is examined, as this is not specified in [b] or [d] and is likely to enable additional functionality.

Any message that fails a validity check shall be discarded without execution.

At Foundation Grade the product **is required to** verify that any message received on a triage interface is a valid message for that device.

If the device provides a triage interface, the developer must provide the evaluators with design documentation and a rationale to demonstrate that any messages received over it are validated, authenticated and authorised using mechanism(s) that meet the triage interface security requirements in this Security Characteristic. For clarity: messages received via the triage interface need to be validated according to the requirements in DEV.*.M44 'Data validation on untrusted input'; messages (other than those used to unlock triage mode) are only accepted on the triage interface after triage mode has been unlocked; and only messages that implement critical refurbishment actions require further authentication and authorisation of the individual messages via authorisation data that is specific to the message instance.

At Foundation Grade the product **is required to** verify that any message received on an operational interface is a valid message for that device from an authentic source that is authorised to perform the operation.

The device shall not accept messages that do not conform to those defined for the device in the Use Cases listed in [d, 19.3] and shall ensure that all messages are subject to the cryptographic and other validity checks in [d, 6.2.4], [d, 6.3.4].

This requirement includes messages received from a Hand-Held Terminal.

Any message that fails a validity check shall be discarded without execution.

The device shall not provide alternative methods of carrying out operations that avoid the need to establish authorisation.

DEV.4.M939: Enable update of security credentials

This mitigation is required to counter use of compromised security credentials

At Foundation Grade the product **is required to** enable remote update of security credentials.

The device shall provide the ability to update security credentials, and this shall be subject to the normal message security checks (according to the type of interface used), and shall be confined to authorised roles/sources only.

Update of each security credential shall be atomic (it shall either complete successfully with complete replacement of all parts of the relevant credential or else shall retain the old credential).

DEV.6.M944: (PIN capability ONLY) Privacy PIN Protection

This mitigation is required to counter an unauthorised request for display of personal data
This mitigation is required to counter replacing the Privacy PIN

At Foundation Grade the product **is required to** enable access to protected data and commands only after receipt of the correct Privacy PIN when Privacy PIN Protection is enabled.

If Privacy PIN Protection is enabled, the SAPC shall require entry of the Privacy PIN before allowing temporary access to the restricted display items annotated [PIN] in [b, 5.5.4] and the restricted User Interface Commands annotated [PIN] in [b, 5.6.2] including the commands to Set Privacy Pin and Disable Privacy PIN Protection.

The design documentation shall define the period for which temporary access is granted and provide a rationale for why it is appropriate.

Note that Privacy PIN Protection may be disabled remotely by an authorised remote party.

(The Privacy PIN, and whether Privacy PIN Protection is enabled, may be reset as a result of triage, if the device supports triage capability.)

The changes below define additional new mitigations associated with the new ‘Triage interface’ functional component.

DEV.8 - Development >> Triage interface

DEV.8.M<001>: (Triage capability ONLY) Characterisation of triage interface

This mitigation is required to counter undocumented uses of the physical triage interface

At Foundation Grade the product **is required to** identify all uses of the triage interface.

Device design information shall identify and describe the triage interface in physical and logical terms. This shall include description of any use of the relevant physical interface for purposes other than triage use case 004 (e.g. if it is used also for triage use cases 001 and/or 002). This may be combined with the description of interfaces for DEV.*.M847 ‘Minimise interfaces’.

Where the triage interface is used for other triage use cases (i.e. other than triage use case 004) then evaluation of the functional requirements of these other use cases (e.g. against requirements in [j]) is not included as part of the CPA evaluation. However, any messages accepted on the triage interface other than for triage use case 004 in [j] shall require: (a) breach of the tamper boundary before use of the triage interface, (b) unlocking of triage mode before acceptance of the messages; (c) justification that they cannot be used to undermine device security; and (d) shall be validated according to the requirements in DEV.*.M44 ‘Data validation on untrusted input’.

References to the triage interface and triage mode in other requirements in this SC shall be understood to apply to its use for triage use case 004 specifically.

DEV.8.M<002>: (Triage capability ONLY) Location of triage interface

This mitigation is required to counter undetected connection to triage interface

At Foundation Grade the product **is required to** ensure that use of the triage interface requires breach of the tamper-protection boundary.

Device design information shall describe how the triage interface is accessed and activated, and shall show that the design requires the tamper-protection boundary to be breached (and consequently an event to be logged in the Security Log and an alert generated) before the triage interface can be unlocked and used.

DEV.8.M<003>: (Triage capability ONLY) Unlocking triage mode

This mitigation is required to counter unauthorised access to the triage interface

At Foundation Grade the product **is required to** ensure that it has received and successfully validated a response to a challenge before unlocking triage mode.

Triage mode on the device shall initially be locked.

Note: For the purposes of triage capability, some inputs to the device may be delivered other than by the messaging interface (e.g. using buttons on a user interface). In this case, the requirements on validation and acting on messages still apply to that input, but any requirement applicable only to the presence of a messaging interface (e.g. fuzz testing) does not apply to that input.

At Foundation Grade the product **is required to** ensure that unlocking triage mode requires strong authentication based on the device triage key.

The device triage key and cryptographic algorithm shall be at least as strong as 128-bit AES-ECB, and unlocking shall require receipt of a correct cryptographic response to a fresh challenge generated by the meter's entropy source in the authentication mechanism.

Compromise of the device triage key in one device shall not enable compromise of a different device.

If the device triage key is generated on the device then this generation must meet the requirements for key generation (e.g. entropy and PRNG aspects, and unique security data for the device) in other parts of this Security Characteristic.

The device triage key shall only be used for the purposes of performing triage operations.

At Foundation Grade the product **is required to** ensure that a response to a challenge message cannot be used to unlock triage mode more than once.

This is to prevent successful access to triage mode using a previously captured response to a triage unlock challenge.

DEV.8.M<004>: (Triage capability ONLY) Require message authorisation for critical refurbishment actions

This mitigation is required to counter unauthorised access to the triage interface

At Foundation Grade the product **is required to** accept triage use case 004 commands and critical refurbishment actions only while triage mode is unlocked.

A critical refurbishment action is one that has (or includes) the effect of a command in [d] that is critical (i.e. SME.C.C, or a variant message that is critical such as CS02b), or an action that downloads a change to the firmware present in the device. The developer shall provide a rationale that identifies all messages accepted by the device over the triage interface and shows that those leading to critical refurbishment actions meet the relevant requirements for authorisation.

At Foundation Grade the product **is required to** accept commands performing critical refurbishment actions only if the command includes valid authorisation.

Valid authorisation for a critical refurbishment action uses one of the cryptographic authorisation methods below, and the authorisation data must be specific to the message and the instance. This means that the authorisation data (e.g. a signature or keyed hash) must be cryptographically bound to the message instance and to all relevant parts of the message, so that it ensures that all parts and parameters of the critical refurbishment action have been authorised.

The method used for authorising critical refurbishment actions shall be one of the following types:

a) Checking an ECDSA signature created using a Manufacturer Signing Key and P-256 with SHA-256, or P-384 with SHA-384
b) Checking a Manufacturer Keyed Hash, which shall use HKDF (as defined in RFC 5869) and HMAC-SHA256, with at least 128 bits of secret data to generate a 256-bit authorisation key, and shall then use that authorisation key with HMAC-SHA256 and the message data to create the authorisation data for the message. The authorisation key shall be changed after each successful unlock of triage mode. (More details of this method are given in the appendices.)

For clarity:

- Deployed firmware may only be activated after an entire firmware image has been received and it has been authorised.
- The trigger to commence this authorisation may be via receipt of a separate activation message or when an entire firmware image has been received (either in a single message or multiple messages).
- In all cases, the rationale for authorisation of critical refurbishment actions shall describe how authorisation of the new firmware is achieved by the authorisation data.
- Responses from the device to messages received over the triage interface are not required to be signed.

DEV.8.M<005>: (Triage capability ONLY) Locking triage mode

This mitigation is required to counter unauthorised access to the triage interface

At Foundation Grade the product **is required to** support automatic re-locking of triage mode.

Relocking triage mode means that the device will not accept any further triage actions until triage mode has been successfully unlocked.

A device for which triage mode has been previously unlocked shall re-lock automatically after a period of inactivity not exceeding 15 minutes.

A device that loses power whilst triage mode is unlocked shall be in the triage mode locked state when it next restarts, so that any further triage actions first require triage mode to be successfully unlocked again.

The device may also support an explicit triage mode lock command that can be used before any automatic lock occurs.

At Foundation Grade the product **is required to** preserve the tamper event representing breach of the tamper-protection boundary to use the triage interface.

This means that the device shall not delete this event from logs when re-locking triage mode (other log events may be deleted during refurbishment). When the device is returned to normal operation, the triage-related tamper event is preserved as normal until the circular log buffer causes it to be overwritten.

DEV.8.M<006>: (Triage capability ONLY) Data deletion before reinstallation

This mitigation is required to counter compromise of consumer data during refurbishment
This mitigation is required to counter inappropriate future-dated actions following refurbishment

At Foundation Grade the product **is required to** ensure that any previous consumer data present in the device is deleted before reinstallation.

