CPA SECURITY CHARACTERISTIC

OVERWRITING TOOLS FOR MAGNETIC MEDIA

Version 2.2

About this document

This document describes the features, testing and deployment requirements necessary to meet CPA certification for overwriting tools for magnetic media 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: NCSC-1844117881-421

Version	Date	Description
1.6	May 2012	Published version
2.0	August 2014	GPMS classification change and SC Library related updates
2.1	December 2014	Minor updates following external review
2.2	October 2018	Amended to reflect formation of NCSC

This document is derived from the following SC Maps.

SC Map	Map version
Data Sanitisation - Overwriting Tools For Magnetic Media	2.1.2
Common Libraries	2.1.4

[1] https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa

Contact NCSC

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

For queries about this document please contact:

CPA Administration Team
NCSC, A2i,
Hubble Road
Cheltenham
Gloucestershire
GL51 0EX
United Kingdom

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

Contents

1.1 Introduction

This document is a CPA Security Characteristic. It describes requirements for assured overwriting tools for magnetic media products for evaluation and certification under NCSC's Commercial Product Assurance (CPA) scheme.

1.2 Product description

This Security Characteristic covers sanitisation of magnetic storage media such as hard disk drives by the method of overwriting. It does not apply to non-magnetic storage media.

Information Assurance Standard 5: Secure Sanitisation [b] is relevant to this Security Characteristic.

1.3 Typical use cases

Overwriting tools may be used with magnetic media to prepare it for re-use or storage. They may reduce handling requirements depending upon the level of overwrite applied.

Overwriting tools are not suitable in scenarios where storage media are damaged, or where regions cannot be accessed via standard interfaces. In these scenarios, an alternative sanitisation procedure such as degaussing or physical destruction may be necessary.

Refer to reference [b], Annex A for sanitisation procedures appropriate for the specific situation.

1.4 Expected operating environment

Overwriting tools for magnetic media may operate in any environment where they are needed to sanitise magnetic media. Any environmental requirements specified by the manufacturer must be adhered to.

1.5 Compatibility

The detailed test requirements in this specification have been written for ATA disks, SCSI and floppy disks. Software that is intended to process other types of disk must be subject to equivalent tests, i.e. with the appropriate disk types. The tester must document the tests performed and justify their equivalence to the requirements in this document.

1.6 Interoperability

Overwriting tools may be used in conjunction with any other sanitisation utility or process approved for use with magnetic media, provided use in this way represents an approved sanitisation procedure as detailed in reference [b], Annex A.

1.7 Additional information

Information Assurance Standard 5: Secure Sanitisation [b] is relevant to this Security Characteristic.

This Security Characteristic refers to terminology defined in reference [b]. This terminology describes attack types that different sanitisation procedures are expected to mitigate, such as 'non-invasive attack'.

Future issues or versions of tested secure overwriting products, which meet the requirements of the test specification, will remain as approved products. However, if the software has been significantly rewritten, with changes to the addressing format, device type, disk type or disk format as shown in Table 1, it will be necessary to retest the product.

A pass for one type of disk, interface, or addressing method will not necessarily translate as a pass for another type, see table 1. For example, for a product to be certified for use with both hard disks and floppy disks, it must be tested with both.

Pass as listed in this column	**Does not count as pass in this column**
CHS addressing	LBA, BIOS
LBA28/LBA48 addressing	CHS addressing, BIOS
BIOS addressing	CHS addressing, LBA28/LBA48 addressing
LBA 28-bit addressing	LBA 48-bit addressing
SCSI device	Other disk types
ATA device	Other disk types
Hard disk	Floppy disk
Floppy disk	Hard disk
Single disk formats, e.g. FAT12, FAT16, FAT32, HFS, HFS+, HPFS, NTFS, Ext	Any other disk format

Table 1: Prohibited Extensions

A pass under one method of addressing an IDE disk must count as a pass for downwards-compatible method of addressing a disk. Table 2 gives some examples of permitted extensions.

Pass as listed in this column	**Count as pass in this column**
Tested in PIO modes 0 to 4	Pass in PIO modes 0 to 4
Tested with or without DMA/UDMA	Pass with or without DMA/UDMA

Table 2: Permitted Extensions

1.8 High level functional components

This security characteristic does not use high level functional components.

1.9 Future enhancements

Overwriting tools may also exist as an integrated function of a storage medium. NCSC may update this Security Characteristic to incorporate this option.

NCSC welcomes feedback and suggestions on possible enhancements to this Security Characteristic.

