



BSI - Guideline

Name:	Requirements to overwrite memory media
Application:	Requirements for manufactures Hard drives with magnetic media
Identification:	BSI - TL 03423
Version:	0.9b/engl.
Published:	March 2010

Bundesamt für Sicherheit in der Informationstechnik

Postfach 20 03 63

53133 Bonn

Tel.: +49 (0) 22899 9582 5321

E-Mail: Referat225@bsi.bund.de

Internet: <https://www.bsi.bund.de>

© Bundesamt für Sicherheit in der Informationstechnik 2010

Contents

1	Generell	4
1.1	Requirements	4
2	Overwriting methods	4
2.1	Method similar to VSITR for magnetic storage media	4
2.2	Method BSI-2009	5
2.3	user selectable overwriting methods	6
3	Requirements for identification	7
4	Protocol/Report Requirements	7
5	Work flow Management Requirements	8
6	Requirements to the manual	8

1 Generell

This requirements specified within the guideline should be used by manufacturers and developers of software and equipment for the overwriting of hard disk drives with magnetic media.

This guideline will supersede all previous requirements which have been provided for the overwriting of hard drives with magnetic media.

Currently this guideline will cover only hard drive with magnetic media. Information an other media such as hybrid disk, SSD or Flashmemorysticks will be given in future.

1.1 Requirements

The specifications herein define the needs for software for the complete overwriting of magnetic hard drives and cover requirements on:

- overwriting methods
- recognition (hard drive parameters)
- overwriting procedures (details on algorithms)
- reporting (display and printing of information)
- work flow management
- manual

2 Overwriting methods

There should be two different overwriting methods. The implementation of method 2.1 is not needed in every case. The method BSI-2009 will only be used for HDDs bigger than 20 GByte.

2.1 Method similar to VSITR for magnetic storage media

There will be 8 steps in total, which has to be worked through in chronological order:

1. Overwriting the whole medium with the pattern “FF” (hex)
2. Overwriting the whole medium with the pattern “00” (hex)
With a *one-to-one identifier* of every sector for the following verification.
It is sufficient to save the sector number (*i.e.LBA*) in every sector
3. Verification of the whole medium
4. Overwriting the whole medium with the pattern “FF” (hex),
with inverted *identifier* of Step 2 (one's-complement)
5. Overwriting the whole medium with the pattern “00” (hex)
6. Overwriting the whole medium with the pattern “FF” (hex)
7. Overwriting the whole medium with the pattern “00” (hex)
8. Overwriting the whole medium with the pattern “AA” (hex)

2.2 Method BSI-2009

Here we will have 4 steps to go through in total and in chronological order. Those 4 steps consists of 1 time overwriting, complete verification followed again by an overwriting but with a different overwriting pattern and a sample verification.

1.Step

Overwriting the whole HDD with a „premium“ Random pattern:

- a) The application takes the number of hits by the user on the keyboard or mouse movements and calculates a 128/160 bit block K with a entropy of minimum 100 Bit out of system time, key values, mouse position and time differences. During the erasure process K should be kept in the RAM and shall not be saved on the HDD until he finally in step f) is overwritten in the RAM
/dev/random may be used to generate this bit block K.
- b) Generation the data pattern the following options are given based on Federal Information Processing Standards (<http://www.itl.nist.gov/fipspubs/by-num.htm>):
(optional, depending on prior consultation with the BSI, you may use another block encryption algorithm)

Possibility 1: with the block encryption algorithm AES-128 (to be seen in FIPS 197)

The 128-bit block K from a) is used as a AES-key for the creation of 128 bit blocks in the OFB-Modus. It will be calculated a sequence b_1, b_2, \dots of 128 bit blocks recursive with:

$$b_1 = \text{AES}_K(0) \text{ and } b_{n+1} = \text{AES}_K(b_n)$$

0 designates a 128 bit block which composed of 128 zero-bits

Possibility 2: with a hash function SHA-1 (to be seen in FIPS 180-3):

Out of the 160 bit block K from a) we calculate a sequence b_1, b_2, \dots of 160 bit blocks recursive through:

$$b_1 = \text{SHA}(K) \text{ and } b_{n+1} = \text{SHA}(b_n \text{ XOR } K)$$

XOR designates a *bitwise exclusive OR* of two 160 bit blocks

- c) The HDD is overwritten with blocks b_1, b_2, \dots . Every block will only be used one time for overwriting (Overwriting a HDD with m byte, m/16 blocks for AES or m/10 for SHA-1 have to be calculated)

$$b_1 = \text{AES}_K(0) \text{ and } b_{n+1} = \text{AES}_K(b_n)$$

$$b_1 = \text{SHA}(K) \text{ and } b_{n+1} = \text{SHA}(b_n \text{ XOR } K)$$

The blocks b_1, b_2, \dots, b_n may be combined and bufferd before writing to the media.