Deletion of the previous consumer data shall be by overwriting. Consumer data, considered personal data under the Data Protection Act 1998, shall be identified in the design information. (The deletion may exclude records of total quantities supplied that cannot be reset according to the Measuring Instruments Directive 2014/32/EU.)

At Foundation Grade the product **is required to** ensure that no future-dated commands are present in the device after triage mode is re-locked.

DEV.8.M<007>: (Triage capability ONLY) No installation with triage mode unlocked

This mitigation is required to counter undocumented uses of the physical triage interface

At Foundation Grade the product **is required to** ensure that the product cannot be installed while triage mode is unlocked.

2.2 Changes to Verification mitigations

The changes below describe updates to existing VER mitigations. Where a VER mitigation is not listed in the changes then it is included unchanged (i.e. absence of the mitigation below does not imply that it is deleted). The changes are specified by stating the entire new mitigation.

VER.1.M347: Verify update mechanism

This mitigation is required to counter causing unauthorised activation of authentic firmware
This mitigation is required to counter inability to load firmware updates required to patch security weaknesses
This mitigation is required to counter unauthorised modification to firmware in situ

At Foundation Grade the evaluator **will** validate the developer's assertions regarding the suitability and security of their update process.

The evaluator shall confirm the following:

- once a complete firmware update image has been received, its cryptographic protection will be validated and, if any checks fail, this will result in the image being rejected such that it cannot subsequently be activated (note: the checks will involve validation of the image's protective signature as per requirements in [d], along with any additional cryptographic checks performed on the image),

- a successfully received firmware update image, cryptographically validated as per the previous point, will not be activated if any of the cryptographic validations required by [d] on the associated Activate Firmware command fail this for both immediate and future-dated firmware activation scenarios,

- similarly, a successfully received and cryptographically validated firmware update image will not be activated if the 'manufacturerImageHash' field in the Activate Firmware command does not match the hash in the firmware update image – this again for both immediate and future-dated firmware activation scenarios,

- attempting to action an Activate Firmware command (either when the command has been received with no 'executionDateTime' specified or when it is time for a previously-received, future-dated command to be executed) will fail when there is no successfully received complete firmware update image – or one has been received but one or more cryptographic checks on that image have failed – and

- where a partially received firmware image – or a full image over which cryptographic checks have not been successfully performed – has been stored, this will not get activated if a device reboot occurs.

In addition to the above checks (that focus on ensuring a firmware update does not occur when not appropriate), the evaluator shall also confirm:

- the design for receiving and activating a firmware update, via authentic Distribute Firmware and Activate Firmware commands, is clearly documented and tested against by the developer, confirming that there are no obvious areas of uncertainty that could result in an unexpected failure to update the firmware,

- where a product does not incorporate anti-replay protection on the Activate Firmware message, product security is not undermined by a subsequent replaying of a valid Activate Firmware message (when used for either immediate or future-dated firmware activation).

(Firmware updates carried out over a triage interface are covered separately by the triage interface requirements in this Security Characteristic and are not subject to the requirements in this mitigation.)

VER.2.M80: Protocol robustness testing

This mitigation is required to counter exploitation of a non-operational interface through crafted input
This mitigation is required to counter exploitation of an additional interface through crafted input
This mitigation is required to counter exploitation of an operational interface through crafted input
This mitigation is required to counter exploitation of a triage interface through crafted input

At Foundation Grade the evaluator **will** perform fuzz testing of the available interfaces.

As per guidance in The Process for Performing Foundation Grade CPA Evaluations [a], structured fuzz testing is expected for all available interfaces, physical AND logical. Based on mandatory functional requirements in [d], the following two interfaces will always require fuzz testing: ZigBee and GBCS application layer messages.

For ZigBee, fuzz testing shall be performed on all the messages that can be received including those that are (a) unencrypted, (b) encrypted with the network key (and thus visible to all devices on the HAN) and (c) encrypted with an APS key set up to protect comms between the product and each other type of HAN device that is not required to be CPA-certified (at time of writing, PPMID, IHD and CAD).

When fuzz testing GBCS Application layer messages ('use cases'), mutations are expected to cover all parts of a message that the product will attempt to decode up to the point of authentication. The point of authentication for these messages (as relevant to [a], for smart metering equipment) is the point at which the protective crypt gets successfully validated (one or both of digital signature and MAC, dependent on the message type); any message decoding performed before this point (even just to check message well-formedness) will be in scope of GBCS Application layer fuzz testing. With this in mind, some message payload fuzz testing is expected (in addition to all the other sections of a GBCS Application layer message that can be present (i.e. GBT header, grouping header, signature field, etc), the amount of payload fuzz testing depending on how much of the message's payload gets decoded by the product before the point of authentication is reached. This minimum expectation is based on some GBCS application messages requiring content in the payload to be decoded and processed as part of the cryptographic validation process for the message type.

If the device includes a triage interface that implements triage use case 004 then this shall be subject to fuzzing up to the point of authentication. For triage use case 004 the relevant point of authentication is the successful unlock of triage mode – i.e. fuzzing shall cover all messages that are accepted before triage mode is successfully unlocked (this might include, for example, messages for other triage use cases).

In addition to the ZigBee and GBCS application layer interfaces, and (optionally) the triage interface, it is possible that the device may have additional interfaces beyond those defined in [d] that might be accessible to an attacker and hence also require fuzz testing. In particular all additional interfaces as identified in DEV.*.M847 'Minimise interfaces' require fuzz testing.

VER.4.M4: Evaluation/Cryptocheck

This mitigation is required to counter exploitation of a cryptographic algorithm implementation error

At Foundation Grade the evaluator **will** ensure all cryptographic algorithms employed for security functionality have been validated as per the "Cryptography Review" section in the CPA Foundation Process document.

The evaluator shall include in this activity a confirmation (by reference to relevant CAVP or equivalent certificates, or by activities in the course of the CPA evaluation) that cryptographic algorithms used by the PRNG (such as DRBG) have been independently validated for correctness.

Where cryptographic algorithms claim certification under CAVP (or equivalent external certification), then the evaluator shall confirm that this certification has been achieved for the relevant hardware/firmware/software components of the product, at the relevant version for the component. For cryptographic algorithms that are not certified using an external process, the evaluator shall confirm the correctness of the implementation by means of known answer tests, as described in the CPA Foundation Process document, Reference [a].

The cryptographic primitives used by the device shall be those specified in [d], including those primitives used by all UTRN validation functionality in the device, and those used by any triage capability present on the device.

VER.4.M855: Receiver replay check

This mitigation is required to counter interception and replay of messages

At Foundation Grade the evaluator **will** verify that messages are not actioned more than once.

The evaluator shall confirm by testing that the device correctly rejects messages with unacceptable count values relative to its current state, and that the device correctly generates count values for which it is responsible. The testing shall cover both commands for immediate execution and future-dated commands (where applicable).

The mechanism for protection against replay is defined in [d, 4.3]. Only certain messages require the protection, as specified in the Use Cases in [d, 19], summarised in [d, Table 20]. However, a different anti-replay mechanism is used for Security Credential commands as defined in [d, 13], and for Pre-Payment Top-Ups as defined in [d, 14].

Notes:

- Evidence is required for ALL commands that incorporate replay protection.

- When testing the anti-replay protection for Pre-Payment Top-Ups (where applicable), the evaluator shall verify that Pre-Payment Top-Up messages are rejected if its UTRN counter value (a) matches any value in the device's UTRN counter cache or (b) is lower than the lowest value in the device's UTRN counter cache. These tests will also cover all the interfaces over which the device can receive a UTRN.

(Messages sent and received over a triage interface are covered separately by the triage interface requirements in this Security Characteristic and are not subject to the requirements from [d] in this mitigation.)

VER.4.M939: Enable update of security credentials

This mitigation is required to counter exploiting incomplete update of security credentials
This mitigation is required to counter installation of an invalid certificate
This mitigation is required to counter use of compromised security credentials

At Foundation Grade the evaluator **will** verify that the update of a security credential is atomic.

The evaluator will test that the update of each security credential either finishes successfully with complete replacement of all parts of the relevant credential or else retains the old credential.

(This testing is not required for updates to credentials performed using the triage interface, if triage capability is supported.)

At Foundation Grade the evaluator **will** verify that, in addition to the general critical message validation checks described elsewhere, certificate path validation (CPV) always successfully completes, where required to do so by [d], before the validated replacement remote party certificate is installed.

The specific type of CPV required by [d] will vary according to the type of certificate and the operation of each type of CPV will be verified by the evaluator.

(This testing is not required for updates to credentials performed using the triage interface, if triage capability is supported.)

At Foundation Grade the evaluator **will** verify that, once validation checks have been successfully performed, the specified security credentials replacement will take place with subsequent product functionality confirming this.

The evaluator shall seek evidence to confirm that all the different types of remote party security credentials defined in [d, 4] (i.e. covering the different types of remote party role, keyUsage and cellUsage, appropriate for the product type) can be replaced, using all the different credentials replacement modes defined in [d].

