National Cyber Security Centre
a part of GCHQ

SEC Smart Energy Code Security Sub-Committee

CPA Security Characteristic

Electricity Smart Metering Equipment

Version 1.3

The production of this document was initiated by BEIS, but responsibility was passed to the SEC Security Sub-Committee from 13 March 2019 who finalised the production and implementation plans with cross industry input throughout the process

Important

Products certified against this Security Characteristic have their aligned product and Build Standard recertification periods defined in the Smart Energy Code, Section F2 - 'Expiry of CPA Certificates' [1]

About this document

This document describes the features, testing and deployment requirements necessary to meet CPA certification for Electricity Smart Metering Equipment (ESME) products. It is intended for vendors, system architects, developers, evaluation and technical staff operating within the security arena.

- Section 1 is suitable for all readers. It outlines the purpose of the security product and defines the scope of the Security Characteristic.
- Section 2 and Section 3 describe the specific mitigations required to prevent or hinder attacks for this product type. Some technical knowledge is assumed.
- For more information about CPA certification, refer to The Process for Performing CPA Foundation Grade Evaluations[2].

Document history

The CPA Authority may review, amend, update, replace or issue new Scheme Documents as may be required from time to time. Soft copy location: NCSC-1844117881-1390

Version	Date	Notes
1.0	July 2014	Initial version based on cross-industry working group input.
1.1	June 2015	Updated to align with Technical Specs (GBCS, CHTS and SMETS) released 28 November 2014.
1.2	Nov 2015	Updated to align with Technical Specs (GBCS, CHTS and SMETS) released 18 November 2015.
1.3	Sep 2019	Updates to include clarifications following initial evaluations

This document is derived from the following SC Maps:

SC Map	Map Version
SmM Meters SC	1.4
SmM Crypt SC Library	1.5
SmM Device SC Library	1.5

[1] https://smartenergycodecompany.co.uk/document-download-centre/

[2] https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa

Contact SEC Security Sub Committee (SSC) or the NCSC

This document is authorised by: Technical Director (Assurance), NCSC and SSC Chair

SSC Contact Details ***(For general queries about this document)***	**NCSC Contact Details** ***(For specific queries about the CPA Scheme)***
SEC Security Sub Committee c/o SECAS, 8 Fenchurch Place, London, EC3M 4AJ, UK. **Email:** SSC@gemserv.com **Tel:** + 44 (0) 207 090 7755	IES Service Management Team NCSC, A2i, Hubble Road, Cheltenham, Gloucestershire, GL51 0EX, UK. **Email:** cpa@ncsc.gov.uk Tel: +44 (0) 300 020 0964

Contents

1 Overview

1.1 Introduction

This document is a CPA Security Characteristic. It describes requirements for assured Electricity Smart Metering Equipment (ESME) for evaluation and certification under NCSC's Commercial Product Assurance (CPA) scheme.

1.2 Product description

The primary purpose of an ESME is to securely control supply and accurately and securely record and transmit, where appropriate, information about electricity flows through smart electricity meters.

1.3 Typical use cases

The product is used within GB Smart Metering and will be installed in domestic premises and smaller non-domestic consumer premises.

1.4 Expected operating environment

As part of GB Smart Metering, the ESME is to be deployed at consumer premises along with other equipment. It will communicate through a Smart Metering Home Area Network (HAN) with a Communications Hub which includes Gas Proxy functionality. The Communications Hub also provides communications between the HAN and a Smart Metering Wide Area Network, the latter connecting the Communications Hub to the Energy Supplier (in the majority of cases via a centralised Communications Broker, the DCC, which will also establish connections with network operators and authorised third parties).

The ESME deployed at consumer premises may be in one of three configurations:

- Single Element Electricity Metering Equipment (which includes one measuring element)
- Twin Element Electricity Metering Equipment (which includes two measuring elements)
- Polyphase Electricity Metering Equipment (which includes three measuring elements).

In cases where an ESME comprises Twin Element Metering Equipment or Polyphase Electricity Metering Equipment there may be multiple instances of components or data within the same device. In these cases, the Security Characteristic requirements shall be applied to, and evaluated in, all such instances.

The ESME will include a Load Switch, and in addition there may be one or more Auxiliary Load Control Switch (ALCS) and a Boost Function. One or more Auxiliary Load Control Switch (ALCS) may also be installed as separate devices with their own HAN interface (HCALCS).

The equipment to be deployed at consumer premises will consist of the Communications Hub, Gas Smart Metering Equipment (GSME) (if the consumer has a gas supply), ESME, an In-Home Display (IHD) and, optionally, a Prepayment Interface Device (PPMID). Consumer Access Devices (CADs) may also be available.

During installation and maintenance, a Hand Held Terminal (HHT) may be used to download messages, as specified in reference [d], from the Supplier to a device via the Communications Hub. This would be transparent to the ESME.

Overarching security obligations on energy suppliers and the DCC can be found in the Smart Energy Code (see reference [g]).

The Business Interactions section of the End to End Technical Architecture document (reference [i]) provides further context on the expected operating environment.

1.5 Compatibility

There are no compatibility requirements.

1.6 Conformance

The ESME should be interoperable with the Communications Broker and other Smart Metering Equipment deployed in the consumer premises. Interoperability on this basis is achieved through the following conformance requirements; those which require external certification are treated as dependency requirements for CPA certification, and must be demonstrated before CPA certification can be achieved.

Requirement	Standard(s)	External Certification
Declaration of intended conformance with a relevant version of SMETS 2.	Reference [b]	N/A – No external certification required for CPA compliance.
Declaration of intended conformance with a relevant version of the Great Britain Companion Specifications (GBCS).	Reference [d]	N/A – No external certification required for CPA compliance.
The ESME shall be certified: i. by the ZigBee Alliance as compliant with the ZigBee requirements identified in the relevant version of SMETS 2 and associated version of GBCS, as set out in the Technical Specification Applicability Tables (TSAT); and ii. by the DLMS User Association as compliant with the DLMS requirements identified in the relevant version of GBCS, as set out in the TSAT.	Reference [b] Reference [d] Reference [h]	ZigBee and DLMS
The ESME must be interoperable with the cryptographic protocols used to secure messages from the Communications Broker and end-to-end messages from authorised Service Users.	Reference [d]	CAVP or CPA[1].

[1] When algorithm certification is included under CPA then it will be assessed as part of the evaluation of the meter: there is no separate CPA evaluation implied.

1.7 High level functional components

The following diagram illustrates various high-level functional components within ESME that relate to specific mitigations listed in Section 3. These are used to structure the Security Characteristic, and to give context to each mitigation. For a full specification of the detailed functional requirements of ESME, see references [b] and [d].

