



## CCTM IA CLAIMS DOCUMENT (ICD)

<b>DATA ENCRYPTION SYSTEMS LTD</b>
DESlock <sup>+</sup>
VERSION 3.2.7

<b>CERTIFICATE DETAILS</b>	
CCTM Certificate Number	2008/05/0036
CCTM Awarded on	13 <sup>th</sup> May 2008
CCTM Award Expires on	12 <sup>th</sup> May 2010
ICD Issue Date	13 <sup>th</sup> May 2008

<b>VENDOR DETAILS</b>
Data Encryption Systems Ltd
Silver St House, Silver St Taunton, Somerset TA1 3DL
Telephone Number: +44 1823 352357
Vendor Website: <a href="http://www.deslock.com">www.deslock.com</a>
Vendor Contact Email: <a href="mailto:Sales@Deslock.com">Sales@Deslock.com</a>

## Table of Contents

### 1 Introduction

#### 1.1 Background

This document outlines the IA claims made by Data Encryption Systems Ltd in regard to the suitability of DESlock<sup>+</sup> for use by the UK Public Sector for an Email and Data Encryption product for Windows based operating systems providing File and Folder encryption, Email encryption, Secure destruction of Data, Mountable files, secure Archives and encryption of data on removable media. DESlock<sup>+</sup> is being tested under the CCTM Scheme which is aimed at providing information assurance at Government Impact Levels 1 and 2, for purchase by central government and the wider public sector, particularly the NHS, education, local authorities, police and criminal justice.

#### 1.2 Objectives

1.2.1 The objectives of this ICD are to provide:

- An overview of “DESlock<sup>+</sup>” and all information related to the security of DESlock<sup>+</sup>,
- Details of the IA claims made by “DESlock<sup>+</sup>”.

#### 1.3 Purpose of Document

##### 1.3.1

This document is the ICD for “DESlock<sup>+</sup>”.

##### 1.3.2

This ICD is the baseline document for the CCTM Claims Test of “DESlock<sup>+</sup>”

#### 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 “DESlock<sup>+</sup>” and all the information related to the security of “DESlock<sup>+</sup>”
- Section 3 details the security functionality claims that are being made.

## 2 Product/Service Description

### 2.1 Product/Service Identification

Product or Service Name: "DESlock<sup>+</sup>"

Version: 3.2.7

Platforms (for Products): PC's running MS Windows XP (SP2)

Operating System	Version	Browser	Version
MS windows XP	SP2	MS internet Explorer	6
MS Outlook	2003		

Period of Assessment (for Services): N/A

### 2.2 Product/Service Overview

#### 2.2.1 Security architecture

DESlock<sup>+</sup> is an encryption product for Windows based operating systems. DESlock<sup>+</sup> encrypts selected data on a computer hard drive, either as individual files, folders, selected text, or emails. The user authentication process includes password entry in combination with a software package. DESlock<sup>+</sup> uses various encryption Key types either on the local token or shared with and from Administrators or other users.

High Level Functional overview

Security offered by DESlock<sup>+</sup> may be summarised as:

- Encryption of selected data on a computer's hard drive with an implementation of various algorithms using a 112 or 128 bit key, depending on algorithm;
- Password based user authentication;
- Optional encryption of data on removable media.

Features of the software include; (bracketed references refer to the detailed claims in section 3)

- **File or Folder Encryption;** DESlock<sup>+</sup> encrypts selected area's of the computer's hard disk(s) using various data encryption algorithms. After successful authentication, data is automatically decrypted and re-encrypted on the fly. If anyone attempts to bypass authentication the data is encrypted and in some cases hidden. (DES001, 008, 009,)

- **Email Encryption;** Using a plug-in to Outlook, DESlock<sup>+</sup> can be used to send and receive encrypted email and attachments. (DES019)
- **Mountable files;** DESlock<sup>+</sup> can be used to create mountable files (files which will appear as separate drives on your computer), which may either be files on your main hard disk or on Removable Media. (CD's DVD's, USB keys). (DES005, 006)
- **Removable Media.** Individual files or folders on removable media may be encrypted and decrypted. It is recommended that Mountable files are used on Removable Media as this will protect the individual filenames on the media. (DES004)
- **Data Shredder;** Using a cryptographic random number stream data may be deleted from the hard disk. (DES021)
- **Archive;** DESlock<sup>+</sup> Archive allows the user to create a compressed, encrypted version of a file or a number of files. This provides a secure method of protecting files removed from the system to save space or to transfer to another user in an efficient manner. (DES024)
- **Key creation and Management:** Depending on configuration, users can have the ability to create, control and share up to 64 encryption keys. In a multi user environment, key generation and transfer can be controlled by administrators using the DESlock<sup>+</sup> Administration tool, thus preventing misuse of the system. In a multi user environment this ensures that only authorised encryption keys are used, and that lost tokens and passwords can be safely recreated with compromising any Data. (DES014)
- **Password protection.** Various methods are employed to protect passwords used to access the Key tokens (hardware and software). These can be set by the user or administrator, and will lock, erase, or lock and erase the Encryption Keys and scratchpad contents if a number of incorrect attempts has been made, or will double the time between each allowable attempt. (DES025)