Checks on subsequent product functionality should, as a minimum, confirm that the new credentials will be used for the associated cryptographic mechanisms, instead of the old ones. For instance, depending on the type of credential replaced, the following tests are suggested: (a) digital signature verification, (b) MAC authentication + generation, (c) certificate path validation and (d) encryption + decryption of sensitive data.

(This testing is not required for updates to credentials performed using the triage interface, if triage capability is supported.)

VER.6.M917: Verify logical protection of security data

This mitigation is required to counter gaining access to security data in a single device (via either operational or non-operational interfaces)

At Foundation Grade the evaluator **will** confirm the protection of security data, such as cryptographic key material.

The evaluator shall confirm that:

- no sensitive key material (private asymmetric keys and any symmetric keys) can be exfiltrated from the product, and

- the following security related data cannot be modified, except as a result of certain authentic messages defined in [d] intended for the purpose: device security credentials, remote party security credentials, including anti-replay counters and (where applicable) the device's UTRN counter cache.

Note: This confirmation shall also take into account any documented product interfaces additional to [d] that have the potential to exfiltrate sensitive key material or modify security related data, including all additional interfaces as identified in DEV.*.M847 'Minimise interfaces'.

Actions performed using the triage interface, if triage capability is supported, are only required to be tested under this mitigation to ensure that the device triage key, and/or any secret data used to derive the device triage key, cannot be exfiltrated.

The changes below define additional new mitigations associated with the new 'Triage interface' functional component.

VER.8 – Verify >> Triage interface

VER.8.M<002>: (Triage capability ONLY) Location of triage interface

This mitigation is required to counter undetected connection to triage interface

At Foundation Grade the evaluator **will** confirm that use of the triage interface requires breach of the tamper-protection boundary.

VER.8.M<003>: (Triage capability ONLY) Unlocking triage mode

This mitigation is required to counter unauthorised access to the triage interface

At Foundation Grade the evaluator **will** confirm that unlocking triage mode requires strong authentication based on the device triage key.

This confirmation is based on performing tests with valid and invalid responses to challenge messages according to the design information.

At Foundation Grade the evaluator **will** confirm that a valid response to a challenge message is not accepted more than once by the device.

VER.8.M<004>: (Triage capability ONLY) Require message authorisation for critical refurbishment commands

This mitigation is required to counter unauthorised access to the triage interface

At Foundation Grade the evaluator **will** confirm that triage use case 004 commands and critical refurbishment actions are accepted and performed only if triage mode is unlocked.

This confirmation is based on demonstrating that available commands to perform triage use case 004 commands and critical refurbishment actions are rejected when triage mode is locked.

At Foundation Grade the evaluator **will** confirm that commands performing critical refurbishment actions are accepted and performed only if the command demonstrates valid authorisation.

VER.8.M<005>: (Triage capability ONLY) Locking triage mode

This mitigation is required to counter unauthorised access to the triage interface

At Foundation Grade the evaluator **will** confirm that the product automatically re-locks triage mode.

This shall include at least the following checks:

a) that the device will not accept any further triage actions until triage mode has been successfully unlocked
b) that the re-lock occurs within the time period stated in the design information
c) that if power is removed whilst triage mode is unlocked then the device triage mode is in the locked state when it next restarts
d) that if the device supports an explicit triage mode lock command then this does re-lock triage mode.

At Foundation Grade the evaluator **will** confirm that the tamper event representing breach of the tamper-protection boundary to use the triage interface has been preserved.

This is confirmed by observing the presence of the tamper event in the Security Log.

VER.8.M<006>: (Triage capability ONLY) Data deletion before reinstallation

This mitigation is required to counter compromise of consumer data during refurbishment
This mitigation is required to counter inappropriate future-dated actions following refurbishment

At Foundation Grade the evaluator **will** confirm that any previous consumer data present in the device is deleted before reinstallation.

This is confirmed by attempting to access consumer data that was known to be previously set to a different value than the 'deleted' value.

At Foundation Grade the evaluator **will** confirm that no future-dated commands are present in the device after triage mode is re-locked.

VER.8.M<007>: (Triage capability ONLY) No installation with triage mode unlocked

This mitigation is required to counter undocumented uses of the physical triage interface

At Foundation Grade the evaluator **will** confirm that the product cannot be installed while triage mode is unlocked.

3 Applying the Build Standard to ESME, GSME & SAPC Triage

3.1 Application of the Build Standard to the Manufacturer's Triage System including Triage Tools and the Triage System Interface

The extensions below apply to Manufacturers who are supporting Triage activities that require compliance with the CPA Security Characteristics for Triage Use Case 004, for GSME, ESME, and/or SAPC Devices. Requirements apply to the Manufacturer's Triage System, including the Triage Tool and Triage System Interface. As explained in Question 8 in section 3.2 below, these extensions apply only to Triage support provided by the Manufacturer from a facility that is within the scope of the main Build Standard validation (i.e. the validation applied to the development environment of the GSME, ESME and/or SAPC Device).

The extensions (when applicable) must be assessed and successfully validated before the Manufacturer's Triage System can be put into live operational use.

Affected Requirements: Requirements 1, 3, 4, 6, 7 & 10

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.
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.

The Build Standard evaluation therefore needs to include assessment of the Manufacturer's Triage System including the development of the Triage Tool and Triage System interface.

The extensions below apply the affected Build Standard Requirements to relevant artefacts and processes that are used to create and operate the triage capability as part of achieving the Build Standard goal of giving "confidence of a secure and well-understood triage capability".

3.1.1 General extension of configuration items (Requirements 1, 3, 4, 6, & 7)

Build Standard Requirements related to configuration management shall be extended to include the Manufacturer's Triage System. They shall also be extended to include artefacts such as the Triage Tool and Triage System interface.

3.1.2 Secure transfer of items to Triage System environment (Requirements 6 & 7)

The evaluators shall examine the Manufacturer's processes and procedures for transfer of configuration items from the development (and build) environment to the Triage System environment, to ensure that the correct versions are picked and that authentication, confidentiality, integrity, and authenticity (as required according to the item being transferred) are maintained at both ends of the transfer as well as during the transfer itself.

The processes for secure transfer of items shall include a secure store of such Device specific Triage information, supporting the secure storage and use of Device Triage Keys in a way that binds each key to the corresponding unique Device ID. There is a capability to cryptographically authorise Triage Tools, and to revoke such authorisation.

3.1.3 Secure transfer of items to Triage Tool (Requirements 6 & 7)

The evaluators shall examine the Manufacturer's ability to securely communicate with the Triage Tool over the Triage System Interface to a remote Triage Facility and to log all events and actions and retain these whilst the Device remains on the CPL.

The evaluators shall examine the communication mechanism between Manufacturer's Triage System and the Triage Facility to ensure it provides authentication, confidentiality and integrity of the communications.

3.1.4 Secure transfer of items to Triage Facility (Requirements 6 & 7)

Build Standard Requirements relate to the secure transfer of relevant tamper-protection seals and the Triage Tool.

The evaluators must examine the method of transfer of the relevant, approved replacement tamper-protection seals to the Triage Facility to secure the Device post-Triage to establish that checks are made to ensure they are only transferred to Triage Facilities approved by the Smart Energy Code (SEC) Security Sub-Committee (SSC).

The evaluators must examine the method of transfer of the Triage Tool to the Triage Facility to establish that checks are made to ensure it is only transferred to Triage Facilities approved by the Smart Energy Code (SEC) Security Sub-Committee (SSC).

3.1.5 Extension of testing to Triage Tool (Requirement 10)

The Manufacturer's processes shall include testing of the Triage Tool, to ensure that it is 'locked down' such that it can only be used for Triage purposes and cannot be given additional capability by an operator in the Triage Facility.

Testing that the Triage Tool can connect through to the Manufacturer's Devices and is the only mechanism through which the Triage System can communicate with a Device that is being triaged.

Each Triage Tool must be cryptographically authorised solely by the Manufacturer's Triage System and must have mechanisms to ensure that it can only be authenticated and operated by authorised Triage Facility personnel.

The Triage Tool must be tested to ensure that communication with the Triage System is required at least at the start of every Triage session (see section 1.5 of *"CPA Security Characteristic Triage interface updates to GSME, ESME, & SAPC SCs"* for the definition of a Triage session), during which the continued authorisation of the Triage Tool by the Triage System is established.

The use of multi-factor authentication and role-based access controls for the GUI log-on to ensure that only authorised operators in the Triage Facility are allowed access.

3.1.6 Evidence Expected

For each of the extensions above, evidence provided by the Manufacturer is expected to include description of processes and procedures covering the security of the Triage System, Triage Tool and Triage System Interface, including the aspects identified above for assessment.

3.2 Guidance on Applying Build Standard Requirements to Triage Use Cases: Questions and Answers

Q1: *Can the report for compliance with the Triage Use Case be combined with the Build Standard Verification Report (BSVR) or is a separate report required?*

A1: If Use Case 004 Triage capability is being evaluated as part of a new model/version evaluation, the Triage Build Standard Report can be included as a separate section of the full BSVR for clarity or can be provided as a separate report.

