CPA SECURITY CHARACTERISTIC

SOFTWARE FULL DISK ENCRYPTION

Version 1.23

About this document

This document describes the features, testing and deployment requirements necessary to meet CPA certification for Software Full Disk Encryption security products. It is intended for vendors, system architects, developers, evaluation and technical staff operating within the security arena.

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

Document history

The CPA Authority may review, amend, update, replace or issue new Scheme Documents as may be required from time to time. Soft copy location: DiscoverID 27289237.

Version	Date	Description
1.00	April 2011	First release of SFDE SC
1.22	August 2012	Added support for a wider range of operating systems
1.23	March 2013	Added TPM support and Common Criteria Protection Profile Mappings appendix

This document is derived from the following SC Maps.

SC Map	Map version
Software Full Disk Encryption	1.23
Common Libraries	1.9
Crypt Libraries	1.5
Hardware Libraries	1.4
Passphrase Libraries	2.1

Contact CESG

This document is authorised by: Deputy Technical Director (Assurance), CESG. For queries about this document please contact:

CPA Administration Team
CESG, Hubble Road
Cheltenham
Gloucestershire
GL51 0EX, UK

Email: cpa@cesg.gsi.gov.uk
Tel: +44 (0)1242 221 491

[1] www.cesg.gov.uk/servicecatalogue/CPA

Contents

1.1 Introduction

This document is a CPA Security Characteristic. It describes requirements for assured Software Full Disk Encryption products for evaluation and certification under CESG's Commercial Product Assurance (CPA) scheme.

1.2 Product description

The primary purpose of a software disk encryption product is to protect the confidentiality of data at rest. Products can also provide some integrity protection of the protected data. This Security Characteristic does not define requirements for removable media encryption. Although some software disk encryption products also support removable media encryption, this is out of scope for this document.

1.3 Typical use cases

The expected use case is to protect a mobile device (laptop or netbook) in case of accidental loss or theft. Provided that the user has followed the guidelines in the product's security procedures, the disk encryption software will prevent an attacker from accessing the data when given access to a powered-off device.

Although this Security Characteristic is primarily targeted towards a single user (plus administrator) per protected device, products which implement multiple users can still be evaluated under it.

1.4 Compatibility

This Security Characteristic is currently only applicable to software disk encryption products that operate on PCs with UEFI or BIOS boot environments (Note: general security considerations for UEFI BIOS can be found in [f]).

No other requirement is placed on the hardware (device and disk), provided that it meets the technical requirements for the product. For example, some products may have specific CPU or memory requirements in order to function correctly – this document places no minimum requirements on such aspects.

No specific requirements are placed on the operating system that hosts a software disk encryption product conforming to this Security Characteristic other than to allow the product to operate correctly whilst meeting the requirements in Section 3. This said, there is a general expectation that the product will be compatible with the latest version of a given operating system.

1.5 Interoperability

Some, but not all, software disk encryption products may be capable of operation with an enterprise management solution. Where a vendor wishes to have this capability assessed, the Enterprise Management of Data at Rest Encryption Security Characteristic ([g]) will be applicable.

1.6 Variants

This Security Characteristic has three variants, regarding the implementation of KEK (Key Encryption Key) protection. These variants are:

- Simple Token - This type of token is simply a storage device, it is not required to offer any protection against unauthorised access to the key data it contains, its contents are cryptographically combined with a user password to permit access to encrypted data.

- Smart Token - This type of token offers some protection against unauthorised access to the key data it contains. The token simply provides the DEK to the product upon successful authentication. See below for more information on assurance requirements for the Smart Token.
- TPM - Use of a Trusted Platform Module (TPM) v1.2 which forms part of the host platform. The TPM must be assured to (at least) the same level as the disk encryption product, to ensure it provides protection against unauthorised access to the key data which it contains. Access to data stored on the TPM is based on 'authentication data' which is cryptographically derived from the user passphrase.

There is no tokenless variant (i.e. password only) that meets this Security Characteristic.

Tokens must not be stored with the device and, as such, should not be lost with it. However, it is assumed that a percentage of devices and tokens will be lost together in practice.

