



## CCTM IA CLAIMS DOCUMENT (ICD) BeCrypt

<b>DISK Protect</b>
<b>Version 5.2</b>

VENDOR DETAILS	TEST LABORATORY DETAILS
BeCrypt Limited	Sogeti UK Ltd
130 Shaftesbury Avenue London W1D 5EU United Kingdom	1-9 Memel Street London EC1Y 0UT United Kingdom
Telephone Number: +44(0)203 145 1050	Telephone Number: +44(0)207 014 8900
Email: info@becrypt.com	Email: ian.mcewen@sogeti.com
Website: www.becrypt.com	Website: www.sogeti.com

CERTIFICATE DETAILS	
CCTM Certificate Number	2009/11/0059
CCTM Awarded on	3 <sup>rd</sup> November 2009
CCTM Award Expires on	2 <sup>nd</sup> November 2011
ICD Issue Date	3 <sup>rd</sup> November 2009

**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 PRODUCT/SERVICE DESCRIPTION .....	4
2.1	Product Identification .....	4
2.2	Product/Service Overview .....	4
2.3	Usage assumptions .....	7
3	CCTM CLAIMS FOR THE IS PRODUCT .....	11
3.1	Claims Statements.....	11
3.2	Existing Assurance Certificates .....	14
Annex A	Glossary Of Terms.....	15
Annex B	Marketing Statement.....	17

# 1 INTRODUCTION

## 1.1 Background

This document outlines the IA claims made by “*BeCrypt Ltd.*” in regard to the suitability of “*DISK Protect*” for use by the UK Public Sector for a full-disk encryption product for Windows based operating systems providing up to three layers of security including full disk encryption, strong pre-boot authentication, and optional removable media encryption.

## 1.2 Objectives

1.2.1 The objectives of this ICD are to:

- Provide a basis for the CESG Claims Tested Mark (CCTM) scheme assessment of the product; and
- Act as the basis of an agreement between the vendor and the CCTM Secretariat regarding marketing claims for the certified product.

## 1.3 Purpose of Document

1.3.1 This document is the ICD for the DISK Protect Version 5.2 product.

1.3.2 This ICD is the baseline document for the CCTM Claims Test of DISK Protect Version 5.2.

## 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 DISK Protect Version 5.2 and all the information related to the security of DISK Protect Version 5.2
- Section 3 details the security functionality claims that are being made.

## 2 IS PRODUCT/SERVICE DESCRIPTION

### 2.1 Product Identification

Product Name: DISK Protect.

Version: 5.2.12

Platforms:

Client (Host)
Windows XP Professional Edition SP3
Windows Vista Business Edition SP1

### 2.2 Product/Service Overview

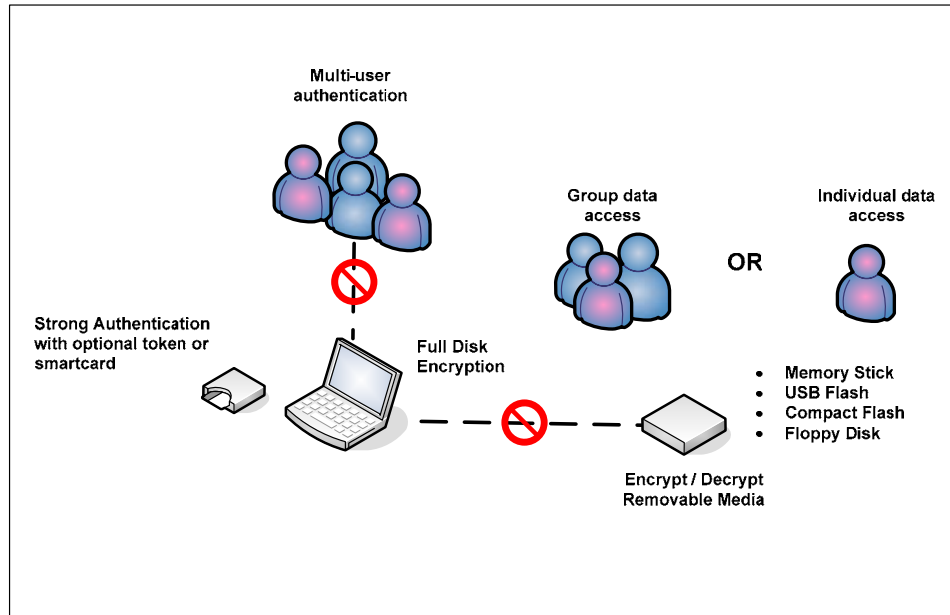
DISK Protect is a full-disk encryption product for Windows operating systems. DISK Protect provides up to three layers of security: full disk encryption, strong pre-boot authentication, and optional removable media encryption.