If the Triage capability is being evaluated as Assurance Maintenance to add the Triage capability to an existing CPA Certified Device, then a separate report is expected along the lines of a change to the development facility in standard CPA evaluation i.e. a condensed report looking at the delta required for Triage.

Q2: *How often does the Triage Build Standard compliance need to be reviewed?*

A2: Normal Build Standard refresh arrangements apply. The Agreed Interpretations section 3.5.6 suggests six questions that help to assess whether the Build Standard evaluation needs to be refreshed.

Q3: *Is it possible to do the Triage part of the BS independently of the Device evaluation?*

A3: Noting that some Manufacturers have made the case for getting a product with Triage capability CPA Certified before submitting the Triage System, Tool and System Interface, it can be done ‘as it happens’. It just needs an agreement between the Manufacturer and the Test Lab to ensure that the Build Standard extensions are applied before a Triage Facility starts to use the Manufacturer’s Triage System, Tool and System Interface.

Q4: *Does the Triage Build Standard require a site visit or can it be a desktop review of documentation?*

A4: Desktop review of documentation is expected rather than a site visit. A Test Lab may use a questionnaire to solicit the information required.

Q5: *The definition of ‘Triage Tool’ refers to ‘cryptographically authorised’. What is expected to evidence this?*

A5: The Triage Tool is expected to be configured such that the operator in the Triage Facility cannot affect the intended functionality. Therefore the Triage Tool must ensure authentication, confidentiality and integrity at the remote Triage Facility and must not allow local admin rights and no local capability to change any settings in the Triage Facility.

Q6: *Requirements 6 and 7 relates to the secure transfer of items to the Triage Facility. What is acceptable for secure transfer?*

A6: Firstly, the manufacturer should satisfy themselves that a Triage Facility has been approved for Triage of Use Case 004 by the SSC before sending the Triage Tool and any accompanying material.

Secondly, the transfer of passwords or other authentication material should be sent separately from the transfer of the Triage Tool.

Thirdly, the manufacturer should obtain an acknowledgement of receipt from the Triage Facility.

Q7: *Requirement 10 relates to testing of the Triage Tool. Does the Test Lab need to test the Triage Tool?*

A7: No. Documentary evidence of testing is acceptable.

Q8: *If the Manufacturer is undertaking Triage of Use Case 004 in the manufacturing facility, does the manufacturer fall under the independent assurance arrangements in the SEC Section G12?*

A8: If the Manufacturer is undertaking Triage of Use Case 004 in an existing or new manufacturing or development facility / site that is already or would be covered by the CPA Build Standard validation, then no additional site assurance is required other than the evaluation of triage extensions required in section 3.1 since that facility / site is trusted for manufacture or development. If the Manufacturer undertakes Triage of Use Case 004 in a Triage specific facility/site that does not perform manufacturing or development then compliance with the SEC Section G12 assurance requirements will be necessary.

Q9: *Requirements 6 and 7 relate to the secure transfer of relevant tamper-protection seals to the Triage facility. Which are the relevant tamper-protection seals to be checked by the evaluator?*

A9: The relevant tamper-protection seals that are checked by the evaluator are those that are normally applied to Devices before they are transferred from the manufacturing site. These include tamper-protection seals applied to operational, non-operational or additional interfaces that are breached for the purposes of triage. Checks do not have to be made for the tamper-protection seals of terminal covers where normal practice is that these are not fitted until installation.

4 Changes to the CH SC Overview and Appendices

4.1 Additional Variant

The following additional variant text is included (in addition to any other variants that the SC may already include):

This document covers an optional triage interface variant which is used for the authorised refurbishment of a device using Use Case 005 functionality to a state ready for Installation and Commissioning.

4.2 Changes to High level functional components

The following diagram[2] replaces the figure showing the functional components of the device. The change can be described as the addition of a functional component named ‘Triage interface’ which is marked ‘Triage capability ONLY’ because it is only applicable to a variant which implements Use Case 005 triage capability.

[2] Note that numbering of replaced figures in this document reflects the numbering in the original SC to which the changes are being applied. Figures 3 and 4 in this document are additional and appear before figure 3 in the original SC.

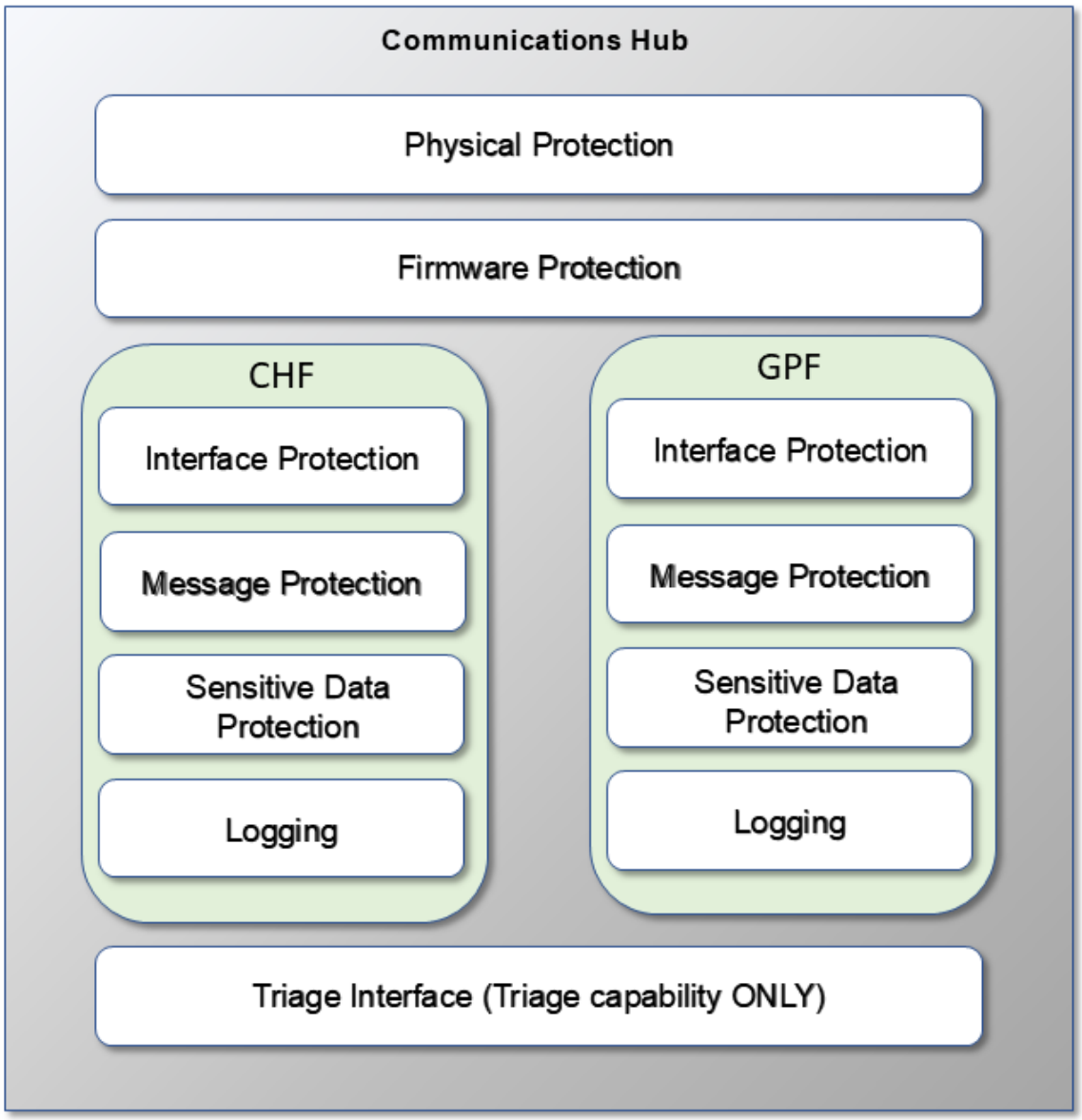

Figure 2: Functional components of a Smart Metering Communications Hub

The following text and figure are added to the description of the functional components figure, to describe the additional functional component.

- **Triage interface.** An optional interface that may be supported in order to allow execution of triage Use Case 005 on the Smart Metering Equipment as described in [j]. Triage Use Case 005 requires the tamper boundary to be breached, and authentication to be carried out based on Access Control Broker (ACB) and WAN Provider keys, before the triage interface can be activated and used. The use of triage mode and the triage interface for triage Use Case 005 is summarised in the figure below.

