



CCTM IA Claims Document (ICD)

Data Eliminate Ltd

Secure Destruction of Data on Hard Drives and Magnetic Storage Media

Version 1.0

CERTIFICATE DETAILS

| | |
|-------------------------|---------------------------------|
| CCTM Certificate Number | 2008/09/0037 |
| CCTM Awarded on | 11 th September 2008 |
| CCTM Award Expires on | 10 th September 2009 |
| ICD Issue Date | 03 rd September 2008 |

VENDOR DETAILS

Data Eliminate Limited

53 Balham Grove,
London
SW12 8AZ

Telephone Number: +44(0)845-1234-400
Website: www.dataeliminate.com
Contact Email: julian.fraser@dataeliminate.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 |
| 1.5 | References | 3 |
| 2 | Service Description | 4 |
| 2.1 | Product/Service Identification | 4 |
| 2.2 | Product/Service 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 |
| 2.3.1.1 | Hard disk drives | 5 |
| 2.3.1.2 | Data tapes | 5 |
| 2.3.1.3 | Other media | 5 |
| 2.3.2 | Threat Scenario..... | 5 |
| 2.3.2.1 | Expected Operational Environment | 5 |
| 2.3.2.2 | Organisational Security Policies | 6 |
| 2.3.2.3 | Security Requirements on the Environment | 6 |
| 3 | Security Claims for the IS Service | 7 |
| 3.1 | Claims Statements | 7 |
| 3.2 | Existing Assurance Certificates | 8 |

1 Introduction

1.1 Background

This document outlines the IA claims made by Data Eliminate Limited in regard to the suitability of Secure Destruction of data on Hard Drives and Magnetic Storage 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 Secure Destruction of Data on Hard Drives and Storage Media 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 the defined service *and* all the information related to the security thereof;
- 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 10, April 2007) |
|--------|--|

2 Service Description

2.1 Product/Service Identification

Service name: Secure Destruction of Data on Hard Drives and Storage Media

Period of assessment: May 2007 to April 2008

2.2 Product/Service Overview

Data Eliminate Ltd provides a secure and convenient service for the destruction of data on hard drives and other magnetic storage media. The service is mobile and carried out on the customer's premises. The customer is responsible for providing a suitable workspace at the customer's premises and for carrying media to be processed to the workspace. The workspace can take the form of a small working area within an office/meeting room. Alternatively, the process can be carried out in one of Data Eliminate Ltd's vans in which case the customer will need to provide a parking space and access to a domestic power supply. As an additional service, Data Eliminate may arrange for the collection or immediate removal of the degaussed material from the customer's premises and the recycling thereof in line with the WEEE Directive.

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 Systems Ltd and the model is SV91 M.

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

Material with a protective marking of Confidential and above is not covered by this service. Although Confidential media may be degaussed using this Verity SV91M it should be noted that such media will be considered to have been "cleared" and, hence, the media will retain the highest classification of data which was ever stored.

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 certification tests of the degausser. 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 certification tests of the degausser. 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 certification tests of the degausser, 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 the:

- Theft or unauthorised disclosure of stored personal data
- Theft or unauthorised disclosure of stored operational data

2.3.2.1 Expected Operational Environment

- Any organisation which uses hard drives and magnetic media to store data which is personal, operational, about clients, customers or users or commercially sensitive needs to prevent the theft or unauthorized disclosure of that data.
- This service mitigates the risk of the theft or unauthorised disclosure of data. It helps to protect the customer from the adverse effects of an incident of data loss such as legal and financial costs and damage to the customer's reputation.
- The service provision is mobile. The operational environment will, in all cases, be the customer's own site. The customer must provide site security as required. The customer must also provide a small workspace as defined in 2.2 above.
- The technician charged with the operation of the equipment is experienced in the use of the equipment, 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 customer's observers.
- The process provides certificates that may be used in accordance with the customer's 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 the customer to comply with security policies related to ISO 27001 controls, Section 15.1.4, Data protection and privacy of personal information. It also helps achieve compliance with the United States Sarbanes Oxley Act.

In addition, users will be able to comply with NHS SyOp 7.13, 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 will be operated at the customer's 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 IS Service

3.1 Claims Statements

| Unique Ref | 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 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 customer's own staff during the process of degaussing. The material with data to be destroyed by the service may be continually witnessed by designated customer 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 customer as requested. |
| 8 | The service provides the customer with the option of having the media shredded 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. At the time of data destruction, Data Eliminate Ltd will provide a serial number label per item for recording purposes. Alternatively, a pre-existing serial number already on the item may be used. The customer is provided with a certificate of data destruction at the time of destruction or shortly afterwards. This provides details of the media degaussed including media type and serial number (where available), date degaussed, by whom it is degaussed and by whom it is witnessed or as required by the customer. |

3.2 Existing Assurance Certificates

The Verity SV9IM degaussing unit used in this service 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](http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=152&id=287)

Annex A: Glossary of Terms

| Term | Meaning |
|-------------|---|
| CESG | Communications-Electronics Security Group |
| CCT Mark | CESG Claims Tested Mark |
| EU | European Union |
| HMG | Her Majesty's Government |
| IA | Information Assurance |
| IT | Information Technology |
| ICD | Information Assurance Claims Document |
| LTO | Linear tape open (magnetic tape media) |
| NHS | National Health Service |
| SDLT | Super Digital Linear Tape |
| SEAP | Security Equipment Assessment Panel |
| UK | United Kingdom |
| WEEE | EU directive on Waste Electrical and Electronic Equipment |

Annex B: Marketing Statement

Our service helps ensure that your organisation is not at risk from a breach of data classified as HMG RESTRICTED or below.

It helps protect your reputation and reduces the legal and financial risks that could result from an incident of data loss or unauthorised disclosure.

The service is provided on site at your premises. It lets you witness that your sensitive data is eliminated from hard drives and magnetic storage media before any IT equipment leaves your control. It is carried out under your supervision and at a time convenient to you.

The process uses CESA approved degaussing equipment. It is fully auditable and certificates of destruction are issued. It facilitates compliance with UK and EU Data Protection and Environmental Recycling regulations (WEEE) and the USA's Sarbanes Oxley Act.

The service is not suitable for material with a protective marking of HMG CONFIDENTIAL or above.

****End of Document****