1.6.1 Smart Token assurance

If the product employs the Smart Token variant, then the Smart Token must be a smartcard in which the integrated circuit has been certified as compliant with the Common Criteria Protection Profile "Security IC Platform Protection Profile" (BSI-PP-0035) to EAL4+ (ALC_DVS.2, AVA_VAN.5) or higher [c]. The Operating System on the Smart Token must also have been certified (as a composite TOE) to EAL4+ (ALC_DVS.2, AVA_VAN.5) or higher in the areas of functionality required to prevent unauthorised access to the DEK, KEK and passphrase, and regarding the prevention of unauthorised application load.

It is recommended that the Smart Token should only be used for the protection of disk encryption keys for the evaluated product. If such a Smart Token is also intended to be used for network authentication, it is important that it is never connected to a less-secure or less-protected system.

1.6.2 TPM assurance

If the product employs the TPM variant, then the TPM must be a TCG-compliant v1.2 TPM, assured to foundation grade as appropriate. If the product employs a TPM as an additional factor (i.e. it is a simple or Smart Token variant, but is using the TPM in addition to these) then it is not necessary to deploy an assured TPM.

1.7 High level functional components

The following diagram illustrates the various high level functional components within this product. All components relate to specific mitigations listed in Section 3. These are used to structure the Security Characteristic, and to give context to each mitigation.

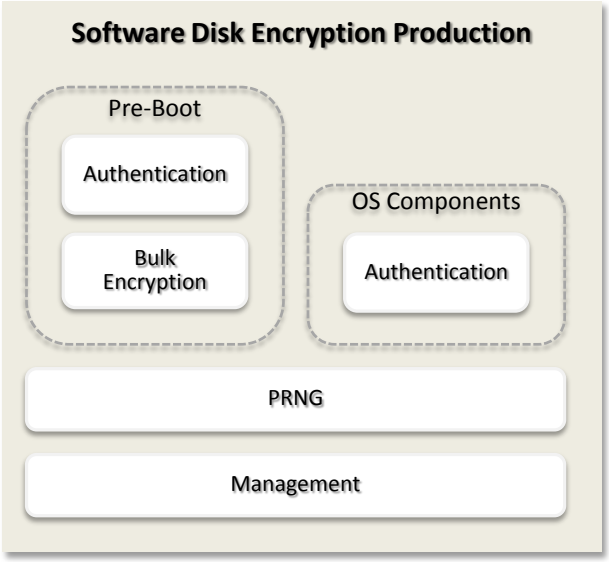

Figure 1: Functional components of a Software Full Disk Encryption product

The functional components in Figure 1 are described as follows.

- **Bulk Encryption**. Handles the encryption and decryption of the data stored on the computer. All data must pass through this component before being written to disk. Cryptographic operations are performed in a pre-boot environment and by a kernel mode component once the operating system is running which encrypts/decrypts data to/from the device.
- **Authentication**. Handles user log in to the disk encryption product. Cryptographically hashes the passphrase and interfaces with the token to verify credentials and unlock the disk encryption key.
- **PRNG**. Handles random generation of the disk encryption key and the passphrases that protect it.
- **Management**. Covers all aspects of the system which control the behaviour/configuration of the product.

1.8 Future enhancements

- CESG welcomes feedback and suggestions on possible enhancements to this Security Characteristic.
- CESG intend to incorporate the use of CPA-approved Smart Tokens once a Security Characteristic has been developed for them.

2.1 Requirement categories

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

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

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

For example, mitigations within a section that begins:

