



## CCTM IA CLAIMS DOCUMENT (ICD)

### DiskShred

**Managed Service for Secure Destruction of Data Storage  
Media and Data Storage Hardware**

**Period of Assessment: June 2009 – June 2010**

VENDOR DETAILS	TEST LABORATORY DETAILS
DiskShred – a division of AMI Ltd	Enex TestLab
Unit 1 Mallusk View Central Park Newtonabbey BT36 4FR United Kingdom	Technium Springboard Centre Llantarnam Park Cwmbran NP44 3AW United Kingdom
Telephone Number: +44(0)8000805083	Telephone Number: +44(0)1633647898
Email: info@diskshred.co.uk	Email: rob.tanner@enextestlab.co.uk
Website: www.diskshred.co.uk	Website: www.enextestlab.co.uk

#### **CERTIFICATE DETAILS**

The table will be on the front cover of the Final ICD when this is published on the CCTM Website

CCTM Certificate Number	2010/02/0067
CCTM Awarded on	5 <sup>th</sup> February 2010
CCTM Award Expires on	4 <sup>th</sup> February 2011
ICD Issue Date	5 <sup>th</sup> February 2010

## TABLE OF CONTENTS

1	INTRODUCTION.....	3
2	IS PRODUCT/SERVICE DESCRIPTION.....	4
3	CCTM CLAIMS FOR THE IS PRODUCT OR SERVICE .....	6

# 1 INTRODUCTION

## 1.1 Background

This document outlines the IA claims made by DiskShred in regard to the suitability of the Managed Service for Secure Destruction of Data Storage Media and Data Storage Hardware for use by the UK Public Sector for the purpose of physically destroying data storage media and data storage hardware using a secure shredding procedure.

## 1.2 Objectives

1.2.1 The objectives of this ICD are to provide:

- An overview of the Managed Service for Secure Destruction of Data storage Media and Data Storage Hardware and all information related to the security of the Managed Service for Secure Destruction of Data Storage Media and Data Storage Hardware.
- Details of the IA claims made by the Managed Service for Secure Destruction of Data Storage Media and Data Storage Hardware.

## 1.3 Purpose of Document

1.3.1 This document is the ICD for the Managed Service for Secure Destruction of Data Storage Media and Data Storage Hardware.

1.3.2 This ICD is the baseline document for the CCTM Claims Test of the Managed Service for Secure Destruction of Data Storage Media and Data Storage Hardware.

## 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 the Managed Service for Secure Destruction of Data Storage Media and Data Storage Hardware and all the information related to the security of the Managed Service for Secure Destruction of Data Storage Media and Data Storage Hardware.
- Section 3 details the security functionality claims that are being made.

## 2 IS PRODUCT/SERVICE DESCRIPTION

### 2.1 Product/Service Identification

Product or Service Name: Managed Service for Secure Destruction of Data Storage Media and Data Storage Hardware

Version: 1.0

Platforms (for Products): Not applicable.

Period of Assessment (for Services): June 2009 – June 2010

### 2.2 Product/Service Overview

The Managed Service for Secure Destruction of Data Storage Media and Data Storage Hardware uses a mobile, vehicle based shredder to physically destroy data storage media and data storage hardware, rendering all such storage materials, and any stored data thereon, realistically unrecoverable. For magnetic media classified at IL3, a CESG approved Degaussing device shall be used prior to physical destruction.

#### 2.2.1 Security architecture

All shredding work is carried out on client premises by fully vetted staff. DiskShred staff count and record the items that need shredding (either before or after the items have been transported to the vehicle). The client has the option to witness the counting and recording process, as well as, the actual shredding of all storage materials on board the vehicle (DiskShred provide Personal Protection Equipment to the client for the purpose of witnessing the shredding process). DiskShred on-site personnel provide the client with a signed record describing the items shredded, and the client is subsequently provided with a signed 'Certificate of Destruction' detailing fully the quantity of items destroyed.

#### 2.2.2 Hardware requirements

Not applicable.

#### 2.2.3 Software requirements

Not applicable.

#### 2.2.4 Out of Scope

Metal based shredded material is recycled by an external organisation, with an estimated 95% material recovery. Shredded plastic material is also externally recycled, with an estimated 60% re-used in low grade plastic products. All recycling activities are excluded from CCTM tests.

DiskShred provide a related hard drive removal service. The removal service is excluded from CCTM tests.

DiskShred provide a related equipment disposal service that recycles and / or remarkets IT hardware (e.g. monitors) that may have re-use value. This disposal service is excluded from CCTM tests.

The use of the service to destroy any data media containing data at Confidential or above.

## 2.3 Usage assumptions

### 2.3.1 Assets

Assets to be protected include any data and IPR contained on discarded optical (IL2) or magnetic data storage media (IL3) and data storage hardware, that could pose a risk or threat to an organisation or individual if electronically copied, transferred, printed, or reproduced elsewhere without the appropriate authorisation.

### 2.3.2 Threat scenario

Threats to assets which are countered are:

- The unauthorised recovery of any data and IPR from discarded data storage media and data storage hardware.

