

CPA Security Characteristic

Smart Metering – Communications Hub

The latest versions of these CPA Security Characteristics are applicable and earlier versions are available for reference.

Note that, from October 2024, the Smart Energy Code (SEC) places the ownership of the CPA Scheme and responsibility for the CPA Security Characteristics with the SEC Security Sub-Committee (SSC).

References to 'NCSC', 'the CPA Authority' or 'CESG' in this document should therefore be read as 'SEC SSC'.

CPA Scheme Operator enquiries should be made to:

CPA.enquiries@cytal.co.uk

SSC and SECAS contact details reported in this document have changed and the following should be used instead:

- Address: 2nd floor, 77 Gracechurch St, City of London, London EC3V 0AS
- Email: SSC@talan.com
- Tel: + 44 (0) 207 090 7755

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 Smart Metering Communications Hub security 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 Evaluations².

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: 54932836

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	Aug 2017	Updated to align with Technical Specs (GBCS, CHTS and SMETS) released 16 September 2016.

This document is derived from the following SC Maps:

SC Map	Map Version
SmM CH SC	1.4
SmM Crypt SC Library	1.3
SmM Device SC Library	1.4

Contact SECAS or the NCSC

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

SECAS Contact Details (For general queries about this document)	NCSC Contact Details (For specific queries about the CPA Scheme)
SECAS 77 Gracechurch Street, London EC3V 0AS Email: ssc@talan.com Tel: + 44 (0) 207 090 7755	CPA Administration Team NCSC, Hubble Road, Cheltenham, Gloucestershire GL51 0EX, UK Email: cpa@ncsc.gov.uk Tel: +44 (0)1242 221 491

¹ www.gemserv.com/industry-initiatives/secas

² www.ncsc.gov.uk/document/cpa-scheme-library

Contents

1	Overview	4
1.1	Introduction	4
1.2	Product description	4
1.3	Typical use cases	4
1.4	Expected operating environment	4
1.5	Compatibility	5
1.6	Interoperability	5
1.7	High level functional components	6
1.8	Future enhancements	7
2	Security Characteristic Format	8
2.1	Requirement categories	8
2.2	Understanding mitigations	8
3	Requirements	10
3.1	Development mitigations	10
3.2	Verification mitigations	26
3.3	Deployment mitigations	34
Appendix A	References	38
Appendix B	Glossary	39
Appendix C	Message Protection	42
Appendix D	Summary of changes to mitigations	44
D.1	Removed mitigations	44
D.2	Modified mitigations	44
D.3	Renamed mitigations	44
D.4	New mitigations	44

1 Overview

1.1 Introduction

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

1.2 Product description

The Communications Hub is a hybrid device which includes two logically separate functions, the Communications Hub Function (CHF) and the Gas Proxy Function (GPF). The CHF manages communications between devices within the premises and acts as a 'bridge' between the Smart Metering Home Area Network (HAN) and the Smart Metering Wide Area Network (WAN). The GPF operates as a proxy device for the Gas Smart Metering Equipment (GSME), in order to accurately and securely record and transmit, where appropriate, information about gas usage in a smart metered property.

The key security concerns relating to the Communications Hub are:

- Protect Personal Data (received by GPF from GSME) from unauthorised access:
 - HAN Only messages sent by GSME to the GPF, including those that may contain Personal Data, are encrypted using ZigBee. Similarly, HAN Only messages sent from the GPF to other in-home devices (e.g. In-Home Display) that may contain Personal Data will also be ZigBee encrypted.
 - Ensure Personal Data sent in Remote Party Messages over the WAN (via the CHF) is encrypted (see Appendix C).
- Availability – the CHF is a single point of failure for communications into consumer premises and must be protected against Denial of Service attacks or compromise of the device 'whitelist'.
- Provision of accurate time source – the CHF is used to regularly synchronise the time for ESME and GSME, which augments message validation checks and execution of future dated action on those devices.

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 Communications Hub is to be deployed at consumer premises along with other equipment. The GSME and Electricity Smart Metering Equipment (ESME) communicate through a HAN with the Communications Hub. The Communications Hub also provides communications between the HAN and a WAN, 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). In certain circumstances, for example non-domestic consumers, Energy Suppliers may elect to communicate directly with Smart Meters without using the DCC. In this case, they are assumed to be performing the role of the Communications Broker.

The equipment to be deployed at consumer premises will consist of the Communications Hub, 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. One or more Auxiliary Load Control Switch (ALCS) may also be installed, either within the ESME or as separate devices with their own HAN interface (HCALCS).