Development>>Management

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

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

2.2 Understanding mitigations

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

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

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

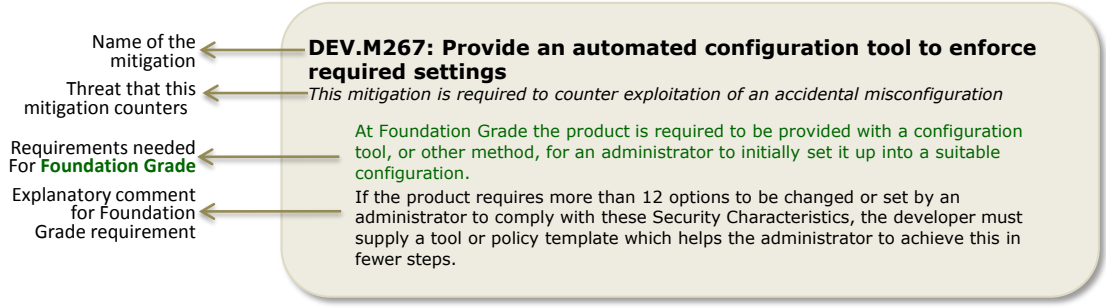

Figure 2: Components of a typical mitigation

This section lists the Development, Verification and Deployment mitigations for the Software Full Disk Encryption Security Characteristic. For a summary of the changed mitigations in this version, please refer to Appendix A.

3.1 Development mitigations

DEV.M41: Crash reporting

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

At Foundation Grade the product **is required to** ensure crashes are logged.

Where it is possible that sensitive data may end up in the crash data, this must be handled as red data and must only be available to an administrator. Crash data from both the product and the underlying operating system must be considered.

DEV.M42: Heap hardening

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

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

DEV.M43: Stack protection

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

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

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

DEV.M46: User least privilege

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

At Foundation Grade the product **is required to** operate correctly from a standard account without elevated privileges.

DEV.M159: Update product

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

At Foundation Grade the product **should** support the use of software updates.

DEV.M319: Keys not accessible by non-admins

This mitigation is required to counter a social engineering attack on user

At Foundation Grade the product **is required to** ensure that the DEK is not accessible from user mode through legitimate means.

It must not be possible for non-administrative users to be able to read or modify the DEK through a product-provided API, even when running as a privileged process.

DEV.M321: Data Execution Prevention

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

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

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

DEV.M340: Address Space Layout Randomisation

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

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

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

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

DEV.M349: Sanitise temporary variables

This mitigation is required to counter reading remnant volatile memory

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

A secure erase must consist of at least one complete overwrite.

DEV.M355: Secure software delivery

This mitigation is required to counter installation of malware on host
This mitigation is required to counter installing compromised software using the update process

At Foundation Grade the product **should** be distributed via a cryptographically protected mechanism, such that the authenticity of software can be ensured.

DEV.1 - Development >> Bulk Encryption

DEV.1.M15: Keys only in volatile storage

This mitigation is required to counter unencrypted storage enabling secrets to be recovered

At Foundation Grade the product **should** ensure that buffers containing keys are not pageable.

DEV.1.M16: Full Disk Encryption

This mitigation is required to counter unencrypted storage enabling secrets to be recovered

At Foundation Grade the product **is required to** ensure that no user data can be written unencrypted to the protected disk. This must include any swap data, kernel crash dumps and hibernation data (if hibernation is enabled).

DEV.1.M317: Approved bulk encryption algorithm

This mitigation is required to counter bit-flipping attacks on sectors containing known data
This mitigation is required to counter exploitation of a weak cryptographic algorithm
This mitigation is required to counter inference of data via reuse of bulk encryption key

At Foundation Grade the product **is required to** use AES-CBC or AES-CFB [e] with a unique DEK and IV.

Each encrypted block (typically disk sector) must be encrypted with a unique DEK-IV pair.

There is no requirement to use non-sequential IVs, but where the product supports multiple disks, the DEK-IV pair must be unique across all disks. This could be achieved with a different DEK for each disk, or an IV offset scheme.

DEV.2 - Development >> Authentication

DEV.2.M13: Passphrase length and complexity enforcement

This mitigation is required to counter dictionary and exhaustion attacks
This mitigation is required to counter exploitation of poor passphrase complexity

At Foundation Grade the product **is required to** have administrator configurable passphrase complexity and length settings.

The system must enforce the administrator-set passphrase complexity, which must support a setting of at least 8 characters, including a mixture of upper and lower case, numbers and/or special characters.

DEV.2.M20: Passphrase and token rollover (DEK rewrap)

This mitigation is required to counter replaying captured credentials

At Foundation Grade the product **is required to** allow the user to update their passphrase when required.