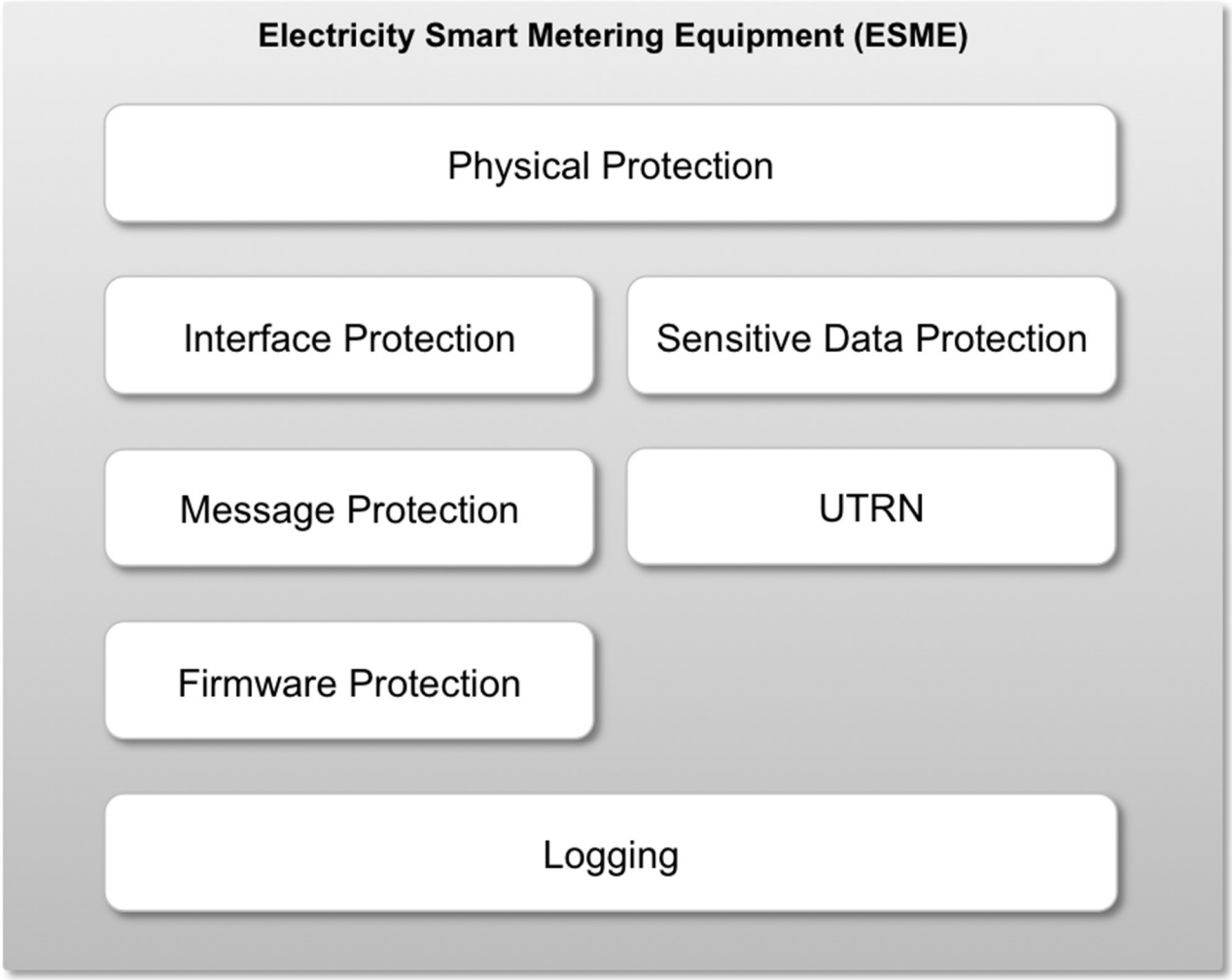

Figure 1: Functional components of an ESME

The functional components in Figure 1 are described as follows.

- **Physical Protection**. A physical border, known as the 'tamper-protection boundary', surrounds the device and is capable of detecting physical access through its Secure Perimeter that could compromise confidentiality and/or data integrity of Personal Data, consumption data, security credentials, random number generator, cryptographic algorithms, the meter, or firmware. On detection of such access the device is capable of recording the event and sending an alert where reasonably practicable. This relates to the physical aspect of the Secure Perimeter described in reference [b, 5.4].
- **Interface Protection**. Operational interfaces on the Smart Metering Equipment comply with security requirements in reference [b, 5.6] and prevent use of any non-operational interfaces. The device includes a HAN interface using ZigBee protocols enabling communications with other devices on the HAN.

- **Message Protection.** Messages received by the Smart Metering Equipment are validated to verify they comply with End-to-End security requirements in reference [d, 4]. These ensure aspects such as protection against replay or unauthorised modification. In addition, the ZigBee protocols include cryptographic measures that protect messages between devices on the HAN. The clock in the device is used to validate some messages that require additional certificate path validation, as well as to ensure that future-dated commands are executed at the correct time. See Appendix C for more details.
- **Sensitive Data Protection.** The User Interface is capable of restricting display of Personal Data by requiring a Privacy PIN as described in reference [b, 5.5.5]. Keys that are used by cryptographic mechanisms to maintain various aspects of the meter security are protected against unauthorised access. Data within the device is held in a data store that is capable of retaining information at all times, including on loss of power, as described in reference [b, 5.7].
- **Firmware Protection.** The Smart Metering Equipment is capable of verifying the integrity and authenticity of its firmware as described in reference [d, 11] and reference [b, 5.5.10].
- **UTRN.** UTRNs received by the Smart Metering Equipment are validated to verify they comply with security requirements in reference [d, 14]. UTRNs may be received in Remote Party Messages or entered manually on the user interface or via a PPMID.
- **Logging.** A logging infrastructure is provided that records Sensitive Events in the Security Log and causes alerts to be sent in certain situations. Entries cannot be modified or deleted from the Security Log (other than through the normal overwriting of the oldest events by newer events as described in reference [b, 5.7.5]) and the log is expected to be regularly read by an authorised Remote Party before unread entries have been overwritten. The clock in the device enables timestamps to be included in the logs.

1.8 Future enhancements

The SSC, NCSC and BEIS welcome feedback and suggestions on possible enhancements to this Security Characteristic.

2 Security Characteristic Format

2.1 Requirement categories

All CPA Security Characteristics contain a list of mitigations that describe the specific measures required to prevent or hinder attacks. The mitigations are grouped into three requirement categories; design, verification and deployment, and appear in section 3 of this document in that order.

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

Within each of the above categories, the mitigations are further grouped into the functional areas to which they relate (as outlined in the High level functional components diagram). The functional area for a designated group of mitigations is prefixed by double chevron characters ('>>'). For example, mitigations within a section that begins:

Development>>Management

- concern **Development** mitigations relating to the Management functional area of the product.

Note: Mitigations that apply to the **whole** product (rather than a functional area within it) are listed at the start of each section. These sections do **not** contain double chevron characters.

2.2 Understanding mitigations

Each of the mitigations listed in Section 3 of this document contain the following elements:

- The name of the mitigation. This will include a mitigation prefix (**DEV**, **VER** or **DEP**) and a unique reference number.
- A description of the threat (or threats) that the mitigation is designed to prevent or hinder. Threats are formatted in *italic text*.
- The explicit requirement (or group of requirements) that *must* be carried out. Requirements for foundation grade are formatted in **green text**.

In addition, certain mitigations may also contain additional explanatory text to clarify each of the foundation requirements, as illustrated in the following diagram.

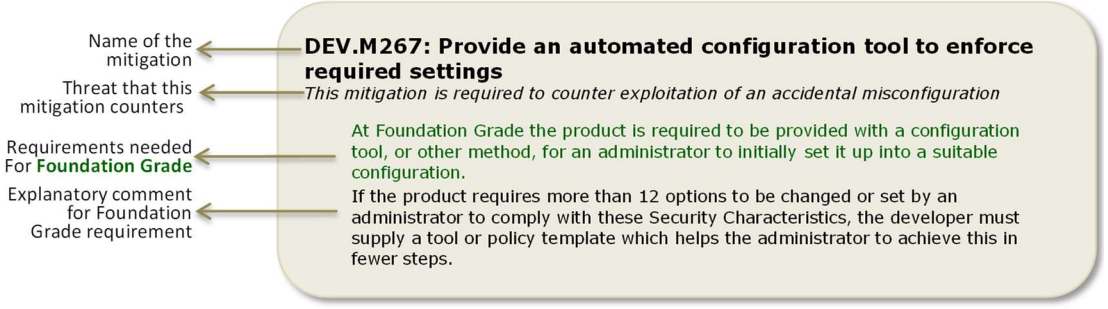

Figure 2: Components of a typical mitigation

3 Requirements

This section lists the Development, Verification and Deployment mitigations for the Electricity Smart Metering Equipment Security Characteristic. For a summary of the changed mitigations in this version, please refer to Appendix D.

3.1 Development mitigations

DEV.M846: Secure failure recovery

This mitigation is required to counter disruption of a device by electromagnetic interference
This mitigation is required to counter exploitation of a software implementation/logic error

At Foundation Grade the product **is required to** employ measures to ensure secure restart of the device after failure.

The device shall implement measures both to detect conditions that lead to failure and to recover automatically from such failures to a normal operating state by, as a minimum, executing the normal power-up sequence. This shall include ensuring that the state of the device leading up to the failure shall not compromise sensitive or security-critical data (e.g. the device shall prevent compromises arising from the memory state at the time of failure).

The recovery action shall also include verification of the integrity of the current firmware.

If any diagnostic information is preserved from failures then this shall not contain unencrypted sensitive data (or data that can be used to gain unauthorised access to sensitive data).

Design information shall describe the failure-related risks identified by the developer and the corresponding device behaviour implemented to deal with the corresponding failure cases in order to show that security is not compromised in such situations. Security activity in this context includes, as a minimum, those defined in the glossary entry for Failure-related activity.

