



CCT MARK IA CLAIMS DOCUMENT (ICD)

Ultratec Limited

Secure Destruction of Data on Magnetic Media
Version 1.0

VENDOR DETAILS	
Ultratec Limited	
Ultratec House, 11-12 London Road, Baldock, Herts. SG7 6NG	
Telephone Number:	+44 (0) 1492 490082
Vendor Website:	www.ultratec.co.uk
Vendor Contact Email:	Bill.Osbourne@Ultratec.co.uk

CERTIFICATE DETAILS	
CCT Mark Certificate Number	2007/09/026
CCT Mark Awarded on:	14 September 2007
CCT Mark Award Expires on	13 September 2008
ICD Issue Date	14 September 2007

Table of Contents

1.	Introduction	3
1.1	Background	3
1.2	Objectives	3
1.3	Purpose of Document	3
1.4	Structure	3
1.5	References	4
2.	Service Description	5
2.1	Service identification	5
2.2	Service Overview	5
2.2.1	Security architecture	5
2.2.2	Hardware requirements	5
2.2.3	Software requirements	5
2.2.4	Out of Scope	5
2.3	Usage assumptions	5
2.3.1	Assets	5
2.3.2	Threat scenario	6
3.	Security Claims for the IA Service	8
3.1	Claims Statements	8
3.2	Existing Assurance Certificates	9

1. Introduction

1.1 Background

This document outlines the IA claims made by Ultratec Limited in regard to the suitability of *Secure Destruction of data on Magnetic Media* 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 service 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 service described herein will remove data on media with coercivities up to the values present in the media used in the tests.

1.2 Objectives

The objectives of this document are to enable testing and certification under the CCT mark scheme.

1.3 Purpose of Document

The purpose of this document is to define the Information Assurance claims for the defined service.

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 *Secure Destruction of Data on Magnetic Media* and all the information related to the security of *Secure Destruction of Data on Magnetic Media*;
- Section 3 details the security functionality claims that are being made.

1.5 References

[CESG] CESG lower level degaussing standard (Amendments to HMG Infosec Standard 5, and CESG Infosec Manual S, Version 1.0, April 2007).

2. Service Description

2.1 Service identification

Service name: *Secure Destruction of Data on Magnetic Media*

Period of assessment: July, 2006 – June, 2007

2.2 Service Overview

The service is currently intended for destruction of data classified as Restricted or below. Higher security markings, Confidential and above, are not covered by this service.

2.2.1 Security architecture

Not applicable

2.2.2 Hardware requirements

The service uses a mobile degausser. The type used is made by Verity and the model is SV91M.

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, therefore, unless magnetic media is so identified on the casing, it should be considered in scope with regard to this testing

2.3 Usage assumptions

2.3.1 Assets

2.3.1.1 Hard disk drives

This includes all drives manufactured prior to the date of manufacture of the disk media used in the tests. These are, typically, up to 5000 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. 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, lomega 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.

2.3.2 Threat scenario

Threats to assets which are countered by the service described are:

- Theft or unauthorised disclosure of stored personal data
- Theft or unauthorised disclosure of stored operational data
- Theft or unauthorised disclosure of stored client/customer/user data

2.3.2.1 Expected operational environment

- The service provision is mobile. The operational environment will, in most cases, be the customers own site. The customer must provide site security as required. The customer must also provide certain facilities such as space (a normal parking space) and power (a convenient 13A socket).
- The technician charged with the operation of the equipment is experienced in the use of the equipment, SC cleared, trained in best practice for degaussing and fully competent to carry out the procedure
- The entire process of data destruction may be overseen by the customers' observers
- The process provides certificates that may be used in accordance with the clients asset management system
- The storage cost of old media is reduced or eliminated
- The risk assessment score is reduced. Data theft risk is eliminated if the data is destroyed rather than securely stored

2.3.2.2 Organisational security policies

The service 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

The service is mobile and may be operated at the customers' own site. If the customer requires a secure environment then the customer must provide this in compliance with their security policy. The service will operate within the secure environment provided.

3. Security Claims for the IA Service

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 service provides the erasure of data (with a protective marking of RESTRICTED or below) from magnetic storage media in compliance with the CESG Lower Level Degaussing Standard.
3	The service provides the customer with the facility to securely destroy the data on magnetic media on-site at the customer's premises. This is achieved by the use of portable equipment taken to the customer site, allowing the entire process to be done within a secure environment as provided by the customer.
4	The service provides secure data destruction on the magnetic media by SC technical staff fully trained in the use of the degaussing equipment and following the equipment manufacturer's guidelines.
5	The service may be observed by the customers' own staff during the process of degaussing. The material with data to be destroyed by the service may be continually witnessed by designated client staff.
6	The provision of the service meets environmental disposal requirements. At the request of the customer, the service provider will ensure that degaussed media is recycled.
7	The service may be booked at reasonable notice and will come to the client as requested.
8	The service provides the customer with the option of having the media smelted or recycled by an approved recycling company. The customer will be issued with a certificate of recycling to confirm disposal.
9	The service is fully auditable from the initial customer request for the service to final media destruction and, if required, disposal. Clients are provided with a certificate of data destruction detailing the media degaussed. Details include media type and serial number (where available), date and time degaussed, by whom it is degaussed and by whom it is witnessed.

3.2 Existing Assurance Certificates

The Verity SV91M degaussing unit used for data destruction complies with the CESG Lower Level Degaussing standard [CESG]. This was originally approved against the SEAP 8500 degaussing standard. Under S(E)N 06/09, degaussers which have been certified as meeting SEAP 8500 will automatically be considered to meet the CESG lower level degaussing standard. See the CESG website for further information:

<http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=152&id=287>

Annex A

Glossary of terms

Term	Meaning
ICD	Information Assurance Claims Document
LTO	Linear tape open (magnetic tape media)
SC	Security Checked
WEEE	EU directive on Waste Electrical and Electronic Equipment http://www.environment-agency.gov.uk/business/444217/444663/1106248/?version=1&lang=_e

Annex B

Marketing statement

This service provides cost effective Secure Data Destruction on your site for a variety of magnetic data storage media. This service uses a CESG approved degausser to remove all data on media marked RESTRICTED or below. This service is operated by our own Defence Vetting Agency Security Check (“SC”) engineers. Van, Engineer, and equipment will arrive on the customer site. If the option for environmentally compliant (WEEE directive) disposal of the processed media has been taken, then the engineer will remove the media for smelting and refining. A certificate detailing all media processed is issued on completion.

****End of Document****