Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2009/64

12 Nov 2009

Version 1.0

Amendment Record

Version	Date	Description
1.0	12/11/2009	Public Release

Executive Summary

1 The target of evaluation (TOE) is the Becrypt DISK Protect v5.2.9 Build 36 which is a full-disk encryption product for Windows-based operating systems. It encrypts all data on a computer hard drive, including user data, the TOE executables when the TOE is not loaded and the operating system files when the operating system is not running.

2 This report describes the findings of the IT security evaluation of the TOE to Common Criteria (CC) evaluation assurance level EAL2. The report concludes that the TOE has met the target assurance level of EAL 2 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by stratsec and was completed in October 2009.

3 With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that:

a) The TOE is used only in its evaluated configuration;

b) The TOE is operated according to it's guidance documentation. (Ref [3]);

c) TOE administrators should configure the TOE password policies to meet or exceed the organisational password policies (a risk assessment for the host device may require a stricter policy to be enforced); and

d) Access to recovery files (.brf) generated by the TOE for challenge-response recovery must be strictly controlled. This is because neither the recovery console application nor the recovery files require user authentication and recovery files are used to generate responses for the challenge-response recovery.

4 This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

5 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target at Ref [1] and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

6 This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

7 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, DISK Protect v5.2.9 Build 36, against the requirements of Common Criteria (CC) evaluation assurance level EAL2, and

b) provide a source of detailed security information about the TOE for any interested parties.

8 This report should be read in conjunction with the TOE's Security Target (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

9 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	DISK Protect v5.2.9 Build 36
Software Version	5.2.9 Build 36
Security Target	Becrypt DISK Protect v5.2.9 Security Target EAL2 Version 1.0
Evaluation Level	EAL 2
Evaluation Technical Report	Becrypt DISK Protect v5.2.9.36 EAL2 Evaluation Technical Report 1.0, October 2009
Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1, September 2007 with interpretations as of 20 January 2009.
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2007, Version 3.1 Revision 2, CCMB-2007-09-004 with interpretations as of 20 January 2009.
Conformance	Common Criteria Part 2 conformant Common Criteria Part 3 conformant
Sponsor/Developer	Becrypt Limited 90 Long Acre, Covent Garden, London, WC2E 9RA, United Kingdom
Evaluation Facility	stratsec Suite 1 50 Geils Court, Deakin, ACT 2600 Australia

Chapter 2 - Target of Evaluation

2.1 Overview

10 This chapter contains information about the Target of Evaluation (TOE), including: a description of functionality provided; its architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

11 The TOE is DISK Protect v5.2.9 Build 36 developed by Becrypt.

12 The TOE is a full-disk encryption product for Windows-based operating systems. It encrypts all data on a computer hard drive, including user data, the TOE executables when the TOE is not loaded and the operating system files when the operating system is not running. The user authentication mechanism is password-based by default, however, the TOE also supports secondary authentication using a USB token or smartcard device. The TOE performs AES encryption of all data on a computer's hard drive using a 128-bit or 256-bit key with a password-based user authentication performed at system boot time.

13 The TOE prevents the host system from booting until after the user has successfully been identified and authenticated. The TOE provides a challenge-response recovery mechanism for administrator-assisted user access in the event of a forgotten password.

2.3 Security Policy

14 The TOE Security Policy (TSP) is a set of rules that defines how the information within the TOE is managed and protected.

The Security Target (Ref [1]) contains no explicit security policy statements, the following TOE Security Policies (TSPs) are implied:

- The TOE will not allow access to protected resources until the user is successfully identified and authenticated;
- The TOE identifies and authenticates users on the basis of either:
    a) user supplied identifier and password; or
    b) user supplied identifier and correct response to a TOE generated challenge; or
    c) hardware token and PIN.
- A TOE administrator is required to generate the correct response to a TOE generated challenge.

2.4 TOE Architecture

15 The TOE consists of the following major architectural components:

a) Initialisation module – responsible for the initial generation of the disk encryption key, the configuration of the TOE parameters and management of TOE users.

b) Encryption module – responsible for the initial encryption of the disk drive, interception of low level disk I/O function calls to perform real time encryption and decryption of data stored on the disk and the decryption of the disk when the TOE is decommissioned.

c) Authentication module – responsible for performing pre-boot identification and authentication of users, loading the encryption module and starting the boot process

d) Hibernation module – responsible for interception of system hibernation function calls to ensure that the hibernation file is encrypted and decrypted as required.

e) Administrative Interface – separate component of TOE used to generate responses to the TOE generated challenges during challenge-response user recovery operations.

16 The TOE is represented by the following subsystems:

a) PC interface subsystem,

b) Protected mode driver subsystem,

c) Real mode subsystem, and

d) User mode driver subsystem.