The device design information shall include:

- a description of how the device provides reliable recovery from any foreseeable errors, the process for recovery (and its impact on normal operational processing, such as recording consumption data and receiving messages) and any error conditions in which it will no longer operate.

- a description of the power-up process, the self-tests that take place automatically (without requiring operator intervention) during this process, and the results of encountering an error or failure at any point in this process. The evaluator shall confirm that, after installation, the power-up process does not allow the device to be launched into any mode other than the normal operating mode (e.g. no access is granted to diagnostic or recovery functions, including engineering menus, other than those permitted via the interfaces in [b]).

DEV.M926: Protected software environment

This mitigation is required to counter exploitation of a software implementation/logic error

At Foundation Grade the product **is required to** implement software protection measures as part of the design process.

The device design information shall describe the process environment in the device in order to allow the evaluator to identify any defensive or robustness mechanisms provided by the platform or OS.

The developer shall provide evidence to demonstrate device firmware compliance with MISRA rules for C (or equivalent for the target language), by application of an appropriately configured static analysis tool. Where the target language is C, MISRA 2012 or later must be used (and, where supported by the static analysis tool, include the additional rules introduced in MISRA:C 2012 Amendment 1). Where the target language is not C, the developer shall demonstrate equivalence by mapping each rule onto the equivalent criterion for the target language, accompanied by the method of demonstrating that the criterion has been met.

The developer shall provide a rationale for how the device firmware protects against stack and heap corruption. Stack protection is typically expected to be provided via a compiler option that uses canaries to protect against a function's return address being overwritten. Whether or not such a compiler option is used, the stack protection implementation needs to comply with the "Stack Protection Expectations" appendix in this document

The developer shall demonstrate that they review all device firmware against a checklist of security flaws, including known vulnerabilities, in other versions of the product or its components (e.g. where 3rd party software/hardware is used), and known vulnerabilities in similar devices. Note: Aspects of this requirement should be covered by the developer's ongoing Build Standard compliance obligations.

DEV.M946: Clock synchronisation

This mitigation is required to counter tampering with the device clock

At Foundation Grade the product **is required to** prevent unauthorised modifications to the device clock.

The device shall synchronise time with the Communications Hub as defined in [d, 9], on receipt of a valid Set Clock command and also periodically.

On receipt of a valid Set Clock command, the time shall be retrieved from the Communications Hub. If the time retrieved is within the tolerance specified in the command, the device shall set its time to that retrieved from the Communications Hub. If it is outside the specified tolerance, the time status shall be marked as Unreliable, and a response or alert (depending on the version of [d] being complied with) sent according to the specific requirements of [d, 9].

Additionally, once every 24 hours (but no more frequently under normal operating conditions) a synchronisation is attempted. If the attempt to retrieve a valid time fails, the synchronisation will be subsequently attempted every 30 minutes until a valid time value has been retrieved according to the specific requirements of [d, 9]. If the result is that the time retrieved from the Communications Hub is not more than 10 seconds different from the device's current time, the device shall set its time to that retrieved from the Communications Hub and mark the time status as Reliable. If it is more than 10 seconds different from the device's current time, the time status shall be marked as Unreliable, a Security Log entry shall be recorded and an alert sent as defined in [d, 9]. Note: Depending on the version of [d] being complied with, the Security Log entry and alert actions might only be needed if the time status has changed to be Unreliable.

Design information shall identify any interface through which the device clock's time can be modified and how it is ensured that no unauthorised modifications can be made.

DEV.1 - Development >> Firmware Protection

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.

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 and an alert shall be sent as identified in [d, 16] to the recipients specified in [d, 16].

DEV.1.M902: Check firmware integrity before execution

This mitigation is required to counter unauthorised modification to firmware in situ

At Foundation Grade the product **is required to** check an integrity measure over the device firmware before execution.

The device shall check the integrity of the firmware to be executed during power-on and during restart from failure (it is not necessary to perform the check when waking from a sleep state). The integrity check shall be at least as strong as a 32-bit cyclic redundancy check (CRC).

Where the device comprises more than one component with its own firmware, the firmware of each component shall be checked.

Where a failure of the integrity check occurs, the device shall record this in the Security Log and send an alert as identified in [d, 16] to the recipients specified in [d, 16].

DEV.2 - Development >> Interface Protection

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 operational 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, 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.M273: General resource management

This mitigation is required to counter flooding the device with messages from the HAN

At Foundation Grade the product **is required to** protect against instability when processing incoming network traffic.

The developer shall provide a rationale to show that large amounts of incoming network traffic do not cause the device to crash or suffer a general failure resulting in loss of functionality (apart from temporarily losing external communications).

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 operational interface through crafted input

At Foundation Grade the product **is required to** ensure that only necessary protocols and services are available 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 developers shall provide details of the functionality with an associated analysis that clearly indicate where security impacting functionality can occur. Where such additional functionality is present and has the potential to be security impacting, its unauthorised use shall be protected against using security mechanisms at least as strong as those in [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.M873: Disable non-operational logical and physical interfaces

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

At Foundation Grade the product **is required to** prevent unauthorised access to all physical and logical interfaces that are not required for normal operation.

If the device has interfaces other than those supporting normal operation (and that are therefore not governed by the RBAC mechanism), then design information shall explain how these interfaces are either:
a) disabled for normal operation, or
b) cannot be used to undermine device security - developer provided rationale required.

It must not be possible to re-enable any disabled interfaces outside the tamper-protection boundary without first breaching the tamper-protection boundary and physically modifying the device in a way that would be detectable via subsequent inspection within the tamper-protection boundary.

Interfaces within the tamper-protection boundary must ensure that their use requires physical modification that would be visible to subsequent inspection within the tamper-protection boundary. This does not apply to bespoke or complex physical connectors such as a bed-of-nails, or integrated circuit test clips although the developer provided rationale must include any such components that are easily accessible.

Device design information shall specify any roles and associated interfaces that are supported in any stage of the device lifecycle (e.g. before installation or after decommissioning). The device design information shall include a complete definition of the logical and physical interfaces (such that the information could be used to create a test tool that will exercise all parts of the interface, with an ability to define expected results for any communication).

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 cannot be made without using operational interfaces.

Design information shall describe how the device prevents unauthorised changes to the configuration data.

DEV.3 - Development >> Logging

DEV.3.M940: Security alerts

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

At Foundation Grade the product **is required to** send alerts for security-related events and error conditions.

The device shall send the alerts identified in [d, 16] to the recipients specified in [d, 16].

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.

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 - Development >> Message Protection

DEV.4.M134: State raw entropy requirements

This mitigation is required to counter prediction of randomly generated values due to a weak Entropy Source

At Foundation Grade the product **is required to** have clearly defined entropy requirements for all operational random number generation.

Device design information shall specify all cryptographic keys employed by the device (including any that are not required for normal operation), and their method of generation or installation.

The developer must state how much raw entropy is required from the product's entropy source (for example, which is used to reseed the PRNG), based on analysis of all security-related random numbers used in the device, including any generated keys. It shall be at least 128 bits as required by the elliptic curve-based asymmetric mechanisms using the P-256 curve, assuming no other security features of the device have significant entropy requirements.

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 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.M141: Reseed PRNG as required

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** follow an approved reseeding methodology.

For instance, if a SP 800-90 series compliant DRBG is being used, the product must implement the reseed mechanism recommended by the relevant SP 800-90 series document.

Reseeds of the PRNG should be performed at least once a month or immediately prior to generating a new random number (e.g. as part of generating a new key), provided, in the latter case, this does not significantly impact on the time taken to generate the random number.

DEV.4.M290: Employ an approved Entropy Source

This mitigation is required to counter prediction of randomly generated values due to a weak Entropy Source

At Foundation Grade the product **is required to** generate random bits using an Entropy Source whose entropy generation capability is understood.

The developer must provide a detailed description of the Entropy Source used, giving evidence that it can generate sufficient entropy for each use of random numbers in the device, including an estimate of entropy per bit. The Entropy Source should be implemented according to guidance in relevant standards such as the NIST SP800-90 series.

If a hardware noise source is used, then the manufacturer's name, the part numbers and details of how this source is integrated into the product must be supplied. If a software Entropy Source is employed, the API calls used must be provided. Where appropriate, details must be given of how the outputs of multiple Entropy Sources are combined.

The device design information shall include an analysis of each noise source used for generating cryptographic keys, detailing the amount of entropy believed to be obtained from this source. This analysis should be supported by relevant datasheets, API specifications and results from the developer testing, as appropriate.