At Foundation Grade the product **is required to** only allow an authenticated administrator to issue a new token and revoke the existing one.

DEV.2.M111: (Simple Token ONLY) Approved key split recombination algorithm

This mitigation is required to counter exploitation of weak KEK protection

At Foundation Grade the product **is required to** use a cryptographically strong mechanism for key split recombination.

The recombination mechanism must prevent compromise of one of the splits reducing the work required to recover the complete key. Bitwise exclusive-OR (XOR) is an example of an acceptable recombination mechanism.

DEV.2.M114: (Smart Token ONLY) The passphrase is used to cryptographically unlock the smart token

This mitigation is required to counter memory reallocation which permits sensitive data to be discovered
This mitigation is required to counter the passphrase or token being issued to the attacker by mistake
This mitigation is required to counter the user entering their passphrase on a fake or unprotected system

At Foundation Grade the product **is required to** encrypt the DEK using a KEK stored on a smart token which is unlocked using the hashed passphrase.

The KEK must be of the same cryptographic strength as the DEK. AES Key Wrap should be used to encrypt the DEK.

DEV.2.M132: (Simple Token ONLY) Key is cryptographically split between the passphrase and the simple token

This mitigation is required to counter memory reallocation which permits sensitive data to be discovered
This mitigation is required to counter the passphrase or token being issued to the attacker by mistake
This mitigation is required to counter the user entering their passphrase on a fake or unprotected system

At Foundation Grade the product **is required to** protect the DEK using a split KEK, where the cryptographic combination of token data with a passphrase hash forms the key to decrypt the DEK.

The KEK is split between the simple token and passphrase and then recombined in memory using an approved recombination algorithm. The complete KEK must not be written to the simple token or the hard disk at any point.

DEV.2.M278: Approved passphrase hashing algorithm

This mitigation is required to counter capture of passphrase stored in the clear

At Foundation Grade the product **is required to** use at least 1 round of SHA-256 as the passphrase hashing algorithm.

DEV.2.M279: Disable old passphrase as soon as a new passphrase is enabled

This mitigation is required to counter use of a user's old passphrase

At Foundation Grade the product **is required to** ensure old passphrases cannot be used to authenticate the user.

DEV.2.M289: Approved passphrase salting mechanism

This mitigation is required to counter dictionary and exhaustion attacks

At Foundation Grade the product **is required to** use at least a 64-bit salt as part of the passphrase hashing algorithm.

This must be unique per user credential and the salt must also be changed when the passphrase is changed.

DEV.2.M618: Passphrases are not displayed on screen in the clear while being entered

This mitigation is required to counter shoulder surfing

At Foundation Grade the product **is required to** ensure the passphrase is never visible in the clear on the screen.

DEV.2.M619: Effective user account revocation

This mitigation is required to counter use of a previous user's credentials

At Foundation Grade the product **is required to** provide the ability to revoke user accounts.

The product must ensure that once a user account has been revoked it does not continue to function.

DEV.2.M841: (TPM ONLY) The passphrase is used to cryptographically create the authentication data for the TPM

This mitigation is required to counter memory reallocation which permits sensitive data to be discovered
This mitigation is required to counter the passphrase or token being issued to the attacker by mistake
This mitigation is required to counter the user entering their passphrase on a fake or unprotected system

At Foundation Grade the product **is required to** encrypt the DEK using a KEK stored on a TPM which is unlocked using the hashed passphrase.

The KEK must be of the same cryptographic strength as the DEK.

The hashed passphrase must be used to form authentication data for the TPM.

DEV.2.M842: Trusted Computing technology is used to protect platform integrity

This mitigation is required to counter installation of BIOS/UEFI malware
This mitigation is required to counter the user entering their passphrase on a fake or unprotected system

At Foundation Grade the product **should** use a TPM as an authentication factor, sealing state to a defined set of Platform Configuration Registers (PCRs).

The product should use a v1.2 TPM as an authentication factor, and use the ability of the TPM to 'seal' secrets to a particular platform configuration. The product should (as a minimum) use PCRs 0, 2 and 4.