### 2.2.2 Hardware requirements

Any windows based PC running MS XP (SP2) with a minimum of:

- 64MB of free hard-disk space
- CD Rom Drive
- VGA (640 X 480) or higher resolution monitor with 256 colours or more

- Pointing Device and Keyboard
- Internet Explorer 6 or later

### 2.2.3 Software requirements

MS windows XP (service pack 2)  
MS Outlook 2003

### 2.2.4 Out of Scope

- The 128 bit Blowfish cryptographic algorithm (64 bit block cipher) is not being tested under the CCTM Scheme.
- USB Token based operation is not being tested under the CCTM Scheme.
- The AES and Triple DES (3DES) encryption algorithms are not being tested under the CCTM scheme.
- DESlock<sup>+</sup> Operates on all windows versions from Windows 95 to Vista, but these are out of scope for the Claims testing. Only Windows XP (SP2) is being tested.
- DESlock<sup>+</sup> Operates with other versions of Outlook from Outlook 98 to Outlook 2007, but these are out of scope for the claims testing; only Outlook 2003 is being tested.
- The RSA algorithm and Public Key cryptography techniques, using a 1024 bit RSA Public-Private Key pair" are not being tested during claims testing of the product

## 2.3 Usage assumptions

### 2.3.1 Assets

Assets to be protected include any data on the client PC or laptop that could pose a risk or threat to an organisation or individual if lost or stolen or copied or transferred elsewhere.

### 2.3.2 Threat scenario

Threats to assets which are countered are:

- Unauthorised access to data encrypted with DESlock<sup>+</sup> at rest on the client PC, laptop or server, once the user has deactivated the product. (DES025)
- Unauthorised access to data encrypted with DESlock<sup>+</sup> held on removable memory devices. (DES004, DES005)
- Unauthorised access to emails encrypted with DESlock<sup>+</sup> at rest on the client PC/laptop, (DES025) and during transmission. (DES019)

- Unauthorised access is prevented through the use of password protection against brute strength attacks. (DES025)

### 2.3.2.1 Expected operational environment

#### Operational Environment

- DESlock<sup>+</sup> operates on PC's running MS windows XP (SP2)
- DESlock<sup>+</sup> supports encryption of Data on removable storage media.
- DESlock<sup>+</sup> supports one or multiple user accounts per protected machine, however, only a single authorised user may gain access to the computing device simultaneously after authentication.

#### Benefits

- Protect sensitive data from internal threats (inquisitive staff, industrial espionage, criminal activity, targeted data theft)
- Stolen or lost laptops or PC's. All data protected with DESlock<sup>+</sup> will remain confidential.
- Comply with corporate compliance issues and Data protection act.
- Offsite backups can be held encrypted.
- Transfers of data by email or via courier can be securely performed.

#### Scale of Use

- Simple to implement on single or multiple machines either on a single site or in a worldwide organisation.

### 2.3.2.2 Organisational security policies

Any Data Security policy is basically stating the following: "Other than data defined as public, which is accessible to all identified and authenticated users, the organisation should ensure that all data and processing resources are only accessible on a need to know basis to specifically identified, authenticated, and authorised entities." DESlock<sup>+</sup> provides the facility to be able to comply with this requirement. The organisation should define what data, or types of data should be encrypted, and in what circumstances. Secure methods of file deletion should also be defined. As DESlock<sup>+</sup> is very flexible, several different grades of sensitivity can be defined, relating, for example, to the number of users that require access to the data. This can be applied both to data held on PC's and Laptops, to emailed data, and especially to data held or transferred on removable media (CD's, DVD's, memory cards and sticks).

### 2.3.2.3 Security requirements on the environment

DESlock<sup>+</sup> operates in the normal windows environment, and once the user is logged onto the product its operation is transparent, in that encrypted folders and files can be opened in the normal way. However, to maintain security, no unencrypted or plain copies of encrypted data should be made for any reason, except under controlled conditions. Physical versions (prints, images, etc) should be controlled in accordance with the organisations normal operating procedures.