Where devices or functions are used that are not dedicated noise sources (for instance, A-D converters), analysis will additionally need to demonstrate that the improvised device or function will reliably provide a stated level of entropy for the operational environments the product may be deployed in. Factors that should be considered vary on the type of improvised noise source but could for instance involve (a) differences in temperature and humidity between the test lab and operational environment, (b) how predictable any input sampled by the improvised device might be in practice.

Important: Entropy measurements are performed on the raw data sampled, i.e. before any subsequent processing of that data that could result in the sampled data being scrambled in a manner that distorts the measured entropy.

DEV.4.M349: Sanitise temporary variables

This mitigation is required to counter reading non-sanitised sensitive data from memory

At Foundation Grade the product **is required to** sanitise temporary variables containing sensitive information as soon as no longer required.

The sensitive information shall include private and secret keys, and the Shared Secret for key agreement. This applies to both volatile and non-volatile memory.

Sanitising a variable must consist of at least one complete overwrite.

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.

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].

DEV.4.M887: Encrypt sensitive data in messages prior to transmission

This mitigation is required to counter interception of messages on WAN

At Foundation Grade the product **is required to** protect the confidentiality of sensitive data in commands, responses and alerts.

Any command or response data that is sensitive shall be encrypted for the whole of its path to or from the device. Data to be encrypted is specified in [d, 19.3]. The encryption shall be as specified in [d, 8].

DEV.4.M911: Self-test of RNG

This mitigation is required to counter prediction of randomly generated values due to a weak RNG

At Foundation Grade the product **is required to** carry out self-testing of RNG output.

The developer shall provide a description of the self-testing performed by the random number generator and why they consider the implemented tests are adequate.

For clarity, the self-tests are expected to be applied to the output of the Entropy Source (checking the final RNG output shall be covered by Evaluation/Cryptocheck of the PRNG, under the VER requirements in this Security Characteristic).

Note: Where a NIST SP800-90 series compliant PRNG is used by the product, the self-tests required by these standards are expected to be implemented.

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.

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].

DEV.4.M914: Demonstrate authenticity of critical responses and alerts

This mitigation is required to counter creation of malicious response or alert messages

At Foundation Grade the product **is required to** protect the authenticity of critical responses and alerts.

Critical responses and alerts sent by the device shall be signed by the device under its private signing key, as specified in [d].

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 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]; however, 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 it doesn't impact the security requirements in this Security Characteristic.

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, 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.5 - Development >> Physical Protection

DEV.5.M849: Tamper response

This mitigation is required to counter access to structures inside the tamper-protection boundary of the device

At Foundation Grade the product **is required to** send an alert and record a Security Log message on breach of tamper-protection boundary.

Removing or opening any part of the tamper boundary that is designed to be separately removed or opened shall be detectable and cause the product to send an alert identified in [d, 16] to the recipients specified in [d, 16] and record an entry in the Security Log.

DEV.5.M897: Protection of security-related physical structure

This mitigation is required to counter unauthorised physical access to security-critical data stored on the device

At Foundation Grade the product **is required to** ensure that physical access to processors and memory carrying sensitive data requires breach of the tamper-protection boundary.

Device design information shall identify the 'tamper-protection boundary' that is protected against tampering, and the methods and mechanisms used to provide this protection. This boundary shall be clearly defined with respect to the physical boundary of the device, and with respect to the components that generate, process and store sensitive data, and that carry out cryptographic operations.

In this context, sensitive data is defined as cryptographic key material and the contents of the Data Store.

Device design information shall specify the physical ports and logical interfaces and all defined input and output paths that are available across the tamper-protection boundary.

Device design information shall specify all cryptographic keys employed by the device (including any that are not required for normal operation) and their storage locations, such that these can be identified as being inside the tamper-protection boundary.

DEV.6 - Development >> Sensitive Data Protection

DEV.6.M928: Restrict data on change of tenancy

This mitigation is required to counter reading previous tenants' information in an operational meter

At Foundation Grade the product **is required to** prevent access to previous Personal Data.

Following receipt of a Restrict Data Command the device shall prevent provision to Type 1 Devices and Type 2 Devices of all items of Personal Data stored in the ESME with a UTC date and time stamp prior to the date and time specified in the Restrict Data Command.

The specific items to which provision is restricted are identified in the Set Change of Tenancy date Use Case in [d, 19].

(For clarity: the data will still be available if the restriction date is changed, in response to an authorised command from the appropriate role.).

DEV.6.M934: Unique security data per device

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 product **is required to** contain no security data that enables compromise of a different device.

Devices shall not contain data which if compromised would directly enable an attacker to compromise one or more other devices deployed in different premises (such as shared keys that would enable the attacker to masquerade as a different device, or a different core device). This requirement applies to all life-cycle stages of the product, following manufacture, and applies to all the interfaces, including any additional to those defined in [d], both external to and within the product's tamper boundary.

DEV.6.M944: 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 meter 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.

DEV.6.M952: Protect access to Privacy PIN

This mitigation is required to counter obtaining the Privacy PIN from stored data

At Foundation Grade the product **is required to** protect the stored Privacy PIN from unauthorised modification or substitution.

Design information shall describe how the device prevents unauthorised attempts to read the Privacy PIN value, or to modify or substitute the stored Privacy PIN to a known value.
The evaluators shall check interface documentation for methods other than normal operational messages by which the Privacy PIN can be accessed or modified.

DEV.7 - Development >> UTRN

DEV.7.M888: Check received UTRNs

This mitigation is required to counter replaying a valid UTRN

At Foundation Grade the product **is required to** reject any UTRN with a UTRN Counter that is lower than the numerically lowest value in the UTRN Counter Cache.

At Foundation Grade the product **is required to** reject any UTRN with a UTRN Counter that matches any of the entries in the UTRN Counter Cache.

DEV.7.M889: Protect UTRN cache

This mitigation is required to counter deleting the UTRN Counter Cache

At Foundation Grade the product **is required to** protect the UTRN Counter Cache from unauthorised modification.

The device shall not allow entries in the UTRN Counter Cache to be modified, nor deleted other than by the normal overwriting action of the circular buffer or by authorised commands.

DEV.7.M892: Validate UTRN authenticity

This mitigation is required to counter attempting to guess a valid UTRN
This mitigation is required to counter modifying credit amount in a UTRN
This mitigation is required to counter modifying target meter of a UTRN

At Foundation Grade the product **is required to** send a response to the Supplier on successful application of UTRN credit entered via the user interface.

A response shall be sent to the Supplier as specified in [d, 14.6] for UTRNs entered via the user interface, or as specified in [d, 14.7] for UTRNs entered via a PPMID.

At Foundation Grade the product **is required to** validate UTRNs received in messages or via the user interface.

A UTRN that fails the authenticity check shall be rejected without being applied.

DEV.7.M893: Notify UTRN validation failures

This mitigation is required to counter attempting to guess a valid UTRN

At Foundation Grade the product **is required to** record UTRN validation failure in the Security Log.

The failures logged are not required to include failures of the UTRN check digit alone.

3.2 Verification mitigations

VER.M846: Secure failure recovery

This mitigation is required to counter disruption of a device by electromagnetic interference
This mitigation is required to counter exploitation of a software implementation/logic error

At Foundation Grade the evaluator **will** attempt to induce failures and observe correct recovery behaviour.

The evaluators shall verify by testing that all of a representative sample of the recognised error conditions are correctly handled. This sample shall include error conditions that do not arise directly as a result of input failures (examples of such a test might be a failure of the power-up firmware integrity verification check or other self-test, or corruption of internal state values; test equipment such as an emulator may therefore be used to enable these tests). The sample shall also include tests of the device's ability to recover from a communications overload (i.e. messages arriving at a rate that exceeds the device's ability to process them), and of the device's ability to resist and/or recover from electromagnetic interference (such as electrostatic discharge).

The evaluators shall provide a rationale that the sample is sufficiently representative, based on the design information relating to error handling.

The evaluator shall also seek evidence that the risk of potentially exploitable bugs in product code (in particular code handling remote incoming messages) will be robustly mitigated against, for instance by one or more product features detecting anomalous code behaviour and responding with a controlled restart.

The recovery action(s) shall be executed only using code that has passed the start-up integrity check for the current execution (since the last reset or power-on). Code that has failed the start-up integrity check shall not be run.