#### 2.3.2.1 Expected operational environment

The operational environment for the shredding service is a vehicle deployed on, or near to, a client site. The vehicle based shredder can concurrently process multiple data storage materials.

#### 2.3.2.2 Organisational security policies

The service is designed to work in line with organisational security policies that enforce good practice for data storage media and data storage hardware disposal (and disposal of the data stored on such items).

#### 2.3.2.3 Security requirements on the environment

Any organisational security requirements including physical, personnel, and procedural matters are entirely independent of the service. Each individual client implements any such requirements based on their security policies and unique environment, for example:

a) The definition of secure handling requirements for the transfer of data storage materials from the client to the shredding vehicle is the sole responsibility of the client.

b) The preferred location of the shredding vehicle may be specified by the client.

### 3 CCTM CLAIMS FOR THE IS PRODUCT OR SERVICE

#### 3.1 Claims Statements

Reference	Claims Statements
<b>DS001</b>	The service is deployed on-site (or as otherwise specified by the client) using a mobile, vehicle based, shredder that operates independently of the client environment, being self-powered and self-contained.
<b>DS002</b>	The service is operated by on-site DiskShred staff, all of whom are formally vetted by the PSNI to an Access NI level.
<b>DS003</b>	The service is operated by on-site DiskShred staff, all of whom are formally checked to BS7858 standard, by an appropriately compliant external company.
<b>DS004</b>	The service shreds hard disk drives (desktop, laptop, server, and solid state based drives), and physically destroys all such drives to ensure that each drive is inoperable and destroyed using commercial best practice.
<b>DS005</b>	The service shreds disks (CD, DVD, Floppy, and zip disks), and physically destroys all such disks to ensure that each disk is inoperable and destroyed using commercial best practice
<b>DS006</b>	The service shreds tapes (DAT, DLT, LTO, Audio, and Video), and physically destroys all such tapes to ensure that each tape is inoperable and destroyed using commercial best practice
<b>DS007</b>	The service shreds portable storage devices (memory sticks, memory pens, memory cards, and flash based devices), and physically destroys all such devices to ensure that each device is inoperable and destroyed using commercial best practice.
<b>DS008</b>	The service shreds mobile telephony devices (PDA and Smartphone), and physically destroys all such devices to ensure that each device is inoperable and destroyed using commercial best practice.
<b>DS009</b>	All data storage materials pass through a maximum grid size opening of 20mm during the shredding process.
<b>DS010</b>	DiskShred staff count and record the items identified for shredding (either before or after the items have been transported to the shredding vehicle, as specified by the client). The client can witness the entire counting and recording process.
<b>DS011</b>	The shredding of all storage materials occurs on board the vehicle and the client can witness the entire shredding process. (DiskShred provide Personal Protection Equipment to the client for the purpose of witnessing the shredding process).
<b>DS012</b>	Following the shredding process, while still on-site, DiskShred personnel provide the client with a signed record describing the items shredded. At a later date, the client is provided with a signed 'Certificate of Destruction' detailing fully the quantity of items destroyed. The certificate corresponds to details found in the asset register maintained at the DiskShred head office.

<b>DS013</b>	Multiple data storage materials can be destroyed approximately concurrently.
<b>DS014</b>	The DiskShred service vendor is accredited to the BS8470 standard.

It should be noted that all claims are only valid up to and including IL3 RESTRICTED for magnetic media and IL2 for other media

### 3.2 Existing assurance certificates

Not applicable.

## ANNEX A GLOSSARY OF TERMS

**Data Storage Hardware:** Fixed physical components used for storing and / or retaining computer data.

**Data Storage Media:** Portable physical components used for storing and / or retaining computer data.

**IL3:** Impact Level 3, defined as 'RESTRICTED' by the appropriate authority on behalf of Her Majesty's Government.

**IL2:** Impact Level 2, defined as 'PROTECTED' by the appropriate authority on behalf of Her Majesty's Government.

**IPR:** Intellectual Property Rights.

**Shred, Shredding:** The process of destroying physical components to render said components inoperable by virtue of being destroyed using commercial best practice, as defined in 'CCTM Secure Destruction Guidance Note v01'.

## **ANNEX B    MARKETING STATEMENT**

DiskShred provides a secure on-site shredding service for Hard Disk Drives and the other electronic storage media devices listed below. This specialist service offers you a fast and foolproof disposal solution for sensitive and private employee, customer and business information.

Using our lorry-based shredder at your premises, we reduce your devices to piles of debris, rendering the materials inoperable.

The vehicle does not require mains power as it operates totally independently. The service is provided right at the client's own premises, where DiskShred's security cleared staff carry out the destruction while you watch. The service is fully auditable and a Certificate of Destruction is provided.

DiskShred destroys the following Electronic Media items up to and including IL3 RESTRICTED\*:

- Hard Disk Drives
- Back-Up Tapes & Disks
- CD-ROMs & Floppy Disks
- USB Keys, PDA's & mobile phones
- CCTV Tapes
- Videos/DVDs

\*IL3 is for magnetic media only