DEV.3 - Development >> Management

DEV.3.M267: Provide an automated configuration tool to enforce required settings

This mitigation is required to counter exploitation of an accidental misconfiguration

At Foundation Grade 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 the 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 or policy template which helps the administrator to achieve this in fewer steps.

DEV.3.M353: 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

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

DEV.4 - Development >> PRNG

DEV.4.M140: Smooth output of entropy source with approved PRNG

This mitigation is required to counter predictable key generation due to a weak entropy source

At Foundation Grade the product **is required to** employ a PRNG of sufficient Security Strength for all random number generation required in the operation of the product.

For more details on a suitable PRNG, please see the Process for Performing Foundation Grade Evaluations.

DEV.4.M141: Reseed PRNG as required

This mitigation is required to counter the prediction of randomly generated values due to repeating PRNG output

At Foundation Grade the product **is required to** follow an approved reseeding methodology.

DEV.4.M290: Employ an approved entropy source

This mitigation is required to counter predictable key generation due to a weak entropy source

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

The developer must provide a detailed description of the entropy source used, giving evidence that it can generate sufficient entropy for use in the device, including an estimate of entropy per bit.

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

DEV.4.M292: State the Security Strength required for key generation

This mitigation is required to counter predictable key generation due to a weak entropy source

At Foundation Grade the product **is required to** employ an entropy source of sufficient Security Strength for all random number generation required in the operation of the product.

The developer must state the Security Strength required of their entropy source based on analysis of all random numbers used in the product. At this grade, the Security Strength is likely to be 128 bits for products that do not use elliptic curve cryptography. For elliptic curve-based asymmetric mechanisms it is likely to be 256 bits, and for finite field based asymmetric mechanisms it is likely to be 192 bits.

3.2 Verification mitigations

VER.M341: Audit permissions on product install

This mitigation is required to counter exploitation of a privileged local service

At Foundation Grade the evaluator **will** audit any system permissions and ACLs set or altered by the product during installation to ensure that no changes are made, which would give a standard user the ability to modify any components that run with higher privileges (either product or system provided).

VER.M347: Verify update mechanism

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

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

The update process must provide a mechanism by which updates can be authenticated before they are applied.

The process and any configuration required must be documented within the Security Procedures.

VER.1 - Verify >> Bulk Encryption

VER.1.M4: Evaluation/Cryptocheck

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

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

VER.2 - Verify >> Authentication

VER.2.M4: Evaluation/Cryptocheck

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

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

3.3 Deployment mitigations

DEP.M1: Require physical protection

This mitigation is required to counter physical destruction of the product
This mitigation is required to counter physical tampering with the device

At Foundation Grade the deployment **is required to** require physical protection of the device.

Users should be given guidance on how to handle devices. The device must not be left unattended whilst powered on or suspended, as the data will not be encrypted when the device is in these states. The device should never be left unattended in public or visible in a locked car.

DEP.M26: Physical tamper evidence

This mitigation is required to counter physical compromise of device

At Foundation Grade the deployment **is required to** educate users to regularly check that tamper labels are intact.

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

Use tamper evidence (e.g. stickers) to make entry to system internals detectable by physical inspection. Tamper stickers should be uniquely identifiable to prevent an attacker successfully replacing it with a new, undamaged sticker.

At Foundation Grade the deployment **is required to** provide administrators with advice on the tamper threat.

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

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.

DEP.M30: Detect modification to system

This mitigation is required to counter installation of malware on host

At Foundation Grade the deployment **is required to** be configured in line with good IT practice as part of a risk-managed accredited system.

Typically, this will include the installation and subsequent updating of a commercial antivirus product.

DEP.M32: Disable all boot methods except encrypted disk

This mitigation is required to counter booting from network or removable media to tamper with the device's integrity

At Foundation Grade the deployment **is required to** configure the boot environment (e.g. BIOS) to set the protected hard disk as the only permitted boot device.

If there is a 'Boot From Other Devices' option, that must be disabled in addition to disabling CD/DVD/Floppy/USB/Network.

