



Future Technology Industry Limited

IA Claims Document (ICD) Hard Disk Magnetic Crusher Model: Combo

CCT Mark Certificate Number: 2007 06 0022
Date CCT Mark Awarded: 13 June 2007
CCT Mark Award expires on: 12 June 2009
ICD Issue Date: 13 June 2007

Vendor Address:

Future Technology Industry Limited
Asmec Centre
The Ring
Bracknell, Berks. RG12 1HB

Telephone Number: 01344 382 100

Vendor Website: www.futuretechnologyindustry.com

Vendor Email: info@futuretechnologyindustry.com

Table of Contents

1.	Introduction	3
1.1	Background	3
1.2	Objectives	3
1.3	Purpose of Document	3
1.4	Structure	3
2.	Product Description	4
2.1	Product identification	4
2.2	Product Overview	4
2.2.1	Security architecture	4
2.2.2	Hardware requirements	4
2.2.3	Software requirements	4
2.2.4	Out of Scope	4
2.3	Usage assumptions	5
2.3.1	Assets	5
2.3.2	Threat scenario	5
3.	Security Claims for the IA Product	7
3.1	Claims Statements	7
3.2	Existing Assurance Certificates	7

1. Introduction

1.1 Background

This document outlines the IA claims made by Future Technology Industry Limited in regard to the suitability of **Hard Disk Magnetic Crusher Combo** for use by the UK Public Sector and other users for ensuring data has been securely destroyed on magnetic media that is no longer required.

There is a growing need for assured destruction of data held on magnetic media. The widespread use of computers for even routine tasks has left many groups, agencies and organisations with large volumes of data stored on magnetic media such as data tapes and hard disk drives. When the computers have reached the end of their useful life and the magnetic storage media is no longer required, a method of secure disposal is required. This product is intended to satisfy part of that secure disposal requirement.

The most widely recognised form of data destruction uses a magnetic field of sufficient strength to align all magnetic domains to a direction where no data can be read. It is recognised that deletion, including reformatting, may not be sufficient to remove all traces of data. The process of degaussing using the product described herein will remove data on media with coercivities up to the values present in the media used in the tests. The product will in addition, physically destroy the media by pushing four spikes through the media.

1.2 Objectives

The objectives of this ICD are to provide the IA claims for **Hard Disk Magnetic Crusher Combo**.

1.3 Purpose of Document

This document is the ICD for **Hard Disk Magnetic Crusher Combo**.

1.4 Structure

The structure of this ICD is as follows:

- Section 1 (this section) contains introductory material;
- Section 2 contains the description of functionality of **Hard Disk Magnetic Crusher Combo**;
- Section 3 details the security functionality claims that are being made.

2. Product Description

2.1 Product identification

Product name: **Hard Disk Magnetic Crusher.**

Model: **Combo**

2.2 Product Overview

The product is currently intended for destruction of data protectively marked at RESTRICTED or below. The use of this product to declassify media carrying a higher protective marking, such as CONFIDENTIAL and above, is beyond the scope of this Claims Tested Mark scheme.

2.2.1 Security architecture

Not applicable

2.2.2 Hardware requirements

The product is hardware and requires no additional hardware.

2.2.3 Software requirements

Not applicable.

2.2.4 Out of Scope

Media packaged with magnetic shielding, specifically designed to prevent intrusion of external magnetic fields, is excluded from the scope of testing. This exclusion refers to highly specialised media such as might be used in space applications, military (particularly radiation hardened materials) and nuclear facilities. This material will be readily identified as such and unless so identified on the casing, should be considered in scope with regard to this testing.

Media known as Magneto-Optical Disks are excluded from the scope of testing.

The COMBO has four modes of operation available to the user. These are:

Auto	This is the most complete mode and delivers two sequential degaussing steps, a crush step and a third degaussing step.	In scope
Erase	This mode delivers two sequential degaussing steps.	In scope

Crush	This mode involves no degaussing step, but instead drives four metal spikes through the drive casing and disks.	In scope
Hi	This mode delivers a single degaussing step.	In scope

2.3 Usage assumptions

2.3.1 Assets

Media covered generally includes storage devices wherein data is stored in magnetic domains with magnetic field intensity up to the most recent high-coercivity devices commercially available at the time of testing (February 2007). Examples of media covered includes: Hard disk drives; LTO data tapes; floppy disks; Iomega Zip media.

2.3.1.1 Hard disk drives

This includes all drives manufactured prior to the date of manufacture of the disks used in the tests (January, 2007). These are, typically, up to 4000 Oersted coercivity.

2.3.1.2 Data tapes

This includes all tapes manufactured prior to the date of manufacture of the tapes used in the tests (January, 2007). These are, typically, up to 2700 Oersted coercivity.

2.3.1.3 Other media

Other media may be erased, up to the coercivity of the media used in the tests, where the coercivity of the media to be erased and the test media is known. For example, floppy disks, Iomega media and SDLT tapes have a significantly lower coercivity rating than the 2700 Oersted expected from LTO tapes used in the tests and may therefore be considered as covered by the scope of the testing. As stated in 2.2.4 above, Magneto-Optical Disks are not covered.

2.3.2 Threat scenario

Threats to assets which are countered are:

- Theft of stored personal data
- Theft of stored operational data
- Theft of stored client/customer/user data

2.3.2.1 Expected operational environment

The expected operational environment is the premises of the product owner and may be an office or IT facility. Other environments are possible provided the necessary services (mains power) are available. It is important that people with cardiac pacemakers are not in the vicinity when the system is in use.

2.3.2.2 Organisational security policies

The product helps customers to comply with security policies related to ISO 17799:2005 controls, Section 15.1.4, Data protection and privacy of personal information. In addition, users will be able to comply with NHS SyOp 7.13 BS7799 Data Protection Act and generally provide protection against identity and data theft

2.3.2.3 Security requirements on the environment

It is incumbent on the user to provide a system to ensure that the equipment is used correctly and with sufficient safeguards to prevent deliberate or accidental misuse. For example, a system will be required to ensure that media to be degaussed is processed and can be proven so.

3. Security Claims for the IA Product

3.1 Claims Statements

1	Magnetic media will have its data destroyed to the extent that there is no possibility that the original data may be read over the device interface or by playback in a reading device.
2	The product erases data (with a protective marking of RESTRICTED or below) from magnetic storage media in compliance with the CESG Lower Level Degaussing Standard.

3.2 Existing Assurance Certificates

CESG confirm that the testing will test the product for compliance with the CESG lower level degaussing standard (Amendments to HMG Infosec Standard 5, and CESG Infosec Manual S, Version 1.0, April 2007).

Annex A

Glossary of terms

Term	Meaning
CESG	Communications Electronics Security Group
ICD	Information Assurance Claims Document
LTO	Linear tape open (magnetic tape media)
SDLT	Super Digital Linear Tape

Annex B

Marketing statement

The consequences of your data being made public are embarrassment, financial loss and reputational loss. To mitigate data theft from discarded computer hard drives and other magnetic recording media, you should destroy the data at source. The Combo's dual function will magnetically degauss and physically destroy the magnetic media to clear all data before disposal. When you need a robust security policy, you need a robust end-of-life data destruction process.