National Protective Security Authority

CYBER ASSURANCE OF PHYSICAL SECURITY SYSTEMS (CAPSS)

CAPSS 2024 – Security Characteristic

Document history

NPSA may review, amend, update, replace or issue new CAPSS documents as may be required from time to time. There will be a regular review period to ensure that the requirements remain up-to-date. The CAPSS scheme is revised from time to time, creating new versions of each of the documents that define the scheme. Different versions of the CAPSS scheme as a whole are denoted by the year – hence for example “CAPSS 2019” or “CAPSS 2021” – version numbers of individual documents are issued within a version of the scheme hence both CAPSS 2019 and CAPSS 2021 have their own version 1.0 of the Security Characteristic.

Version	Date	Description
1.0	29 Jan 2024	CAPSS 2024 v1.0 First Release

Any comments or suggestions regarding this document should be directed to: cse@npsa.gov.uk

Contents

Executive Summary

This document describes the features, testing and deployment requirements necessary to meet NPSA CAPSS certification for physical security systems. It is intended for vendors, system architects, developers, evaluation and technical staff operating within the security arena.

This document is the Security Characteristic for the Cyber Assurance of Physical Security Systems (CAPSS) – it describes minimum baseline requirements for physical security systems for evaluation and certification under NPSA's Cyber Assurance of Physical Security Systems (CAPSS) standard for inclusion in the Catalogue of Security Equipment (CSE) published by NPSA. Where there is already a CSE chapter, a product developer should also confirm that the product meets any functional requirements for that category in the CSE. Although it is possible to carry out a CAPSS evaluation before addressing CSE functional requirements, if the CSE requirements lead to product architecture and design changes then this may require CAPSS re-evaluation activities. Where there is no CSE chapter, the product only needs to be CAPSS evaluated.

- 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 against physical security systems. Some technical knowledge is assumed.

CAPSS evaluation is not a guarantee of freedom from security vulnerabilities. There remains a probability that exploitable security vulnerabilities may exist in the product or the information systems environment supporting the product. However, the purpose of CAPSS evaluation of products is to raise the bar of these products when they will be deployed in critical locations.

1 Section 1 – Overview

1.1 Overview

This document is the Security Characteristic for the Cyber Assurance of Physical Security Systems (CAPSS) – it describes minimum baseline requirements for physical security systems for evaluation and certification under NPSA's CAPSS standard for inclusion in the Catalogue of Security Equipment (CSE) published by NPSA. Where there is already a CSE chapter, a product developer should also confirm that the product meets any functional requirements for that category in the CSE. Although it is possible to carry out a CAPSS evaluation before addressing CSE functional requirements, if the CSE requirements lead to product architecture and design changes then this may require CAPSS re-evaluation activities[1]. Where there is no CSE chapter, the product only needs to be CAPSS evaluated.

CAPSS evaluation is not a guarantee of freedom from security vulnerabilities. There remains a probability that exploitable security vulnerabilities may exist in the product or the Information Systems environment supporting the product. However, the purpose of CAPSS evaluation of products is to raise the bar of these products when they will be deployed in critical locations.

1.2 System description

The physical security systems covered by this document, are those that provide physical security measures while using IT systems and communicating over IP networks. These include Automatic Access Control Systems, Visitor Management Systems, Closed Circuit Television, Intrusion Detection Systems, and Physical Security Information Management Systems. Each of these may employ distinct network services and protocols, distinct client and server elements, and a variety of sensors or other interface devices. Some elements will be deployed in a secure area while others will be deployed in public or non-secure areas. Some will be automatic while others will be attended or monitored by staff.

Although there is a wide variety of systems that are addressed by this document, the requirements contained in the mitigations are intended to be applicable, where appropriate to the implementation technologies used, to all systems. Thus, the mitigations are not defined in terms that are specific to a particular solution or technology, but in terms that can be applied by evaluators in the context of the specific system under evaluation.

1.3 Exclusions

Products that do not use IP networks.

1.4 Typical use case(s)

The products will be used to provide physical security for buildings within the Critical National Infrastructure (CNI) estate, although the products may be used for non-CNI related areas as well.

1 In general, re-evaluation is likely to be required when the attack surface of the product changes (e.g. by adding interfaces or changing the content or form of those interfac4398es). Further information on changes requiring re-evaluation is available from NPSA. It remains the developer's responsibility to ensure that changes to the product do not require re-evaluation, and it is noted that the periodic reviews of CAPSS-approved products (as indicated in the CAPSS lifecycle) will examine product changes since the last evaluation to confirm that re-evaluation has been carried out where required.

1.5 Expected operating environment

In most cases, a Physical Security System will consist of a number of different products addressing various aspects of a protection objective, where each product may have been provided by one or more suppliers from one or more manufacturers. Figure 1 below illustrates the types of element that are likely to be included in such a system. Some elements will necessarily be deployed in exterior, public or otherwise non-secure areas, and will generally be unattended once deployed. Other elements such as controllers and management systems must be deployed in one or more secure areas. Some must be deployed in a secure enclave (such as a secured server room or a control room – see Appendix B Glossary). External services may be required, including provision of network connectivity, reliable time services, or for sending alarms to other organisations such as emergency services. Typically, subsets of products will be installed as a subsystem consisting of elements in both secure and non-secure areas, requiring communications between them. Such subsystems may operate independently or integrated with other subsystems.

Figure 2 shows a typical implementation, where a command & control subsystem implements the integrated management, logging and admin functions; an AACS subsystem is an example of a controller with a deployment of interactive devices to permit access for authorised users; a CCTV subsystem is used for monitoring; a physical intrusion detection system deploys movement and infra-red sensors; a perimeter monitoring system deploys exterior sensors; and a Visitor Management System manages access by visitors with a reception workstation.