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 device.

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

Section 3.1.4 (Business Interactions) of the End to End Technical Architecture document provides further context on the expected operating environment, the document is available on the SECAS website: (<https://www.smartenergycodecompany.co.uk>).

1.5 Compatibility

There are no compatibility requirements.

1.6 Interoperability

The Communications Hub should be interoperable with the Communications Broker and other Smart Metering Equipment deployed in the consumer premises. Interoperability is achieved through the following 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	External Certification
Conformance with CHTS.	Reference [e]	N/A – No external certification required for CPA compliance.
Conformance with the Great Britain Companion Specifications. The Communications Hub shall be certified by the ZigBee Alliance as compliant with the ZigBee requirements identified in the Great Britain Companion Specifications.	Reference [d]	ZigBee, as per details in GBCS
The Communications Hub shall be interoperable with DCC systems such that the DCC need not make any adjustments to its systems in order to establish Communications Links with the Communications Hub via its WAN Interface.	Reference [d]	N/A – No external certification required.

1.7 High level functional components

The following diagram illustrates the various high level functional components within this product 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 the Communications Hub, see reference [e].

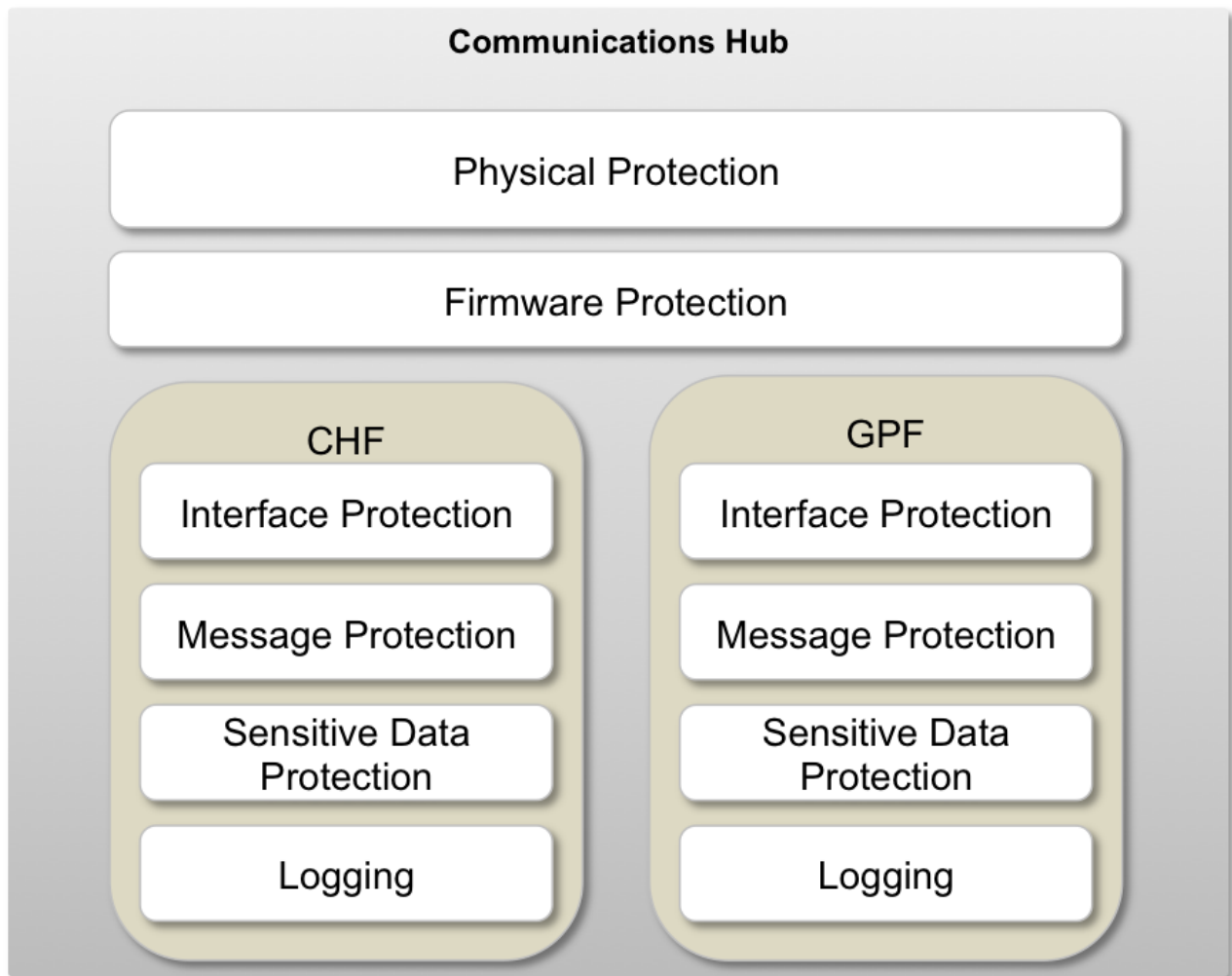


Figure 1: Functional components of a Smart Metering Communications Hub

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, 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 [e, 4.3].
- **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 [e, 4.4.6].
- **CHF.** Communications Hub Function, functionality specific to the operation of the Communications Hub as a bridge between the WAN and the HAN.

- **GPF.** Gas Proxy Function, functionality specific to the operation of the Communications Hub as a proxy device for the GSME.
- **Interface Protection.** Operational interfaces on the Smart Metering Equipment comply with security requirements in reference [e, 4.5] 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. ZigBee Inter-PAN can also be enabled to allow an authorised HHT to connect for the installation and maintenance of Smart Metering Equipment. The device also includes a WAN interface to enable secure communications with the WAN Provider. Any additional non-operational interfaces should be considered by evaluators in the context of both CHF and GPF if they do not apply specifically to either.