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.

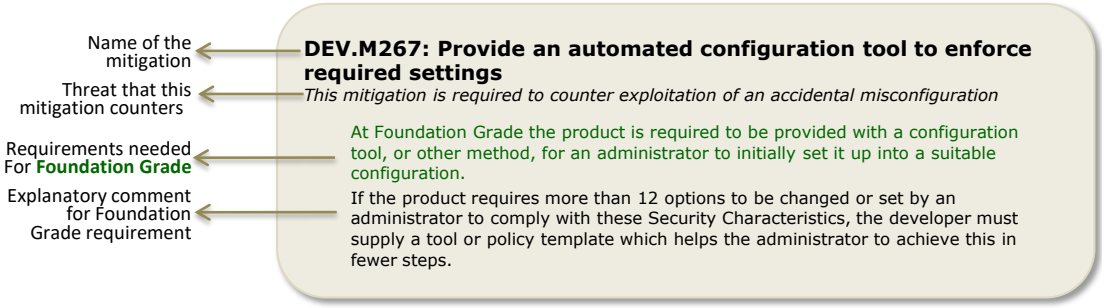

Figure 1: Components of a typical mitigation

This section lists the Development, Verification and Deployment mitigations for the overwriting tools for magnetic media Security Characteristic. For a summary of the changed mitigations in this version, please refer to Appendix A.

3.1 Development mitigations

DEV.M355: Secure software delivery

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.M557: Overwrite the media

This mitigation is required to counter an attacker replacing components damaged by rudimentary destructive techniques
This mitigation is required to counter mounting drive in general purpose PC to read content
This mitigation is required to counter reading data using readily available recovery tools
This mitigation is required to counter reading data using specialist lab tools

At Foundation Grade the product **is required to** perform three overwrites to all addressable areas.

The product must perform three separate overwrites to all addressable areas. The overwriting sequence must be as specified. The first overwrite should be a single binary value of 8 bits, followed by a second overwrite using the complement of this value. The third overwrite should consist of a random stream of bits, however it is permissible for the third overwrite to use a single random binary value of 8 bits. Where a random 8-bit value is used, it must not be the same as that used for either the first or second overwrites. Each of the three overwrite values must be written to all addressable areas.

DEV.M562: Overwrite all areas of the media

This mitigation is required to counter exploiting a failed or partial sanitisation

At Foundation Grade the product **is required to** accurately report disk capacity.

The product must report the actual disk capacity to be overwritten.

At Foundation Grade the product **is required to** accurately verify the success of the overwrite.

Verification of successful secure sanitisation must be carried out for all overwriting instances.

The product must generate a report that declares the number of user addressable areas that have been overwritten and the number that have not been overwritten.

The product must report any bad or unusable sectors that cannot be overwritten.

3.2 Verification mitigations

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.M556: Confirm overwrite is effective

This mitigation is required to counter an attacker replacing components damaged by rudimentary destructive techniques
This mitigation is required to counter mounting drive in general purpose PC to read content
This mitigation is required to counter reading data using readily available recovery tools
This mitigation is required to counter reading data using specialist lab tools

At Foundation Grade the evaluator **will** confirm that software recovery tools are rendered ineffective.

This is a multi-stage process with two main parts:

1. Prepare for verification by setting up lab environment as per the requirements in Appendix D (Initial Test Requirements).

2. Verify the correct operation of the software using the procedures defined in Appendix E (Verification of the Software under Test).

VER.M558: Representative test media

This mitigation is required to counter exploiting a failed or partial sanitisation

At Foundation Grade the evaluator **will** test the product using an adequate range of storage media.

At a minimum, the tester must verify the product using known-good disks, disks with one or more unusable or bad sectors (where available), and disks supporting the HPA and DCO feature sets.

VER.M563: Confirm accurate reporting of the sanitisation outcome

This mitigation is required to counter exploiting a failed or partial sanitisation

At Foundation Grade the evaluator **will** confirm that the software generates a report indicating success or failure.

The evaluator must check that the software generates a report that all addressable areas have been overwritten. The tester must also check that, for disks with bad or unusable sectors, a report is generated that shows at a minimum the number of bad or unusable areas that could not be overwritten.

The evaluator must document the results obtained.

At Foundation Grade the evaluator **will** verify that additional feature sets are supported.

The product must continue to operate successfully where feature sets such as the Host Protected Area (HPA) and the Device Configuration Overlay (DCO) are present.

3.3 Deployment mitigations

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 by the operating system for applications, services and drivers, where supported and where the product makes use of it.