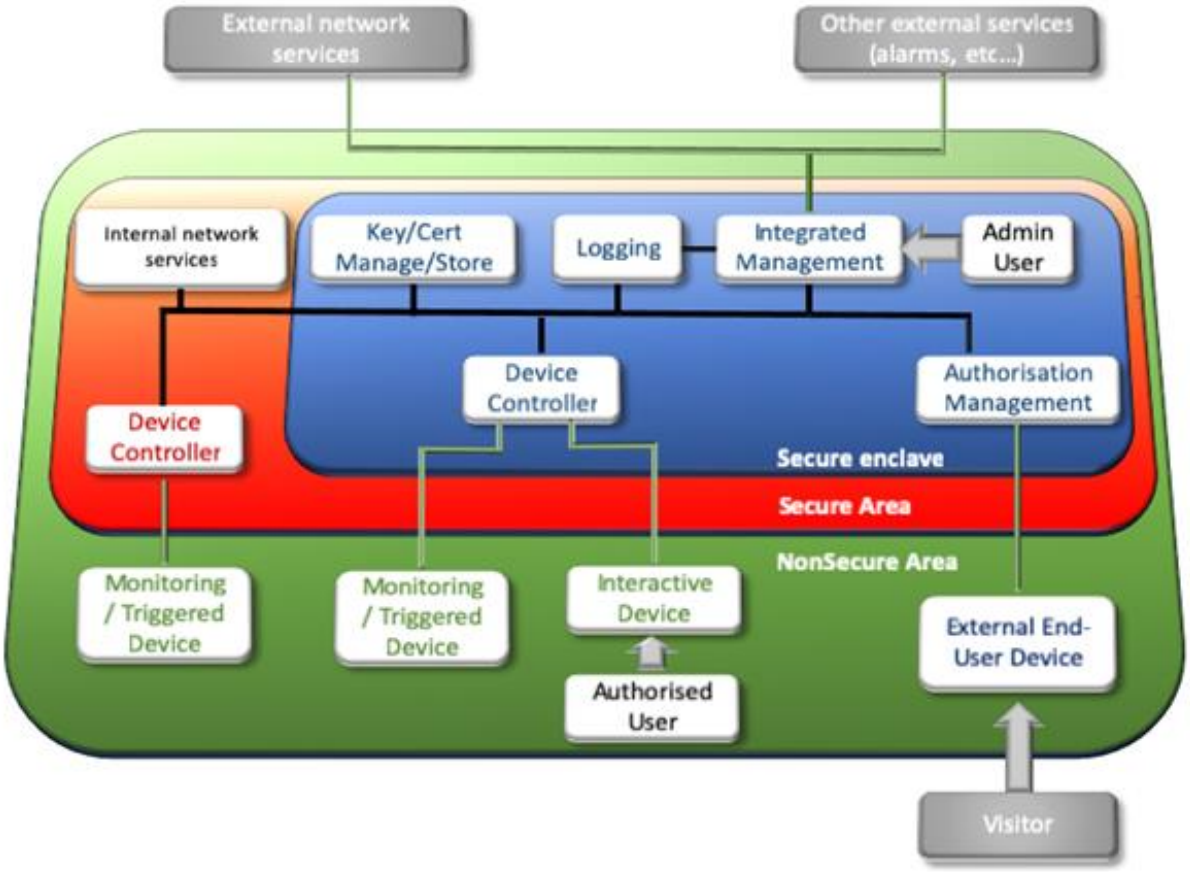

Figure 1: Elements of a physical security system

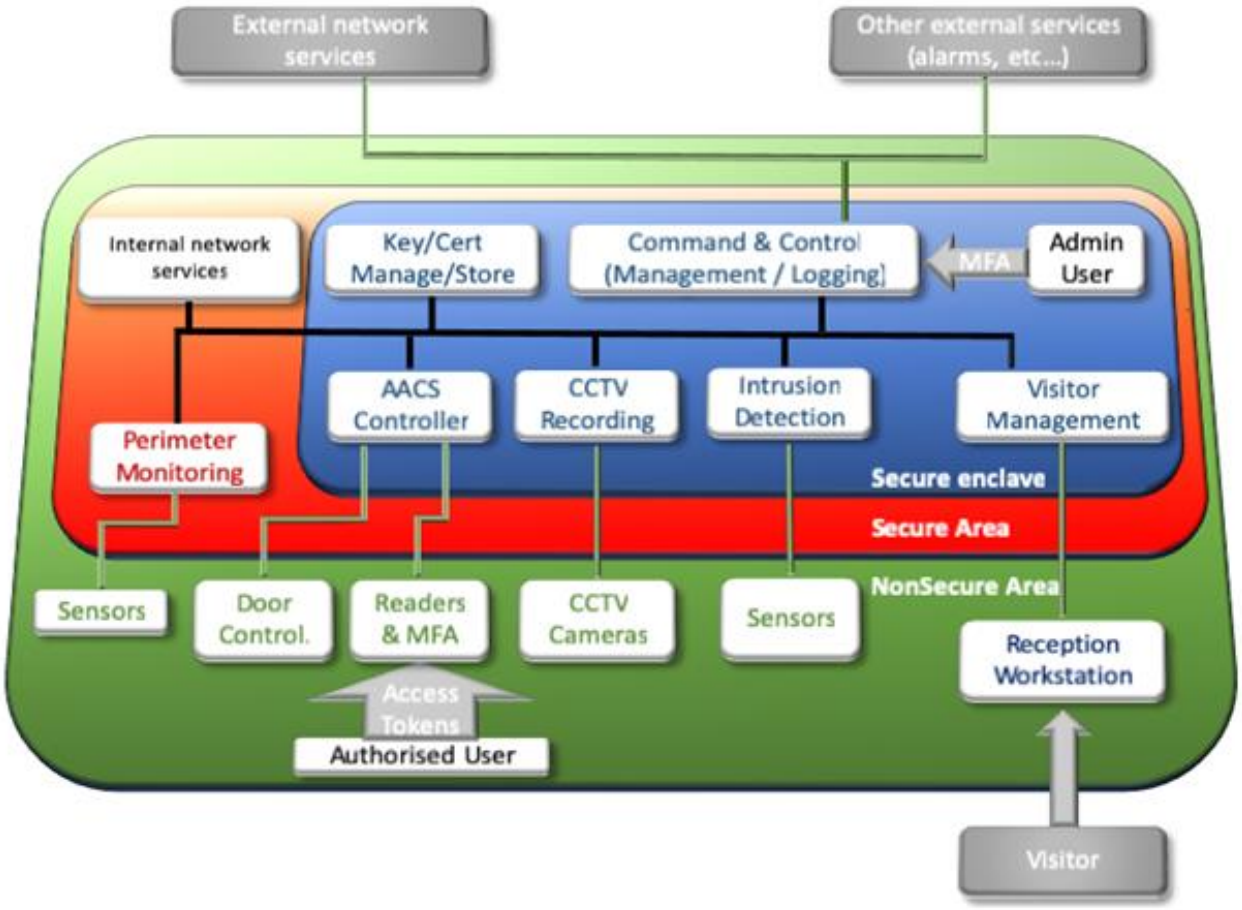

Figure 2: Typical implementation of a physical security system

1.6 Core and peripheral elements

A product evaluated under CAPSS will consist of “core” elements, and may also include a number of “peripheral” elements.

- Core elements are those elements that provide the main functionality of the product
- Peripheral elements are those elements that are added to the core elements in order to make it functionally work (and that may need to meet certain requirements in the CAPSS standard[2]), but that are not themselves treated as NPSA assured items as a result of the evaluation.

Peripheral elements will typically be items that can be exchanged for alternatives without affecting the primary functionality of the product. Examples of peripheral elements in a CAPSS evaluated product are tokens and token readers used in an automated access control system, or cameras in a video management system.

It is important to note that the peripheral elements may be important in meeting the CAPSS requirements and in providing the primary functionality of the product. Specific elements will therefore be used in evaluating the product against the CAPSS requirements, and the peripheral elements may be required to meet certain CAPSS requirements in order for the product to pass the CAPSS evaluation. However, the CAPSS evaluation does not result in the specific peripheral elements being treated as NPSA-assured.

[2] For example, the peripheral element may need to support appropriate cryptographic protection of data in transit on its connection to the product.

1.6.1 Identifying core and peripheral elements

The core and peripheral elements of a product must be identified in the CAPSS Tailored Security Characteristic (TSC)[3].

1.6.2 Evaluating core and peripheral elements

Core elements are evaluated in detail against the CAPSS requirements. Peripheral elements are supplied to the evaluators as part of the product configuration provided by the developer to enable them to test CAPSS requirements for the product as a whole. (This is referred to as the 'test configuration').

The evaluators use peripheral elements in order to operate the system functionality and demonstrate that the CAPSS requirements are met for the core elements (e.g. that the product's connections to the peripheral elements support appropriate cryptographic protection to meet CAPSS requirements for data in transit). The evaluators also check that the peripheral elements supplied in the test configuration demonstrate that the system can be deployed in practice with appropriate security (i.e. the evaluated configuration of the core components is demonstrated to work in at least the test configuration). For example, a specific token reader is used with an automated access control system to enable the test configuration to demonstrate that the core elements can be configured to use appropriate authentication and encryption between the core elements and the reader, and that at least one type of reader exists that supports the CAPSS configuration.

Deploying a product in its CAPSS evaluated configuration may therefore rely on using appropriate peripheral components that meet requirements listed in the product documentation. The product documentation may either list specific peripheral components or may define requirements for recognising appropriate peripheral components. The evaluation will examine this documentation in conjunction with the test configuration to determine the adequacy of the developer's description of appropriate peripheral components. In general an adequate requirement would need to refer to meeting an NPSA-agreed external standard. For example, a product might require the use of token readers that meet the NPSA Reader and Keypad Security Characteristics.

1.6.3 NPSA listing of core and peripheral elements

A product that passes CAPSS evaluation will be recorded under the 'CAPSS Approved' category in NPSA's Catalogue of Security Equipment (CSE). The listing will identify core and peripheral elements and the particular versions of these that were used in the test configuration (where applicable). The peripheral components are *not* themselves treated as CAPSS approved as a result of this listing.

Where there are other NPSA requirements related to the peripheral components then they may be evaluated and listed under those separate categories – for example, token readers may be separately evaluated under the separate NPSA scheme that uses the NPSA Reader and Keypad Security Characteristics. However, not all types of peripheral component will have a relevant NPSA standard and evaluation scheme.

1.7 Interoperability

In order that products from one manufacturer will operate correctly with products from another manufacturer where they are required to communicate, it is expected that open, published, industry standards will be used by default. The Tailored Security Characteristic (see Section 1.8

[3] See section 1.8 for further description of the TSC.

below) shall identify the minimum version number of each element[4] of the Physical Security System under evaluation and the versions of any protocols that it uses.

1.8 How to use this security characteristic

Because this Security Characteristic is based around a generic model and generic requirements, the evaluator first produces a Tailored Security Characteristic (TSC) that defines the requirements specific to the particular product being evaluated. The concept of a Tailored Security Characteristic is to describe the architecture and scope of a product, and to identify the SC mitigations that apply to each of the elements that make up the product. Terminology mappings may also be included if required. The evaluator is reminded that it is vital that the TSC always covers all of the requirements from the Security Characteristic. In the case of a Physical Security System product, because there is a significant benefit to potential end-users from understanding what mitigations have been applied, and to which elements of the product, it is expected that the TSC will be published as a separate document.

To ensure a consistent approach to the evaluation of multi-device products, it is recommended that for such a product the multiple devices are all included in a single TSC, with separate sections for the mitigations applicable to each device, and marking different iterations of the same requirements using a label such as ‘DEV.105/<device name>’.

1.9 High level functional components

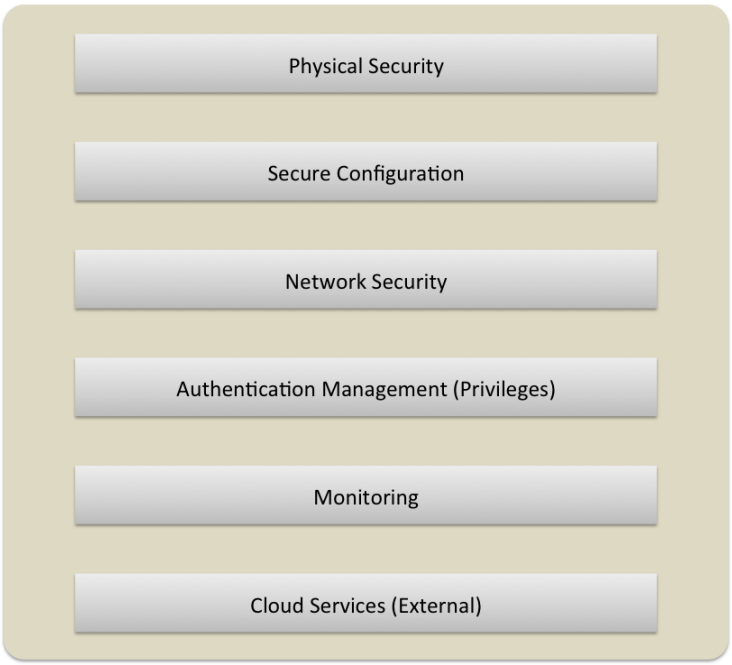

Figure 3: Functional components of a physical security system

Figure 3 above shows the functional components of a physical security system – these “functional components” are defined in order to put some structure on the requirements, and

[4] Versions are required for each element that is separately identifiable to customers: the intention is that customers can relate the element version identifiers to any reported vulnerabilities in the element, and to the versions tested in evaluations and assurance maintenance activities. (See Appendix B for the definition of element”.)

may therefore be different from the *physical* parts of a product being evaluated[5]. The applicability of some of these functional components (such as *Cloud Services*) to a particular Physical Security System product is determined by the architecture and communications between elements. Some functional component mitigations may not be required for specific product variants, as indicated in Appendix D. When evaluating a product, the evaluation team must determine the applicability of the mitigations for each element and document this in the Tailored Security Characteristic as described in Section 1.7. Note that cryptographic functions are not identified as a separate functional component, but are addressed where applicable within the mitigations relating to other functional components.

The functional components are:

- Physical security – this includes access to physical ports, removable media, debug interfaces, tamper-protection boundary and resistance to attacks such as loss of power.
- Secure configuration – the product must follow NCSC Device Security Guidance [DSG] where applicable, with controls over who can change configurations.
- Network security – the product will consist of elements that need to communicate with each other or to other systems. There must be controls on the other devices with which the product can communicate protection for data in transit on communication channels outside the secure enclave, and an ability to limit the impact of a DoS attack from network interfaces.
- Authentication management (Privileges) – use of MFA and a suitable password policy, with unique credentials for each individual user, with privileges based on roles. Software installations and updates must be verified before being applied.
- Monitoring – the product must include resilient logging of significant security-related events.
- Cloud services (External) – if the product uses external cloud services, they must meet the NCSC Cloud Security Principles [Cloud].