Features of the software include:

- **Full Disk Encryption:** DISK Protect encrypts a computer's hard disk(s) using 128 or 256 bit AES data encryption. After successful authentication, data is automatically decrypted and re-encrypted on the fly. If anyone attempts to bypass authentication the data is encrypted and unintelligible.
- **Pre-Boot Authentication:** DISK Protect can be configured to authenticate the user by password, by USB token or smart card and PIN. Authenticating the user pre-boot allows DISK Protect to encrypt the entire hard drive, including the Operating System, which ensures that data cannot be accessed using low level tools.
- **Removable Media Encryption:** Optional removable media encryption secures data on removable storage devices and floppy disks.
- **Multiple User Support:** DISK Protect supports one or more DISK Protect Administrator and multiple user accounts per protected machine. The hard disk is encrypted using a single encryption key but each user has a unique password or password and token.
- **Single Sign On (SSO) into Windows:** This feature simplifies start up by synchronising the user's DISK Protect and Windows passwords allowing users to automatically log into Windows. DISK Protect

supports integration with Windows logon for both password and token based authentication. If authentication is by smart card (RSA SecurID, Gemalto and Alladin), the integration provides automatic PIN entry to confirm the user's Windows certificate.

- **Secure Hibernation:** Hibernation allows a computer to start up rapidly by storing an image of system memory at shutdown. DISK Protect intercepts the hibernation process, encrypting the hibernation file as it is written to disk and decrypting it on start up, allowing the system to boot rapidly with no threat to security.
- **Device Recovery:** Crypto Officers can perform machine unlocking for users that have forgotten their passwords or lost their tokens. The user must contact the Crypto Officer and provide the challenge code, which is then used to generate a **response code** that must be entered into the locked computer to regain access. The user is then allowed to update the password. At no time in this procedure is the user's original password exposed. Alternatively, Crypto Officer credentials may be used to log in to Windows, and use the Management Tool to reset the user's password.
- **Package Installation:** DISK Protect may be installed and configured on individual client computers; or installed on multiple client computers via an Installation Package and then (for security reasons) each machine must be configured with a password and a unique encryption key.
- **Token Support:** DISK Protect supports **Aladdin eToken™**, **Common Access Card (FIPS-201 Compliant)**, **Common Access Card (Javacard)**, **Gemalto .NET** and **RSA SecureID®** smart cards to provide dual-factor authentication. Extended smart card support allows an organisation to use a card that is already part of its security systems, issuing its staff with a single card for access control and authentication.



**Figure 1. High Level Functional Overview**

### 2.2.1 Security architecture

DISK Protect is a full-disk encryption product for Windows based operating systems. DISK Protect encrypts all data on a computer hard drive including operating system files. The product includes a boot-loader component that requires user authentication to be completed before the custom BeCrypt driver is primed with the disk encryption key so that on-the-fly encryption and decryption can commence. The user authentication process includes password entry, and token based secondary authentication using a USB token or smartcard device.

Security offered by DISK Protect may be summarised as:

- Encryption of all data on a computer's hard drive with a valid implementation of the AES algorithm using either a 128 or 256 bit key;
- Password based user authentication at system boot time;
- Optional token-based secondary authentication via USB tokens or smartcards;
- Optional encryption of removable media and floppy disks.

### 2.2.2 Hardware requirements

Laptops or desktops with X86 based processors and 30MB disk space

### 2.2.3 Software requirements

Software: DISK Protect version 5.2

### 2.2.4 Out of Scope

The cryptographic algorithms used in DISK Protect Version 5.2 are not tested under the CCTM Scheme and are out of scope for this assessment.