- **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. Messages are protected while they are buffered waiting to be delivered to the WAN, and while they are buffered waiting to be delivered to the GSME. The clock in the device provides a time source against which ESME and GSME can synchronise their clocks, and 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.** Personal Data is protected against unauthorised access. Keys that are used by cryptographic mechanisms to maintain various aspects of the Communications Hub 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 [e, 4.6].
- **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 [e, 4.6.3]) 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

SECAS, BEIS and NCSC 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.

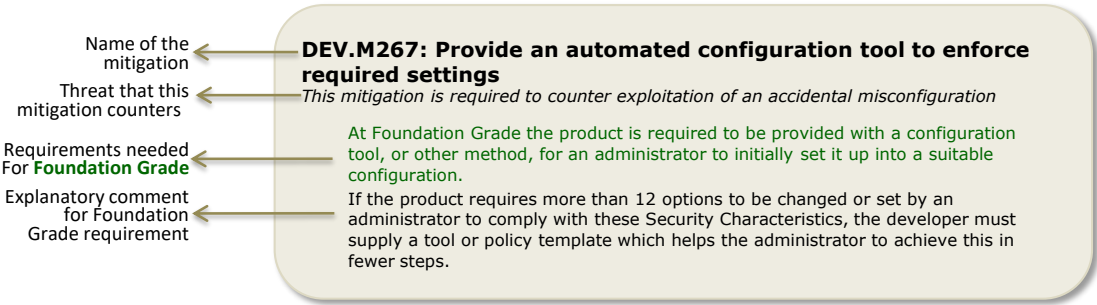


Figure 2: Components of a typical mitigation

3 Requirements

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

3.1 Development mitigations

DEV.M42: Heap hardening

This mitigation is required to counter exploitation of a software implementation/logic error in the Communications Hub

At Foundation Grade the product **should** use the memory management provided by the operating system. Products should not implement their own heap.

DEV.M43: Stack protection

This mitigation is required to counter exploitation of a software implementation/logic error in the Communications Hub

At Foundation Grade the product **is required to** be compiled with support for stack protection including all libraries, where the tool chain supports it.

If more recent versions of the tool chain support it for the target platform then they should be used in preference to a legacy tool chain.

DEV.M321: Data Execution Prevention

This mitigation is required to counter exploitation of a software implementation/logic error in the Communications Hub

At Foundation Grade the product **is required to** support Data Execution Prevention (DEP) when enabled on its hosting platform and must not opt out of DEP.

If the product is to be specifically deployed on a platform that does not support either Software DEP or Hardware-enforced DEP, there is no requirement for DEP compatibility.

DEV.M340: Address Space Layout Randomisation

This mitigation is required to counter exploitation of a software implementation/logic error in the Communications Hub

At Foundation Grade the product **is required to** be compiled with full support for ASLR, including all libraries used.

If the product is to be specifically deployed on an operating system that does not support ASLR, there is no requirement for ASLR compatibility.

Note: ASLR may be disabled for specific aspects of the product, provided there is justification of why this is required.

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 2012 rules for C (or equivalent for the target language), by application of a static analysis tool. 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.