VER.M946: Clock synchronisation

This mitigation is required to counter tampering with the device clock
This mitigation is required to counter vulnerabilities associated with significant clock inaccuracy

At Foundation Grade the evaluator **will** verify correct device behaviour in response to both a Set Clock command and the recurring 24-hour clock synchronisation event.

The evaluator shall confirm, possibly with the assistance of testing performed by the developer, that the device's clock synchronisation functionality complies with section 9 of the version of [d] that the device has been designed to comply with. More specifically, this confirmation will focus on checking that:

- the meter's time gets set to the value expected according to each of the different scenarios in [d, 9].

- the meter's time remains unchanged in all other scenarios in [d, 9].

- the meter's time status gets set to the value expected in all scenarios in [d, 9].

- any responses or alerts are constructed appropriately (containing the expected resultant time and time status where required) and sent to the appropriate destinations as required by the different scenarios in [d, 9].

- any Security Log entries are written as required by the different [d, 9] scenarios.

Additionally, the evaluator shall confirm that if the device fails to receive a response from the Comms Hub with a valid time value, or any response at all, during a recurring 24-hour clock synchronisation event, the meter will attempt to perform the clock synchronisation again, 30 minutes later as required by [d, 9].

At Foundation Grade the evaluator **will** verify that, if any other mechanisms exist to update the device time and time status, that these operate as specified and are protected from unauthorised use.

VER.1 - Verify >> Firmware Protection

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).

VER.2 - Verify >> Interface Protection

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 operational 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.

In addition to the ZigBee and GBCS application layer interfaces, 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.

VER.2.M903: Verify disabled interfaces

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

At Foundation Grade the evaluator **will** verify that ZigBee Inter-PAN is not enabled.

The evaluator shall verify that ZigBee Inter-PAN is disabled on the device (after installation). This shall be confirmed by attempts to use the interface (including transactions that would be valid if the interface had not been disabled).

At Foundation Grade the evaluator **will** verify the state of each disabled interface.

All disabled interfaces present in the operational state of the device (after installation) shall be identified and the disabled state of each shall be verified by visual inspection to verify that it is not possible to use the interface without breaching the tamper-boundary and making the required physical modifications.

The evaluator will ensure that justification has been provided for any interface that is not disabled.

VER.3 - Verify >> Logging

VER.3.M940: Security alerts

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

At Foundation Grade the evaluator **will** confirm raising of alerts for security-related events and error conditions.

The evaluator shall confirm by testing that the device correctly raises the alerts defined in [d, 16] for security-related events and error conditions.

VER.3.M941: Security logging

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

At Foundation Grade the evaluator **will** confirm Security Log recording.

The evaluator shall confirm by testing the correct logging of each type of event that can be recorded in the Security Log as defined in [d, 16].

VER.4 - Verify >> Message Protection

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 only those specified in [d], including those primitives used by all UTRN validation functionality in the device.

VER.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 evaluator **will** confirm device behaviour leading to cancellation of future-dated actions.

The evaluator shall confirm by testing:

- that when the device clock is updated it neither misses nor repeats actions previously stored for future action nor misses calendar-based events

- that a future-dated action can only be added, replaced, modified or cancelled by an authentic message from a source authorised to issue the command, and that a response is sent by the device, identifying the successful processing of the new command.

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

VER.4.M887: Encrypt sensitive data in messages prior to transmission

This mitigation is required to counter interception of messages on WAN

At Foundation Grade the evaluator **will** verify encryption of sensitive data in commands, responses and alerts.

The evaluator shall confirm by testing that the device correctly encrypts the sensitive data specified in [d, 19.3] in accordance with the encryption mechanisms specified in [d, 8].

VER.4.M904: Confirm standard protocol certification

This mitigation is required to counter exploitation of incorrect protocol implementation

At Foundation Grade the evaluator **will** confirm standard protocol certification of the device has been successfully completed.

The device shall be certified as specified in this document in section 1.6 Interoperability.

VER.4.M927: Check only valid messages accepted

This mitigation is required to counter creation of unauthorised commands

At Foundation Grade the evaluator **will** verify that critical commands are not executed if the sender of the command cannot be successfully authenticated or is not authorised to send that command.

The evaluator will attempt to issue critical commands that should be rejected. This will include commands sent from an unauthorised sender, and a non-authentic sender, as well as commands that are not valid for the type of device under test, and commands that are intended for a different device.

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.

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.

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.

VER.4.M951: Mutual authentication on the HAN

This mitigation is required to counter connecting an unauthorised device to the HAN

At Foundation Grade the evaluator **will** confirm that removal of the other device's entry from the product's Device Log will result in the encrypted link between the product and other HAN device being terminated (i.e. it will no longer be possible for application data to be exchanged between the two devices).

At Foundation Grade the evaluator **will** confirm that the product authenticates a device on the HAN before securely exchanging information with it.

The evaluator shall confirm that:

- The product will only successfully join to another HAN device according to the different scenarios permitted for the join to occur in [d, 13.7].

- The product will not attempt to join to the other HAN device in other scenarios such as (a) the other device is of a type that the product is not permitted to communicate with, (b) the other device's details are not in the product's Device Log, (c) the other device's details are mismatched with details in the product's Device Log and (d) the other device's key pair is mismatched with the security credentials held for that device in the product's Device Log.

- Only once a successful join has occurred, will application data be exchanged between the product and the other HAN device, this data being encrypted using a symmetric key agreed by the two devices in accordance with [d, 13.7].

VER.4.M954: Verify security credential protection

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

At Foundation Grade the evaluator **will** verify the authenticity protection of security credentials.

The evaluator shall attempt to modify or substitute (by circumventing the documented protection mechanisms) stored Device Security Credentials and Remote Party Security Credentials, without having authorised access to modify this data. The testing should include a search of interface documentation for methods other than normal operational messages.

VER.5 - Verify >> Physical Protection

VER.5.M849: Tamper response

This mitigation is required to counter access to structures inside the tamper-protection boundary of the device

At Foundation Grade the evaluator **will** validate the developer's assertions regarding tamper response.

The evaluator shall verify by testing that removing or opening any part of the tamper boundary that is designed to be separately removed or opened results in an entry being recorded in the Security Log and the sending of an alert.

VER.5.M897: Protection of security-related physical structure

This mitigation is required to counter unauthorised physical access to security-critical data stored on the device

At Foundation Grade the evaluator **will** confirm the tamper-protection boundary.

The evaluator shall confirm that the outer casing of the device is a metal, hard plastic, or equivalent Production Grade enclosure. The device casing shall not allow inspection or visibility of the internal layout or components of the device, other than by breach of the tamper-protection boundary, and shall therefore be opaque within the visible spectrum (other than areas required to provide visibility of a user interface). This may be achieved by the case itself or by a lining applied to the case.

VER.6 - Verify >> Sensitive Data Protection

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 the meter'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.

VER.6.M928: Restrict data on change of tenancy

This mitigation is required to counter reading previous tenants' information in an operational meter

At Foundation Grade the evaluator **will** verify correct meter response after a Restrict Data command.

The evaluator shall confirm by testing that the ESME correctly omits the restricted data from any data returned to Type 1 and Type 2 Devices, according to the date of restriction.

The specific items to which provision is restricted are identified in the Set Change of Tenancy date Use Case in [d, 19].

VER.6.M944: 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 evaluator **will** verify that a Privacy PIN must be 4 digits.

At Foundation Grade the evaluator **will** verify that the Privacy PIN is required before access to protected data and commands.

The evaluator shall confirm by testing that, if Privacy PIN Protection is enabled, the meter shall require entry of the Privacy PIN through the user interface to enable temporary access to the restricted display items and the restricted User Interface Commands.

The evaluator shall confirm, by testing, the period for which temporary access is granted.

VER.7 - Verify >> UTRN

VER.7.M894: Limit rate of UTRN validation attempts

This mitigation is required to counter attempting to guess a valid UTRN
This mitigation is required to counter blocking UTRN acceptance by causing repeated validation failures by manual entry

At Foundation Grade the evaluator **will** confirm the rate limiting of unsuccessful UTRN validation attempts.

The mechanism for limiting the rate of validation attempts shall not result in a period of nonacceptance of longer than 60 minutes. UTRNs input by manual entry, through the user interface or via a PPMID, during any period of non-acceptance shall be discarded without attempting to validate the UTRN.