The product allows for the selection of either 128 bit or 256 bit AES encryption. However, for the purposes of this assessment only 256 bit AES will be used, 128 bit encryption is out of scope.

The product operates a wide variety of Windows PC platforms, as listed below:

- Microsoft Windows Vista (SP1)
- Microsoft Windows XP (SP1, SP2, SP3)
- Microsoft Windows XP Tablet
- Microsoft Windows 2000 Professional (SP4)
- Microsoft Windows Server 2003

However, for the purposes of this claims test only Windows Vista (SP1) and Windows XP (SP3) will be used; all others are out of scope for this assessment.

The uses of optical disks (CD or DVD) are excluded from being tested as removable media.

The use of DISK Protect Version 5.2 in handling data above IL2 is out of scope for this assessment.

## 2.3 Usage assumptions

### 2.3.1 Assets

Assets to be protected include any data and IPR at IL1 or IL2 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 via introduction of removable storage devices to the client.

### 2.3.2 Threat scenario

Threats to assets which are countered are:

- Unauthorised access to data at rest on the client PC, laptop or server through use of low level recovery tools that can mount the disk image and circumnavigate the boot authentication process.
- Unauthorised access to data held on removable memory devices encrypted with DISK Protect.
- Inappropriate data transfer from the client to an unauthorised removable storage device.

#### 2.3.2.1 Expected operational environment

- DISK Protect operates on a standard Windows operating system environments running on general IBM PC architectures. Non-windows partitions may be optionally encrypted.
- DISK Protect optionally supports encryption of removable storage media. It is also optionally possible to prevent unencrypted removable storage devices from being used on machines fitted with DISK Protect.
- DISK Protect supports one or more DISK Protect Administrator and multiple user accounts per protected machine, however, only a single authorised user may gain access to the mobile computing device simultaneously after authentication.
- DISK Protect can be easily rolled out to large install bases (from hundreds of users to hundreds of thousands) using standard software deployment tools.

#### **Business Benefits**

The DISK Protect product can provide the following business benefits;

- Reduced risk to your business from threat models such as: inquisitive and / or disgruntled staff, industrial espionage from competitors, criminals or others focusing on targeted data theft from laptops for network access.
- Lost or Stolen Laptops - In the statistical likelihood that laptops are lost or stolen that all government, corporate, customer and partner information remains confidential.

- Reduced Expensive Auditing Costs - Full disk and removable media encryption helps reduce the internal requirement and cost to audit specific types or categories of information that a user has stored on their laptop or removable devices.
- Aid adherence to corporate compliance issues (ISO 27001, SOX, BASLE II) and US legal requirements - Senate Bill 1386 and Assembly Bill 700, effective July 1, 2003.
- Scalable for the enterprise. DISK Protect can be easily deployed in small to large corporate organisations.
- Some organisations may save costs on disposal once encryption has been implemented onto a device because they no longer see the need to send the device to have the hard disk purged or decommissioned at the end of the device's life.
- Secure management of removable storage within the organisation, by restricting use to authorised users and even optionally mandating that encrypted media is used always.

### 2.3.2.2 Organisational security policies

DISK Protect is designed to work in line with an organisations security policy. Policy can be applied at machine level as per the organisations requirements.

When deploying DISK Protect, it is important to recognise the two operational roles supported by DISK Protect, i.e., the DISK Protect administrator or Crypto Officer and the standard user.

### 2.3.2.3 Security requirements on the environment

Users and Crypto Officers must observe conventional good security practices as per their organisations security policies when using DISK Protect, including:

- using strong passwords and not writing passwords down;
- changing passwords on a regular basis;
- not sharing credentials between users or Crypto Officers;
- not sharing tokens between users or Crypto Officers;
- not leaving the system unattended and logged-in in environments that are unsecured. It is recommended that the machine should be powered down or hibernated when the system is not being used;
- To minimise data leakage in an organisation, it is recommended that removable media should be used with encryption turned on.
- Auditing the use of DISK and media keys.