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.M936: Function Separation

This mitigation is required to counter exploitation of a software implementation/logic error in the Communications Hub

At Foundation Grade the product **is required to protect resources used by CHF and GPF from unauthorised access.**

The protection must ensure there is no unauthorised access to either Function's assets from the other Function or any other functionality on the Communications Hub.

This must include protecting access to the firmware (loaded and any firmware image waiting to be loaded).

To clarify, the following GPF assets must not be accessible from the CHF or other Communications Hub functionality, except through authorised channels:

- Operational Data, including Personal Data stored by the GPF.

Similarly, the following CHF assets must not be accessible from the GPF or other Communications Hub functionality, except through authorised channels:

- Configuration Data, including the CHF Device Log;
- Communications Buffers used in the CHF for GSME messages and WAN messages.

As firmware updates are managed by the Communications hub, the developer needs to explain the measures its product takes to mitigate against a compromised Communications hub from modifying firmware in a manner which can affect GPF functionality and/or assets. It is likely that developer test evidence will also be required to demonstrate the effectiveness of the separation mechanism, illustrating a situation in which a potential breach of separation is trapped.

DEV.1 - Development >> CHF

DEV.1.1 - Development >> CHF >> Interface Protection

DEV.1.1.M44: Data validation on untrusted input

This mitigation is required to counter exploitation of a non-operational interface through crafted input
This mitigation is required to counter exploitation of an 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.1.1.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.1.1.M847: Minimise interfaces

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

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.

DEV.1.1.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 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.1.1.M947: Mutual authentication on the WAN

This mitigation is required to counter connection to CHF with an incorrect WAN

At Foundation Grade the product **is required to** mutually authenticate with the WAN Provider prior to communications with Remote Parties.

Mutual authentication shall be successfully completed between the CHF and the WAN Service Provider before any communications with Remote Parties. The WAN Service Provider will issue security credentials to enable this to take place.

The CHF shall only establish and maintain a Communications Link via its WAN Interface with the Wide Area Network Provider for the premises in which it is installed and shall not be capable of establishing a Communications Link via its WAN Interface with any other entity.

DEV.1.1.M949: Secure Inter-PAN connection

This mitigation is required to counter sending commands on an unauthorised Inter-PAN connection

At Foundation Grade the product **is required to** only enable ZigBee Inter-PAN temporarily on power-up and only allow authorised connections.

The communications hub shall only enable Inter-PAN joining after power-up for a short period, defined in [e, 4.4.7], to enable an authorised HHT to establish a secure connection as specified in [d, 10.5] for installation or maintenance.

DEV.1.1.M950: Protect configuration

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

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

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

DEV.1.2 - Development >> CHF >> Logging

DEV.1.2.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.1.2.M941: Security logging

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

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

The device shall record entries in the Security Log as identified in [d, 16]. Where the entry relates to a command, the command and outcome details shall be recorded in the entry. All entries shall include the UTC date and time of the event.

(For clarity it is noted that this requirement does not imply that all commands must be logged, only that relevant details must be included in all cases where a log entry is made).

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

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

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.1.3 - Development >> CHF >> Message Protection

DEV.1.3.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 (i.e. used to reseed the PRNG), based on analysis of all 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 features of the device have significant entropy requirements.

DEV.1.3.M140: Smooth output of Entropy Source with approved PRNG

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

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

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

For more details on RNG requirements, see the description of key pair generation in [d, 4].

DEV.1.3.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.

DEV.1.3.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.

DEV.1.3.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.1.3.M853: Prevent unauthorised changes to future-dated actions

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 when the clock is updated.

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.1.3.M855: Receiver replay check

This mitigation is required to counter interception and replay of messages

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

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

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

DEV.1.3.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.1.3.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 believe 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).

DEV.1.3.M913: Command, response and alert integrity protection

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

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

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

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

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

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

DEV.1.3.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.1.3.M927: Check only valid messages accepted

This mitigation is required to counter circumventing message signature protection by entering messages via other interfaces

This mitigation is required to counter creation of unauthorised commands

This mitigation is required to counter modification of stored data in the device

At Foundation Grade the product **is required to** verify that any message received on an 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.1.3.M930: Protect WAN message buffer

This mitigation is required to counter modification of messages buffered on communications hub for WAN

At Foundation Grade the product **is required to** protect messages queued for the WAN in the communications hub buffer.

Messages that are queued in the buffer on the communications hub while awaiting delivery to the WAN, must be protected against modification and removal.