Note: Rate-limiting via the PPMID should be independent to that via the user interface. For instance, a temporary block on UTRN entry via PPMID does not in itself cause UTRN entry via the user interface to also be blocked.

VER.7.M961: Confirm correct UTRN processing

This mitigation is required to counter attempting to guess a valid UTRN
This mitigation is required to counter modifying credit amount in a UTRN
This mitigation is required to counter modifying target meter of a UTRN

At Foundation Grade the evaluator **will** confirm that the product correctly processes valid UTRN values, received via the user interface and PPMID.

The evaluator will confirm that a sample of valid UTRNs are accepted via both user interface and PPMID and, in each instance, will result in (a) the meter's balance being adjusted by the amount specified in the given UTRN and (b) an appropriate response message being sent to the Supplier to reflect the adjustment. Note: There is an expectation that evaluator may be able to reuse testing that developers are performing in this area as evidence for this requirement.

At Foundation Grade the evaluator **will** seek evidence of developer testing that demonstrates the product will always reject a non-authentic UTRN value, received via the user interface and PPMID.

This is intended to supplement other testing requirements elsewhere in the Security Characteristic and confirm that the code handling incoming UTRNs is sufficiently robust that, if any exceptional circumstances are encountered during processing, the default behaviour will be to reject the UTRN (i.e. fail-safe).

3.3 Deployment mitigations

DEP.M906: Installation, initialisation and operation guidance

This mitigation is required to counter exploitation of a software implementation/logic error
This mitigation is required to counter exploitation of device with incorrect installation or configuration

At Foundation Grade the deployment **is required to** state device manufacturer guidance on secure installation, initialisation and operation.

Guidance shall address any manufacturer required actions and recommendations for establishing and maintaining secure operation of the device.

(For clarity: this requirement is stated here explicitly, in addition to the implicit guideline in [a], to ensure attention is given to completeness of product-specific guidance, including any additional functionality, especially as the installation, initialisation and operation may be the responsibility of different parties in the GB Smart Metering operational environment.).

DEP.M946: Clock synchronisation

This mitigation is required to counter incorrect initialisation of the device clock

At Foundation Grade the deployment **is required to** set the clock on a device on installation.

On installation the device has unreliable time until it receives a command to set its clock. To reduce the risk of time-based commands and functions being carried out at the wrong time, Suppliers should send the appropriate Set Clock commands to the device within a reasonable period of receiving notice that the device has been commissioned.

DEP.1 - Deployment >> Interface Protection

DEP.1.M873: Disable non-operational logical and physical interfaces

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

At Foundation Grade the deployment **is required to** include guidance on requirements to manage non-operational interfaces.

DEP.2 - Deployment >> Logging

DEP.2.M39: Audit log review

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

At Foundation Grade the deployment **is required to** regularly review the Security Log for unexpected entries.

The device is required to record security-significant events in the Security Log, in order to help prevent attacks from remaining undetected. The deployment should take appropriate steps to ensure all log entries are read from the device before being overwritten.

DEP.3 - Deployment >> Message Protection

DEP.3.M871: Data reconciliation

This mitigation is required to counter blocking of messages/responses
This mitigation is required to counter modification of stored data in the device

At Foundation Grade the deployment **is required to** implement procedures for reconciliation of data read from the meter with data expected to be present as a result of commands sent.

Reconciliation should address the potential for uncertainty over both the correct completion of meter actions taken in response to messages, and confirmation of expected meter state.

DEP.3.M876: Restrict ability for devices to join HAN

This mitigation is required to counter observing inter-device HAN messages

At Foundation Grade the deployment **is required to** ensure that only appropriately authorised devices can join a meter related HAN.

'Appropriate authorisation' is obtained from the DCC or other relevant authority to enable the device to join the HAN according to [f, 5.4], as specified in [d, 4] and [d, 13].

DEP.4 - Deployment >> Physical Protection

DEP.4.M925: Tamper evident seals on the perimeter

This mitigation is required to counter access to structures inside the tamper-protection boundary of the device

At Foundation Grade the deployment **is required to** place tamper evident seals at access points on product.

Use tamper evidence seals (e.g. stickers) to make entry to system internals detectable by physical inspection. Tamper seals should be of restricted availability, or should require use of a special tool with restricted availability, to prevent an attacker successfully replacing one with a new, undamaged seal.

At Foundation Grade the deployment **is required to** provide advice on the tamper threat and tamper seal inspection.

Advice should include looking for possible damage to tamper evident seals.

DEP.5 - Deployment >> Sensitive Data Protection

DEP.5.M921: User advice on Privacy PIN entry

This mitigation is required to counter guessing the Privacy PIN
This mitigation is required to counter observing the Privacy PIN during PIN entry

At Foundation Grade the deployment **is required to** issue advice to users on selection, secure handling and entry of Privacy PIN.

DEP.5.M928: Restrict data on change of tenancy

This mitigation is required to counter reading previous tenants' information in an operational meter

At Foundation Grade the deployment **is required to** issue a Restrict Data command on change of tenancy.

DEP.5.M933: Protect devices after decommissioning

This mitigation is required to counter directly accessing structures and interfaces in a decommissioned device

At Foundation Grade the deployment **is required to** implement procedures for secure recommissioning when previously-installed devices are re-installed.

The operating procedures shall include secure deletion of previous sensitive data before a device is re-installed, and secure disposal procedures for devices that are not to be re-installed (whether due to failure, age, or other reasons).

At Foundation Grade the deployment **is required to** recover and ensure secure disposal of devices at the end of their life.

DEP.5.M953: Initialisation of Security Credentials

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 deployment **is required to** ensure new Security Credentials are generated by the device once it is installed.

Although there will already be Device Security Credentials on the device before installation, once an installed device becomes operational it should be sent commands to ensure that new Security Credentials are issued by the device to replace those already present.

DEP.6 - Deployment >> UTRN

DEP.6.M895: Reconcile UTRN usage

This mitigation is required to counter attempting to guess a valid UTRN

At Foundation Grade the deployment **is required to** reconcile records of UTRNs successfully applied with those issued.

Appendix A References

This document references the following resources.

Label	Title	Location	Notes
[a]	Process for Performing CPA Foundation Grade Evaluations	https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa	Latest
[b]	Smart Metering Equipment Technical Specifications (SMETS)	https://smartenergycodecompany.co.uk/ (Navigate to “Smart Energy Code”, then “SEC Sections”, then “SEC Schedule 9”.)	There will be at least one version of SMETS relevant to this Security Characteristic, that version (or versions) being defined in the TS Applicability Tables that can be found via the stated URL.
[c]		(Intentionally blank)	
[d]	Great Britain Companion Specifications (GBCS)	https://smartenergycodecompany.co.uk/ (Navigate to “Smart Energy Code”, then “SEC Sections” , then “SEC Schedule 8”.)	There will be at least one version of GBCS relevant to this Security Characteristic, that version (or versions) being defined in the TSAT [h].
[e]	Communications Hub Technical Specifications (CHTS)	https://smartenergycodecompany.co.uk/ (Navigate to “Smart Energy Code”, then “SEC Sections” , then “SEC Schedule 10”.)	There will be at least one version of CHTS relevant to this Security Characteristic, that version (or versions) being defined in the TSAT [h].
[f]	ZigBee Smart Energy (ZSE) Profile Specification	http://zigbee.org/About/GBCSPartner.aspx	Version(s) of the ZigBee documents used in the development of GBCS are stated in the relevant version of GBCS [d].
[g]	Smart Energy Code	https://smartenergycodecompany.co.uk/ (Navigate to “Smart Energy Code”)	Latest
[h]	Technical Specification Applicability Tables (TSAT)	https://smartenergycodecompany.co.uk (Navigate to “Smart Energy Code”, then “SEC Sections”, then “SEC Schedule 11”.)	The TSAT identifies the relevant version of the CPA SC’s to be used to ascertain compliance with requirements stated in the relevant version of GBCS associated with the version of SMETS that the product is being developed to meet.

Label	Title	Location	Notes
[i]	End to End Technical Architecture	https://smartenergycodecompany.co.uk (Specific link, correct at time or writing, is: https://smartenergycodecompany.co.uk/download/14738/.)	Provides an entry point into a wider set of technical specifications that describe the requirements for the GB SMIP. This document is informative only and should be treated as such.

Appendix B Glossary

The following definitions are used in this document.