DEP.M36: Protect/disable ports

This mitigation is required to counter exporting the DEK from device via a bus

At Foundation Grade the deployment **is required to** educate users to protect their devices when the device is turned on.

There are various attacks that can be performed on a powered up device to obtain the data. The user should be instructed to never leave a device unattended when it is powered up or in 'sleep' mode and always shut it down when it is left. If hibernation is supported by the Disk Encryption product, then this may be used when the device is left unattended.

DEP.M39: Audit log review

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

At Foundation Grade the deployment **is required to** regularly review audit logs for unexpected entries.

DEP.M46: User least privilege

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

At Foundation Grade the deployment **is required to** ensure all user accounts have the fewest privileges required to enable business functionality.

DEP.M112: Notification procedure for loss assessment

This mitigation is required to counter finding or stealing a device

At Foundation Grade the deployment **is required to** provide users with a procedure for notifying their organisation of the theft/loss of their device in a timely fashion.

Users should be informed to continue to protect their token and passphrase after the device is lost and inform their IT support organisation immediately.

DEP.M131: Operating system verifies signatures

This mitigation is required to counter installation of a malicious privileged local service

At Foundation Grade the deployment **is required to** enable signature verification for applications, services and drivers in the host operating system, where supported and where the product makes use of it.

DEP.M137: Product must be securely disposed of

This mitigation is required to counter insufficient sanitisation of sensitive information at point of device disposal leaving sensitive information in a retrievable state

At Foundation Grade the deployment **is required to** ensure that the product is disposed of in accordance with IS5.

DEP.M159: Update product

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

At Foundation Grade the deployment **is required to** update to the latest version where possible.

DEP.M339: Host system is free of malware

This mitigation is required to counter installation of malware on host

At Foundation Grade the deployment **is required to** use only managed endpoints to host the product and, where possible, keep software (including antivirus products) up to date.

DEP.M340: Address Space Layout Randomisation

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

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

DEP.M348: Administrator authorised updates

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

At Foundation Grade 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's security procedures.

DEP.M661: Protect key backups

This mitigation is required to counter exporting the DEK from device via a bus

At Foundation Grade the deployment **is required to** store any copies of the key in a manner appropriate to its classification.

DEP.M662: Protect device boot settings from modification

This mitigation is required to counter installation of BIOS/UEFI malware

At Foundation Grade the deployment **is required to** configure a password to prevent changes to the device boot configuration.

Passwords that protect the boot configuration should not be guessable by a human although there is no requirement to enforce regular changes to such passwords. It is acceptable to re-use a single password across an estate of devices, but different passwords should be used on systems accredited for different security domains.

At Foundation Grade the deployment **should** use a Trusted Computing Group-compliant v1.2 TPM.

DEP.1 - Deployment >> Bulk Encryption

DEP.1.M318: Prevent duplication of keys

This mitigation is required to counter accessing multiple devices from a single compromise due to DEK reuse

At Foundation Grade the deployment **is required to** install each device (DEK and token) with unique entropy.

Cloning encrypted disks will duplicate the DEK, so a single DEK compromise will allow access to multiple devices. If disks are to be cloned as part of the build process, they must be re-keyed individually. Alternatively a cloning tool which is specifically designed for use with the Disk Encryption product which prevents DEK re-use may be used.

DEP.1.M660: Await completion of encryption before use

This mitigation is required to counter unencrypted storage enabling secrets to be recovered

At Foundation Grade the deployment **is required to** instruct users not to store any sensitive information on the device until it is fully encrypted.

DEP.2 - Deployment >> Authentication

DEP.2.M12: Passphrase is set to suitable size and complexity

This mitigation is required to counter exploitation of poor passphrase complexity

At Foundation Grade the deployment **is required to** set passphrase complexity requirements to be at least 8 characters, including a mixture of upper and lower case, numbers and/or special characters.

DEP.2.M17: User guidance on token storage

This mitigation is required to counter gaining access to token

At Foundation Grade the deployment **is required to** inform users to keep the token, passphrase and device physically separate when not in use.

DEP.2.M19: Credential change awareness

This mitigation is required to counter replaying captured credentials

At Foundation Grade the deployment **is required to** make the user aware of the requirement to change their passphrase and/or token if they believe it may have been compromised.