Developer design documentation must include details of how messages are overwritten or discarded once the buffer is full (bearing in mind the priorities for messages specified in [e, 4.4.4]), as well as a rationale to justify the size of the buffer and demonstrate that it is sufficient for normal operation.

DEV.1.3.M931: Protect GSME message buffer

This mitigation is required to counter modification of commands buffered on communications hub for GSME

At Foundation Grade the product **is required to** protect commands queued for the GSME in the communications hub buffer.

Commands that are queued in the buffer on the communications hub while awaiting retrieval by the GSME, must be protected against modification and removal.

However, if the GSME fails to retrieve a command within the period defined in [d, 10.3] the CHF may discard the command and inform the GPF which will raise an alert.

Developer design documentation must include details of how messages are overwritten or discarded once the buffer is full as well as a rationale to justify the size of the buffer and demonstrate that it is sufficient for normal operation.

DEV.1.3.M932: Use whitelist before routing messages

This mitigation is required to counter creation of unauthorised commands, responses or alerts

At Foundation Grade the product **is required to** check that messages are from a device on the whitelist or the WAN interface, and to a device on the whitelist or WAN interface.

Commands, Responses, and Alerts being routed by the communications hub must have come from a Device in the CHF Device Log or from the WAN Interface for delivery to another Device in the CHF Device Log or to the WAN Interface.

DEV.1.3.M939: Enable update of security credentials

This mitigation is required to counter use of compromised security credentials

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

The device shall provide the ability to update security credentials, and this shall be subject to the normal message security checks, 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.1.3.M951: Mutual authentication on the HAN

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

At Foundation Grade the product **is required to** authenticate a device on the HAN before exchanging information with it.

The product and the other device must have successfully paired as described in [f].

DEV.2 - Development >> GPF

DEV.2.1 - Development >> GPF >> Interface Protection

DEV.2.1.M44: Data validation on untrusted input

*This mitigation is required to counter exploitation of a non-operational interface through crafted input
This mitigation is required to counter exploitation of an 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.2.1.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.2.1.M847: Minimise interfaces

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

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.

DEV.2.1.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 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.2.1.M950: Protect configuration

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

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

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

DEV.2.2 - Development >> GPF >> Logging**DEV.2.2.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.2.2.M941: Security logging

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

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

The device shall record entries in the Security Log as identified in [d, 16]. Where the entry relates to a command, the command and outcome details shall be recorded in the entry. All entries shall include the UTC date and time of the event.

(For clarity it is noted that this requirement does not imply that all commands must be logged, only that relevant details must be included in all cases where a log entry is made).

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

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

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.2.3 - Development >> GPF >> Message Protection

DEV.2.3.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 (i.e. used to reseed the PRNG), based on analysis of all 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 features of the device have significant entropy requirements.

DEV.2.3.M140: Smooth output of Entropy Source with approved PRNG

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

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

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

For more details on RNG requirements, see the description of key pair generation in [d, 4].

DEV.2.3.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.**

DEV.2.3.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.

DEV.2.3.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.2.3.M853: Prevent unauthorised changes to future-dated actions

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 when the clock is updated.

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.2.3.M855: Receiver replay check

This mitigation is required to counter interception and replay of messages

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

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

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

DEV.2.3.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.2.3.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 believe 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).

DEV.2.3.M913: Command, response and alert integrity protection

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

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

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

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.2.3.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.2.3.M927: Check only valid messages accepted

This mitigation is required to counter circumventing message signature protection by entering messages via other interfaces

This mitigation is required to counter creation of unauthorised commands

This mitigation is required to counter modification of stored data in the device

At Foundation Grade the product **is required to** verify that any message received on an 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.2.3.M939: Enable update of security credentials

This mitigation is required to counter use of compromised security credentials

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

The device shall provide the ability to update security credentials, and this shall be subject to the normal message security checks, 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.2.3.M951: Mutual authentication on the HAN

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

At Foundation Grade the product **is required to** authenticate a device on the HAN before exchanging information with it (other than that required to complete the joining).

The product and the other device must have successfully joined as described in [d, 13.7].

DEV.2.4 - Development >> GPF >> Sensitive Data Protection**DEV.2.4.M928: Restrict data on change of tenancy**

This mitigation is required to counter reading previous tenants' information

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

On receipt of a Restrict GPF Data command the device shall restrict provision to Type 1 Devices and Type 2 Devices of items of Personal Data stored in the GPF with a UTC date and time stamp prior to the date and time specified within the 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.3 - Development >> Firmware Protection

DEV.3.M863: Check authentic activation message required

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

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

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

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

DEV.3.M866: Check firmware update signature

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

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

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

DEV.3.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.4 - Development >> Physical Protection

DEV.4.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.4.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.