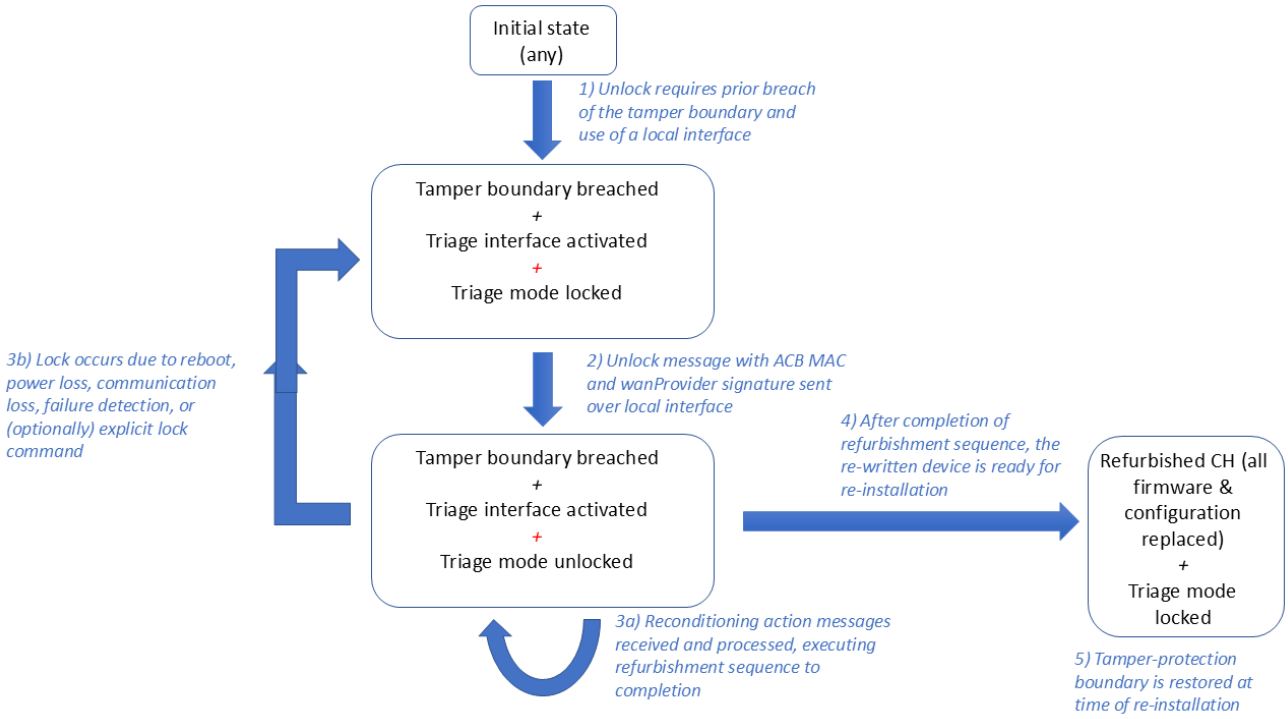

Figure 3: Use of triage mode and triage interface for triage use case 005 (4G)

As shown in the figure ('Use of triage mode and triage interface for triage use case 005 (4G)'), before the triage interface can be unlocked, the interface requires an 'activation' action as described for Use Case 005 in [j] in order to make the physical interface usable for triage. An example of this activation could be settings of pins on the ICHI that are different from the normal operational settings (and different from the unpowered state).

After unlock, diagnostic messages (which do not result in critical refurbishment actions, and do not update or modify the CH) may optionally be used to determine whether the CH is suitable for refurbishment. If the CH is not found to be suitable for refurbishment then it is subject to secure disposal. If the CH is suitable for refurbishment then the 'refurbishment sequence' is sent: this consists of one or more messages 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.

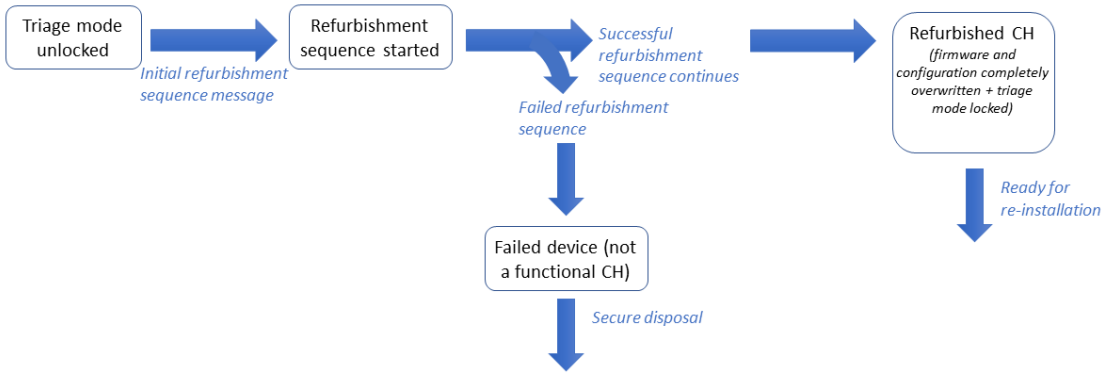

Figure 4: Refurbishment sequence for a 4G CH

4.3 Changes to SC Appendix A (References)

The following reference is added:

Label	Title	Location	Notes
[j]	SSC Guidance for Device Security Assurance & Triage Part 2: Security Requirements & Guidance for Approved Use Cases	https://smartenergycodecompany.co.uk/ssc-guidance-on-device-security-assurance-and-triage/	Provides surrounding system context for the device refurbishment process based on using a device's (optional) triage interface.

4.4 Changes to SC Appendix B (Glossary)

The following glossary entry is added:

Term	Definition
Refurbishment sequence	one or more messages that can only be applied to a CH while triage mode is unlocked, and which result in a complete overwrite of the CH device firmware and configuration.
Triage interface	An interface that is optionally present on the device, meeting the requirements for the 'triage interface' functional component in this SC, and used for operations related to diagnosing the state of a product and restoring a product to a state ready for installation and commissioning. It is distinguished from a 'non-operational interface' and from an 'additional interface' by its integration with the refurbishment system described in [j] for performing critical actions.

4.5 Assurance Maintenance of a CH with a triage interface

When a CH has been evaluated against the triage requirements in this document, then any future security impact assessments and Assurance Maintenance activities shall use the mitigation text from this document (including the updated versions of existing mitigations).

5 Changes to the CH Requirements

This section uses mitigation text from the CH SC to describe the changes applicable for triage capability.

5.1 Changes to Development mitigations

The changes below describe updates to existing DEV mitigations. Where a DEV mitigation is not listed in the changes then it is included unchanged (i.e. absence of the mitigation below does not imply that it is deleted). The changes are specified by stating the entire new mitigation.

DEV.*.1.M44: Data validation on untrusted input

This mitigation is required to counter exploitation of a non-operational interface through crafted input
This mitigation is required to counter exploitation of an additional interface through crafted input
This mitigation is required to counter exploitation of an operational interface through crafted input
This mitigation is required to counter exploitation of a triage interface through crafted input

At Foundation Grade the product **is required to** validate all inputs before attempting to process them.

For example, malformed and random inputs must not cause insecure behaviour.

In normal operation, when a message specified in [d] is delivered via any interface, data validation, as specified by [d] for the type of message in question, must be applied.

When a message not specified in [d] is delivered via any interface (in particular on the other types of interface as identified in DEV.*.M847 'Minimise interfaces'), data validation, as specified by the manufacturer for the type of message in question, must be applied. Where the device is capable of processing messages not specified in [d] the manufacturer must demonstrate the measures in place to ensure these cannot be used to undermine device security.

DEV.*.1.M847: Minimise interfaces

This mitigation is required to counter exploitation of a non-operational interface through crafted input
This mitigation is required to counter exploitation of an additional interface through crafted input
This mitigation is required to counter exploitation of an operational interface through crafted input
This mitigation is required to counter exploitation of a triage interface through crafted input

At Foundation Grade the product **is required to** ensure that only necessary protocols and services are available on the device.

The developer shall provide a list of all types of interface ('operational', 'non-operational', 'additional', and 'triage') present on the device. Where a device provides additional functionality, beyond that required to meet the functional requirements detailed in [b], [d] and [e], via additional protocols and services, the developer shall provide details of the functionality with an associated analysis that clearly indicates where security impacting functionality can occur. Requirements for protecting triage interfaces against unauthorised use are covered separately by the triage interface requirements in this Security Characteristic, but if the product provides a triage interface then the developer shall describe the messages that are sent and received over that interface. For other interface types, where 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 [d] that protect against unauthorised use of critical commands, using the same RBAC model. As a guide, "security impacting functionality" here is that functionality that would have the same material impact as a GBCS "critical command" (e.g. with the SME.C.C categorisation).

DEV.*.1.M950: Protect configuration

This mitigation is required to counter exploitation of insecure internal or external interfaces

At Foundation Grade the product **is required to** ensure that operational configuration changes cannot be made without using operational and triage interfaces.

Design information shall describe how the device prevents unauthorised changes to the configuration data. In particular it shall describe how configuration data is protected from unauthorised changes via any additional interfaces as identified in DEV.*.M847 'Minimise interfaces'.

DEV.*.2.M941: Security logging

This mitigation is required to counter making attack actions that leave no trace on the device

At Foundation Grade the product **is required to** ensure Sensitive Events, security failures and other security events are recorded in the Security Log.