## 3 Security Claims for the IS Product or IS Service

### 3.1 Claims Statements

Ref	Claim
DES001	The Product Encrypts and decrypts individual files, or portions of plain text, using an encryption key or a password.
DES002	The Product will Encrypt/Decrypt data on local hard drives.
DES003	The Product Encrypts and Decrypts data stored on network drives using mountable files.
DES004	The Product will encrypt/decrypt data on external writeable media – Hard disks, solid state memory drives (EG memory cards), USB memory drives.
DES005	The Product will create encrypted mountable files on internal hard drives and external writeable media.
DES006	The Product makes mountable files appear in Windows Explorer as an additional local disk drive, once they are mounted.
DES007	Encrypted Files, Encrypted Mountable Files and Encrypted Archives may be stored on and accessed from any computer drive or media, provided the Product and Encryption keys are available.
DES008	Where Folders, Files, mountable files or archives are encrypted using an encryption key, decryption is only possible with the same encryption key.
DES009	Where Folders, Files, mountable files or archives are encrypted using an encryption key, and the user has the correct encryption key available, decryption is automatic.
DES010	Where Folders, mountable files or archives are encrypted using an encryption key, and the user has the correct encryption key available, encryption of new or saved files within the Folder, Mountable File or Archive is Automatic.
DES011	Where an encrypted folder is in use and the user has the correct encryption key, its operation is identical to a normal Windows folder except that anything within the folder is encrypted.
DES012	Under the control of an authorised user or Administrator, the product will allow encryption keys to either be: Generated, exported to another user, imported from another user, or deleted.
DES013	An Authorised Administrator can prevent users from creating or adding encryption keys.
DES014	Depending on configuration, users can have the ability to create, control and share up to 64 encryption keys. In a multi user environment, key generation and transfer can be controlled by administrators, using the DESlock <sup>+</sup> Administration tool (additional program, tested as part of this process), thus preventing misuse of the system. In a multi user environment this ensures that only authorised encryption keys are used, and that lost tokens and passwords can be safely recreated without compromising any Data.
DES015	Encryption keys are stored in an encrypted Key File.

DES016	Where an Encryption key is exported to another user, the person exporting the key may set the Terminator Count Value in the exported Key to be any value between zero and one less than the current value. This controls the number of possible daughter copies that may be made of that Encryption Key.
DES017	If the Terminator Count Value is already Zero, the encryption key cannot be exported.
DES018	The product provides the facility to securely exchange encryption keys with other users.
DES019	The product provides facilities to encrypt and decrypt plain text email and file attachments, using Outlook 2003.
DES020	If the Product is installed with its Microsoft Outlook plug-in component, the Encryption key exchange process may be carried out directly from Microsoft Outlook.
DES021	The product will delete files through the use of the DESlock <sup>+</sup> Shredder facility. This writes a Cryptographic random number over the original data, then deletes the file location information using the Operating Systems delete function.
DES022	Using the DESlock <sup>+</sup> Shredder, the product can delete the contents of the Windows Recycle Bin, the contents of the "My Recent Documents" Folder, the Microsoft Internet Explorer Browser History files, the contents of the Windows Temporary Files Folder, and the Microsoft Internet Explorer Cache. In the event that any files are locked open by the system and cannot be deleted, the product will warn the user.
DES023	The product can create an encrypted copy of User folders in the windows environment. This also Encrypts all files and subfolders within the selected folder. Files and Folders "dragged and dropped" into encrypted folders will be automatically encrypted. The user can select if an unencrypted or plain version of the original folder is left on the system or not.
DES024	The product provides the facility to create a compressed, encrypted Archive version of a file or a number of files. This provides a secure method of protecting files removed from the system to save space or to transfer to another user in an efficient secure manner.
DES025	A key-file (Software) can have its password retry count set by the user. Beyond this count value, the computer must be restarted before the password can be re-entered.

### 3.2 Existing Assurance Certificates.

None

## Annex A: Glossary

The following terminology is used within this ICD.

- Token – Physical USB key, or software version of the key.
- Key – Encryption key created using AES, Blowfish or 3DES
- 3DES – Triple DES, is a variant form of the DES (Data Encryption Standard) algorithm, developed by IBM in 1974.
- AES – Advanced Encryption Standard
- RSA – Asymmetric Algorithm named after Ronald Rivest, Adi Shamir and Leonard Adelman, from MIT, who developed and patented the algorithm in 1977.
- USB – Universal Serial Bus
- User Folders. DESlock<sup>+</sup> will not allow the encryption of Windows essential folders. User folders are folders that can be created by the user.
- Data – information held in an electronic medium. This does not include any operating system components, paper prints, photocopies, images of printed pages, etc.
- Cryptographic Random Number – A Cryptographic random number created by the CryptGenRandom function within the Windows CryptoAPI.
- Encrypted Mountable file – A single file that appears to the Windows explorer as an additional hard drive when the user is logged onto Deslock+ and the file is “mounted”. It then will act as a normal drive, with the exception that files within it are encrypted and any files added to it will be automatically encrypted.
- TCV – Terminator Count Value

## **Annex B Marketing Statement**

DESlock<sup>+</sup> is a flexible, transparent encryption tool aimed at providing information assurance at Government Impact Levels 1 and 2, for purchase by central government and the wider public sector, particularly the NHS, education, local authorities, police and criminal justice. DESlock<sup>+</sup> provides encryption, decryption and deletion of data on Hard disk drives and removable media at file and folder levels, and also the facility to easily Email encrypted data. Each software token holds up to 64 different keys, which can be shared with other users, providing a multilevel solution to Data Security needs