1.10 Pre-requisites

1. In addition to meeting the requirements of this Security Characteristic, the developers of a product must demonstrate that their development approach complies with the engineering principles and practices that are expected from a product developer creating a good quality, secure product. Validation of the Product Developer against the NCSC Build Standard [BS] is required, to provide confidence of a secure and well-understood product throughout the product's lifecycle. It covers both development processes and the general security approach taken by the Product Developer. While the Security Characteristic addresses building the right features into the product, the Build Standard addresses building the product in the right way. Adherence with the Build Standard alone will not result in a secure product. However, the absence of key elements of the Build Standard makes assurance impracticable. A successful Build Standard validation for a developer is required to provide on-going assurance that subsequent versions of a product will continue to meet requirements.
2. Alongside the Build Standard, the evaluators will expect to see evidence that the developer has a management system that encompasses information security. This can be demonstrated by [ISO9001] certification, and either [ISO27001] certification or Cyber Essentials PLUS [CEPlus] certification (or both), that include the product development organisation and processes in their scope.

5 For this reason, the terms "element" and "device" (as defined in Appendix B) are used instead of "component" in the requirements, to avoid ambiguity.

3. The developers must have a publicly stated vulnerability disclosure policy consistent with the recommendations in [ISO29147], and should have vulnerability handling processes consistent with [ISO30111].
4. The developers must have a publicly stated end-of-life / support lifetime policy for the product.
5. Note that use of cloud services or wireless communications may be subject to additional deployment restrictions outside the scope of this SC.

1.11 Additional information

This document has been produced by NPSA with input from, and review by, NCSC.

1.12 Information on future changes

With regard to DEV.402: [IEEE802.1X] may be required over MAC filtering in future.

With regard to VER.407: it is preferred that developers undertake their own fuzz testing as part of one or more stages in the product development lifecycle. Fuzz testing by the developer may become a mandatory requirement in future.

With regard to DEV.111: requirements for assurance in entropy sources and DRBGs are expected to increase in future. At present the CAPSS requirement is for general documentation of the design; in future it is likely that more specific requirements will be made, and will require description of certain key properties of the entropy source and DRBG including:

- The purposes for which entropy is required (e.g. generation of keys, authentication challenges, or salts) and the amount of entropy required in each case
- The frequency with which the entropy is required
- The entropy source used to meet each entropy requirement and a rationale for why it provides the required entropy (including, where applicable, any demonstrations of conformance to relevant standards such as the NIST SP800-90 series)
- Details of any combination of entropy from different sources
- Any techniques such as oversampling of entropy, that might be used to overcome imperfect entropy extraction
- The reseeding applied to any DRBG used
- The tests applied (e.g. Repetition Count Test and Adaptive Proportion Test as described in NIST SP 800-90B) and any relevant parameter values for the tests (e.g. sample sizes, window sizes, or the cut-off and α values for an Adaptive Proportion Test)
- How the sample bits are gathered for the health tests
- When the health tests are run.

The future requirements are also expected to call for demonstrable adherence to standards, such as use of DRBGs and entropy sources (including health tests) that have demonstrated conformance to the NIST SP 800-90 series, ISO/IEC 18031, or equivalent.

With regard to DEV.402: manufacturers are encouraged to investigate implementation of stronger device authentication and attestation architectures (e.g. using TPM), especially for devices that can execute arbitrary code (e.g. an operating system environment allowing download and execution of multiple applications – note that [DSG] recommends the use of TPM for high functioning devices).

2 Section 2 – Security Characteristic Format

2.1 Security Characteristic Format

This NPSA Security Characteristic contains a list of mitigations that describe the specific measures required to prevent or hinder attacks. The mitigations are grouped into three requirement categories: development, verification and deployment. They 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 design and implementation. Development mitigations are checked by an evaluation team during a CAPSS evaluation.
- **Verification mitigations** (indicated by the **VER** prefix) are specific measures that an evaluator must test (or observe) during a CAPSS 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. As part of the CAPSS evaluation, the evaluation team must check that the deployment mitigations are included in the product's deployment manual.

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 >> Network Security

concern **Development** mitigations relating to the **Network Security** functional area of the product.

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 are formatted in *green text*.

In addition, certain mitigations may also contain additional explanatory text to clarify specific details of the mandatory requirements. This is illustrated in the following diagram.

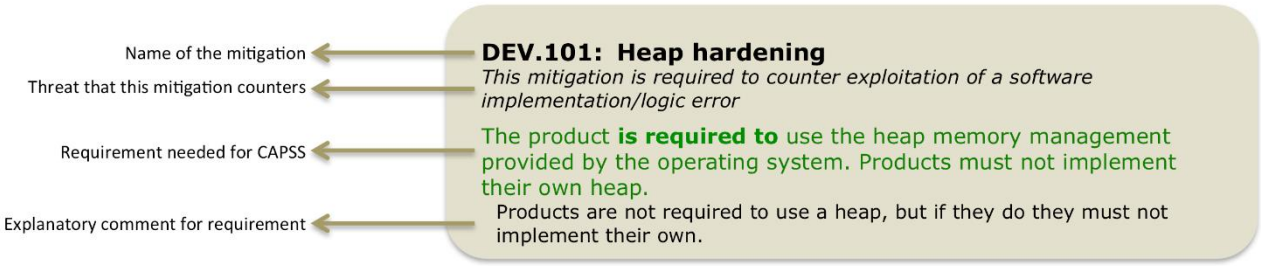

Figure 4: Parts of a typical mitigation

3 Section 3 Mitigations

3.1 Development mitigations

3.1.1 Development >> General

DEV.100: Evaluation/Cryptocheck

This mitigation is required to counter exploitation of a weak cryptographic architecture.

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

The product **is required to** use only cryptographic algorithms that have been validated as per the 'Cryptography Review' section in the NCSC CPA Process for Performing Foundation Grade Evaluations document [PPFGE], for any security functionality covered by this SC.

The developer shall provide a rationale for the cryptographic algorithms used in the product, and evidence that they have been independently validated for correctness under CAVP (or equivalent external certification).

This must include all cryptographic algorithms used in communications protocols.

DEV.101: Heap hardening

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

The product **is required to** use the heap memory management provided by the operating system. Products must not implement their own heap.

Products are not required to use a heap, but if they do, they must not implement their own.

DEV.102: Stack protection

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

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 stack protection for the target platform, then they should be used in preference to a legacy tool chain.

If the tool chain does not provide stack protection support, the developers are expected to implement robust measures that offer equivalent protection, ensuring that they are not optimised out by the compiler. The following features are expected as a minimum:

- Detect corruption of a function return address before the function returns to that address, such as by using a shadow stack. The corrupted return address will not be used, and appropriate remediation action will be performed instead, such as rebooting the product into a good known state.

- Be present in functions that have one or more arrays declared in the function's stack frame (this includes third party library code within the same runtime environment as the application code).
- If canaries are used to detect corruption, then:
  - The size of the canaries must be at least that of a memory pointer for the device's platform (e.g. canary size would need to be at least 32 bits for a 32-bit architecture)
  - The values used for the canaries must vary across different devices in a non-predictable manner (thus any exploit based on a known canary value in one device cannot be used to compromise lots of other devices).
  - Additionally, the canary value should also change in a specific device each time the product (re)boots, though this is not mandatory.

DEV.103: Data Execution Prevention

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

The product **is required to** support Data Execution Prevention when enabled on its hosting platform and must not opt out of Data Execution Prevention.

If the product is to be exclusively deployed on a platform that does not support either software Data Execution Prevention or hardware-enforced Data Execution Prevention, or equivalent, there is no requirement for Data Execution Prevention compatibility.

DEV.104: Address Space Layout Randomisation

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

The product **is required to** be compiled with full support for ASLR, including all libraries used.

If the product is to be exclusively 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 a valid justification of why this is required (such as a single process device with no underlying operating system, or deployment on a FPGA/ASIC device).

DEV.105: Encrypt sensitive data

This mitigation is required to counter extraction of sensitive data held on the device

The product **is required to** store sensitive data using encrypted data protection functions of the host platform.

Sensitive data includes personal data and configuration data. This ensures that, if a device is stolen, the sensitive data will be protected (such as the protection afforded by BitLocker or equivalents). Refer to [DSG] for specific guidance for end-user devices. The product design information must identify sensitive data types that it processes and stores, and the measures taken to protect each type.

Sensitive data must be encrypted using hardware-backed encryption where available (e.g. TPM or Trusted Execution Environment), otherwise using

software encryption. As well as being encrypted, measures must include integrity protection.

In general, sensitive data should not be stored on devices that are exposed outside of the secure enclave.

Encryption of stored data must use AES in one of the following modes: AES-CBC with 128/256 bit key, or AES-CCM with 128/256 bit key, or AES-GCM with 128/256 bit key, or AES-XTS with 256/512 bit key.

DEV.106: Updateable product

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

The product **is required to** support the use of software updates.

In exceptional cases, such as a Low Functioning device (see Appendix B Glossary), updates may not be feasible. In such cases a suitable rationale must be provided to enable the evaluators to determine whether the lack of updates is justified.

DEV.107: Secure software delivery

This mitigation is required to counter installing compromised software

The product and its updates **are required to** be distributed via a cryptographically protected mechanism, such that the authenticity of software can be ensured.

While some simple devices, such as sensors, may be supplied with pre-installed software, most products will include software which is installed prior to deployment and capable of being subsequently updated. Software for the initial installation and also for subsequent updates must be delivered by a secure mechanism to ensure that its authenticity can be assured. The software must be signed in such a way that it can be verified before installation or before an update is applied.

In exceptional cases, such as a Low Functioning device, software installation may not be feasible. In such cases a suitable rationale must be provided to enable the evaluators to determine whether the lack of secure software delivery is justified.

DEV.108: Protected software environment

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

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

The product design information shall describe the process environment in the product in order to allow the evaluator to identify any defensive or robustness mechanisms provided by the platform or OS, including exception handling, memory management and sandboxing functionality where available.

The developer shall provide static analysis evidence to demonstrate product firmware compliance with MISRA 2012 rules for C (or equivalent for the target language); or evidence from the lint-like tool available for the toolchain or language in use.