DEP.2.M117: (Smart Token ONLY) Use of an appropriately assured Smart Token

This mitigation is required to counter exploitation of weak KEK protection

At Foundation Grade the deployment **is required to** use an assured smartcard in accordance with the guidelines in the Smart Token Assurance section of this Security Characteristic.

DEP.2.M277: User guidance on social engineering

This mitigation is required to counter a social engineering attack on the user

At Foundation Grade the deployment **should** educate users about social engineering methods used by attackers.

DEP.2.M280: Distribute initial credentials out of band

This mitigation is required to counter interception of initial passphrase during distribution

At Foundation Grade the deployment **is required to** ensure that credentials are sent to users separately to the product that they will be protecting.

DEP.2.M281: Only administrators can modify passphrase settings

This mitigation is required to counter modification of passphrase settings

At Foundation Grade the deployment **is required to** ensure only system administrators have access to minimum passphrase length, complexity and automatic generation settings.

DEP.2.M283: User guidance on passphrase management

This mitigation is required to counter exploitation of poor management of passphrases by the user

At Foundation Grade the deployment **is required to** provide user training on passphrase management.

Users should be provided with guidance regarding the secure handling of passphrases which allow access to sensitive systems. Users must be taught never to disclose passphrases, even to their superiors.

Users must also be made aware of the risks of using protectively marked devices in public or untrusted areas. Passphrases should not be entered in areas where others could see them being entered.

DEP.2.M285: Secure storage of user passphrases

This mitigation is required to counter poor passphrase storage

At Foundation Grade the deployment **is required to** ensure any hardcopies of passphrases are stored securely.

DEP.2.M617: User guidance on passphrase selection

This mitigation is required to counter dictionary and exhaustion attacks

This mitigation is required to counter obtaining and using a user passphrase from a different system

At Foundation Grade the deployment **is required to** provide user training on passphrase selection.

Users must be provided with guidance regarding the selection of passphrases which allow access to sensitive systems.

Passphrases must be unique per device to prevent compromise of multiple systems.

DEP.2.M843: (TPM ONLY) Use of an appropriately assured TPM

This mitigation is required to counter exploitation of weak KEK protection

At Foundation Grade the deployment **is required to** use a Foundation Grade assured TPM.

DEP.3 - Deployment >> Management

DEP.3.M38: Use automated configuration tool

This mitigation is required to counter exploitation of an accidental misconfiguration

At Foundation Grade the deployment **is required to** be configured using automated tools if provided.

Appendix A Summary of changes to mitigations

CESG has updated the Software Full Disk Encryption Security Characteristic 1.23 (previously version 1.22) for the following reasons.

- Addition of TPM related requirements
- Removal of augmented requirements

This has resulted in the following changes to mitigations.

A.1 Removed mitigations

The following mitigations have been removed.

- DEV.M44: Data validation on untrusted input
- DEV.M49: Function in a locked-down environment
- DEV.2.M663: Wrapped keys sanitised on credential rollover and account revocation
- DEV.4.M142: Perform statistical testing of generated entropy prior to smoothing
- VER.M349: Sanitise temporary variables
- VER.1.M16: Full Disk Encryption
- VER.2.M132: Key is cryptographically split between the passphrase and the simple token
- VER.3.M564: Cryptocheck PRNG implementation
- VER.3.M565: Validate vendor's entropy assertions

A.2 Modified mitigations

The following mitigations have been modified.

- DEP.M662: Protect device boot settings from modification

A.3 Renamed mitigations

(No mitigations have been renamed.)

A.4 New mitigations

The following mitigations have been added.

- DEV.2.M841: The passphrase is used to cryptographically create the authentication data for the TPM
- DEV.2.M842: Trusted Computing technology is used to protect platform integrity
- DEP.2.M843: Use of an appropriately assured TPM

Appendix B Common Criteria Protection Profile Mappings

This appendix provides important mappings between this SC document and the Protection Profile for Software Full Disk Encryption v1.0 (reference [h]).