Term	Definition
ALCS	Auxiliary Load Control Switch. A switch controlling a load on the supply.
Alert	A message generated by a device including in response to a problem or the risk of a potential problem
API	Application Programming Interface
CAD	Consumer Access Device – a component that allows consumer devices to be connected to the SMHAN to retrieve certain information.
CAVP	Cryptographic Algorithm Validation Programme – a scheme administered by the US National Institute of Standard and Technology (NIST) for validation testing for Federal Information Processing Standards (FIPS) approved and NIST recommended cryptographic algorithms and components of algorithms.
CHF	Communications Hub Function
Command	An instruction to perform a function, received or sent via any interface.
Communications Broker	Data and Communications Provider serving as an intermediary between Service Users and Smart Metering Equipment.
Communications Hub	A device or set of devices located at the consumer's premises which will have the capability to communicate with the SMHAN and the SMWAN.
Communications Link	The exchange of Commands, Responses, Alerts and other information between a system or Device and another system or Device which is independent of the transport mechanism used.
Configuration Data	Describes data that configures the operation of various functions of the Smart Metering Equipment.
Constant Data	Describes data that remains constant and unchangeable at all times.
CoS	Change of Supplier. The process initiated by a consumer resulting in a change of ownership with respect to their registered energy supplier.
CPA	Commercial Product Assurance. A scheme run by NCSC providing certificate-based assurance of commercial security products.
Credit Mode	A mode of operation of GSME or ESME whereby consumers are billed for some or all of their consumption retrospectively
Critical Commands	Those Commands which relate to supply being affected, financial fraud or the compromise of consumer premises equipment security.

Term	Definition
Data Store	An area of storage in the Device capable of storing data. In the ESME this contains Constant Data, Configuration Data and Operational Data.
Day	The period commencing 00:00:00 Local Time and ending at the next 00:00:00
Device	A physically or logically distinct part of a system.
Device Log	The Security Credentials and Device identifier for each of the Type 1 Devices and the Device identifier for each of the Type 2 Devices with which ESME can establish Communications Links.
DLMS COSEM	Device Language Message Specification / Companion Specification for Energy Metering – an application layer protocol.
Entropy Source	A source of unpredictable data. There is no assumption that the unpredictable data has a uniform distribution. The Entropy Source includes a noise source, such as thermal noise or hard drive seek times; a digitization process; an assessment process; an optional conditioning process and health tests.
ESME	Electricity Smart Metering Equipment
Event Log	A log for storing UTC date-and-time-stamped entries of non-security related information for diagnosis and auditing
Failure-related activity	Security relevant activity for a meter when recovering from a failure: - power-on processing - storage of sensitive data - performing cryptographic processing - random number generation - maintaining supply state.
Firmware	The embedded software programs and/or data structures that control electronic Devices.
Foundation Grade	In this document, Foundation and Foundation Grade are used in the context of the CPA scheme as in reference [a].
Gas Proxy Function	A device used to store GSME and related data
GPF	Gas Proxy Function
GSME	Gas Smart Metering Equipment
HAN	Smart Metering Home Area Network
HCALCS	HAN Connected Auxiliary Load Control Switch. An ALCS with its own HAN interface.
HHT	Handheld Terminal – an optional device used in the installation and maintenance of Smart Metering Equipment within the consumer's premises.
IHD	In-Home Display
Key Agreement	A means to calculate a shared secret between two parties, without that shared secret being sent between the two parties.

Term	Definition
Load Switch	A component or combination of components that can close or open (including on receipt of a Command to that effect) to enable or disable the flow of electricity to and from the premises.
Local Time	The UTC date and time adjusted for British Summer Time.
MAC	Message Authentication Code
Message	A message, as defined in [d, 3.1], sent or received by a Device, which is one of a Command, a Response or an Alert. Messages are categorised as either Critical or Non-Critical. Messages sent by a Device on the HAN to another Device on the same HAN are classified as HAN Only Messages. Messages that are sent between a Device on the HAN and another entity external to the HAN (a Remote Party) routed through the Communications Hub and (usually) the WAN, are classified as Remote Party Messages.
MISRA	Motor Industry Software Reliability Association
Non-operational interface	Interface that is not required for normal operation of the device and that is not therefore governed by the requirements in reference [b].
Normal operation	Steady State Operation.
Operational Data	Describes data used by the functions of the Smart Metering Equipment for output of information.
Operational interface	Interface that is required for normal operation of the device and that is therefore governed by the requirements in reference [b].
Personal Data	Any information comprising Personal Data as such term is defined in the Data Protection Act 1998.
PPMID	Prepayment Interface Device – an optional device that replicates the prepayment user interface of a GSME and ESME.
Prepayment Mode	A mode of operation of GSME or ESME whereby payment is generally made in advance of consumption
Privacy PIN	A number used by the consumer to access Personal Data on the user interface of ESME and GSME
PRNG	Pseudo Random Number Generator – software for generating a sequence of numbers that approximates the properties of random numbers.
Production Grade	Designed to meet commercial-grade specifications for power, temperature, reliability, shock and vibration, etc.
RBAC	Role-Based Access Control. Smart Metering Equipment is capable of restricting Authorisation to execute Commands and of issuing Alerts according to Role permissions.
Response	A message sent on or received from, the User Interface or HAN Interface or any other interface, containing information in response to a Command.

Term	Definition
RNG	Random Number Generator – A component used to generate a sequence of numbers that can be interpreted as numbers, letters or symbols that lack any predictable pattern.
SC Map	Diagrammatic representation of a Security Characteristic (or part of one).
Security Characteristic	A standard which describes necessary mitigations which must be present in a completed product, its evaluation or usage, particular to a type of security product.
Security Credentials	Information used to identify and/or authenticate a Device, individual or system.
Security Log	A log for storing UTC date-and-time-stamped entries of security related information for diagnosis and auditing
Security Strength	A number associated with the amount of work (that is, the number of operations) that is required to break a cryptographic algorithm or system; a security strength is specified in bits and is a specific value from the set (112, 128, 192, 256). The amount of work needed is $2^{security\_strength}$.
Security-Critical Data	Data that would enable an unauthorised person to defeat cryptographic or secret-based mechanisms. This therefore includes data such as cryptographic keys or PIN values.
Security Sub-Committee	The Sub-Committee established by the panel in accordance with Smart Energy Code Section 7.1
Sensitive Data	Data which is defined as personal data under the Data Protection Act 1998, or which is considered to be Personal Data due to public perception of the system. This will include cryptographic key material, and the contents of the Data Store.
Sensitive Event	Each of the following events: a failed authentication or authorisation; a change in the executing firmware version; the detection of unauthorised physical access or any other occurrence that has the potential to put Supply at risk and/or compromise the Integrity of GSME or ESME; and unusual numbers of malformed, out-of-order or unexpected commands received.
Shared Secret	A number which is established by two parties through the Key Agreement technique specified in [d] and which can be used as input to a Key Derivation Function (KDF).
Smart Energy Code	The regulatory code designated by the Secretary of State pursuant to the Data Communications Company (DCC) Licence, and subject to modification in accordance with the Secretary of State's statutory powers and the DCC Licence.
Smart Metering Equipment	Equipment that meets the Smart Metering Equipment Technical Specification [b].

Term	Definition
Steady State Operation	The phase in a Device's lifecycle where it is (1) installed in a consumer's premises and (2) is configured so that it can perform the range of operational functions required by [b].
Time-of-use Band	A contiguous or non-contiguous number of Days for GSME or half-hour periods for ESME over which tariff prices are constant.
Time-of-use Pricing	A pricing scheme with one or more Time-of-use Bands.
TSAT	Technical Specification Applicability Tables, reference [h]
Type 1 Device	A Device, other than GSME, ESME, Communications Hub, CHF or GPF, that stores and uses the Security Credentials of other Devices for the purposes of communicating with them via its HAN Interface
Type 2 Device	A Device that does not store or use the Security Credentials of other Devices for the purposes of communicating with them via its HAN Interface.
UTC	Coordinated Universal Time
UTRN	Unique Transaction Reference Number. A cryptographic code used to convey credit to GSME or ESME operating in Prepayment Mode.
UTRN Counter Cache	An array of stored entries relating to validated UTRNs.
WAN	Smart Metering Wide Area Network
Whitelist	The CHF Device Log acts as a whitelist for all devices that are allowed to communicate on the HAN.