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 evaluators shall also seek evidence (performing additional tests where necessary) 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/unexpected code behaviour and responding with a controlled restart.

The recovery action shall also include verification of the integrity of the current firmware prior to execution. The product is expected to only run firmware that has passed an integrity check.

VER.1 - Verify >> CHF

VER.1.1 - Verify >> CHF >> Interface Protection

VER.1.1.M80: Protocol robustness testing

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

This mitigation is required to counter exploitation of an operational interface through crafted input

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

Fuzz testing is described in more detail in the Process for Performing Foundation Grade Evaluations [a]. Interfaces that are disabled and that cannot be directly accessed without physical modification involving breach of the tamper-protection boundary are not included in the scope of fuzz testing.

If the device includes separate components each with their own tamper-protection boundary, and with inter-component interfaces between the components (which can therefore be accessed without breaching the tamper-protection boundary) then these inter-component interfaces shall be included in the scope of fuzz testing.

VER.1.1.M273: General resource management

This mitigation is required to counter flooding the CHF with messages from the WAN

At Foundation Grade the evaluator will verify that the device's behaviour is stable when processing incoming network traffic.

The evaluator shall confirm by testing that large amounts of incoming network traffic do not cause the CHF to crash or suffer a general failure resulting in a denial of service (either through implementation weakness or simple resource exhaustion).

VER.1.1.M903: Verify disabled interfaces

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

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.1.1.M947: Mutual authentication on the WAN

This mitigation is required to counter connection to CHF with an incorrect WAN

At Foundation Grade the evaluator **will** verify that connection to the WAN requires mutual authentication.

The evaluator shall confirm by testing that the CHF establishes the Communications Link to the WAN Service provider only after successfully completing mutual authentication using the provided security credentials.

VER.1.1.M949: Secure Inter-PAN connection

This mitigation is required to counter sending commands on an unauthorised Inter-PAN connection

At Foundation Grade the evaluator **will** verify that ZigBee Inter-PAN is only enabled temporarily on power-up and only allows authorised connections.

The evaluator shall verify that Inter-PAN joining is only enabled after power-up for the period defined in [e, 4.4.7].

The evaluator shall verify that only authorised devices are able to connect to the Inter-PAN as specified in [d, 10.5].

VER.1.2 - Verify >> CHF >> Logging**VER.1.2.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.1.2.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.1.3 - Verify >> CHF >> Message Protection

VER.1.3.M4: Evaluation/Cryptocheck

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

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

The evaluator shall include in this activity a confirmation (by reference to relevant CAVP or equivalent certificates, or by activities in the course of the CPA evaluation) that component cryptographic primitives of the PRNG (such as SHA) 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].

VER.1.3.M853: Prevent unauthorised changes to future-dated actions

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.1.3.M855: Receiver replay check

This mitigation is required to counter interception and replay of messages

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

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

VER.1.3.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.1.3.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.1.3.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.1.3.M939: Enable update of security credentials

This mitigation is required to counter exploiting incomplete update of 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.

VER.1.3.M948: Confirm ZigBee CBKE operation

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

At Foundation Grade the evaluator **will** confirm ZigBee CBKE configuration and operation.

The evaluators will confirm that the device establishes the HAN with security as specified in [f, 5.4].

Specifically the evaluators shall check that the HAN is established in such a way that the required encryption and mutual authentication cannot be bypassed or disabled. If this is not the default configuration of the device there must be guidance to ensure that it is configured correctly on installation. If it is the default configuration of the device, but can be changed, there must be guidance to ensure that it is not changed.

VER.1.3.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.1.4 - Verify >> CHF >> Sensitive Data Protection**VER.1.4.M917: Verify logical protection of keys**

This mitigation is required to counter gaining access to security data in a single device

At Foundation Grade the evaluator **will** confirm the protection of access to cryptographic key material.

The evaluator shall confirm by testing that security credentials and other cryptographic keys to which the tester does not have authorised access cannot be accessed for read or for modification. The testing should include a search of interface documentation for methods other than normal operational messages.