The device shall record entries in the Security Log as identified in [d, 16]. Where the entry relates to a command, the command and outcome details shall be recorded in the entry. All entries shall include the UTC date and time of the event.
(For clarity it is noted that this requirement does not imply that all commands must be logged, only that relevant details must be included in all cases where a log entry is made).

At Foundation Grade the product **is required to** prevent modification or deletion of entries in the Security Log.

The device shall not allow entries in the Security Log to be modified, nor deleted other than by the normal overwriting action of the circular log buffer.

(Deletion of security logs carried out over a triage interface, after unlocking triage mode, is not subject to the requirements in this mitigation.)

At Foundation Grade the product **is required to** provide capacity for at least 100 entries in the Security Log.

If the developer is logging events in the Security Log beyond those identified in [d, 16], they shall provide a rationale that the size of the Security Log is sufficient for normal operation, to reduce the risk of entries being overwritten before they have been retrieved.

DEV.*.3.M140: Smooth output of Entropy Source with approved PRNG

This mitigation is required to counter prediction of randomly generated values due to insufficient raw entropy reaching the PRNG

At Foundation Grade the product **is required to** ensure that all random data used originate from a PRNG that is seeded by an approved entropy source.

The device design information shall include a description of how the output from all Entropy Sources and their associated PRNG can generate sufficient entropy for all keys and random numbers used in the product's regular operation (and triage functionality, if supported) including, where applicable, demonstrations of conformance to relevant standards such as the NIST SP800-90 series.

Note: The PRNG implementation may be based on standards other than the NIST SP800-90 series if it is believed they provide an equivalent level of security; if so, the rationale for this will need to have been agreed with the CPA Authority beforehand.

Device design information shall also describe how the entropy in PRNG's state will persist for any power-loss / device restart scenarios.

For more details about which key pairs need to be generated by the product, see [d, 4].

DEV.*.3.M853: Prevent unauthorised changes to future-dated actions

This mitigation is required to counter future-dated actions not being carried out at the specified time
This mitigation is required to counter unauthorised addition, modification or removal of a future action

At Foundation Grade the product **is required to** carry out relevant future-dated actions at the time specified.

The device design information will describe why a future-dated command will execute at the future time, according to [d, 9], regardless of other events that the device is expected to encounter that could conceivably impact when a future-dated action may occur (such as the device rebooting or a clock change taking place).

When the device clock is updated it shall neither miss nor repeat actions previously stored for future action nor miss calendar-based events.

At Foundation Grade the product **is required to** ensure that only authentic messages can cause a future-dated command to be added.

The device shall ensure that a future-dated message can only be added by receipt of a message from a source that is authorised to send that message type.

At Foundation Grade the product **is required to** ensure that only authentic messages can cause a future-dated command to be deleted, replaced or modified.

The device shall ensure that a future-dated message can only be modified, replaced or cancelled by receipt of another message of the same type from a source that is authorised to send that message type, or on change of control of the device.

(Future-dated events may also be deleted as a result of triage, if triage capability is supported by the device.)

DEV.*.3.M855: Receiver replay check

This mitigation is required to counter interception and replay of messages

At Foundation Grade the product **is required to** check that messages are not actioned more than once.

The device shall protect against replayed messages causing the same action to be carried out more than once.

The mechanism for protection against replay is defined in [d, 4.3]. Only certain messages require the protection, as specified in the Use Cases in [d, 19], summarised in [d, Table 20]. However, a different anti-replay mechanism is used for Security Credential commands as defined in [d, 13], and for Pre-Payment Top-Ups as defined in [d, 14].

(Messages sent and received over a triage interface are covered separately by the triage interface requirements in this Security Characteristic and are not subject to the requirements from [d] in this mitigation.)

DEV.*.3.M913: Command, response and alert integrity protection

This mitigation is required to counter interception and modification of commands, responses or alerts

At Foundation Grade the product **is required to** protect authenticity of security credentials.

The device shall not allow unauthorised replacement or modification of stored security credentials.

(Messages sent and received over a triage interface are covered separately by the triage interface requirements in this Security Characteristic.)

At Foundation Grade the product **is required to** protect integrity of commands, responses and alerts.

Critical messages shall be protected by digital signature of the sender; critical and non-critical messages that comply with [d, 4.3.3] shall be protected by MAC using a key shared with the broker. If the MAC or signature on a message is not valid then that message shall be rejected by the recipient without executing the actions requested by the message, and without sending a response. The device shall implement the detailed integrity protection requirements specified in [d, 4.3.3].

(Messages sent and received over a triage interface are covered separately by the triage interface requirements in this Security Characteristic and are not subject to the requirements in this mitigation.)

Where other commands provide functionality beyond that detailed in [b], [d] and [e], the developers must provide the evaluators with design documentation and a rationale to demonstrate that it doesn't impact the security requirements in this Security Characteristic.

DEV.*.3.M927: Check only valid messages accepted

This mitigation is required to counter circumventing message signature protection by entering messages via other interfaces
This mitigation is required to counter creation of unauthorised commands
This mitigation is required to counter modification of stored data in the device

At Foundation Grade the product **is required to** verify that any message received on an additional interface is a valid message for that device from an authentic source that is authorised to perform the operation.

If there is any additional functionality provided in the device beyond that required to meet the functional requirements detailed in [b], [d] and [e], the developers must provide the evaluators with design documentation and a rationale to demonstrate that messages received are validated, authenticated and authorised using mechanism(s) that the evaluators determine to be suitably robust, and that the functionality available does not impact the security requirements in this Security Characteristic. In particular this shall address all additional interfaces identified in DEV.*.M847 'Minimise interfaces'.

Any message that fails a validity check shall be discarded without execution.

At Foundation Grade the product **is required to** verify that any message received on a triage interface is a valid message for that device.

If the device provides a triage interface, the developer must provide the evaluators with design documentation and a rationale to demonstrate that any messages received over it are validated, authenticated and authorised using mechanism(s) that meet the triage interface security requirements in this Security Characteristic. For clarity: messages received via the triage interface need to be validated according to the requirements in DEV.*.M44 'Data validation on untrusted input'; messages (other than those used to unlock triage mode) are only accepted on the triage interface after triage mode has been unlocked.

At Foundation Grade the product **is required to** verify that any message received on an operational interface is a valid message for that device from an authentic source that is authorised to perform the operation.

The device shall not accept messages that do not conform to those defined for the device in the Use Cases listed in [d, 19.3] and shall ensure that all messages are subject to the cryptographic and other validity checks in [d, 6.2.4], [d, 6.3.4].

This requirement includes messages received from a Hand-Held Terminal.

Any message that fails a validity check shall be discarded without execution.

The device shall not provide alternative methods of carrying out operations that avoid the need to establish authorisation.

DEV.*.3.M939: Enable update of security credentials

This mitigation is required to counter use of compromised security credentials

At Foundation Grade the product **is required to** enable remote update of security credentials.

The device shall provide the ability to update security credentials, and this shall be subject to the normal message security checks (according to the type of interface used), and shall be confined to authorised roles/sources only.

Update of each security credential shall be atomic (it shall either complete successfully with complete replacement of all parts of the relevant credential or else shall retain the old credential).

DEV.3.M863: Check authentic activation message required

This mitigation is required to counter causing unauthorised activation of authentic firmware

At Foundation Grade the product **is required to** activate downloaded firmware only on receipt of an authentic activation command.

(Firmware updates carried out over a triage interface are covered separately by the triage interface requirements in this Security Characteristic and are not subject to the requirements in this mitigation.)

At Foundation Grade the product **is required to** activate only the version of the firmware identified in the activation command.

At Foundation Grade the product **is required to** record the version of its current executing firmware and of any firmware updates currently stored.

DEV.3.M866: Check firmware update signature

This mitigation is required to counter unauthorised modification to a firmware update in transit

At Foundation Grade the product **is required to** check a secure signature over downloaded firmware on receipt of the firmware update.

If the signature check defined in [d, 11] fails then the firmware update shall be rejected. The failure shall be recorded in the Security Log as identified in [d, 16].

(Firmware updates carried out over a triage interface are covered separately by the triage interface requirements in this Security Characteristic and are not subject to the requirements in this mitigation.)

The changes below define additional new mitigations associated with the new 'Triage interface' functional component.

DEV.5 - Development >> Triage interface

DEV.5.M<101>: (Comms Hub Triage capability ONLY) Characterisation of triage interface

This mitigation is required to counter undocumented uses of the physical triage interface

At Foundation Grade the product **is required to** identify all uses of the triage interface.

Device design information shall identify and describe the triage interface in physical and logical terms. This shall include description of any use of the relevant physical interface for purposes other than triage use case 005 (e.g. if it is also an Intimate Communications Hub Interface). This may be combined with the description of interfaces for DEV.*.M847 'Minimise interfaces'.

The triage interface shall be validated up to the point of a successful Unlock (i.e. including the Unlock message itself) according to the requirements in DEV.*.M44 'Data validation on untrusted input

References to the triage interface and triage mode in other requirements in this SC shall be understood to apply to its use for triage use case 005 specifically.