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 elements (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 on-going Build Standard compliance obligations.

DEV.109: Unique security data per device

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

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

Devices shall not contain data which if compromised would directly enable an attacker to compromise another device (such as shared keys that would enable the attacker to masquerade as a different device).

DEV.111: Entropy and DRBG description

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

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

This mitigation is required to counter prediction of randomly generated values due to a breakdown of the entropy source

The product **is required to** describe its use of DRBGs, entropy, the entropy sources that it relies on for security features, and the entropy health tests used.

DEV.113: Cryptographic key architecture

This mitigation is required to counter exploitation of a weak cryptographic architecture.

The product **is required to** describe its cryptographic key architecture.

The description shall include at least the following information for all keys:

- The purpose of the key and the security features it is used in
- The type and size of the key
- How and when the key is generated/derived (including any relationship to other keys – e.g. where a sub-key is derived from a master key)
- Whether the key is stored in non-volatile memory
- How and when the key is stored, and any protection applied to its stored form (e.g. kept exclusively in a hardware security module for its lifetime, or stored in a file encrypted under a temporary key for the session; or public keys stored in the form of a certificate signed under some Certification Authority)
- Method of destruction of the key.

3.1.2 Development >> Physical Security

DEV.200: Disable non-operational logical and physical interfaces

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

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

Normal operation is day to day operation after installation and configuration. For some devices this may need to include regular maintenance activities.

If the device has interfaces other than those supporting normal operation (e.g. installation or engineering interfaces or menus etc.) 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.

Debug interfaces (such as JTAG, SWD, UARTs, or I2C) must be disabled in normal operation; if re-enablement is possible then it must require multi-factor authentication by the manufacturer or installer/integrator using (in either case) credentials that are unique per device, or else must require a breach of the tamper boundary resulting in a visible physical change, and an alert sent on (or before) use of the interface. If the device is intended to be deployed in a non-secure area, then disablement may be achieved by the use of epoxy potting over debug interfaces to prevent their use, or stronger methods.

Physical interfaces include external interfaces for removable media (such as USB, thunderbolt or lightning) as well as internal removable media (such as an internal SD card or SIM).

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.201: Tamper response

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

The product **is required to** cause an alert and log entry on breach of the tamper-protection boundary.

Removing or opening any part of the tamper-protection boundary that is designed to be separately removed or opened shall be detectable and cause the product to cause an alert and a log entry. The alert may be indicated by various means such as an alarm or flashing indicator or an alert raised at a connected controller when the connection is lost.

Attempts to tamper with a device that is not designed to be opened should be detectable and result in an alert and log entry.

End user devices, servers, and other high functioning devices, that are protected by appropriate measures specified in [DSG] guidance (or equivalent measures) to encrypt local data, such as Bitlocker, are not required to

generate a tamper alert but their disconnection from a controller must be alerted by the controller.

DEV.202: Fail secure on power loss

This mitigation is required to counter exploitation by removing power

The product **is required to** remain secure in the event of power loss.

In the event of a loss of power the device must not fail in a way that undermines the security requirements.

When power is restored, the device must restart in a state that does not undermine the security requirements.

DEV.203: Protection of security-related physical structure

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

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 elements that generate, process and store sensitive data (including cryptographic keys), and that carry out cryptographic operations.

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.

End user devices, servers, and other high functioning devices, that are protected by appropriate measures specified in [DSG] guidance (or equivalent measures) to encrypt local data, such as Bitlocker, are not required to have a tamper-protection boundary.

3.1.3 Development >> Secure Configuration

DEV.300: Provide a configuration tool to enforce required settings

This mitigation is required to counter exploitation of an accidental misconfiguration

The product **is required to** be provided with a configuration tool, or other method, for an administrator to initially set it up into a suitable configuration.

If a software product requires more than 12 options to be changed or set by an administrator to comply with these Security Characteristics, the developer must supply a tool, policy template, or specific configuration guide which helps the administrator to achieve this in fewer steps.

DEV.301: Ensure product security configuration can only be altered by an authenticated system administrator

This mitigation is required to counter unauthorised alteration of product's configuration

The product **is required to** ensure that only authenticated administrators are able to change the product's security enforcing settings.

This includes configuration of any key and certificate management required in support of authentication or other cryptographic functionality of the product.

DEV.302: Ensure product security configuration can be backed up

This mitigation is required to counter unauthorised alteration of product's configuration

The product **is required to** ensure that the product's security enforcing settings can be securely backed up.

In the event of a failure, the security configuration must be able to be restored in a timely fashion by an appropriately authorised administrator.

DEV.303: Deploy onto suitably protected endpoint

This mitigation is required to counter malware on endpoint

The product **is required to** ensure that endpoints are configured in line with good IT practice as part of a risk-managed accredited system.

If the endpoint device is provided with the product, the developer must provide assurances that the relevant NCSC [DSG] Guidance for the platform has been met or, if such guidance is not available, then provide a rationale that they implement best practice for the platform.

3.1.4 Development >> Network Security

DEV.400: 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

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

Network ports and services shall only be opened if required for the device to function. If there is any additional functionality provided in the device beyond that required for normal operation, the developers must provide documentation and a rationale to demonstrate that it does not impact the security requirements in this Security Characteristic.

DEV.401: Wireless network must be secured

This mitigation is required to counter exploitation of unsecured wireless network

The product **is required to** ensure that wireless networks are secured.

If the product uses wireless technologies it must enforce the use of suitable security mechanisms to protect the communications channels. WiFi connections using WPA2 Enterprise as a minimum are preferred. Where the use of Bluetooth or other wireless networking protocols is unavoidable, the product must enforce the use of secure protocols at higher levels in the communications stack to provide encryption and authentication protection such as TLS, employing NIST approved cryptographic algorithms.

(Note also DEP.408, which requires that wireless networks are not used on any site requiring more than a basic level of protection.)

DEV.402: Use device authorisation

This mitigation is required to counter messages from unauthorised devices

The product **is required to** only communicate with authorised devices.

The product should use an allow-list feature (or stronger check) to ensure that communications are from devices that have been previously authorised. Although this can be as straightforward as MAC filtering, [IEEE802.1X] is preferred.

DEV.403: Use time synchronisation

This mitigation is required to counter exploitation of variations in time between devices

The product **is required to** use time synchronisation to ensure all devices have a reference time source.

The time synchronisation can be obtained from an external time server or an internal time server with a trusted time source, using a suitable protocol such as NTP or PTP. This must only use a major version that is still supported, for which all up to date security patches have been applied.

DEV.404: Use segregated networks

This mitigation is required to counter an attack through a connected network

The product **is required to** use segregated networks.

If the product is supplied with network setup, this must use VLANs or other network segregation approaches to separate unrelated elements. As a minimum, any management interface must be on a separate VLAN.

DEV.405: General resource management

This mitigation is required to counter a DoS attack from a network interface

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.406: Encrypt communications traffic over untrusted link

This mitigation is required to counter interception of data from unencrypted links

The product **is required to** use approved cryptographic algorithms to protect communications traffic on untrusted links.

Any communications link that is partially or entirely outside the secure enclave must be regarded as untrusted.

Data must be protected in transit. Non-sensitive data needs to be provided with integrity protection at minimum. Sensitive data must be encrypted and integrity protected. The cryptographic algorithms and cipher suites used must be NIST approved.

Guidance on suitable means to protect data in transit can be found at [TLS_NCSC] and [IPsec_NCSC].

3.1.5 Development >> Authentication Management (Privileges)

DEV.500: Role based access control

This mitigation is required to counter privilege escalation on management application

This mitigation is required to counter unauthorised use of management privilege

The product **is required to** allow users to be assigned to specific roles.

Users must be able to be assigned to specific roles, with the roles determining what operations may be performed, ensuring that users are only able to perform operations and access data appropriate to their role.

If the definition of user roles is customisable, this must only be able to be performed by an admin user with an appropriate privilege.

DEV.501: User least privilege

This mitigation is required to counter taking advantage of existing user privilege

The product **is required to** operate correctly from a standard account with the minimum privileges required for the user's role.

For a non-admin role, the product must operate correctly from a standard account without elevated privileges. For an admin role, or other role that requires some elevated privileges, the developer must provide a rationale identifying and justifying the use of such privileges. Privileges include both OS and product-defined privileges.

DEV.502: User authentication and re-authentication

This mitigation is required to counter exploitation of weak user passwords

This mitigation is required to counter exploitation of unattended workstations

The product **is required to** enforce a password policy defined by an administrator, or an MFA authentication mechanism that is unique to each user.

If users are not required to use an MFA authentication mechanism that is unique to each user, there must be a password policy that, as a minimum, meets the requirements defined in Appendix C of this document.

The developer shall identify all passwords for which default values are defined in the product.

The product **is required to** lock out a session after a defined period of inactivity, requiring the user to re-authenticate.

Inactivity period may be configurable but must be no longer than 15 minutes for admin roles and any roles used outside the secure area; but may be up to 120 minutes for roles that are used in a secure area for passive review of data (such as CCTV).

DEV.506: Management interface protection

This mitigation is required to counter exploitation of poorly protected management interfaces

The product **is required to** use a secure protocol to authenticate all management connections and to protect the confidentiality and integrity of traffic on any management interface.

Examples of secure protocols for these purposes are IPsec, SNMPv3, TLS or SSH.

Secure protocols are not required for management consoles connected by serial links (provided those serial connections are not converted to IP at any point).

Remote access to management interfaces must be disabled by default, and must require specific action during installation (or subsequently) to enable it.

The product **is required to** authenticate all administrators by using MFA.

3.1.6 Development >> Monitoring

DEV.600: Log all relevant events

This mitigation is required to counter product usage that could be indicative of attacker activity

The product **is required to** log all events deemed of interest to an operator investigating a potential event or incident.

Logs here are intended to cover event and information logs rather than diagnostic or debug logs. Log data must be detailed enough to allow forensic investigation during any incident management. Sensitive data such as passwords and keys must not be written to the logs.

Note that in producing a Tailored Security Characteristic for a specific product evaluation, the evaluators shall determine the specific events of interest for each element.