17 The identified subsystems and the environment have been illustrated in Figure 1 below.

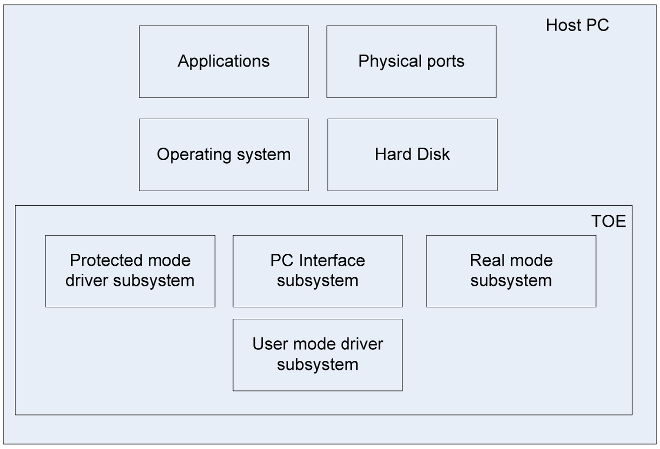

Figure 1 The Subsystems of the TOE

18 The ‘PC interface subsystem’ constitutes all the hardware, firmware and software needed for connecting the TOE to the necessary operating system and hardware components of the host PC. As the TOE does not include the operating system of the host PC or any of the hardware components of the host PC, it implements a security layer on top of the hardware layer to intercept essential operating system calls and to mediate access to the hardware so that the security measures are independent of the hardware and not visible to the hardware devices.

19 The ‘Protected mode driver subsystem’ implements AES encryption and provides protection of user data and protection of the hibernation file.

20 The ‘Real mode subsystem’ contributes towards user authentication and secure boot-up. It also supports data protection by processing the data for reads and writes and determining if that data needs to be encrypted or decrypted. In addition, it also supports secondary authentication which is outside the scope of the TSF.

21 The ‘User mode driver subsystem’ contains the user-mode applications of the TOE. They interact with the protected-mode encryption driver during product installation, password change events and event auditing. Additionally, user-mode applications are used for product configuration.

2.5 Clarification of Scope

22 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]) and includes only the Becrypt DISK Protect software. The optional removable media encryption, multiple-user support, single sign-on, package installation and token support is not part of the TOE.

23 The device recovery console used to recover the TOE from lockdown mode is not part of the TOE but is a valid interface to recover the TOE and has been used in testing the security feature – this application is included in the install media and, if used, the user data associated with it must be strictly controlled to prevent bypass of the TOE security functionality.

2.5.1 Evaluated Functionality

24 The TOE provides the following evaluated security functionality:

a) Full disk encryption.;

b) Secure hibernation;

c) Device recovery; and

d) Pre-boot authentication.

2.5.2 Non-evaluated Functionality and Services.

25 Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information Security Manual

(ISM) (Ref [2]) for policy relating to using an evaluated product in an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

26 The functions and services that have not been included as part of the evaluation are identified below:

a) **Removable media encryption.** The TOE encrypts mass storage devices, such as USB memory sticks and floppy disks, to protect data in transit.

b) **Multiple user support.** The TOE allows more than a single user to gain access to an encrypted hard disk. All data is encrypted with a single key but several user accounts may be created, each with a unique username password combination, to access the key.

c) **Single Sign-on.** The TOE synchronises the user's password and Windows passwords to allow users to automatically log into Windows. The TOE can be integrated with Windows logon for both password and token based authentication. In the case of smart card based authentication the integration also provides automatic PIN entry to confirm the user's Windows certificate.

d) **Package installation.** The TOE may be installed and configured on individual client computers or on multiple client computers via an Installation Package. After installation to multiple clients each PC must be configured with a password and a unique encryption key.

e) **Token support.** The TOE supports a number of smart cards and USB tokens for dual-factor authentication. Extended smartcard support allows an organisation to use a card that is already part of its security systems, providing it's staff with a single card for access control and authentication.

2.6 Usage

2.6.1 Evaluated Configuration

27 This section describes the configuration of the TOE that was included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in this defined evaluated configuration. Australian Government users should refer to the ISM (Ref [2]) to ensure that configuration meet the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

28 The evaluated configuration of the TOE is based on the default installation of the TOE. A host PC is required for power and connectivity. The host PC must run the operating system platform on which the TOE executes. The host PCs and operating system platforms supported are any X86 based processors running Windows XP (SP1, SP2, SP3), Windows 2000 SP4, Windows 2003 Server and Windows Vista Operating Systems.

2.6.2 Delivery procedures

29 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product.

30 The TOE is delivered to customers via download from a Becrypt FTP server. TOE customers are issued with a temporary login credential and link to the correct location. The ISO image is burnt to CD by the customer prior to installation.

31 The software cannot be installed without a product key, which is delivered to the customer via email.

2.6.3 Determining the Evaluated Configuration

32 The downloaded ISO image file can be verified and validated by calculating a SHA-1 hash of the file and comparing it to the developer supplied value: D40A73FFD3FC94EC6D878B55DE4B05C50EE0CE2F

33 The file properties for each of the TOE executables should be queried to confirm that they are DISK Protect v5.2.9 Build 36 (the recoveryconsole.exe should be DISK Protect v5.2).