VER.2 - Verify >> GPF

VER.2.1 - Verify >> GPF >> Interface Protection

VER.2.1.M80: Protocol robustness testing

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

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

Fuzz testing is described in more detail in the Process for Performing Foundation Grade Evaluations [a]. Interfaces that are disabled and that cannot be directly accessed without physical modification involving breach of the tamper-protection boundary are not included in the scope of fuzz testing.

If the device includes separate components each with their own tamper-protection boundary, and with inter-component interfaces between the components (which can therefore be accessed without breaching the tamper-protection boundary) then these inter-component interfaces shall be included in the scope of fuzz testing.

VER.2.1.M903: Verify disabled interfaces

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

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.2.2 - Verify >> GPF >> Logging

VER.2.2.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.2.2.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.2.3 - Verify >> GPF >> Message Protection

VER.2.3.M4: Evaluation/Cryptocheck

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

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

The evaluator shall include in this activity a confirmation (by reference to relevant CAVP or equivalent certificates, or by activities in the course of the CPA evaluation) that component cryptographic primitives of the PRNG (such as SHA) 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].

VER.2.3.M853: Prevent unauthorised changes to future-dated actions

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.2.3.M855: Receiver replay check

This mitigation is required to counter interception and replay of messages

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

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

VER.2.3.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.2.3.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.2.3.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.2.3.M939: Enable update of security credentials

This mitigation is required to counter exploiting incomplete update of 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.

VER.2.3.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.2.4 - Verify >> GPF >> Sensitive Data Protection

VER.2.4.M917: Verify logical protection of keys

This mitigation is required to counter gaining access to security data in a single device

At Foundation Grade the evaluator **will** confirm the protection of access to cryptographic key material.

The evaluator shall confirm by testing that security credentials and other cryptographic keys to which the tester does not have authorised access cannot be accessed for read or for modification. The testing should include a search of interface documentation for methods other than normal operational messages.

VER.2.4.M928: Restrict data on change of tenancy

This mitigation is required to counter reading previous tenants' information

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

The evaluator shall confirm by testing that the GPF 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.3 - Verify >> Firmware Protection

VER.3.M347: Verify update mechanism

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

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 validation shall include testing of the following:

- the security of the download process to ensure authenticity and integrity of the update
- atomicity of attempted updates: the update shall either completely succeed or completely fail
- the security of the activation process (including a check that the firmware version in the activation request corresponds to a version previously received and whose integrity and authenticity has been checked)
- confirmation that the secure process applies to all firmware that can be updated.

VER.4 - Verify >> Physical Protection

VER.4.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.4.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.

3.3 Deployment mitigations

DEP.M340: Address Space Layout Randomisation

This mitigation is required to counter exploitation of a software implementation/logic error in the Communications Hub

At Foundation Grade the deployment **is required to** enable ASLR in the host Operating System where available.

Note: ASLR may be disabled for specific aspects of the product, provided there is justification of why this is required.

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.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.1 - Deployment >> CHF

DEP.1.1 - Deployment >> CHF >> Interface Protection

DEP.1.1.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.1.1.M947: Mutual authentication on the WAN

This mitigation is required to counter connection to CHF with an incorrect WAN

At Foundation Grade the deployment **is required to** issue security credentials to enable mutual authentication with the WAN Provider.

The appropriate security credentials will be issued to the CHF to enable mutual authentication to take place between the CHF and the WAN Service Provider for the premises in which it is installed.

DEP.1.2 - Deployment >> CHF >> Logging

DEP.1.2.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.1.3 - Deployment >> CHF >> Message Protection

DEP.1.3.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.1.3.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.1.4 - Deployment >> CHF >> Sensitive Data Protection

DEP.1.4.M934: Unique security data per device

This mitigation is required to counter gaining access to security data in a single device

At Foundation Grade the deployment **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 another core device (such as shared keys that would enable the attacker to masquerade as a different device, or a different core device).

DEP.1.4.M953: Initialisation of Security Credentials

This mitigation is required to counter gaining access to security data in a single device

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.2 - Deployment >> GPF

DEP.2.1 - Deployment >> GPF >> Interface Protection

DEP.2.1.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.2.2 - Deployment >> GPF >> Logging

DEP.2.2.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.2.3 - Deployment >> GPF >> Message Protection

DEP.2.3.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.2.3.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.2.4 - Deployment >> GPF >> Sensitive Data Protection

DEP.2.4.M928: Restrict data on change of tenancy

This mitigation is required to counter reading previous tenants' information

At Foundation Grade the deployment **is required to** ensure a Restrict GPF Data command is issued on change of tenant.