DEV.5.M<102>: (Comms Hub Triage capability ONLY) Location of triage interface

This mitigation is required to counter undetected connection to triage interface

At Foundation Grade the product **is required to** ensure that use of the triage interface requires generation of a tamper event and use of a local physical interface.

Device design information shall describe how the triage interface is accessed and activated, and shall show that the design requires:

(a) a tamper event to take place (and consequently an event to be logged in the Security Log and an alert generated, subject to available power in the device) before the triage interface can be unlocked and used; and

(b) unlocking and use of the triage interface to be only via a local physical interface (i.e. one that requires the connecting entity to be physically present), and that requires a physical activation action (separate from the tamper event and based on an external input) to enable that physical interface to be used.

Note: it is permitted that the tamper event might not be logged if the device does not have power at the time of the event, and that there might be no tamper event if the device has never been attached to a host ESME.

At Foundation Grade the product **is required to** ensure that activation of the local physical interface for triage causes the device to prevent access to operational functionality.

Device design information shall describe how, when the triage local physical interface is activated, the device prevents access to normal operational functionality such as GPF and CHF commands and the ability to use other interfaces (e.g. radio interfaces) for operational purposes (e.g. participating in a HAN, or WAN, or sending and receiving GBCS messages in any other way).

DEV.5.M<103>: (Comms Hub Triage capability ONLY) Unlocking triage mode

This mitigation is required to counter unauthorised access to the triage interface

At Foundation Grade the product **is required to** ensure that it has received and successfully validated an unlock message before unlocking triage mode.

Triage mode on the device shall initially be locked.

Validation of the unlock message shall include checking that:

a) The Business Target ID in the Command matches the device's Entity Identifier
b) The Message Code is recognised as correct for the unlock command
c) The Business Originator ID is the wanProvider
d) The message payload conforms to the expected structure
e) The ACB MAC is verified as in [GBCS, 6.2.4.1.2]
f) The message includes a wanProvider signature that is verified according to [GBCS, 6.3.4]
g) The unlock message is not future-dated.

The design information shall include a rationale to justify that triage mode cannot be unlocked by any other means than receiving a valid unlock message.

At Foundation Grade the product **is required to** ensure that an unlock message cannot be used to unlock triage mode more than once.

The originator counter on the unlock message shall be checked to provide 'Protection Against Replay', as in GBCS section 6.2.4.2. This is to prevent successful access to triage mode using a previously captured unlock message.

At Foundation Grade the product **is required to** ensure that successful transition to the unlock state is recorded in a log on the device.

The event must be distinct from those 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). (The event and its content may be outside the event definitions in [d], but must in that case be defined in a DCC specification.)

At Foundation Grade the product **is required to** ensure that unlock messages shall only be processed when received on the triage interface, and shall be discarded without processing if received on any other interface.

DEV.5.M<104>: (Comms Hub Triage capability ONLY) Limit commands in unlocked state

This mitigation is required to counter unauthorised access to the triage interface

At Foundation Grade the product **is required to** accept only triage use case 005 commands while triage mode is unlocked.

Commands available after unlock shall be limited to the commands that implement the refurbishment sequence, and (optionally) diagnostic commands that do not perform any critical refurbishment actions. No commands available after unlock shall be capable of future-dated invocation.

A critical refurbishment action is one that has (or includes) the effect of a command in [d] that is critical (i.e. SME.C.C, or a variant message that is critical such as CS02b), or an action that downloads a change to the firmware present in the device. The developer shall provide a rationale that identifies all messages accepted by the device over the triage interface and shows that none (other than the refurbishment sequence) lead to critical refurbishment actions.

The 'refurbishment sequence' is a defined sequence of actions (caused by one or more messages) that, once started, must be completed successfully in order for the device to behave as a functional CH (i.e. a device that is capable of being installed and subsequently acting as a CH) The refurbishment sequence must include a complete overwrite of the firmware and configuration, and may include other critical refurbishment actions.

The design information shall include a description of the commands available after unlock and a rationale that includes:

(a) a description of the refurbishment sequence and a demonstration that the refurbishment sequence must complete once started, or else the device will not be capable of behaving as a functional CH, and
(b) a list of any other commands available, with a description of each that shows that they do not result in critical refurbishment actions; and
(c) a description of the action if an unlock command is received while triage mode is already unlocked (covering both valid and invalid unlock messages), showing that this behaviour does not undermine security (including protection against replay).

DEV.5.M<105>: (Comms Hub Triage capability ONLY) Locking triage mode

This mitigation is required to counter unauthorised access to the triage interface

At Foundation Grade the product **is required to** support automatic re-locking of triage mode.

Relocking triage mode means that the device will not accept any further triage actions until triage mode has been successfully unlocked again.

A device for which triage mode has been previously unlocked shall re-lock automatically when any of the following events occur (other than as part of the refurbishment sequence):

a) reboot
b) loss of external power (battery backup must not keep the device unlocked)
c) loss of communication session over the triage interface (e.g. on detection of physical disconnection of the triage interface)
d) detection of a failure requiring recovery action (as in DEV.M846).

The device may also support an explicit triage mode lock command that can be used before any automatic lock occurs.

DEV.5.M<106>: (Comms Hub Triage capability ONLY) Data deletion before reinstallation

This mitigation is required to counter compromise of consumer data during refurbishment
This mitigation is required to counter inappropriate future-dated actions following refurbishment

At Foundation Grade the product **is required to** ensure that any previous consumer data present in the device is deleted before reinstallation.

Deletion of the previous consumer data shall be by overwriting. Consumer data, considered personal data under the Data Protection Act, shall be identified in the design information. (The deletion may exclude records of total quantities supplied that cannot be reset according to the Measuring Instruments Directive.) Design information shall include a rationale that the consumer data cannot be extracted during the refurbishment sequence.

Note: deletion may be achieved by encryption of the data and deletion of the key (without the need to overwrite the encrypted data).

DEV.5.M<107>: (Comms Hub Triage capability ONLY) No installation with triage mode unlocked

This mitigation is required to counter undocumented uses of the physical triage interface

At Foundation Grade the product **is required to** ensure that the product cannot be installed while triage mode is unlocked.

DEV.5.M<108>: (Comms Hub Triage capability ONLY) Completeness of overwrite

This mitigation is required to counter compromise of consumer data during refurbishment

At Foundation Grade the product **is required to** render the previous content of all firmware and configuration memory areas unobtainable as a result of carrying out the refurbishment sequence.

For clarity: this will include ensuring that no future-dated commands are present on completion of the refurbishment sequence.

At Foundation Grade the product **is required to** ensure that any failures arising when carrying out the refurbishment sequence will result in a clearly identified and visible state that does not allow normal operation.

The overwrite (as part of the refurbishment sequence) may take place in multiple stages, but must not leave the device in a partially overwritten state unless such a state is clearly identified and visible, and prevents the device from being installed and put into normal operation as a Communications Hub.

5.2 Changes to Verification mitigations

The changes below describe updates to existing VER mitigations. Where a VER mitigation is not listed in the changes then it is included unchanged (i.e. absence of the mitigation below does not imply that it is deleted). The changes are specified by stating the entire new mitigation.

VER.*.1.M80: Protocol robustness testing

This mitigation is required to counter exploitation of a non-operational interface through crafted input
This mitigation is required to counter exploitation of an additional interface through crafted input
This mitigation is required to counter exploitation of an operational interface through crafted input
This mitigation is required to counter exploitation of a triage interface through crafted input

At Foundation Grade the evaluator **will** perform fuzz testing of the available interfaces.

As per guidance in The Process for Performing Foundation Grade CPA Evaluations [a], structured fuzz testing is expected for all available interfaces, physical AND logical. Based on mandatory functional requirements in [d], the following two interfaces will always require fuzz testing: ZigBee and GBCS application layer messages.

For ZigBee, fuzz testing shall be performed on all the messages that can be received including those that are (a) unencrypted, (b) encrypted with the network key (and thus visible to all devices on the HAN) and (c) encrypted with an APS key set up to protect comms between the product and each other type of HAN device that is not required to be CPA-certified (at time of writing, PPMID, IHD and CAD).

When fuzz testing GBCS Application layer messages ('use cases'), mutations are expected to cover all parts of a message that the product will attempt to decode up to the point of authentication. The point of authentication for these messages (as relevant to [a], for smart metering equipment) is the point at which the protective crypt gets successfully validated (one or both of digital signature and MAC, dependent on the message type); any message decoding performed before this point (even just to check message well-formedness) will be in scope of GBCS Application layer fuzz testing. With this in mind, some message payload fuzz testing is expected (in addition to all the other sections of a GBCS Application layer message that can be present (i.e. GBT header, grouping header, signature field, etc), the amount of payload fuzz testing depending on how much of the message's payload gets decoded by the product before the point of authentication is reached. This minimum expectation is based on some GBCS application messages requiring content in the payload to be decoded and processed as part of the cryptographic validation process for the message type.

If the device includes a triage interface that implements triage use case 005 then this shall be subject to fuzzing up to the point of authentication. For triage use case 005 the relevant point of authentication is the successful unlock of triage mode – i.e. fuzzing shall cover all messages that are accepted before triage mode is successfully unlocked.