Events logged must include as a minimum:

- Authentication attempts
- Loss of connection with devices/loss of network connectivity (if available)
- Change of software or firmware versions
- Tamper events (if available)
- Change of configuration
- Change of time
- Deletion of logs (or log entries), including archiving of logs if this causes the deletion
- Redaction of log entries (if supported).

DEV.601: Protect access to logs and timestamp log entries

This mitigation is required to counter modification of logging generation

This mitigation is required to counter sanitisation of illegitimate access from logs

The product **is required to** ensure that all log entries are time stamped.

Timestamps must be accurate and synchronised with a reliable time source. The deployment must take measures to ensure this.

The product **is required to** ensure that no modification of log entries is allowed.

It must not be possible to delete log entries. Some simple devices with memory constraints may treat the log as circular, causing older entries to be overwritten by the latest entry if the log is full; in this case the log must be capable of holding at least 100 entries and must be exported to another device (such as a controller or central logging facility) regularly enough that log entries are unlikely to be lost. The overwriting of log entries in this way is acceptable provided that the developer supplies a valid justification for this behaviour, the size of the log and the frequency of export.

There may be an exception to this rule in cases where a redaction function is provided to enable data (over a certain age) concerning particular individuals to be removed in conformance with data protection regulations. Where a

redaction function is provided then this shall be available only to specific users who have been granted a relevant privilege. It is preferred that the redaction function can be granted separately from administrator roles or privileges.

The product **is required to** ensure that only an authenticated administrator can manage logs.

Only an authenticated administrator should be able to read log entries.

The product **is required to** alert the administrator before overwriting logs.

In order to avoid the loss of log files, the administrator should have the opportunity to ensure that log files have been exported or backed up in sufficient time before they are overwritten.

DEV.602: Export logs with integrity protection

This mitigation is required to counter modification of locally stored logs

The product **is required to** provide the ability to automatically transfer log records to an external device.

This functionality could be provided by a host operating system, where available. Log records shall be transferred as soon as possible after creation. Logs shall be transferred for archiving and possibly also analysis, which would be facilitated by the use of a common format such as syslog.

The product **is required to** protect the integrity of log records in transit.

DEV.604: Record when device last seen

This mitigation is required to counter product usage that could be indicative of attacker activity

The product **is required to** be able to identify when a connected device was last seen

A device (such as a controller) that has contact with other devices must be able to identify when it last had contact with another device.

Where a device has not been seen for a period above a preset (possibly configurable) limit, a log record must be generated identifying the device that has not been seen. The trigger limit is likely to vary depending on the type of device and appropriate periods of inactivity.

3.1.7 Development >> Cloud Services (External)

DEV.700: Suitable cloud services

This mitigation is required to counter exploitation of insecure cloud services

The product **is required to** ensure that cloud services meet NCSC Cloud Security Principles.

If the product uses external cloud services, the developer must state how they meet the NCSC Cloud Security Principles as defined in the NCSC Cloud security guidance [Cloud]. The cloud service provider must have published their response to the NCSC Cloud Security Principles.

Note that in producing a Tailored Security Characteristic for a specific product evaluation, the evaluators shall include an identification of the services and assets that are to be deployed using external cloud services.

3.2 Verification mitigations

3.2.1 Verification >> General

VER.100: Evaluation/Cryptocheck

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

The evaluator **will** ensure that all cryptographic algorithms employed for security functionality have been validated as per the 'Cryptography Review' section in the NCSC CPA Process for Performing Foundation Grade Evaluations document [PPFGE].

The evaluator shall include in this activity a confirmation (by reference to relevant CAVP or equivalent certificates) that cryptographic primitives 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 elements of the product, at the relevant version for the element.

Where cryptographic algorithms have not been certified under CAVP (or equivalent external certification), the developers must discuss the suitability with NPSA before the product evaluation commences. NPSA will confirm the suitability of the implementation with NCSC before the evaluation can proceed.

This must include all cryptographic algorithms used in communications protocols.

The evaluators shall verify that the product does not include any other cryptographic algorithms that have not been validated.

VER.106: Updateable product

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

The evaluator **will** ensure that the product supports the use of software updates.

The evaluator will demonstrate that a successful update can be performed.

VER.107: Secure software delivery

This mitigation is required to counter installing compromised software

The evaluator **will** ensure that the product rejects update attempts using software with missing or invalid proof of authenticity.

Software for the initial installation and also for subsequent updates must be signed in such a way that it can be verified before installation or before an update is applied.

In exceptional cases, such as a Low Functioning device, software installation or updating may not be feasible. In such cases suitable rationales must have been examined under DEV.106 and DEV.107.

3.2.2 Verification >> Physical Security

VER.200: Disable non-operational logical and physical interfaces

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

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 to confirm that it is not possible to use the interface. The evaluator will ensure that justification has been provided that any interface that is not disabled is required during normal operation. Physical interfaces include removable media.

The evaluator **will** verify that disabled interfaces can only be re-enabled using multi-factor authentication or after breach of the tamper boundary resulting in a visible physical change, and an alert sent on (or before) use of the interface.

Authentication must use credentials that are unique per device.

VER.201: Tamper response

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

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-protection boundary that is designed to be separately removed or opened shall be detectable and cause an alert and a log entry. The alert may be indicated by various means such as an alarm or flashing indicator or an alert raised at a connected controller when the connection is lost.

Attempts to tamper with a device that is not designed to be opened should be detectable and result in an alert and log entry being caused.

End user devices, servers, and other high functioning devices, that are protected by appropriate measures specified in [DSG] guidance (or equivalent measures) to encrypt local data, such as Bitlocker, are not required to generate a tamper alert but their disconnection from a controller must be alerted by the controller.

VER.202: Fail secure on power loss

This mitigation is required to counter exploitation by removing power

The evaluator **will** verify that the product remains secure in the event of power loss.

The evaluator shall confirm that, in the event of a loss of power, the failure of the device does not undermine the security requirements or cause other devices to fail or behave in a way that undermines the security requirements.

The evaluator shall confirm that, when power is restored after a failure, the device restarts in a state that does not undermine the security requirements or

cause other devices to fail or behave in a way that undermines the security requirements.

VER.203: Protection of security-related physical structure

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

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 parts, other than by breach of the tamper-protection boundary, and shall therefore be opaque within the visible spectrum (other than areas required for a sensor or to provide visibility of a user interface). This may be achieved by the case itself or by a lining applied to the case.

End user devices, servers, and other high functioning devices, that are protected by appropriate measures specified in [DSG] guidance (or equivalent measures) to encrypt local data, such as Bitlocker, are not required to have a tamper-protection boundary.

3.2.3 Verification >> Secure Configuration

VER.300: Provide a configuration tool to enforce required settings

This mitigation is required to counter exploitation of an accidental misconfiguration

The evaluator **will** confirm that the configuration tool, or other method, initially sets the product up into a suitable configuration.

The evaluator will employ the tool, policy template, or specific configuration guide to ensure that it works successfully and results in a configuration of the product that meets the requirements.

VER.301: Ensure product security configuration can only be altered by an authenticated system administrator

This mitigation is required to counter unauthorised alteration of product's configuration

The evaluator **will** confirm that only authenticated administrators are able to change the product's security enforcing settings.

VER.302: Ensure product security configuration can be backed up

This mitigation is required to counter unauthorised alteration of product's configuration

The evaluator **will** confirm that the product's security enforcing settings can be securely backed up and restored.

The evaluator will confirm that backup and restore can only be carried out by an appropriately authorised administrator.

3.2.4 Verification >> Network Security

VER.400: 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

The evaluator **will** confirm that only necessary protocols and services are available on the device.

The evaluator will verify that the only network ports and services open on the device are those that are necessary for operation of the device as claimed by the developer.

VER.401: Wireless network must be secured

This mitigation is required to counter exploitation of unsecured wireless network

The evaluator **will** confirm that wireless networks are secured.

The evaluator will confirm that wireless technologies used by the product enforce the use of suitable security mechanisms to protect the communications channels. WiFi connections must use WPA2 Enterprise as a minimum. Where the use of Bluetooth or other wireless networking protocols is unavoidable, the product must enforce the use of secure protocols at higher levels in the communications stack to provide encryption and authentication protection such as TLS, employing NIST approved cryptographic algorithms.

Where wireless capability of a product is required to be disabled, the evaluator will confirm that, when they have taken the relevant action to disable a wireless interface, the interface is in fact disabled.

VER.402: Use device authorisation

This mitigation is required to counter messages from unauthorised devices

The evaluator **will** verify that the product only communicates with authorised devices.

If the product offers an allow-list feature such as MAC filtering, or [IEEE802.1X], the evaluator will verify that a device that is not allow-listed cannot connect.

VER.403: Use time synchronisation

This mitigation is required to counter exploitation of variations in time between devices

The evaluator **will** verify that time synchronisation is used to ensure all devices have a reference time source.

The time synchronisation can be obtained from an external time server or an internal time server with a trusted time source, using a suitable protocol such as NTP or PTP. This must only use a major version that is still supported, for which all up to date security patches have been applied. Where the time can be set on a device directly, the evaluators will verify that this can only be performed by an authorised and authenticated security administrator. Where the time is obtained from a time server, the evaluators will verify that the time

on a device is synchronised with the time server. Where multiple protocols are supported for establishing a connection with the time server, the evaluators shall repeat test for each supported protocol.

VER.404: Use segregated networks

This mitigation is required to counter an attack through a connected network

The evaluator **will** verify that the network setup uses segregated networks.

If the product is supplied with network setup, the evaluators will verify that this uses VLANs or other network segregation approaches to separate unrelated elements. As a minimum, the evaluators will verify that any management interface is on a separate VLAN.

VER.405: General resource management

This mitigation is required to counter a DoS attack from a network interface

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 device to crash or suffer a general failure resulting in a denial of service (either through implementation weakness or simple resource exhaustion).

VER.406: Encrypt communications traffic over untrusted link

This mitigation is required to counter interception of data from unencrypted links

The evaluator **will** verify that sensitive data is encrypted on untrusted communications links.

The evaluator will examine the content of captured traffic to confirm that sensitive data is suitably encrypted.

VER.407: 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

The evaluator **will** analyse fuzz testing results for the available interfaces.

Fuzz testing is described in more detail in the Process for Performing Foundation Grade Evaluations [PPFGE], and additional information is given in the CAPSS Application Notes. The fuzz testing evidence analysed by the evaluators may be generated by the evaluator, the developer, or a combination of both. 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 product includes separate elements with interfaces that provide a channel between them partially or entirely outside the secure enclave, then these interfaces shall be included in the scope of fuzz testing.

