



CCTM IA CLAIMS DOCUMENT (ICD) R&R Data Managed Services Limited

Secure Destruction of Data on Magnetic Media
Version 1, March 2008 – February 2009

VENDOR DETAILS	TEST LABORATORY DETAILS
R&R Data Managed Services Limited	SiVenture
R&R House Normandy Lane Stratton Business Park Biggleswade Beds. SG18 8QB	Unit 6, Cordwallis Park Clivemont Road Maidenhead Berkshire SL6 7BU
Telephone Number: 0845 257 8181	Telephone Number: 01628 651360
Email: dsinfo@datadestroyed.com	Email: info@siventure.com
Website: www.randrplc.com	Website: www.siventure.com

CERTIFICATE DETAILS	
CCTM Certificate Number	2010/01/0065
CCTM Awarded on	20 th January 2010
CCTM Award Expires on	19 th January 2011
ICD Issue Date	20 th January 2010

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 IS SERVICE DESCRIPTION..... 4

 2.1 Service Identification 4

 2.2 Service Overview 4

 2.3 Usage assumptions..... 5

3 CCTM CLAIMS FOR THE IS SERVICE..... 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 R&R Data Managed Services 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

- 1.2.1 The objective of this ICD is to provide the IA claims for *Secure Destruction of Data on Magnetic Media*.

1.3 Purpose of Document

- 1.3.1 This document is the ICD for *Secure Destruction of Data on Magnetic Media*.
- 1.3.2 This ICD is the baseline document for the CCTM Claims Test of *Secure Destruction of Data on Magnetic Media*.

1.4 Structure

The structure of this ICD is as follows:

- Section 1 (this section) contains the 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.

2 IS SERVICE DESCRIPTION

2.1 Service Identification

Product or Service Name: Secure Destruction of Data on Magnetic Media

Version: 1

Period of Assessment: March 2008 – February 2009

2.2 Service Overview

R&R Data Managed Services Limited will provide for its clients a secure and convenient service for destruction of data on magnetic media. The service is mobile and may be called to the client's premises upon request. The client is responsible for providing a suitable place at the client's premises for the operation to be carried out, but it should be noted that the equipment resides in a small van and requires little more than a parking place and a nearby domestic power socket (for extended operation as small batches can be done on internal battery power). The client is also responsible for carrying the media to the van. As an additional service, R&R may smelt and recycle the degaussed material at the client's request. R&R's data destruction service offers both on-site and secure collection services, but the secure collection service is not claims tested under the CCTM scheme.

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 Kroll Ontrack (IBAS) and the model is DG02¹.

2.2.3 Software requirements

Not applicable.

2.2.4 Out of Scope

Material with protective marking of Confidential and above is not covered by this service. Media packaged with magnetic shielding, specifically designed to prevent intrusion of external magnetic fields,

¹ The specific IBAS DG02 degausser was tested using the same test strategy used for testing products according to the Lower Level Degaussing Standard as described in HMG Infosec Standard 5. However, while this particular degausser, with serial number 20030, meets the conditions set out in the standard, the result does not apply generally to all degaussers of this make and model.

is not covered. This service covers on-site data destruction and does not cover media degaussed at any site other than that of the service client. The service does not cover secure collection of media

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. Examples of media covered includes: Hard disk drives; tapes up to LTO and SDLT, floppy disk drives; lomega media such as Zip and Jaz.

2.3.1.1 Hard disk drives (HDD)

This includes all drives manufactured prior to the date of manufacture of the disks used in the tests. 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. These are, typically, up to 2700 Oersted coercivity.

2.3.1.3 Other media

Other media may be included, 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.

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 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 customers' observers
- The process provides certificates that may be used in accordance with the clients asset management system

- The risk assessment score is reduced. Data theft risk is significantly reduced 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 27001. 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 vendor provides mobile equipment taken to a customer's site, enabling the media to remain within a secure environment provided by the customer. The customer is responsible for providing the secure environment complying with their security policies.

3 CCTM 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 the 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 customers' own staff during the process of degaussing. The material with data to be destroyed by the service may be continually witnessed by any designated client staff.
6	The service may be booked at reasonable notice and will come to the client as requested. The service is mobile and requires a normal car parking space and a normal (13A) power socket to operate. No emissions are produced and no appreciable noise (sound) is generated.
7	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.
8	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 specific IBAS DG02 degausser was tested using the same test strategy used for testing products according to the Lower Level Degaussing Standard as described in HMG Infosec Standard 5. However, while this

particular degausser, with serial number 20030, meets the conditions set out in the standard, the result does not apply generally to all degaussers of this make and model.

REFERENCES

- [TLG] Test Lab Guide, Version 3.0.0, 19 March 2009
- [DES] CCTM Description of Scheme, Version 3.0.0, 19 March 2009
- [CESG] CESG lower level degaussing standard (HMG Infosec Standard 5, issue 3.0, March 2009 and CESG Infosec Manual S, issue 2.0, September 2007)

ANNEX A GLOSSARY OF TERMS

Term	Meaning
CESG	Communications Electronics Security Group
HDD	Hard Disk Drive
ICD	Information Assurance Claims Document
LTO	Linear tape open (magnetic tape media)
UKAS	United Kingdom Accreditation Service
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

Our unique mobile Data Destruction Service makes it easy for clients to comply with their statutory duty to securely remove data classified at RESTRICTED and below from obsolete and surplus IT equipment's magnetic media. The data destruction process can be part of the quality and security policy of any organisation, allowing proof of compliance with security needs and the law. In addition, the media can be safely destroyed in an environmentally approved way to comply with statutory disposal requirements.