In addition to the ZigBee and GBCS application layer interfaces, and (optionally) the triage interface, it is possible that the device may have additional interfaces beyond those defined in [d] that might be accessible to an attacker and hence also require fuzz testing. In particular all additional interfaces as identified in DEV.*.M847 ‘Minimise interfaces’ require fuzz testing.

VER.1.3.M4: Evaluation/Cryptocheck

This mitigation is required to counter exploitation of a cryptographic algorithm implementation error

At Foundation Grade the evaluator **will** ensure all cryptographic algorithms employed for security functionality have been validated as per the "Cryptography Review" section in the CPA Foundation Process document.

The evaluator shall include in this activity a confirmation (by reference to relevant CAVP or equivalent certificates, or by activities in the course of the CPA evaluation) that cryptographic algorithms used by the PRNG (such as DRBG) have been independently validated for correctness.

Where cryptographic algorithms claim certification under CAVP (or equivalent external certification), then the evaluator shall confirm that this certification has been achieved for the relevant hardware/firmware/software components of the product, at the relevant version for the component. For cryptographic algorithms that are not certified using an external process, the evaluator shall confirm the correctness of the implementation by means of known answer tests, as described in the CPA Foundation Process document, Reference [a].

The cryptographic primitives used by the device shall be only those specified in [d] , including those primitives used by all UTRN validation functionality in the device, and those used by any triage capability present on the device.

VER.*.3.M855: Receiver replay check

This mitigation is required to counter interception and replay of messages

At Foundation Grade the evaluator **will** verify that messages are not actioned more than once.

The evaluator shall confirm by testing that the device correctly rejects messages with unacceptable count values relative to its current state, and that the device correctly generates count values for which it is responsible. The testing shall cover both commands for immediate execution and future-dated commands (where applicable).

The mechanism for protection against replay is defined in [d, 4.3]. Only certain messages require the protection, as specified in the Use Cases in [d, 19], summarised in [d, Table 20]. However, a different anti-replay mechanism is used for Security Credential commands as defined in [d, 13], and for Pre-Payment Top-Ups as defined in [d, 14].

Notes:

- Evidence is required for ALL commands that incorporate replay protection.

- When testing the anti-replay protection for Pre-Payment Top-Ups (where applicable), the evaluator shall verify that Pre-Payment Top-Up messages are rejected if its UTRN counter value (a) matches any value in the device's UTRN counter cache or (b) is lower than the lowest value in the device's UTRN counter cache. These tests will also cover all the interfaces over which the device can receive a UTRN.

(Messages sent and received over a triage interface are covered separately by the triage interface requirements in this Security Characteristic and are not subject to the requirements from [d] in this mitigation.)

VER.*.3.M939: Enable update of security credentials

This mitigation is required to counter exploiting incomplete update of security credentials
This mitigation is required to counter installation of an invalid certificate
This mitigation is required to counter use of compromised security credentials

At Foundation Grade the evaluator **will** verify that the update of a security credential is atomic.

The evaluator will test that the update of each security credential either finishes successfully with complete replacement of all parts of the relevant credential or else retains the old credential.

(This testing is not required for updates to credentials performed using the triage interface, if triage capability is supported.)

At Foundation Grade the evaluator **will** verify that, in addition to the general critical message validation checks described elsewhere, certificate path validation (CPV) always successfully completes, where required to do so by [d], before the validated replacement remote party certificate is installed.

The specific type of CPV required by [d] will vary according to the type of certificate and the operation of each type of CPV will be verified by the evaluator.

(This testing is not required for updates to credentials performed using the triage interface, if triage capability is supported.)

At Foundation Grade the evaluator **will** verify that, once validation checks have been successfully performed, the specified security credentials replacement will take place with subsequent product functionality confirming this.

The evaluator shall seek evidence to confirm that all the different types of remote party security credentials defined in [d, 4] (i.e. covering the different types of remote party role, keyUsage and cellUsage, appropriate for the product type) can be replaced, using all the different credentials replacement modes defined in [d].

Checks on subsequent product functionality should, as a minimum, confirm that the new credentials will be used for the associated cryptographic mechanisms, instead of the old ones. For instance, depending on the type of credential replaced, the following tests are suggested: (a) digital signature verification, (b) MAC authentication + generation, (c) certificate path validation and (d) encryption + decryption of sensitive data.

(This testing is not required for updates to credentials performed using the triage interface, if triage capability is supported.)

VER.*.4.M917: Verify logical protection of security data

This mitigation is required to counter gaining access to security data in a single device (via either operational or non-operational interfaces)

At Foundation Grade the evaluator **will** confirm the protection of security data, such as cryptographic key material.

The evaluator shall confirm that:

- no sensitive key material (private asymmetric keys and any symmetric keys) can be exfiltrated from the product, and

- the following security related data cannot be modified, except as a result of certain authentic messages defined in [d] intended for the purpose: device security credentials, remote party security credentials, including anti-replay counters and (where applicable) the device's UTRN counter cache.

Note: This confirmation shall also take into account any documented product interfaces additional to [d] that have the potential to exfiltrate sensitive key material or modify security related data, including all additional interfaces as identified in DEV.*.M847 ‘Minimise interfaces’.

Actions performed using the triage interface, if triage capability is supported, are only required to be tested under this mitigation to ensure that the key used to protect unlock messages, and/or any secret data used to derive keys used in triage, cannot be exfiltrated.

The changes below define additional new mitigations associated with the new 'Triage interface' functional component.

VER.5 – Verify >> Triage interface

VER.5.M<102>: (Comms Hub Triage capability ONLY) Location of triage interface

This mitigation is required to counter undetected connection to triage interface

At Foundation Grade the evaluator **will** confirm that use of the triage interface requires generation of a tamper event.

As noted in DEV.5.M<102> it is permitted that the tamper event might not be logged if the device does not have power at the time of the event, and that there might be no tamper event if the device has never been attached to a host ESME.

At Foundation Grade the evaluator **will** confirm that use of the triage interface requires use of a local physical interface.

At Foundation Grade the evaluator **will** confirm that while the triage physical interface is activated, the device will not provide operational functionality.

"Operational functionality" here means performing GBCS functions as a GPF or CHF.

VER.5.M<103>: (Comms Hub Triage capability ONLY) Unlocking triage mode

This mitigation is required to counter unauthorised access to the triage interface

At Foundation Grade the evaluator **will** confirm that unlocking triage mode requires a successfully validated unlock message.

This confirmation is based on performing tests with valid and invalid unlock messages according to the validation criteria and the design information.

At Foundation Grade the evaluator **will** confirm that a valid unlock message is not accepted more than once by the device.

At Foundation Grade the evaluator **will** confirm that successful transition to the unlock state is recorded in a log on the device, and that the log entry conforms to the specification.

At Foundation Grade the evaluator **will** confirm that both invalid and valid unlock messages are discarded without processing when received on any interface other than the triage interface.

VER.5.M<104>: (Comms Hub Triage capability ONLY) Limit commands in unlocked state

This mitigation is required to counter unauthorised access to the triage interface

At Foundation Grade the evaluator **will** confirm that triage use case 005 commands are accepted and performed only if triage mode is unlocked.

This confirmation is based on demonstrating that available commands to perform triage use case 005 commands and critical refurbishment actions are rejected when triage mode is locked.

At Foundation Grade the evaluator **will** confirm that only the commands listed in the design information are accepted after unlock.

At Foundation Grade the evaluator **will** confirm that, once started, the refurbishment sequence must be completed in order for the device to behave as a functional CH.

This confirmation is based on demonstrating that CH functionality is not available at any point between the messages that comprise the refurbishment sequence.

At Foundation Grade the evaluator **will** confirm that messages in the refurbishment sequence that result in critical refurbishment actions are not accepted out of the defined order.

VER.5.M<105>: (Comms Hub Triage capability ONLY) Locking triage mode

This mitigation is required to counter unauthorised access to the triage interface

At Foundation Grade the evaluator **will** confirm that the product automatically re-locks triage mode.

This shall include at least the following checks:

a) that, after re-locking, the device will not accept any further triage actions until triage mode has been successfully unlocked
b) that the re-lock occurs on reboot
c) that if power is removed whilst triage mode is unlocked then the device triage mode is in the locked state when it next restarts
d) that if the communication session over the triage interface is ended then the device triage mode is in the locked state when it next restarts
e) that if the device supports an explicit triage mode lock command then this does re-lock triage mode.

VER.5.M<106>: (Comms Hub Triage capability ONLY) Data deletion before reinstallation

This mitigation is required to counter compromise of consumer data during refurbishment

At Foundation Grade the evaluator **will** confirm that any previous consumer data present in the device is deleted before reinstallation.

This is confirmed by attempting to access consumer data that was known to be previously present.

VER.5.M<107>: (Comms Hub Triage capability ONLY) No installation with triage mode unlocked

This mitigation is required to counter undocumented uses of the physical triage interface

At Foundation Grade the evaluator **will** confirm that the product cannot be installed while triage mode is unlocked.