3.2.5 Verification >> Authentication Management (Privileges)

VER.501: User least privilege

This mitigation is required to counter taking advantage of existing user privilege

The evaluator **will** verify that the product will operate correctly from a standard account with the minimum privileges required for the user's role.

If the configuration of users is set up by a configuration tool supplied with or as part of the product, the evaluator shall examine the account privileges set up for each user role to determine whether only the privileges required for that role have been assigned.

If the configuration is not set automatically, the evaluator will verify that, following installation according to the product guidance documentation, the account privileges set up for each user role have been assigned only the privileges required for that role.

VER.502: User authentication and re-authentication

This mitigation is required to counter exploitation of weak user passwords

This mitigation is required to counter exploitation of unattended workstations

The evaluator **will** test that the password policy defined by an administrator is enforced.

If an MFA authentication mechanism is not in use for non-admin users, the evaluators shall verify that the defined password policy (meeting the requirements in Appendix C of this document) is enforced.

The evaluator **will** verify that sessions are locked after a defined period of inactivity, requiring the user to re-authenticate.

VER.506: Management interface protection

This mitigation is required to counter exploitation of poorly protected management interfaces

The evaluator **will** verify that the product uses a secure protocol to authenticate all management connections and to protect the confidentiality and integrity of traffic on any management interface.

(As noted for DEV.506, serial console connections are not required to use secure protocols.)

The evaluators shall also verify that remote access is disabled by default and requires specific action during installation (or subsequently) to enable it.

The evaluator **will** verify that the product authenticates all administrators by using MFA.

3.2.6 Verification >> Monitoring

VER.600: Log all relevant events

This mitigation is required to counter product usage that could be indicative of attacker activity

The evaluator **will** test that the log includes all events deemed of interest.

The evaluator will test that appropriate events are written to a log, based on those events identified for DEV.600.

VER.601: Protect access to logs and timestamp log entries

This mitigation is required to counter modification of logging generation

This mitigation is required to counter sanitisation of illegitimate access from logs

The evaluator **will** verify that all log entries are time stamped.

The evaluator will confirm that timestamps are synchronised to a reliable reference time source.

The evaluator **will** verify that no modification of log entries is allowed.

This includes confirmation that it is not possible to delete log entries.

The evaluator **will** verify that only an authenticated administrator can manage logs.

If a redaction function is implemented in the product then the testing includes confirmation that only the configured administrators can use it.

The evaluator **will** verify that the administrator is alerted before logs are overwritten.

VER.604: Record when device last seen

This mitigation is required to counter product usage that could be indicative of attacker activity

The evaluator **will** verify that it is recorded when a connected device was last seen.

The evaluator shall confirm that it is possible to identify when a connected device was last seen. Where a device has not been seen for a period above a preset (possibly configurable) limit, a log record must be generated identifying the device that has not been seen. The trigger limit is likely to vary depending on the type of device and appropriate periods of inactivity.

3.2.7 Verification >> Cloud Services (External)

VER.700: Suitable cloud services

This mitigation is required to counter exploitation of insecure cloud services

The evaluator **will** verify that cloud services meet NCSC Cloud Security Principles.

If the product uses external cloud services, they must meet the NCSC Cloud Security Principles as defined in the NCSC Cloud security guidance [Cloud]. The evaluators will confirm that the product uses the cloud services in accordance with the cloud service provider's response to the NCSC Cloud Security Principles.

3.3 Deployment mitigations

3.3.1 Deployment >> General

DEP.105: Encrypt sensitive data

This mitigation is required to counter extraction of sensitive data held on the device

The deployment **is required to** ensure that sensitive data is stored using encrypted data protection functions of the host platform.

Devices containing sensitive data must be configured to use the protection afforded by mechanisms such as BitLocker or equivalents. Refer to [DSG] for specific guidance for end-user devices.

If devices that contain sensitive data are removed from the secure enclave (e.g. for specialist analysis) then this must be done under procedural controls that minimise the specific risks to the deployment.

DEP.106: Updateable product

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

The deployment **is required to** regularly update to the latest version.

For critical vulnerabilities the update must be applied within 14 days of the update becoming available. The product guidance documentation must make clear where and how an administrator is to be made aware of update availability and obtain them.

DEP.110: Administrator authorised updates

This mitigation is required to counter installing compromised software using the update process

The deployment **is required to** confirm the source of updates before they are applied to the system.

The administrator is required to have authorised the updates before use. If an automatic process is used, the administrator must also configure the product to authenticate updates. The update procedure to be used by the administrator must be described within the product guidance documentation.

3.3.2 Deployment >> Physical Security

DEP.200: Disable non-operational logical and physical interfaces

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

The deployment **is required to** include guidance on requirements to manage non-operational interfaces.

Physical interfaces include removable media.

DEP.201: Tamper response

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

The deployment **is required to** ensure that tamper alerts are collected.

If a device generates an alert, it must be capable of being delivered and acted upon. Some simple devices with memory constraints may treat the log as circular, causing older entries to be overwritten by the latest entry if the log is full; in this case the log must be capable of holding at least 100 entries and must be exported to another device (such as a controller or central logging facility) regularly enough that log entries are unlikely to be lost.

DEP.203: Protection of security-related physical structure

This mitigation is required to counter physical compromise of the device

The deployment **is required to** employ tamper evident measures at access points on product.

Use tamper evidence measures (e.g. stickers) to make entry to system internals detectable by physical inspection. Measures such as 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. NPSA approved tamper products (such as a NPSA Rated seal) should be used.

End user devices, servers, and other high functioning devices, that are protected by appropriate measures specified in [DSG] guidance (or equivalent measures) to encrypt local data, such as Bitlocker, are not required to have a tamper-protection boundary.

The deployment **is required to** provide advice on the tamper threat and tamper evidence inspection.

Advice should include looking for possible damage to tamper evident measures. In the event of tampering, the event should be reported as soon as possible, and the product must be removed from use immediately. Any product that shows evidence of tampering must not be returned to service.

The deployment **is required to** implement physical security for secure area and secure enclave devices such that only an administrator can gain local access to the product (e.g. product sited in a locked room).

The product guidance documentation must make it clear which devices need to be deployed in the secure area or secure enclave with appropriate physical protection.

DEP.204: Physical security of management interfaces

This mitigation is required to counter physical compromise of management interfaces

The deployment **is required to** ensure that management interfaces are not accessible in non-secure areas.

End user devices that are employed to access management interfaces must not be accessible in a non-secure area. Admin access to subsystems that are deployed within the secure enclave, must also be within the secure enclave. Admin access to subsystems that are deployed outside the secure enclave but within a secure area, may be within the same secure area.

3.3.3 Deployment >> Secure Configuration

DEP.300: Provide a configuration tool to enforce required settings

This mitigation is required to counter exploitation of an accidental misconfiguration

The deployment **is required to** ensure that an administrator is provided with a configuration tool, or other method, to initially set it up into a suitable configuration.

The product guidance documentation must ensure that an administrator is advised to perform the initial configuration using a supplied tool, policy template, or specific configuration guide to achieve this in as few steps as possible.

The product guidance documentation must describe how an administrator can check that the deployment is in the evaluated configuration after initial installation and during subsequent operation.

The product guidance documentation must describe any security assumptions for the environment (secure enclave/secure area/non-secure area) in which each element is intended to be deployed.

DEP.302: Ensure product security configuration can be backed up

This mitigation is required to counter unauthorised alteration of product's configuration

The deployment **is required to** ensure that the product's security enforcing settings can be securely backed up.

The product guidance documentation must ensure that an administrator is advised to use the product's features to securely backup their configuration, and provided with guidance on the process of restoring the security configuration in a timely fashion in the event of a failure.

DEP.303: Deploy onto suitably protected endpoint

This mitigation is required to counter malware on endpoint

The deployment **is required to** configure endpoints in line with good IT practice as part of a risk-managed accredited system.

If the endpoint device is provided with the product, configuration guidance must be provided equivalent to the relevant NCSC Device Security Guidance. If the endpoint device is not provided with the product, the relevant security guidance for end user devices provided at [DSG] must be followed where possible.

3.3.4 Deployment >> Network Security

DEP.401: Wireless network must be secured

This mitigation is required to counter exploitation of unsecured wireless network

The deployment **is required to** ensure that wireless networks are secured

The product documentation, and any CSE entry for the product, shall identify and describe its use of wireless technology and shall identify any wireless capabilities that are required to be disabled to meet the requirements of its Tailored Security Characteristic.

If the product uses wireless technologies, it must be configured to use suitable security mechanisms to protect the communications channels. WiFi connections must use WPA2 Enterprise as a minimum. Where the use of Bluetooth or other wireless networking protocols is unavoidable, this means enforcing the use of secure protocols at higher levels in the communications stack to provide encryption and authentication protection such as TLS, employing NIST approved cryptographic algorithms.

Wireless technologies must not be used on any site requiring more than a basic level of protection (see DEP.408).

Where wireless capabilities need to be disabled, the product documentation shall describe how to carry out this disabling, and how the disabled status can be checked at any point.

DEP.402: Use device authorisation

This mitigation is required to counter messages from unauthorised devices

The deployment **should** ensure that device authorisation is correctly configured.

If the product uses an allow-list feature (such as MAC filtering, or [IEEE802.1X]) the product guidance documentation must provide advice on how to correctly configure this during installation.

DEP.403: Use time synchronisation

This mitigation is required to counter exploitation of variations in time between devices

The deployment **is required to** establish a reference time source.

Devices will use the time source to ensure time synchronisation. If this is not part of the product, the product guidance documentation must provide advice on how this can be implemented and configured. This must only use a major version that is still supported, for which all up to date security patches have been applied.

DEP.404: Use segregated networks

This mitigation is required to counter an attack through a connected network

The deployment **is required to** use segregated networks.

Product guidance documentation must state how the product can be configured using segregated networks (e.g. using VLANS). If the product is supplied with network setup, this should use VLANs or other network segregation approaches to separate unrelated elements. As a minimum, any management interface must be on a separate VLAN.

