



## CCT MARK IA CLAIMS DOCUMENT (ICD)

### SDMS

Secure Data Media Solutions Service

<b>VENDOR DETAILS</b>
Secure Data Media Solutions Ltd
11 Berkshire House County Park Shrivenham Road Swindon Wilts SN1 2NR
Telephone Number: +44 (0) 1793 490234
Vendor Website: <a href="mailto:INFORMATION@SDMS.UK.COM">INFORMATION@SDMS.UK.COM</a>
Vendor Contact Email: <a href="mailto:heather@sdms.uk.com">heather@sdms.uk.com</a>

<b>CERTIFICATE DETAILS</b>	
CCT Mark Certificate Number	2007 09 0028
CCT Mark Award Expires on	26 <sup>th</sup> September 2008
ICD Issue Date	27 <sup>th</sup> 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
2	Service Description .....	3
2.1	Service Identification.....	4
2.2	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
2.3.2	Threat scenario.....	5
2.3.3	Expected operational environment.....	5
2.3.4	Organisational security policies .....	6
2.3.5	Security requirements on the environment.....	6
3	Security Claims for the IS Service .....	7
3.1	Claims Statements.....	7
3.2	Existing assurance certificates .....	7
	Annex A Glossary of Terms .....	8
	Annex B Marketing Statement .....	9

## **1 Introduction**

### **1.1 Background**

This document states the Information Assurance (IA) claims made by Secure Data Media Services Ltd. (SDMS) in regard to the suitability of their services for use by the UK Public Sector. SDMS provide a through-life, cradle-to-grave service relating to secure data media covering procurement, marking, accounting, training, consultancy and advice.

This service is offered to commercial and public sector clients by Secure Data Media Solutions Ltd. SDMS is a small, specialist company whose principals each have over 20 years experience in the field of secure data media management and are routinely consulted by UK National and Departmental security authorities on issues of policy, guidance and implementation relating to secure data storage, destruction and remanence

### **1.2 Objectives**

The objectives of this ICD are twofold:

To provide a basis for the CSIA Claims Tested Mark (CCTM) scheme assessment of the service; and

To act as the basis of an agreement between the vendor and the CCTM Secretariat regarding marketing claims for the certified service.

### **1.3 Purpose of Document**

1.3.1 This document is the ICD for Secure Data Media Solutions Service.

1.3.2 This ICD is the baseline document for the CCT Mark Claims Test of Secure Data Media Solutions Service

### **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 the Secure Data Media Solutions Service and contains all the information related to the security of the service.
- Section 3 details the security functionality claims that are being made.

## **2 Service Description**

Service Name : Secure Data Media Solutions

Assessment Period: September 2006 – August 2007

Platforms: N/A

## 2.1 Service Identification

Service Name : Secure Data Media Solutions

Assessment Period: September 2006 – August 2007

Platforms: N/A.

## 2.2 Service Overview

### 2.2.1 Security architecture

SDMS provide a trusted source of supply for digital storage media. This service offering to customers is a 'cradle to grave' secure data media solution which includes:

- Pre-sales consultancy
- Digital Storage Media procurement and customization, including as required;
  - Colour Coding
  - Marking with appropriate organizational/ownership identification and branding printed directly onto the product
  - Allocation and printing of Unique Serial Numbers on the casing of each item
  - Maintenance of accounting records of serial numbers for audit purposes.
  - User training
  - Through-life consultancy and support

SDMS operate within secure premises, which are HMG (List X) approved to CONFIDENTIAL.

### 2.2.2 Hardware Requirements

N/A.

### 2.2.3 Software requirements

N/A

### 2.2.4 Out of Scope

The security training and consultancy services provided by SDMS will be outside the scope of CCTM testing.

## **2.3 Usage assumptions**

### **2.3.1 Assets**

The service provides an auditable supply of securely marked, printed, accountable digital storage media designed to meet the customers' requirements.

### **2.3.2 Threat scenario**

Threats to assets which are countered are:

- Information assets being inadvertently removed from authorized premises and/or disposed of.
- Anonymous and unaccountable loss/disposal of information assets.
- Misuse of information storage assets – e.g. used to store inappropriate sensitivity levels
- Disruption of system availability due to the introduction of Malicious Mobile Code (MMC) inherited from the production process
- Disruption of data integrity and/or availability due to the introduction of Malicious Mobile Code (MMC) inherited from the production process

### **2.3.3 Expected operational environment**

The service can only operate effectively if an appropriate security policy is implemented within the vendor and client organisations. The key issues are:

- Security training of administrative staff and users
- Appropriate physical and procedural security
- Accounting and audit procedures for data media used for valuable and/or sensitive information assets
- Incident investigation procedures for loss or misuse of data media

Effective storage processes and environmental controls.

#### 2.3.4 Organisational security policies

This service assists organisations in supporting security policies relating to the following ISO/IEC 27001:2005 control objectives (however, it should not be inferred that the use of the service constitutes compliance against the standard).

A.7.1 Responsibility for assets.

A.7.2 Information classification.

A.10.5 Backup.

A.10.7 Media handling.

A.11.3 User responsibilities.

A.13.2 Management of information security incidents and improvements.

A.14.1 Information security aspects of business continuity management

A.15.1 Compliance with legal requirements.

#### 2.3.5 Security requirements on the environment

##### Vendor

- An effective secure environment is maintained.
- Effective security procedures are in place.
- Accounting records are protected and held securely

##### Client

- Administrative staff and users receive appropriate training.
- Accounting records for data media items supplied are maintained.
- Appropriate incident investigation procedures and supporting policies are in place
- Appropriate storage processes and environmental controls are in place

### 3 Security Claims for the IS Service

#### 3.1 Claims Statements

The table below sets out the claims for Secure Data Media Services.

Ref.	Claim
	<b>Media Production</b>
001	All digital storage components are sourced from reputable manufacturers/suppliers
002	The packing and distribution of assembled data storage units is performed within a controlled environment that includes physical security mechanisms installed and maintained by the Government-approved Secure Services Group (SSG) and inspected by SSG at 6 monthly intervals, and which has been accredited for handling and storage of HMG material at up to CONFIDENTIAL
003	A regime is in place which minimises the risk of contamination of data storage products with malicious code during the assembly process.
	<b>Media Customisation</b>
004	All data storage units can be customized by printing a colour block onto the case in a colour scheme to match any eye visible convention in use by customer organizations to indicate sensitivity
005	All data storage units can be customized by printing directly on to the case with text or graphics to meet customer organization's ownership marking and other security control requirements
006	All data storage units can be customized by printing the case with a Unique Serial Number using a solvent based ink to meet customer organization's security control requirements
	<b>Accounting and Audit</b>
007	An audit record showing: reference, client, date of delivery to client, location of delivery is produced and maintained.
008	Audit records are retained for at least 7 years

#### 3.2 Existing assurance certificates

SDMS is accredited against ISO 9001/2000

SDMS premises are HMG (List X) accredited to CONFIDENTIAL

## **Annex A Glossary of Terms**

The following terminology is used in the ICD:

- **CSIA:** Central Sponsor for Information Assurance, part of the Cabinet Office
- **GSA:** Government Security Advisor – appointed to accredit List X sites and monitor compliance.
- **ISO/IEC 27001:2005:** The international standard for Information Security Management

## **Annex B Marketing Statement**

The SDMS service provides for the supply of premium brand, security marked, printed, accountable and auditable computer, audio and video storage media.

The marking, printing and identification of media can be customised to meet specific customer security requirements.

Packing and distribution is performed within a government accredited secure location.

Records of despatched products are retained for at least 7 years, to assist in any related incident investigation by the customer