DEP.2.4.M934: Unique security data per device

This mitigation is required to counter gaining access to security data in a single device

At Foundation Grade the deployment **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 another core device (such as shared keys that would enable the attacker to masquerade as a different device, or a different core device).

DEP.2.4.M953: Initialisation of Security Credentials

This mitigation is required to counter gaining access to security data in a single device

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.3 - Deployment >> Physical Protection

DEP.3.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.

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/document/cpa-scheme-library	Latest
[b]	Smart Metering Equipment Technical Specifications (SMETS)	https://www.smartenergycodecompany.co.uk/sec/sec-and-guidance-documents	The latest version(s) to which this document is ultimately relevant as identified in the TS Applicability Tables, in the SEC Schedule Appendices
[c]		(Intentionally blank)	
[d]	Great Britain Companion Specifications (GBCS)	https://www.smartenergycodecompany.co.uk/sec/sec-and-guidance-documents	The latest version(s) to which this document is relevant as identified in the TS Applicability Tables, in the SEC Schedule Appendices
[e]	Communications Hub Technical Specifications (CHTS)	https://www.smartenergycodecompany.co.uk/sec/sec-and-guidance-documents	The latest version(s) to which this document is ultimately relevant as identified in the TS Applicability Tables, in the SEC Schedule Appendices
[f]	ZigBee Smart Energy (ZSE) Profile Specification	http://zigbee.org/About/GBCSPartner.aspx	Version(s) as stated in reference [d]
[g]	Smart Energy Code	https://www.smartenergycodecompany.co.uk/sec/sec-and-guidance-documents	Latest

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 HAN 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
CBKE	ZigBee Certificate Based Key Establishment – a mechanism for the secure exchange of cryptographic keys as defined by the ZigBee Key Establishment Cluster.
Command	An instruction to perform a function, received or sent via any interface.
CHF Device Log	The Security Credentials and Device identifier for each of the Type 1 Devices, Type 2 Devices, GSME, ESME and GPF with which the CHF can establish Communication Links.
Communications Broker	Data and Communications Provider serving as an intermediary between Service Users and Smart Metering Equipment.
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.
Critical Commands	Those Commands which relate to supply being affected, financial fraud or the compromise of consumer premises equipment security.
Data Store	An area of storage in the Device capable of storing data. In the Communications Hub, 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.
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 communications hub when recovering from a failure: - power-on processing - storage of sensitive data - performing cryptographic processing - random number generation.
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
GPF Device Log	The Security Credentials and Device identifier for the GSME and each of the Type 1 Devices and the Device identifier for each of the Type 2 Devices with which the GPF can establish Communication Links.
GSME	Gas Smart Metering Equipment.
HAN	Smart Metering Home Area Network

Term	Definition
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.
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 [e].
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 [e].
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.
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.
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.
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; and • 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 the CHF or the GPF.
Shared Secret	A number which is established by two parties through the Key Agreement technique specified in reference [d] and which can be used as input to a Key Derivation Function (KDF).
Smart Metering Equipment	Equipment that meets the Smart Metering Equipment Technical Specification in reference [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 reference [e].
TS Applicability Tables	The document of that name contained within Schedule 11 of the Smart Energy Code, reference [g].
Type 1 Devices	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 Devices	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
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].

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 Smart Metering Communications Hub Security Characteristic v1.3 (previously version 1.2) for the following reasons.

- Make wording clearer for several requirements, for instance those relating to RNG

This has resulted in the following changes to mitigations.

D.1 Removed mitigations

(No existing mitigations have been removed.)

D.2 Modified mitigations

The following mitigations have been modified.

- DEV.1.3.M138: State the Security Strength required for random numbers (title also changed to: "DEV.1.3.M134: State raw entropy requirements")
- DEV.1.3.M140: Smooth output of Entropy Source with approved PRNG
- DEV.1.3.M141: Reseed PRNG as required
- DEV.2.3.M138: State the Security Strength required for random numbers (title also changed to: "DEV.2.3.M134: State raw entropy requirements")
- DEV.2.3.M140: Smooth output of Entropy Source with approved PRNG
- DEV.2.3.M141: Reseed PRNG as required
- DEV.3.M866: Check firmware update signature
- VER.M846: Secure failure recovery

D.3 Renamed mitigations

The following mitigations have been renamed (also modified – see “Modified mitigations” above).

- DEV.1.3.M138: State the Security Strength required for random numbers
- DEV.2.3.M138: State the Security Strength required for random numbers

D.4 New mitigations

(No new mitigations have been added.)