DEP.408: Do not deploy wireless technology at sites requiring more than a basic level of protection

This mitigation is required to counter a Denial of Service attack

This mitigation is required to counter identification of a device through network advertising

This mitigation is required to counter a man-in-the-middle attack on device communications

The deployment **is required to** ensure that all device communications occur over wired network connections in a CNI site requiring more than a basic level of protection.

Wireless networks must not be used on any site requiring more than a basic level of protection.

3.3.5 Deployment >> Authentication Management (Privileges)

DEP.500: Role based access control

This mitigation is required to counter privilege escalation on management application

This mitigation is required to counter unauthorised use of management privilege

The deployment **is required to** enforce separate accounts for device management, account administration and user access.

The product guidance documentation should identify what each role allows to be performed, so that users can be assigned to specific appropriate roles.

DEP.501: User least privilege

This mitigation is required to counter taking advantage of existing user privilege

The deployment **is required to** ensure that users are provided with a standard account with the minimum privileges required for the user's role.

The product guidance documentation should identify the (OS and/or product-defined) privileges required for each user role, enabling the system administration to ensure that unnecessary privileges are not assigned to users.

DEP.502: User authentication and re-authentication

This mitigation is required to counter exploitation of weak user passwords

The deployment **is required to** enforce a password policy that requires passwords to be changed upon suspicion that a password has been compromised.

The password policy must be at least as robust as that defined in Appendix C of this document. No previous password shall be allowed by the product, in case they have been breached.

The deployment **is required to** ensure that default passwords are changed at installation.

Default passwords must be changed, at installation, to passwords that comply with the password policy. An installation will not be considered CAPSS compliant if the default passwords have not been changed. Note that in future versions of this SC, this requirement may be strengthened to require the product to enforce the change of passwords at installation.

DEP.503: One administrator per account

This mitigation is required to counter the unauthorised use of an admin account

The deployment **is required to** use one admin account per administrator.

The product guidance documentation should prohibit two or more users using the same user account.

DEP.506: Management interface protection

This mitigation is required to counter exploitation of poorly protected management interfaces

The deployment **is required to** authenticate and protect the confidentiality and integrity of all management connections using a secure protocol.

The product guidance documentation must specify that access be protected by a secure protocol configured to provide authentication and confidentiality protection.

(As noted for DEV.506, serial console connections are not required to use secure protocols.)

The product guidance documentation must specify that remote access is disabled by default and identify the specific actions required during installation (or subsequently) to enable it.

The deployment **is required to** authenticate all administrators by using MFA.

The product guidance documentation must specify the use of MFA authentication for admin users.

3.3.6 Deployment >> Monitoring

DEP.600: Log all relevant events

This mitigation is required to counter suspicious product usage that could be indicative of attacker activity

The deployment **should** where available, automatically export logs to a management device in a secure area.

The deployment **is required to** assess impact of log entries and follow organisational procedures for incident resolution.

The deployment **is required to** configure the product to log all actions deemed of interest.

Where the events to be logged are configured by an admin user, the product guidance documentation must include information on how to configure the product to ensure that the events logged include as a minimum those identified for DEV.600.

DEP.601: Protect access to logs and timestamp log entries

This mitigation is required to counter modification of logging generation

This mitigation is required to counter sanitisation of illegitimate access from logs

The deployment **is required to** describe any redaction function that has been implemented.

The description must include information on how the redaction is performed, how to limit access to the functionality so that only the nominated administrators can perform a redaction, and the effect of redaction on log records (giving examples to cover all different types of redaction that can result, e.g. for different logs and/or different record types).

DEP.602: Export logs with integrity protection

This mitigation is required to counter modification of locally stored logs

The deployment **is required to** provide the ability to automatically transfer log records to an external device.

The product guidance documentation must advise an administrator to configure the product to automatically transfer logs to an external device and provide sufficient information to enable it to be configured.

The deployment **is required to** protect the integrity of log records in transit.

The product guidance documentation must advise an administrator to ensure that the integrity of logs are protected in transit, and provide sufficient information to enable it to be configured.

DEP.603: Audit log review

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

The deployment **is required to** regularly review audit logs for unexpected entries.

DEP.605: Synchronised event time-stamps

This mitigation is required to counter modification of logging generation

The deployment **is required to** ensure that event time-stamps are synchronised with a reliable time-source.

3.3.7 Deployment >> Cloud Services (External)

DEP.700: Suitable cloud services

This mitigation is required to counter exploitation of insecure cloud services

The deployment **is required to** ensure that cloud services meet NCSC Cloud Security Principles.

If the product uses external cloud services, the product guidance documentation must provide advice to ensure that the configuration meets the NCSC Cloud Security guidance [Cloud]. The cloud service provider must have published their response to the NCSC Cloud Security Principles.

APPENDIX A – References

This document references the following resources.

Label	Title	Version	Date	Location	Reference
BS	NCSC CPA Build Standard	1.4	Oct 2018	https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa	NCSC-1844117881-312
CAVP	Cryptographic Algorithm Validation Program			https://csrc.nist.gov/Projects/Cryptographic-Algorithm-Validation-Program	
CEPlus	NCSC Cyber Essentials Plus			https://www.cyberessentials.ncsc.gov.uk	
Cloud	NCSC Cloud security guidance		7 Jun 2023	https://www.ncsc.gov.uk/collection/cloud	
Control_Room	NPSA Control Rooms Guidance		Dec 2016	https://www.npsa.gov.uk/resources/control-rooms-guidance-document-2016	
DSG	Device Security Guidance *(This was formerly the 'End User Device Security Collection' and 'Mobile Device Guidance')*	2.0	10 May 2022	https://www.ncsc.gov.uk/collection/device-security-guidance	
IEEE802.1X	IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control	2010	2010	https://standards.ieee.org/standard/802_1X-2010.html	
IPsec_NCSC	NCSC Guidance – using Ipsec to protect data	2.0	9 Mar 2022	https://www.ncsc.gov.uk/guidance/using-ipsec-protect-data	
ISO27001	Information Security Management Systems: Requirements	2022	2022	https://www.iso.org/isoiec-27001-information-security.html	
ISO29147	Information technology — Security techniques — Vulnerability disclosure	2018	2018	https://www.iso.org/standard/72311.html	
ISO30111	Information technology — Security techniques — Vulnerability handling processes	2019	2019	https://www.iso.org/standard/69725.html	
ISO9001	Quality Management Systems: Requirements	2015	2015	https://www.iso.org/iso-9001-quality-management.html	
MISRA	MISRA C: 2012 – Guidelines for the use of C language in critical systems	2012	March 2013	https://misra.org.uk/	

Label	Title	Version	Date	Location	Reference
MISRA Comp	MISRA Compliance:2020 – Achieving compliance with MISRA Coding Guidelines	2020	February 2020	https://www.misra.org.uk/misra-c/	
Pwned_NCSC	Suitable list of compromised passwords			https://www.ncsc.gov.uk/static-assets/documents/PwnedPasswordsTop100k.txt	
PPFGE	Process for Performing CPA Foundation Grade Evaluations	2.7	Sep 2023	https://www.ncsc.gov.uk/information/commercial-product-assurance-cpa	HV4NKQ6VV52Y-1968710376-6682
SP 800-63B	NIST Special Publication 800-63B – NIST Digital Identity Guidelines – Authentication and Lifecycle Management		June 2017 Including updates as of March 2020	https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf	
TLS_NCSC	NCSC Guidance – using TLS to protect data	1.0	21 Jul 2021	https://www.ncsc.gov.uk/guidance/using-tls-to-protect-data	

APPENDIX B – Glossary

The following definitions are used in this document.

Term	Definition
AACS	Automated Access Control System
AACS Controller	Back office system which controls the AACS
CAPSS	Cyber Assurance of Physical Security Systems
CAVP	NIST Cryptographic Algorithm Validation Program – including use of automated cryptographic algorithm validation
CCTV	Closed Circuit Television
CNI	Critical National Infrastructure
CPA	Commercial Product Assurance
CSE	Catalogue of Security Equipment – the catalogue maintained by NPSA that includes the CAPSS approved product category
Device	A physically distinct part of a product. Some products may consist of only one device.
DoS	Denial of Service
DRBG	Deterministic Random Bit Generator
Element	A physically or logically distinct part of a system. An element may consist of a device or software (or both).
IA	Information Assurance
Low Functioning device	A device such as an FPGA/ASIC device, a simple circuit, or a simple device with very minimal firmware.
MFA	Multi-Factor Authentication
Non-secure area	An area that is not secured, such as public spaces and building exteriors.
NTP	Network Time Protocol
OS	Operating System
PIR	Passive Infrared
Product	The target of the evaluation. A product may consist of a single device, a subsystem or a system.
PTP	Precision Time Protocol, also known as IEEE 1588
SC	Security Characteristic
Secure area	A secured area with access limited to authorised personnel and escorted unauthorised personnel.
Secure enclave	A secured area with access limited to individually authorised personnel, no unescorted access for unauthorised personnel, with records of access. Typically a secure server room or secure control room. See [Control_Room] for guidance.

Term	Definition
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.
Sensitive data	Data which, if compromised, would undermine the cyber security of the product, or the physical security of the site (or of assets that the product is supposed to protect according to its own requirements or requirements in its intended deployment environment), or a person's expectation of privacy. This includes personal data (related to the person and their expectation of privacy), configuration data and cryptographic material such as keys and passwords.
System	A group of related elements, especially when dedicated to a single application.
Subsystem	A self-contained system within a larger system.
Test configuration	The configuration of the product that is used in the evaluator testing against CAPSS requirements. This includes both core and peripheral elements as described in section 1.6.

APPENDIX C – Password Policy

The following requirements are the minimum for an acceptable password policy.

- The system will require the user to change the password when logging in for the first time.
- The password must be a minimum of nine characters in length.
- The password must have a maximum length of at least 64 characters.
- Account lock out shall be set at ten attempts or less (min of three).
- Passwords must not be:
    - Passwords obtained from previous breach corpuses (by checking against an offline list obtained from a reliable source such as [Pwned_NCSC]).
    - Dictionary words. (Where the whole password is a single dictionary word).
    - Three or more repetitive or sequential characters (e.g. ‘aaa’, ‘1234abcd’).
    - Context-specific words, such as the name of the service, the username, and derivatives thereof.

Passwords should only be required to be changed upon suspicion that a password has been compromised. No previous password shall be allowed by the product (because they’re suspected to have been breached)

Passwords should be stored hashed and salted with a unique salt per password.