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.M553: Physically protect media

This mitigation is required to counter intercepting media in transit

This mitigation is required to counter stealing media from storage

At Foundation Grade the deployment **is required to** protect media according to IS5 requirements.

Users should ensure that storage and handling aspects of the requirements in IS5 [b], in particular those outlined in Annex A, are observed for the media type. Users may request sanitisation guidance and/or a copy of IS5 from the NCSC enquiries desk.

DEP.M560: Maintain integrity of the product

This mitigation is required to counter exploiting a failed or partial sanitisation

At Foundation Grade the deployment **is required to** obtain and use the product in a trusted manner.

The user of the product must be required to boot up the computer in such a way that the risk of malicious code executing is mitigated. The acceptable ways of performing this are booting up the computer from known-good media or in circumstances where the system to be overwritten is to be booted from a network source, a trusted and dedicated LAN and boot server must be used.

DEP.M561: Confirm that sanitisation has been successful

This mitigation is required to counter exploiting a failed or partial sanitisation

At Foundation Grade the deployment **is required to** ensure users are aware of their obligations.

The user must ascertain the actual disk capacity by two or more of the methods listed in Appendix F. Any discrepancies in the actual disk capacity must be explained and the addressing method that gives the highest capacity must be used to wipe the disk. The user must be required to ensure that the disk capacity reported by the operating system is commensurate with the actual disk capacity. If the operating system does not report the actual disk capacity, the documentation must explain how to relate the actual disk capacity to the reported capacity. The user must select the correct overwriting procedure.

The user must ensure that the overwrite process completes. The user must inspect and act as per IS5 [b] upon the generated report to assess sanitisation success or failure.

Appendix A Summary of changes to mitigations

NCSC has updated the Overwriting Tools for Magnetic Media Security Characteristic v2.1 (previously version 1.6) for the following reasons.

- GPMS classification change.
- Removal of augmented requirements.

This has resulted in the following changes to mitigations.

A.1 Removed mitigations

(No mitigations have been removed.)

A.2 Modified mitigations

The following mitigations have been modified.

- DEV.M22: Update Signing (title also changed to "DEV.M355: Secure Software Delivery")
- DEV.M557: Overwrite the media
- VER.M556: Confirm overwrite is effective
- VER.M558: Representative test media
- DEP.M553: Physically protect media

A.3 Renamed mitigations

No mitigations have been renamed (except those that have been modified as well – see above).

A.4 New mitigations

The following mitigations have been added.

- DEP.M131: Operating system verifies signatures

Appendix B References

This document references the following resources.

Label	Title	Location	Notes
[a]	The Process for Performing Foundation Grade CPA Evaluations	https://www.ncsc.gov.uk/scheme/commercial-product-assurance-cpa	
[b]	Information Assurance Standard 5 'Secure Sanitisation'	NCSC IA Policy Portfolio	v.5.0 April 2014

Appendix C Glossary

The following definitions are used in this document.

Term	Definition
CPA	Commercial Product Assurance. A scheme run by NCSC providing certificate-based assurance of commercial security products.
SC Map	Diagrammatic representation of a Security Characteristic (or part of one).
Security Characteristic	A standard which describes necessary mitigations which must be present in a completed product, its evaluation or usage, particular to a type of security product.
ATA	Advanced Technology Attachment
BIOS	Basic Input/Output System
CD-ROM	Compact Disk Read Only Memory
CHS	Cylinder-head-sector
DCO	Device Configuration Overlay
DMA	Direct Memory Access
FAT	File Allocation Table
HPA	Host Protected Area
HPFS	High Performance File System
HFS	Hierarchical File System
HFS+	Hierarchical File System Plus
IDE	Integrated Drive Electronics
LAN	Local Area Network
LBA	Logical Block Addressing
NTFS	New Technology File System
PATA	Parallel ATA
PIO	Programmed Input/Output
SATA	Serial ATA
SCSI	Small Computer System Interface
UDMA	Ultra DMA