B.1 Protection Profile selections

There are a number of specific selections which must be made by the author of a Security Target derived from the above Protection Profile to ensure overlap with the Security Characteristic:

1. FCS_COP.1.1(1) CBC mode must be selected. Other modes may also be acceptable, please discuss with CESG.
2. FCS_CKM.1.1(Y) The selection must be using 'NIST SP 800-132 with a salt generated using a Random Bit Generator as specified in FCS_RBG_EXT.1'. Other selections within this option can be made at the developer's discretion.
3. If the product supports protecting hibernation mode (a power-saving mode in which the contents of memory are saved to disk) then the requirements in section C.5.1 must have been included in the assessment.

B.2 Authentication modes

The Security Characteristic defines a number of 'authentication modes'; products can implement one or more of these modes and have each of these assessed as desired. The Protection Profile defines a different set of authentication modes, and whilst there is an overlap, it is not a complete match. Developers whose products implement modes which are not in the Protection Profile but which are in the Security Characteristic will therefore require additional testing beyond that performed by the Common Criteria evaluation. Details of this are given in the table below:

	Security Characteristic Authentication Mode		
PP Requirement	Simple Token	Smart Token	Assured TPM and PIN
FCS_CKM.1.1(2)	Must select "*passphrase*" AND "*external token*".	Must select "*external token*". The product must use the output from the Smart Token as the input to the XOR function (as described in the figure on page 14 of the Protection Profile) as if it were from an external token.	Must select "*external token*". The product must use the output from the TPM as the input to the XOR function (as described in the figure on page 14 of the Protection Profile) as if it were from an external token.
FMT_SMF.1.1(c)	The selections must include *"change passphrase-based authorisation factor"*.	No specific requirements.	
Additional requirements	Nothing additional required.	The passphrase or PIN must be cryptographically hashed by the product, prior to being passed to the Smart Token or TPM, as per DEV.2.M114. The Security Procedures for the product must note the importance of using an appropriately assured Smart Token or TPM, as per DEP.2.M117.	

If the product is able to use an un-assured TPM with the Simple or Smart Token variants, then this is acceptable. In this case, the TPM should be used as an 'additional factor' in the relevant points in the Protection Profile – such as in FCS_CKM.1.1(2).

Appendix C Glossary

The following definitions are used in this document.

Term	Definition
CC	Common Criteria
CPA	Commercial Product Assurance
DEK	Disk Encryption Key
DMA	Direct Memory Access
Entropy Source	As NIST SP800-90 [b]
GAP	Government Assurance Pack
KEK	Key Encryption Key
MBR	Master Boot Record
PRNG	As NIST SP800-90 [b]
Random Numbers	As NIST SP800-90 [b]
Security Characteristic	A standard which describes necessary mitigations which must be present in a completed product, its evaluation or usage, particular to a type of security product.
Security Strength	As NIST SP800-90 [b]
TPM	A Trusted Platform Module, as defined by the Trusted Computing Group.

Appendix D References

This document references the following resources.

Label	Title	Location	Notes
[a]	The Process for Performing Foundation Grade CPA Evaluations	www.cesg.gov.uk/servicecatalogue/CPA	
[b]	NIST Special Publication 800-90, Recommendation for Random Number Generation Using Deterministic Random Bit Generators	http://csrc.nist.gov/publications/PubsSPs.html	
[c]	Security IC Platform Protection Profile v1.0 (BSI-PP-0035)	www.commoncriteriaportal.org/pps	
[d]	HMG IA Standard No. 5 - Secure Sanitisation	CESG IA Policy Portfolio	April 2011 Issue No: 4.0
[e]	FIPS 197 – Advanced Encryption Standard (AES)	http://csrc.nist.gov/publications/PubsFIPS.html	2001
[f]	CESG Information Assurance Notice: UEFI BIOS Security Considerations	CESG IA Policy Portfolio	June 2011
[g]	CPA Security Characteristic for Enterprise Management of Data at Rest Encryption	www.cesg.gov.uk/servicecatalogue/CPA	
[h]	Protection Profile for Software Full Disk Encryption	www.niap-ccevs.org	Version 1.0, February 2013