Appendix C Message Protection

A message sent or received by a Device will be one of a Command, a Response or an Alert. A Response is the result of a Command, while an Alert may be triggered by other events.

Messages are categorised as either Critical or Non-Critical. All messages are required to have integrity and authenticity protection, while Critical messages must have non-repudiation protection, and some specific data content (such as personal data) must have confidentiality protection.

Messages sent by a Device on the HAN to another Device on the same HAN are classified as HAN Only Messages and the cryptographic protections applied to such messages are those provided by ZigBee, as detailed in [f, 5.4].

Messages that are sent between a Device on the HAN and another entity external to the HAN (a Remote Party) routed through the Communications Hub and (usually) the WAN, are classified as Remote Party Messages and are protected by an End-to-End security architecture, detailed in [d, 4], based upon asymmetric cryptography using certificates as Security Credentials, detailed in [d, 12]. See below for information about the cryptographic primitives.

Remote Parties include organisations such as Suppliers, Network Operators, the Access Control Broker (ACB) and WAN Providers. Each Remote Party has a Public-Private Key Pair, with a Security Credential to make its Public Key available, enabling messages from it to be authenticated by a Device. Note that Remote Parties have separate credentials for signing and key agreement, see [d, 4.3] for details.

Protection of Remote Party Messages, described in [d, 4], [d, 5] and [d, 6], is achieved as follows:

- A Command that is sent from a Remote Party to a Device is constructed by the Remote Party and sent to the ACB.
  The ACB adds integrity and authenticity protection to the message by applying a MAC.
  The message is sent to the Device which will validate and check the message, including verifying the ACB's MAC.
  If the checks are successful the Device will execute the Command.
  The Device will construct a Response and apply a MAC that can be verified by the Remote Party, then send the Response to the ACB.
  The ACB will pass the Response back to the Remote Party which will verify the MAC.
- If the Command is a Critical Command the Remote Party will sign the Command to provide non-repudiation, before sending it to the ACB.
  In this case the Device checks will include verifying the Remote Party's signature as well as the ACB's MAC.
  If the checks are successful the Device will execute the Command.
  The Device will construct a Response and sign it, then send the Response to the ACB.
  The ACB will pass the Response back to the Remote Party which will verify the signature.
- Similarly, an Alert that is sent by a Device has a MAC applied that can be verified by the Remote Party.
  If it is a Critical Alert, it will have a signature rather than a MAC.

Where data items require confidentiality protection within a message, the AES GCM primitives (see below) are used to encrypt the data as described in [d, 8].

Each Device on the HAN (apart from Type 2 Devices) has its own Public-Private Key Pair, and a Device Security Credential to make its Public Key available, enabling it to be identified and authenticated. It is capable of securely holding a set of Security Credentials for Remote Parties with which it will need to communicate. It also maintains a Device Log in which it holds the Device Security Credentials of other Devices on the HAN with which it is authorised to communicate.

To communicate on the HAN, a Device must establish a secure ZigBee connection with the Communications Hub. The Communications Hub Function maintains its own Device Log that acts as a whitelist for those Devices allowed to communicate on the HAN. Device Security Credentials are added to a Device's Device Log by a command from an appropriate Remote Party, see [d, 13] for details.

Some messages require anti-replay protection as described in [d, 4.3]. Some messages may be future-dated as described in [d, 9.2].

C.1 Cryptographic primitives

Remote Party Messages are protected using:

- SHA-256, as specified in FIPS 180-4, as the Hash function;
- the AES-128 cipher, as specified in FIPS 197, as the block cipher primitive;
- the Galois Counter Mode (GCM) mode of operation as specified in NIST Special Publication 800-38D;
- the GMAC technique, based on the use of AES-128, for the calculation of Message Authentication Codes (MACs), as specified in NIST Special Publication 800-38D;
- the Digital Signature technique, ECDSA (as specified in FIPS PUB 186-4) in combination with the curve P-256 (as specified in FIPS PUB 186-4 at Section D.1.2.3) and SHA-256 as the Hash function; within messages, Signatures shall be in the Plain Format;
- calculation of a Shared Secret Z, using the Static Unified Model, C(0e, 2s, ECC CDH) Key Agreement technique (as specified in *NIST Special Publication 800-56Ar2* save for the requirement to zeroise the Shared Secret) with:
  - the Single-step Key Derivation Function (KDF) based on SHA-256, as specified in *NIST Special Publication 800-56Ar2*; and
  - the P-256 curve for the elliptic curve operations.

  Resulting DerivedKeyingMaterial (with its meaning in *NIST Special Publication 800-56Ar2*) shall only ever be used in relation to one Message Instance. Any Shared Secret that is not 'zeroised' shall be stored and used with the same security protections as Private Keys.

A Random Number Generator with a suitable Entropy Source is used in the generation of the Public-Private Key Pair on the Device.

The ZigBee HAN encryption uses the AES-128 cipher in CCM* mode with MMO as the hash function. Key establishment is achieved using Certificate-Based Key Establishment (CBKE), between a device and the Communications Hub which acts as a ZigBee Trust Center. Further details can be found in [f, 5.4] and [f, c.4].

Appendix D Summary of changes to mitigations

NCSC has updated the Electricity Smart Metering Equipment Security Characteristic v1.3 (previously version 1.2) for the following reasons.

- Clarifications to certain SC wording where it was potentially open to interpretation.
- Improvements to some assurance activities for certain product security-enforcing functionality.

This has resulted in the following changes to the mitigations.

D.1 Removed mitigations

The following mitigation has been removed.

- VER.7.M4: Evaluation/Cryptocheck (Note: All cryptographic checks are covered by VER.4.M4)

D.2 Modified mitigations

The following mitigations have been modified.

- DEV.M926: Protected software environment
- DEV.M946: Clock synchronisation
- DEV.2.M847: Minimise interfaces
- DEV.4.M138: State the Security Strength required for random numbers (title also changed to: "DEV.4.M134: State raw entropy requirements")
- DEV.4.M140: Smooth output of Entropy Source with approved PRNG
- DEV.4.M141: Reseed PRNG as required
- DEV.4.M290: Employ an approved Entropy Source
- DEV.4.M853: Prevent unauthorised changes to future-dated actions
- DEV.4.M911: Self-test of RNG
- DEV.4.M951: Mutual authentication on the HAN (title also changed to: "VER.4.M951: Mutual authentication on the HAN")
- DEV.7.M894: Limit rate of UTRN validation attempts (title also changed to: " VER.7.M894: Limit rate of UTRN validation attempts")
- VER.M846: Secure failure recovery
- VER.M946: Clock synchronisation
- VER.1.M347: Verify update mechanism
- VER.2.M80: Protocol robustness testing
- VER.4.M4: Evaluation/Cryptocheck
- VER.4.M853: Prevent unauthorised changes to future-dated actions
- VER.4.M855: Receiver replay check
- VER.4.M939: Enable update of security credentials
- VER.6.M917: Verify logical protection of keys – (title also changed to “VER.6.M917: Verify logical protection of security data”)
- DEP.5.M934: Unique security data per device (title also changed to “DEV.6.M934: Unique security data per device”)
- DEP.5.M953: Initialisation of Security Credentials

D.3 Renamed mitigations

Some mitigations have been renamed as part of being modified, please see Modified Mitigations above

D.4 New mitigations

The following new mitigations have been added.

- VER.7.M961: Confirm correct UTRN processing

Appendix E Stack Protection Expectations

A sufficiently robust level of stack protection is expected by products complying with this Security Characteristic that provides the following features as a minimum (which are typically on a par with those provided via a stack protection compiler option):

- Detect corruption of a function return address before the function returns to that address. i.e. The corrupted return address will not be used, and appropriate remediation action will be performed instead, such as rebooting the product into a good known state.
- Be present in functions that have one or more arrays declared in the function's stack frame (this includes third party library code within the same runtime environment as the application code).
- If canaries are used to detect corruption, then:
    - The size of the canaries must be at least that of a memory pointer for the device's platform (e.g. canary size would need to be at least 32 bits for a 32-bit architectural).
    - The values used for the canaries must vary across different devices in a non-predictable manner (not necessarily reliant on the same RNG function used to generate cryptographic key material).
    - Additionally, the canary value should also change in a specific device each time the product (re)boots, though this is not mandatory.

Note: Although it would be desirable to detect overflow of one stack variable into another, this is not mandatory for products complying with this Security Characteristic.