For systems with remote access, MFA should be used in line with NIST requirements [SP 800-63B].

APPENDIX D – Applying Mitigations

The mitigations identified in section 3 are generally intended to apply to all Physical Security System products and their elements. However it is recognised that in some deployment situations certain threats may not apply to some elements of the PSS – for example, a low functioning device such as a PIR sensor will have different applicable threats compared to a high functioning server.

The relevance of each threat may vary according to the deployed location, the architecture and communications protocols of each specific product.

The tables below identify DEV, VER and DEP mitigations for which it may be allowable to accept a rationale as to why the mitigation has not been met.

The rationale must show that the relevant threat does not apply to the element, given

a) its level of functionality (i.e. whether it is a low functioning device), and
b) the applicable threats in its deployment environment (e.g. a PIR sensor located in a non-secure area might not contain sensitive data and therefore might not have the threat 'extraction of sensitive data').

Development Mitigations	
DEV General	
101	Heap hardening
102	Stack protection
103	Data Execution Prevention
104	Address Space Layout Randomisation
105	Encrypt sensitive data
108	Protected software environment
DEV Secure Configuration	
303	Deploy onto suitably protected endpoint
DEV Network Security	
403	Use time synchronisation
404	Use segregated networks
405	General resource management
406	Encrypt communications traffic over untrusted link
DEV Authentication Management (Privileges)	
500	Role based access control
501	User least privilege
502	User authentication and re-authentication
506	Management interface protection
DEV Monitoring	
600	Log all relevant events
601	Protect access to logs and timestamp log entries
602	Export logs with integrity protection
604	Record when device last seen
DEV Cloud Services (External)	
700	Suitable cloud services

Development Mitigations	
Verification Mitigations	
403	Use time synchronisation
404	Use segregated networks
405	General resource management
406	Encrypt communications traffic over untrusted link
VER Authentication Management (Privileges)	
501	User least privilege
502	User authentication and re-authentication
506	Management interface protection
VER Monitoring	
600	Log all relevant events
601	Protect access to logs and timestamp log entries
604	Record when device last seen
VER Cloud Services (External)	
700	Suitable cloud services

Deployment Mitigations	
DEP General	
105	Encrypt sensitive data
106	Updateable product
110	Administrator authorised updates
DEP Secure Configuration	
303	Deploy onto suitably protected endpoint
DEP Network Security	
403	Use time synchronisation
404	Use segregated networks
DEP Authentication Management (Privileges)	
500	Role based access control
501	User least privilege
502	User authentication and re-authentication
503	One administrator per account

Deployment Mitigations	
506	Management interface protection
DEP Monitoring	
600	Log all relevant events
601	Protect access to logs and timestamp log entries
602	Export logs with integrity protection
603	Audit log review
605	Synchronised event time-stamps
DEP Cloud Services (External)	
700	Suitable cloud services

It is important to note that whenever the functionality referred to in a CAPSS requirement is provided by an element, then the evaluation of the product *must* include evaluation of that requirement and any related requirements.

This means that a product must implement a mitigation if:

a) that mitigation is required, or
b) the mitigation is not required but has been voluntarily implemented.

Example 1

Regarding DEV.105: any device that contains sensitive data must implement sensitive data protection as in DEV.105 *Encrypt sensitive data*

Or

If no sensitive data is held on the device then DEV.105 can be limited to the details, and acceptance, of the rationale (which demonstrates the absence of sensitive data)

Or

When encryption is undertaken (whether required or not) this must be done in a manner compliant with DEV.100 *Evaluation/Cryptocheck* to confirm that the encryption and its implementation is robust.

Example 2

If a device includes a stack, then it is required to meet DEV.102 *Stack Protection*, but a Low Functioning device that is purely hardware and does not contain executable firmware, would not have a stack and therefore DEV.102 can be limited to the details, and acceptance, of the rationale (which demonstrates the absence of a stack).

Each element of a CAPSS product must be examined against its own set of applicable threats when applying this methodology. It is not permissible to simply state “encryption not required” without justifying *why* the encryption is not required. Different rationales would therefore be expected for a low functioning device such as a PIR sensor, and a high functioning server.

The Tailored Security Characteristic for the product identifies which mitigations apply for a particular device and describes the scope of their application (e.g. a device might have some firmware that is updateable and some that is not, and this would determine the scope of DEV.106 for that device).

APPENDIX E – Change History

This appendix describes the main changes made in the Security Characteristic starting from CAPSS 2019 as the baseline.

E.1 CAPSS 2019 to CAPSS 2021 v1.0

(Note that no separate CAPSS 2020 version was published.)

The approach to determining relevant mitigations for an element has been revised in CAPSS 2021. The intent has generally been to maintain the same requirements but to make it clearer how to determine relevant mitigations for each target part of the PSS. This high-level change has the following pieces:

- The table in CAPSS 2019 SC Appendix D has been replaced with a list of mitigations for which a rationale may in some cases be accepted to show that the mitigation is not required.
- The use of variants (and therefore the associated section) has been removed from the SC.
- Additional guidance on determining the applicability of a mitigation has been added in the Application Notes.

The term ‘highly constrained device’ has been replaced with ‘low functioning device’ (previously both were used with effectively the same meaning).

The definition of sensitive data, and its use in DEV.105 has been updated.

The requirements for protection of debug interfaces in DEV.200 (and VER.200) have been modified to identify alternatives to MFA.

Notes have been added to draw attention to the following:

- servers and other high functioning devices need to implement equivalent measures to those in [EUD]
- wireless may not be used on sites requiring more than a basic level of protection (this was already noted in DEP.401, but additional notes have been included in other places where wireless is mentioned)

DEP.300 now requires a description of how an administrator can check that the deployment is in the evaluated configuration after initial installation and during subsequent operation, and documentation of secure area assumptions related to each element.

DEP.401 now requires product documentation and CSE entries to note any necessary use of wireless by the PSS. Where wireless is present but must be disabled to meet CAPSS requirements this must also be documented, and VER.401 requires evaluator testing to confirm that the interface is actually disabled by the documented action.

References have been updated, including replacing the previous NCSC guidance on ‘End User Devices’ with guidance for ‘Mobile Devices’. However, the term ‘End User Device’ has been retained for CAPSS 2021.

E.2 CAPSS 2021 v1.0 to CAPSS 2021 v1.1

Additional information on order of undertaking NPSA functional standard or NPSA CAPSS evaluations has been added in this updated CAPSS 2021 v1.1, but no changes have been made to the mitigations. Additional interpretations and clarifications can be found in the CAPSS 2021 v1.1 Application Notes.

E.3 CAPSS 2021 v1.1 to CAPSS 2022 v1.0

An additional note has been added to pre-requisite 2 (section 1.9) to clarify that the scope of any accreditation must include the CAPSS product.

Some mitigation names (DEV.402, DEV.502, DEV.601, DEV.602, VER.502, VER.601 DEP.502, DEP.602) have been updated to better reflect their content.

Requirement DEV.111 has been added, which requires description of the use of DRBGs and entropy in the product. DEV.113 has been added, to clarify documentation required for the cryptographic key architecture.

ACVP has been mentioned to confirm that it is an acceptable alternative to CAVP.

The text of DEV.402 has been updated (and changed from 'should' to 'shall' for the more general requirement text) to better reflect the overall requirement for device authorisation, but still allowing a variety of implementations.

DEV.504, DEV.505, VER.504, VER.505, DEP.504 & DEP.505 have been replaced by DEV.506, VER.506 & DEP.506: the requirements for local and remote management interfaces have been integrated under one heading.

References have been updated to reflect changes on the NCSC website by replacing the previous NCSC guidance on 'Mobile Devices' with 'Device Security Guidance'. The reference identifier in Appendix A has been changed from [EUD] to [DSG], and references to the guidance have been updated.

E.4 CAPSS 2022 v1.0 to CAPSS 2023 v1.0

The term "element" has replaced "component" in a number of places, to align on a Glossary-defined term where appropriate. The term "guidance documentation" has replaced "deployment guidance" (and some similar terms) to align with terminology being used in other NPSA cybersecurity documents.

Updates have been made to the following mitigations in order to accommodate a possible need for redaction of log content in support of data protection regulations (e.g. UK or EU GDPR):

- DEV.600 (Log all relevant events)
- DEV.601 (Protect access to logs and timestamp log entries)
- VER.601 (Protect access to logs and timestamp log entries)
- DEP.601 (Protect access to logs and timestamp log entries) was added.

References have been updated to reflect latest changes in versions and locations.

E.5 CAPSS 2023 v1.0 to CAPSS 2024 v1.0

"CPNI" has been replaced by "NPSA" throughout.

The term "ACVP" was removed and a note added for CAVP to note that this now includes automated validation ("ACVP" refers to the "Automated Cryptographic Validation Protocol" that is now used for the automated version).

New section 'Core and peripheral elements' added to clarify the definition and evaluation of core and peripheral elements within the product. This creates a new section 1.6 and therefore previous sections 1.6-1.11 have been renumbered. The term 'test configuration' was also added to the Glossary in Appendix B.

The description of the TSC in section 1.8 (after renumbering to add the new section 1.6 as above) has been updated to reflect the changes in [PPFGE].

In DEV.402 the word “shall” has been changed to “is required to” for consistency with the other requirements. (This is a cosmetic change only, and does not affect the nature of the requirement.)

References have been updated to reflect latest changes in versions and locations.

Freedom of Information Act (FOIA)
This information is supplied in confidence and may not be disclosed other than to the agreed readership, without prior reference to NPSA. Within the UK, this material is exempt from disclosure under the relevant Freedom of Information Acts and may be subject to exemption under the Environmental Information Regulations and the Data Protection Act 1998.

Disclaimer
This document has been prepared by the National Protective Security Authority (NPSA). This document is provided on an information basis only, and whilst NPSA has used all reasonable care in producing it, NPSA provides no warranty as to its accuracy or completeness. To the fullest extent permitted by law, NPSA accepts no liability whatsoever for any expense, liability, loss, damage, claim, or proceedings incurred or arising as a result of any error or omission in the document or arising from any person acting, refraining from acting, relying upon or otherwise using the document. You should make your own judgment with regard to the use of this document and seek independent professional advice on your particular circumstances.