

11.10.10

Amended 12.11.10/ 13.6.11

**Encryption and Erasure Products
NOTE FOR PANEL COUNSEL**

Introduction

This note provides guidance in relation to the selection of encryption and erasure products to protect information with a protective marking up to and including RESTRICTED and provides a list of products for you to consider.

Background

Guidelines agreed with the Bar Council on information security and government work state that whole disk encryption must be applied to removable devices or removable storage media and laptop computers. The level of encryption must meet the minimum standards sets out below.

A. Encryption

Encryption is used to protect data such as files on computers and storage devices (e.g. USB drives). Encrypting files helps protect them should physical security measures fail and is also used to protect data in transit, for example data being transferred via networks (e.g. over the Internet).

FIPS140-2 is a US government computer security standard and encryption of USB drives and laptops on which data will be stored should be to at least the FIPS140-2 or CCTM (CESG Claims Tested Mark) standard unless there has been specific agreement to the contrary.

FIPS 140 -2 validation only applies to the specific product on the FIPS 140 -2 validation list. It should not be assumed that the listing of a particular version of a product gives any indication of the assurance of any other version of the product or of other products from the same vendor.

If you choose a software based solution, you should ensure that the underlying IT systems operating system is modern, that the solution is fully supported on that operating system, and that it is patched/updated on a regular basis. The assessment of a FIPS 140 -2 product does not need to be complex. Internet-based open source research using mainstream search engines, coupled with an assessment of information from the vendor's website, user manuals and administration manuals for the product will provide you with an adequate understanding of the likely residual risk.

When considering which FIPS 140 -2 product to use, you should check to verify the following:

1) That the vendor is committed to the ongoing development of the product.

Evidence to verify this might include:

- a. observing when the last update to the product occurred; and
- b. that the current version (or a very recent generation) is approved on the FIPS 140 -2 validation list.

2) That the vendor is committed to patch vulnerabilities and other issues

Evidence to verify this might include:

- a. the developer responding to public vulnerability disclosures;
- b. a publicised way of researchers reporting vulnerabilities directly; and
- c. the developer responding to a vulnerability disclosure in a meaningful way (e.g. by issuing a patch).

Encryption Products

You may find the following list of FIPS 140 -2 products of assistance. This list is not exhaustive but provides a number of suitable products for consideration:

Vendor/ Product	Operating System
BeCrypt <ul style="list-style-type: none"> • DISK Protect (Baseline) 	Windows 2000 Windows XP
GuardianEdge <ul style="list-style-type: none"> • Hard Disk encryption 	Windows 2000 Windows XP Windows Vista Enterprise
McAfee <ul style="list-style-type: none"> • Endpoint Encryption 	Windows 2000 Windows XP Windows Vista
Novell ZENworks <ul style="list-style-type: none"> • Endpoint Security Management 	Windows 2000 Windows XP Windows Vista
PGP <ul style="list-style-type: none"> • Whole Disk Encryption 	Microsoft Vista Microsoft Windows XP Professional Microsoft Windows XP Home Microsoft Windows 2000 Mac OS X (including Boot Camp)
Sophos (Utimaco) <ul style="list-style-type: none"> • SafeGuard Private Disk 	Windows 2000 Windows XP Windows Vista
Stonewood Group <ul style="list-style-type: none"> • Eclipt Baseline • FlagStone Baseline 	Windows 2000 Windows XP
Check Point End Point Security <ul style="list-style-type: none"> • Check Point Full Disk Encryption 	Microsoft Windows XP Professional Microsoft Windows 2000 Mac OS X 10.6 (Snow Leopard)
WINMAGIC <ul style="list-style-type: none"> • Secure Doc Disk Encryption 	Microsoft Windows XP Professional Microsoft Windows 2000 Microsoft Windows 7 Mac OS X 10.6 (Snow Leopard)

These products are all available directly from the relevant supplier. Additionally, Windows 7/ Vista Enterprise Bitlocker is an acceptable product (provided the correct configuration is used).

Further information and more products on the FIPS140-2 list can be found at the following website <http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2009.htm>.

Use of TrueCrypt not compliant

The TrueCrypt Encryption application has been examined by the TSol Security Team, this involved compliance checks against the FIPS 140 part 2 standard. The conclusion of these checks indicated that while a component (XTS-AES module) of the True Crypt application has been certified to the FIPS 140 standard, the application as a whole has not and does not feature on the CESG list of approved whole disk encryption products. Checks confirm that TrueCrypt, fitted with the XTS-AES module has not been tested by FIPS 140 standard's authority and therefore cannot be listed as an approved product.

TSol will continue to follow the progress of TrueCrypt, but at this stage, cannot approve its use on laptops to protect TSol information.

B. Deletion

When information is deleted from computer systems, it is not removed completely but simply removed from the index that tells the computer where to find the information. Until the space that the electronic records sit in is used for something else, the information still exists, and is relatively easy to retrieve. It is therefore important to ensure that a secure method of deletion is used when protectively marked material is removed.

To permanently remove information from a computer, the file must be overwritten with random data, multiple times. This is often referred to as secure deletion or shredding files. Only formal secure deletion processes are acceptable by HMG departments if protectively marked material is removed and the media (computer hard disks) will be reused.

Many secure deletion tools exist and a list of these products can be found on the CESG (HMG) website at http://www.cesg.gov.uk/find_a/cert_products/index.cfm. Some secure deletion tools are FIPS compliant and are free. An example is Eraser - <http://eraser.heidi.ie/> - this is very easy to use for windows systems and is quick and simple to apply. Alternatively, a suite of free tools is available for use on a trial basis from PGP at <http://www.pgp.com/downloads/desktoptrial/desktoptrial2.html>. These include encryption, zip and shredding tools and are approved by CESG and FIPS140-2.

Please note that for any protectively marked data, the full disk must be erased using a product from the CESG Approved list referred to above. Of course, remember that you can always take a hammer to the disk or hard drive as an alternative.

For Civil Panel Counsel TSol's security team can provide further advice if required when deleting protectively marked material from systems, you can contact them at security@tsol.gsi.gov.uk.

TSol Security Team
11.10.10
Amended 12.11.10