2. Step

Verification over the whole HDD:

- d) The blocks will be calculated again
- e) The content of the HDD will be read-out again (every sector has to be identified by unique) and compared with the calculated blocks
- f) The 128 Bit block K inside the RAM will be erased, overwritten completely with "00h".

The number of incorrect read sectors / blocks will be documented by the application.

3. Step

Method 3a or 3b shall be used

1. if the „Enhanced Secure Erase“-procedure of the ATA-specification has been identified. It should be started
2. alternatively the HDD can be overwritten with Zeros

A first boot sector „Master Boot Record (MBR)“, which is overwritten with zeros makes it easier to reuse the HDD.

4. Step

- it follows a sample verification of some sectors to proof the success of step 3 . As a minimum we should check the first (MBR), some middle and some of the last sectors. We have to proof that they are overwritten with the pattern in step 3.
When using "Enhanced Secure Erase" a sector may be read from the disk as a reference to be used to compare the other sectors.
- The user has to be able to choose the number of the total checked sectors via the user interface. The selection should be done as an absolute specification. The smallest number of sectors to be proofed should not be lower than 10000.
*The verified sectors should be evenly distributed all over the disk.
Software manufacturer specific verification methods may be used upon approval by the BSI.*

The number of faulty read sectors/blocks has to be documented/reported by the application.

2.3 user selectable overwriting methods

The following overwriting methods had to be allocated:

1. Method according to VSITR (optional), which is defined in section 2.1
2. Method BSI-2009 step 1. To 4.; name: BSI-2009-VS, as in section 2.2
3. Method BSI-2009 step 3. To 4.; name: BSI-2009, part of section 2.2

The methods have to be implemented in a way that the memory medium will be overwritten complete.

3 Requirements for identification

It is needed that minimum the following characters will be detected (and if existing it should be shown):

- Interface of the HDD (IDE/ATA, SATA, SCSI, USB, fire wire etc.)
- Whole capacity of the HDD(s), number of sectors
- HDD-identification (type, manufacturer, ID, serial number)
- If partitioning will be shown the type and name of the partition has to be shown
- Blocked areas (HPA, DCO etc.) had to be detected and had to be unlocked for the erasing process. If these areas cannot be overwritten at PCs which are depending on it, the feature can be optional switched off.(User selectable feature)
- If distinguishable: Solid State Disk (SSD), Hybrid-HDD or FLASH memory stick
- Count of the bad remapped sectors (reallocated block counter, supported ATA-version)

- (S-)ATA- HDD: (enhanced) Secure erase2 –function based on (S-)ATA-specification

4 Protocol/Report Requirements

Following data had to be recorded (shown in the protocol):

- All HDD parameters (interface, type, manufacturer, ID, serial number)
- In a particular case at RAID systems additional: type of the RAID, number of HDD, capacity, access method
- The chosen erase options
- The performed steps (only if there has been a failure in performing the complete selected option) respectively the used erase option
- Number of erased sectors respectively erased capacity
- Particularly reporting of appeared errors, e.g. at writing phase, verification phase etc.
- Information about HPA, DCO and the number of “reallocated sectors”. HPA and DCO – as well if they are detected and erased
- The reporting can be done in a electronic way; but protocol/hard copy have to be created independent from a manufacturers format

5 Work flow Management Requirements

The following requirements are valid

- A reduced operating system had to be used, that is applied on a tamper proofed medium (e.g. CD-ROM)
- The needed programs had to be on the boot medium
- The boot media had to be booted and the erasure process had to be started in this environment
- There had to be arrangements to check the integrity of the CD/program

Optional for RAID-systems

- RAID-system in general had to be dismantled

6 Requirements to the manual

The manual has to be in German language

It shall include:

- There have to be arrangements to check the integrity of the CD/program by the user
- Complete instructions (how to use)
- Description of the erasure methods
- Details of the range of use (IDE, SATA, USB, magnetic media, SSD, Flash, ...)
- details on user information in case of error messages with comments
- Details of usage limitation due to hard- and firmware on which the product is be used (Chipset, BIOS, driver, RAID, bad or defective hardware, not connected cables etc.)
- Description of the (possible) content of the protocol/report
- Details of needed qualifications of the operator (normal PC-user, IT-Professionals), that the program can be used problem less and in a proper way.