Only Crypto Officers with DISK Protect Administrative Privileges may carry out configuration (operational policy and user policy), maintenance and recovery tasks. It is recommended that standard users should not be given sufficient rights to:

- change the local security policy settings;
- stop or start services on the system;
- install or uninstall services;
- install or uninstall system software;
- Modify registry settings.

### 3 CCTM CLAIMS FOR THE IS PRODUCT

#### 3.1 Claims Statements

Unique Reference	Claim Statements
	<b>Encryption</b>
<i>BC001</i>	The product will encrypt all Windows partitions on one or more internal hard disk drives on the platform on which it is installed
<i>BC002</i>	The product will encrypt Windows and Non Windows partitions on internal hard disk drives on the platform on which it is installed
<i>BC003</i>	Under the control of an authorised Administrator, it is possible to configure the product to enable the encryption of items of removable storage media
<i>BC004</i>	Under the control of an authorised Administrator, it is possible to configure the product to disable the encryption of items of removable storage media
<i>BC005</i>	When appropriately configured, the product will encrypt items of removable media mounted on the platform on which it is installed
<i>BC006</i>	The product will provide the means to read items of removable storage media which it has encrypted
<i>BC007</i>	When appropriately configured, the product will prevent the use of items of removable storage media which it has not encrypted, on the platform on which it is installed
<i>BC008</i>	DISK Protect can be installed in either of the following configurations: <ul style="list-style-type: none"> <li>• fixed disk encryption only</li> <li>• removable media encryption only</li> </ul> or both fixed disk and removable media encryption
<i>BC009</i>	Items of removable storage media which have been encrypted by the product may be shared by users or groups of users on a local machine or different machines via the use of a media key
<i>BC010</i>	Media keys may be exported or imported (in encrypted format) to facilitate sharing of encrypted removable media between users on the same or different machines.
<i>BC011</i>	DISK Protect provides a facility to securely decommission a PC. All pre-boot data including the protected encryption key is destroyed, rendering the PC unbootable and any data held on it remains encrypted.
	<b>Access Control</b>
<i>BC012</i>	The product will support multiple accounts (maximum 14) on a single machine, in single user mode, for password method of boot time authentication.
<i>BC013</i>	The product will support multiple accounts on a single machine, in single user mode, for token based boot time authentication

<b>BC014</b>	Token users may be given access to multiple machines, protected by DISK Protect, via administrator controlled registration of their token details to those machines.
<b>BC015</b>	The product supports Single Sign On into Windows XP and Vista, for boot time authenticated users using password authentication. It also supports Single Sign On into Windows XP for boot time authenticated users using token based (Gemalto and Aladdin) authentication and into Windows Vista for boot time authenticated users using token based (Gemalto, Aladdin and RSA5200) authentication
	<b>Identification and Authentication</b>
<b>BC016</b>	The product provides boot time authentication of users using a password and user identity
<b>BC017</b>	The product supports boot time authentication of users using hardware tokens and an associated PIN
<b>BC018</b>	The product provides boot time support for Aladdin eToken, Common Access Cards (FIPS-201 and Javacard versions), Gemalto .NET and RSA SecureID smart cards.
	<b>Administration and Management</b>
<b>BC019</b>	Under the control of an Administrator, it is possible to enforce a local machine policy for manual creation of passwords, including: <ul style="list-style-type: none"> <li>• Password lifetime</li> <li>• Password length</li> </ul> Password format
<b>BC020</b>	Under the control of an authorised Administrator, the product will enforce the generation and use of strong passwords rather than allowing manual password creation
<b>BC021</b>	The product will ensure that the creation of accounts on a machine is under the control of an authorised individual
<b>BC022</b>	The product will ensure that the deletion of accounts on a machine is under the control of an authorised individual, and that it is not possible to delete the last Administrator account
<b>BC023</b>	Under the control of an authorised individual, the product will perform machine unlocking in cases where users have forgotten their passwords or lost their tokens; New tokens will require administrator registration of their token details to those machines.
<b>BC024</b>	DISK Protect can be deployed via packages using standard tools.
<b>BC025</b>	The product provides a media keyfile creation utility to generate keys for use on items of removable storage media.
<b>BC026</b>	The product provides a RSA key creation utility to create RSA keypairs for protection of recovery.
<b>BC027</b>	The product ensures that administration functions and features are kept under access control
	<b>Audit</b>