Appendix D Initial Test Requirements

1. If the erasure of a hard disk is being verified, the tester must document the configuration of the disk access methods (e.g. LBA) in the computer used to perform the tests in the evaluation report.
2. The tester must configure the BIOS of the computer so that the boot sector of the hard disk is write-protected. The tester must check that the software-under-test reports an error or that the boot sector is overwritten as required.
3. The computer used for the test must be booted up in a trustworthy manner in accordance with the user instructions.
4. If the instructions on how to perform a trusted boot permit more than one method, the organisation performing the tests must document the method used to ensure that the computer boot was trustworthy,
5. The tester must carry out tests for all of:
   - A fully functional disk configured to have one single logical partition;
   - A fully functional disk configured to have multiple logical partitions;
   - A disk with known unusable or bad sectors;
   - A disk supporting the HPA feature set;
   - A disk supporting the DCO feature set.
6. The actual size and configuration of the disks used for testing must be ascertained to ensure that the testers know the real values. These values and the method used to determine them must be documented in the test results. Acceptable methods are shown in Appendix D.
7. The tester must fill the disk with known data until the disk is full. The known data must be different from that used by the overwriting process being tested.
8. If the disk used has a write-protect option that prevents software writing to it, the disk must be write-protected. The tester must start the software and check that errors are reported.

Appendix E Verification of the Software under Test

1. The tester must start the software-under-test as specified in the user documentation. Whilst the software is approximately in the middle of performing the first cycle of overwriting, the tester must switch off the computer. The tester must then perform a reboot of the computer in such a way that malicious code cannot be executed, and verify that at least 257 sectors on the disk have been overwritten by the same octet.
2. The tester must either restore the original contents from a backup or refill the disk with the same known data until the disk is full. The tester must restart the software under test. Whilst the software is approximately in the middle of performing the second phase of overwriting, the tester must switch off the computer. The tester must then perform a reboot of the computer in such a way that malicious code cannot be executed, and verify that at least 257 sectors on the disk have been overwritten by the complement of the octet written to the disk in first pass of the software.
3. The tester must then either restore the original contents from a backup or refill the disk with the same known data until the disk is full. The tester must restart the software under test and allow it to run to completion, as specified in the user documentation.
4. The tester must check that the software generates a report that all addressable areas have been overwritten.
5. For tests 4 and 6 in Table 3 (below), the tester must document the block numbers tested.
6. The tester must verify that the same octet, or seemingly random pattern (depending on the write) has been written to all sectors of the disk listed in Table 3 unless the disk has less than 3074 sectors in which case all the sectors must be examined. No mathematical tests are required of randomness. It is sufficient to make a reasonable visual inspection that no pattern is apparent.
7. For a disk with known bad or unusable sectors, the tester must check that a report is generated that shows, as a minimum, the number of bad or unusable areas that could not be overwritten. The tester must document the results obtained.
8. If the hard disk supports the Host Protected Area (HPA) feature set, the disk must be configured with an HPA that starts at least 1025 sectors before the last sector on the disk. The software-under-test must be run to completion and verify that at least the last 1025 sectors of the disk have been overwritten. The tester must document results obtained.
9. If the hard disk supports the Device Configuration Overlay (DCO) feature set, the disk must be configured with a DCO that starts at least 1025 sectors before the last sector on the disk. The software-under-test must be run to completion and verify that at least the last 1025 sectors of the disk have been overwritten. The tester must document the results obtained.

	Minimum physical sectors on disk to be checked
1	First 2049 sectors of the disk.
2	129 sectors before and after the middle of the disk, including the middle sector.
3	Last 1025 sectors of the disk.
4	10 separate sectors chosen by the tester at random in the remaining area of the disk.
5	If the disk has over 268,435,456 sectors (28-bit LBA limit) then sectors 268,435,327 to 268,435,585 sectors of the disk.
6	If the disk has over 4,294,967,296 sectors (32-bit LBA limit) then sectors 4,294,967,167 to 4,294,967,425 sectors of the disk.
7	Sectors that the tester believes should be tested, if any.

Table 3: List of Sectors to be Verified

Appendix F Methods of Ascertaining Actual Disk Capacity

1. From the disk manufacturers disk specification;
2. If it is an IDE/ATA drive, issuing the ATA command IDENTIFY DEVICE and the following if supported by the device from trusted software:
   - DEVICE CONFIGURATION IDENTIFY if a DCO feature set is supported;
   - READ NATIVE MAXIMUM ADDRESS is a HPA feature set is supported from trusted software;
   - NATIVE MAX ADDRESS EXT if a Host Protected Area feature set and 48-bit Address feature sets are supported;
3. If it is a SCSI disk, issue a SCSI Identify command and SCSI Read Capacity command from trusted software;
4. If using a floppy disk, by visual inspection of the label or high density marker;
5. By using an auto-configure BIOS option, provided that the user is sure that the computer can handle disks of that capacity and configuration. For example, a BIOS that uses CHS addressing cannot be used to wipe disks that exceed the CHS limits