

CCTM Test Report Summary

DESlock+ v3.2.7



## CCTM TEST REPORT SUMMARY

### DES

<b>DESlock+</b>
<b>Version: 3.2.7 Assessed April 2008</b>

<b>VENDOR DETAILS</b>	<b>TEST LABORATORY DETAILS</b>
Data Encryption Systems	West Coast Labs
Silver Street House, Silver Street Taunton, Somerset TA1 3DL	Unit 9, Oak Tree Court, Mulberry Drive Cardiff Gate Business Park Cardiff, CF23 8RS
Telephone Number: 01823 352357	Telephone Number: 02920 548400

Test Report Summary Issue Date: 13<sup>th</sup> May 2008

Further details about the claims tested are included in the Information Assurance Claims Document (CCTM Certificate Number 2008/05/0036) published on the CCTM website ([www.cctmark.gov.uk](http://www.cctmark.gov.uk))

## **CCTM Test Report Summary**

### **DESlock+ v3.2.7**

#### **1. Test Result**

- 1.1 The CSIA claims testing of the DESlock+ v 3.2.7, assessed April 2008, by West Coast Labs concluded that the security functionality claims made within the IA Claims Document v. 1.2.1 are valid for this IS Product or Service.

#### **2 References**

- [ICD] IA Claims Document, version 1.2.1, dated 11/03/2008
- [AG] IS Product/Service Administration Guide, version 3.2.7, date downloaded 28<sup>th</sup> March 2008
- [TLG] Test Lab Guide, version 2.4.0, dated 27<sup>th</sup> February 2008
- [TM] Test Method LAB24\_03\_08 v.1.1, dated 19<sup>th</sup> March 2008

#### **3 Scope of testing**

- 3.1 The DESlock+ v.3.2.7 was tested using the Test Method TLG v. 2.4.0 and TM LAB\_24\_03\_08 v. 1.1 against the claims made in the ICD v. 1.2.1.
- 3.2 The following features of DESlock + v.3.2.7 were not tested under the CCTM Scheme: The 128 bit Blowfish cryptographic algorithm (64 bit block cipher), USB Token based operation, the AES and Triple DES (3DES) encryption algorithms, versions of Windows other than XP SP2, versions of Outlook other than Outlook 2003, the RSA algorithm and Public Key cryptography techniques, using a 1024 bit RSA Public-Private Key pair
- 3.3 The DESlock v.3.2.7 consists of: Software downloaded from DES' website and MD5 checksum verified with the company as having the checksum of 4745D9D3F47B2EDE05D771DE828E9008. Also tested was the DESlock+ Admin Tool that was downloaded from the DESlock+ site and verified as version 1.0.5. This requires a DESkey DK5 to activate. DESkeys used in this testing had the serial numbers of 0000015264 and 0000015263.
- 3.4 The Claims Tests were conducted at West Coast Labs' premises located at the address specified on the front of this Test Report.
- 3.5 The following product/platform combinations (including version numbers and service packs) were used:

## CCTM Test Report Summary

### DESlock+ v3.2.7

Operating System	Version	Browser	Version
Windows XP	SP2	N/A	N/A
Microsoft Outlook	2003	N/A	N/A

- 3.6 IS Service Claims concerning procedures, performance and user aspects over the period of assessment were validated as follows:

Not appropriate

## 4 Ease of use

- 4.1 Installation of the product is difficult for testers to comment on, as the engineers conducting the testing are not average PC users. However, the installation for the components was very straightforward and should easily be accomplished by anyone familiar with installing Windows Software. Similarly, in use, if the time is taken to read the manuals and understand the capabilities of the software then, in accordance with the caveats described under section 4.2 of this document, the product should be easy to use in day-to-day situations. West Coast Labs always recommends that users of any security service fully read the manuals and ensure that they clearly understand the operation of solutions before deploying them.
- 4.2 The administrator should note that with relation to claim DES001, it has been discovered that upon encrypting plain text in a document, if a Windows Undo functionality is available, the original text may be recovered if the document is not closed in the intervening time. This has no bearing on the claim as it stands, as it is not strictly speaking decrypting, but users should be aware that Windows applications store such replacement data in application caches for the lifetime of the current open session and should employ good practice by not leaving such a document unattended.

The administration tool referenced in Claim DES014 and used in Claims DES013 and DES014 requires a physical hardware token to be able to set up and use, however the use of this can also control the software versions.

With relation to claim DES019, the standard installation of Microsoft Outlook 2003 uses Microsoft Word 2003 as the text editor. Once again, this has no bearing on the claim, as it specifically states that it only encrypts plain text, but this installation default on Outlook may potentially lead to some confusion when an administrator looks for the encryption buttons that are added to the toolbar.

## CCTM Test Report Summary

### DESlock+ v3.2.7

#### 5 Quality of User and Administrator Documentation

5.1 All documentation supplied offered clear guidance and advice at each stage. The documentation consisted of downloads made from the DES web site on 28th March 2008 of the following documents:

dlpadmin.pdf – describing the operation of the administrative tool

dlpmanual327.pdf – describing the operations, installation, and usage methods of the DESlock+ solution.

#### 6 Resistance to publicly known vulnerabilities

Not tested as part of this CCTM review.

#### 7 Validation of Existing Assurance Certificates

N/A

#### 8 Disclaimer

CSIA Claims Testing is not a guarantee of freedom from security vulnerabilities. There remains a probability that exploitable security vulnerabilities may exist in the IS Product or IS Service, or the Information System environment supporting the IS Product or IS Service. The issue of a Test Report is not an endorsement of a product or service.

This Test Report serves solely to summarise the results of testing carried out for the CCTM Scheme and should not be taken as an endorsement or otherwise of the IS Product or Service.

#### 9 Abbreviations

The following terminology is used within this Test Report

**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+ will not allow the encryption of Windows essential folders. User folders are folders that can be created by the user.

## **CCTM Test Report Summary**

### **DESlock+ v3.2.7**

**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