<b>BC028</b>	DISK Protect audits encryption status events
<b>BC029</b>	The product provides the facility for users and administrators to view the encryption status of a machine on which it is installed
	<b>Fault Tolerance</b>
<b>BC030</b>	The product will survive abrupt power down incidents; if the laptop battery is discharged completely or the power is removed during the encryption wave, DISK Protect will resume encryption from the point where it stopped and continue until the encryption wave is completed

### 3.2 Existing Assurance Certificates

All cryptographic functionality including cryptographic algorithms and security services are implemented via BeCrypts FIPS 140-2 approved cryptographic library (Certificate no. 1025).

<http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140crt/140crt1025.pdf>

## Annex A Glossary Of Terms

Terms	Definitions
AES	Advanced Encryption Standard is a block cipher adopted as an encryption standard by the U.S. government
BASLE II	Basle II is an advanced approach for calculating risk-based capital requirements: the advanced internal ratings-based (IRB) approach for credit risk and the advanced measurement approaches (AMA) for operational risk.
BeCrypt Disk Protect Removable Media Encryption	BeCrypt™ DISK Protect is an enterprise security solution designed to ensure reduced operational risk by encrypting the data written to removable media and may either employ a personal Encryption Key or a shared Encryption Key (allowing authorised users to exchange protected data).
CCTM	CESG Claims Tested Mark
CD	Compact Disc
CF	Compact Flash, a solid state memory technology.
Crypto Officer	These accounts have Trusted Client Platform and Windows system administrative privileges. Crypto officers can perform operational, administrative and maintenance tasks using Trusted Client Platform management utilities.
DVD	Digital Video (Versatile) Disc an optical disc storage media format that can be used for data storage.
FIPS	Federal Information Processing Standard
Flash Memory	Non-volatile computer memory that can be electrically erased and re-programmed.
Group Policy	Group Policy is a feature of Microsoft Windows family of operating systems and provides centralised management and configuration of computers and remote users in an Active Directory environment. Group Policy can also be used to distribute and control software installation in the same environment.
Hash	A complex digital signature calculated to uniquely identify each executable file that can be run. The hash is calculated using the SHA-1 algorithm, which takes into account the entire binary content of the file.
HDD	Hard Disk Drive
ICD	Information Assurance Claims Document
IPR	Intellectual Property Rights
OEM	Original Equipment Manufacturer
'On the fly'	'On the fly' describes activities that develop or occur dynamically rather than as the result of something that is statically predefined.
OS	Operating System
PC	Personal Computer
PIN	Personal Identification Number
Removable Media	External storage devices which can be used to easily move data between

	computers with the right readers.
SP	Service Pack
SHA-1 algorithm	Secure Hash Algorithm 1, as defined in the Federal Information Processing Standards Publication 180-1. This algorithm produces a one-way 160-bit hash that can be used for a variety of applications including authentication and cryptography.
SD	Or SD card, Secure Digital card, flash memory card format used for data storage.
SOX	Sarbanes-Oxley Act of 2002 (Pub. L. No. 107-204, 116 Stat. 745, also known as the Public Company Accounting Reform and Investor Protection Act of 2002)
USB	Universal Serial Bus
USB flash drive	USB flash drives are flash memory data storage devices integrated with a USB interface. They are typically small, lightweight, removable and rewritable

## **Annex B Marketing Statement**

BeCrypt™ DISK Protect V.5.2 is a feature rich enterprise security solution designed to ensure reduced operational risk by protecting information on PCs and removable media, such as Floppy disks accessed through a USB floppy disk drives, USB memory sticks, USB External Hard Drives, SD cards through a usb card reader, CF cards through a usb card reader on which critical information could be compromised if lost or stolen. It is a flexible and scalable solution that is easy to design, deploy and support in line with organisational security requirements on a range of Windows™ XP Professional Edition SP3 and Windows Vista Business Edition SP1 platforms. Implementation and ongoing management can be achieved with a low Total Cost of Ownership.