2.6.4 Documentation

34 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation (Ref [3]) is provided with the TOE:

a) DISK Protect 5.2 Administration Guide, 01 April 2009;

b) DISK Protect 5.2 User Guide, 09 April 2009;

c) DISK Protect 5.2 Client User Guide, 25 March 2009;

d) DISK Protect 5.2 Removable Media Module Administration Guide, 01 April 2009;

e) DISK Protect 5.2 Removable Media Module User Guide, 01 April 2009; and

f) DISK Protect 5.2 MediaViewer User Guide, 25 March 2009.

2.6.5 Secure Usage

35 The evaluation of the TOE took into account certain assumptions about the TOE and its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

36 The following assumptions were made:

a) **A.PASSWORD:** The end users of the TOE are aware of the importance of the quality of passwords to the security of the TOE and the sensitive data residing on the hard disk of the host PC and only select passwords of good quality when initialising the TOE. End users also keep the passwords secret and do not write them down or disclose them to any other system or user.

37 In addition, the following organisational security policies must be in place:

a) **OSP.OS_CONF:** The operating system of the host PC is configured to be secure and preventing end users from having administrative rights is of particular concern. Furthermore, the credentials for entering an administrative role within the OS are sufficiently secure to prevent with a high likelihood, unauthorised, potentially malicious users from succeeding in becoming administrators.

Chapter 3 - Evaluation

3.1 Overview

38 This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

39 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 2 (Refs [4], [5] and [6]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 2 (CEM) (Ref [7]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [8], [9], [10] and [11]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [12]) were also upheld.

3.3 Functional Testing

40 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers. The evaluators also developed and executed independent tests of the TOE's security functionality.

3.4 Penetration Testing

41 The evaluators performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE.

42 This analysis included a search for possible vulnerability sources using publicly available information and an examination of the developer's design documentation. The evaluators estimated the attack potential required to exploit each identified potential vulnerability. The evaluators then devised and executed penetration tests to confirm their initial estimation of attack potential.

43 The evaluators were unable to find any vulnerability that could be exploitable by an attacker with Basic attack potential only.

Chapter 4 - Certification

4.1 Overview

44 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Certification Result

45 After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref [13]), the Australasian Certification Authority (ACA) certifies the evaluation of DISK Protect v5.2.9 Build 36 performed by the Australasian Information Security Evaluation Facility, stratsec.

46 stratsec has found that DISK Protect v5.2.9 Build 36 upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL2.

47 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

48 EAL2 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and interface specification, guidance documentation and a basic description of the architecture of the TOE, to understand the security behaviour.

49 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with a basic attack potential.

50 EAL2 also provides assurance through use of a configuration management system and evidence of secure delivery procedures.

4.4 Recommendations

51 Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref [2]) and New Zealand Government users should consult the GCSB.

52 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [3]), the ACA also recommends that :

a) TOE administrators should configure the TOE password policies to meet or exceed the organisational password policies (a risk assessment for the host device may require a stricter policy to be enforced);

b) Access to recovery files (.brf) generated by the TOE for challenge-response recovery must be strictly controlled. Neither the recovery console application nor the recovery files require user authentication, and recovery files are used to generate responses for the challenge-response recovery.

Annex A - References and Abbreviations

A.1 References

[1] Becrypt DISK Protect v5.2.9 Security Target EAL2 Version 1.0, November 2009

[2] Australian Government Information Security Manual (ISM), September 2009, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] User Documentation suite comprising:

a) DISK Protect 5.2 Administration Guide, 01 April 2009

b) DISK Protect 5.2 User Guide, 09 April 2009

c) DISK Protect 5.2 Client User Guide, 25 March 2009

d) DISK Protect 5.2 Removable Media Module Administration Guide, 01 April 2009

e) DISK Protect 5.2 Removable Media Module User Guide, 01 April 2009

f) DISK Protect 5.2 MediaViewer User Guide, 25 March 2009

[4] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 3.1, Revision 1, September 2006, CCMB-2006-09-001

[5] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components (CC), Version 3.1, Revision 2 , September 2007, CCMB-2007-09-002

[6] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components (CC), Version 3.1, Revision 2, September 2007, CCMB-2007-09-003

[7] Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1, Revision 2 September 2007, CCMB-2007-09-004

[8] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[9] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.3, September 2007, Defence Signals Directorate.

[10] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, Defence Signals Directorate.

[11] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4. Version 3.1, 29 September 2006, Defence Signals Directorate.

[12] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

[13] Becrypt DISK Protect v5.2.9.36 EAL2 Evaluation Technical Report 1.0, October 2009

A.2 Abbreviations

ACA	Australasian Certification Authority
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
ISO	International Organisation for Standardization.
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SHA	Secure Hash Algorithm
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy