Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2009/63

5 Nov 2009

Version 1.1

Amendment Record

Version	Date	Description
1.1	05/11/2009	Public release.

Executive Summary

1 The Target of Evaluation (TOE), Trusted Client 2.3, is a bootable operating environment that resides on an encrypted USB storage device which allows users to use an unprotected or unmanaged computer for remote access to their corporate IT systems. The intent of the TOE is to provide customers with a secure and low cost remote access solution.

2 The functionality defined in the Security Target that was subsequently evaluated is as follows:

- **Trusted environment and isolation.** The TOE provides a Linux based operating system that is isolated from the hard disk of the Host PC and protects the sensitive user data from exposure to the potentially hostile Host PC. The operating system is part of the TOE, but the web browser, thin-clients and other applications residing in the trusted environment are not part of the TOE.
- **Encryption and authentication.** The TOE protects all data on the TOE device including (the operating system files) by encryption using AES 256 and strong authentication.
- **Trusted configuration.** The TOE encrypts all configuration files on the TOE devices and the files cannot be altered by unauthorised users.
- **Device recovery.** The TOE allows forgotten passwords to be recovered through an administrator-assisted challenge-response mechanism. The mechanism uses specific recovery data generated during the initiation of the TOE.
- **Clone protection.** The TOE device automatically performs a self-test during boot-up. If it fails the clone test, the device erases the data.

3 This report describes the findings of the IT security evaluation of Becrypt’s Trusted Client 2.3, to the Common Criteria (CC) evaluation assurance level EAL2. The report concludes that the product has met the target assurance level of EAL2 and that the evaluation was conducted in accordance with the relevant criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by stratsec and was completed on 26 October 2009.

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

a) Care should be taken when configuring the network address restrictions. During the conduct of testing, the evaluators noticed that when configuring the network address restrictions, if a subnet mask is specified for an allowed address, the TOE applies the authorisation to the entire subnet.

b) As the application used to perform the administrator actions during challenge-response recovery does not require identification and authentication (and is common to both the Trusted Client and Disk Protect products), the recovery files used by these applications should be subject to strict access control to prevent unauthorised use.

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

6 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

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

1.2 Purpose

8 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Trusted Client 2.3, against the requirements of the Common Criteria (CC) evaluation assurance level EAL2; and

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

9 This report should be read in conjunction with the TOE's Security Target at 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

10 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	Trusted Client 2.3
Software Version	2.3
Security Target	Becrypt Trusted Client v2.3 Security Target EAL2, version 1.0, October 2009
Evaluation Level	EAL2
Evaluation Technical Report	Becrypt Trusted Client EAL2 Evaluation Technical Report 1.0, October 2009
Criteria	Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1 Revision 2, 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
Conformance	Part 2 conformant. Conforms with Common Criteria for Information Technology Security Evaluation Part 2: Security

	functional requirements, version 3.1, Revision 2. Part 3 conformant, EAL2. Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, Revision 2. Evaluation level is EAL2.
Sponsor and Developer	Becrypt Limited 90 Long Acre, Covent Garden, London WC2E 9RA United Kingdom
Evaluation Facility	stratsec Suite 1/50 Geils Court, Deakin ACT

Chapter 2 - Target of Evaluation

2.1 Overview

11 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

12 The TOE is Trusted Client 2.3 developed by Becrypt.

13 The TOE is a bootable operating environment that resides on an encrypted USB storage device which allows users to use an unprotected or unmanaged computer for remote access to their corporate IT systems. The intent of the TOE is to provide customers with a secure and low cost remote access solution.

14 Trusted Client 2.3 is based on a Linux distribution that has been hardened and modified to provide additional security features such as encryption and restrictions on IO devices. The TOE is installed onto a user supplied USB storage device.

15 The following is a summary of the key security features of the TOE:

- The TOE employs file system encryption to protect the TOE software from modification and to protect user and session data from disclosure;
- Users must be identified and authenticated before the TOE will boot;
- Self-integrity checks are performed during the boot process;
- Once booted, the TOE cannot access the fixed storage media on the host machine – this prevents data spillage from the corporate network to the host machine;

- The TOE can be configured (using a white list) to restrict network connectivity on the basis of network address, protocol and port number.

2.3 Security Policy

16 The Security Target at Ref [1], contains no explicit security policy statements.

2.4 TOE Architecture

17 Trusted Client 2.3 is a Linux-based operating environment that is installed on a portable USB storage device. It provides a GUI for users to launch remote access client software (such as Citrix client and Cisco VPN client), a web browser and an email client. The scope of the TOE does not include these client applications.

18 The kernel has been modified to prevent any access to the TOE host's fixed storage media.

19 The TOE is represented by the following subsystems:

- Interface subsystem,
- Authentication subsystem,
- Cryptographic subsystem,
- OS Kernel, and
- Initialization subsystem.

2.5 Clarification of Scope

20 The scope of the evaluation was limited to those claims made in the Security Target at Ref [1].

21 The scope of the evaluation includes only the Becrypt Trusted Client trusted environment. The USB flash drive that it resides in is not included in the evaluation. The thin-client applications hosted on the TOE are not within the scope of the TOE. The TOE consists of two distinct software components:

- the Trusted Client operating environment; and
- the software used to configure and recover the Trusted Client environment.

2.5.1 Evaluated Functionality

22 The functionality defined in the Security Target that was subsequently evaluated is as follows:

23 **Trusted environment and isolation.** The TOE provides a Linux based operating system that is isolated from the hard disk of the Host PC and protects the sensitive user data from exposure to the potentially hostile Host PC. The operating system is part of the TOE, but the web browser,

thin-clients and other applications residing in the trusted environment are not part of the TOE.

24 **Encryption and authentication.** The TOE protects all data on the TOE device including (the operating system files) by encryption using AES 256 and strong authentication.

25 **Trusted configuration.** The TOE encrypts all configuration files on the TOE devices and the files cannot be altered by unauthorised users.

26 **Device recovery.** The TOE allows forgotten passwords to be recovered through an administrator-assisted challenge-response mechanism. The mechanism uses specific recovery data generated during the initiation of the TOE.

27 **Clone protection.** The TOE device automatically performs a self-test during boot-up. If it fails the clone test, the device erases the data.

2.5.2 Non-evaluated Functionality

28 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) at 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).

29 The following functionality defined in the Security Target (and identified as not part of the TOE) was not in the scope of the evaluation:

30 **Dual factor authentication.** The TOE supports additional dual factor authentication using smart cards such as the US Department of Defence issued Common Access Card.

31 **Management.** The TOE device can automatically contact a management server, if configured, on boot-up so that the boot-up details may be viewed by the administrator.

2.6 Usage

2.6.1 Evaluated Configuration

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

33 The evaluated configuration is derived from the Security Target at Ref [1] and is based on the default installation of the TOE. The host PC is required for power and connectivity and must run a BIOS that controls the USB interfaces. The supported platforms are any general x86 PC platforms with

either Intel or AMD processors that allow booting from USB devices. The following options are configured:

- No un-encrypted partitions on the USB media;
- Challenge-response recovery enabled;
- IP address network restrictions must be enabled;

34 During testing, the TOE was configured with the optional un-encrypted partition to test the storage device access control policies.

35 The TOE relies on the following hardware:

a) USB Removable Storage Device (minimum capacity of 1GB);

b) Host machine configured to boot from USB.

2.6.2 Delivery procedures

36 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.

37 The ISO downloaded image is burnt to a CD by the customer prior to installation.

38 A product key is delivered to the customer via email. This product key is required to install the Trusted Client configuration software. This software is used by the customer to configure the Trusted Client operating environment and to write the operating environment to a suitable USB storage device.

2.6.3 Determining the Evaluated Configuration

39 The evaluated product may be verified in the first instance by the fact that it is obtained direct from the developer's FTP site. The file properties for each of the TOE executables should be queried to confirm that they are Trusted Client v2.3 (the recoveryconsole.exe should be DISK Protect v5.2).

40 The guidance supplement provides the following hash value that can be used to verify the integrity and validity of the ISO image:

File Name	TC 2.3.0 24-09-2008.iso
SHA-1 Hash	E73859B4289866A9810882F6E42E53FAE12BBD07

41 The version number of the TOE is displayed (or can be queried) at multiple points during the installation, configuration and operation of the product.

42 When writing the configured TOE image to the target USB device, the writer application displays a screen showing the details of the configuration to be written to the device. The TOE version must be displayed as v2.3 in this screen.

43 The TOE pre-boot authentication dialogue should display the TOE version number in red type at the top left hand corner of the screen. Once the user

has authenticated and the desktop is loaded, a welcome screen is displayed which indicates the TOE version.

2.6.4 Documentation

44 The Trusted Client product includes the following documentation on the installation CD:

- Trusted Client v2.3 User Guide;
- Trusted Client v2.3 Administration Guide.

2.6.5 Secure Usage

45 The evaluators assumed that the TOE is primarily intended to be used to enable secure remote access to corporate systems for off-site employees without incurring an overhead for managing additional hardware.

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

Table 1 - Assumptions

Identifier	Assumption statement
A.APPL	The end users of the TOE are aware of the security issues of uploading and executing applications on the TOE and follow the regulations on application management established by the deploying organisation so that only approved applications are installed on the TOE.

Chapter 3 - Evaluation

3.1 Overview

47 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

48 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation at Refs [4], [5] and [6]. The methodology used is described in the Common Methodology for Information Technology Security Evaluation (CEM) at Ref [7]. The evaluation was also carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) at 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 at Ref [12] were also upheld.

3.3 Functional Testing

49 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.

3.4 Penetration Testing

50 Penetration testing was conducted based on an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description as well as available public information. The evaluators used these tests to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential.

51 The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit;

b) Specialist technical expertise required;

c) Knowledge of the TOE design and operation;

d) Window of opportunity; and

e) IT hardware/software or other equipment required for exploitation.

52 The evaluators were unable to successfully attack the TOE in the context of an attacker with Basic level attack potential.

Chapter 4 - Certification

4.1 Overview

53 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

54 After due consideration of the conduct of the evaluation as witnessed by the certifiers, and of the Evaluation Technical Report at Ref [15], the Australasian Certification Authority certifies the evaluation of Trusted Client 2.3 performed by the Australasian Information Security Evaluation Facility, stratsec.

55 stratsec has found that Trusted Client 2.3 upholds the claims made in the Security Target at Ref [1] and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL2.

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

4.3 Assurance Level Information

57 EAL2 provides assurance by a complete 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.

58 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.

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

4.4 Recommendations

60 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 the ISM at Ref [2] and New Zealand Government users should consult the GCSB.

61 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance documents are followed at Refs [3], [13], and [14], the ACA also recommends that:

a) Care should be taken when configuring the network address restrictions. During the conduct of testing, the evaluators noticed that if, when configuring the network address restrictions, if a subnet mask is specified for an allowed address, TOE applies the authorisation to the entire subnet.

b) As the application used to perform the administrator actions during challenge-response recovery does not require identification and authentication (and is common to both the Trusted Client and DISK Protect products), the recovery files used by these applications should be subject to strict access control to prevent unauthorised use.

Annex A - References and Abbreviations

A.1 References

[1] Becrypt Trusted Client v2.3 Security Target EAL2, version 1.0, October 2009

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

[3] Becrypt Trusted Client Assurance class AGD: Guidance documents EAL2, version 0.2, 12 May 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 Requirements (CC), Version 3.1, Revision 2, September 2007, CCMB-2007-09-002

[6] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Requirements (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 3.1, 29 September 2006, 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] Trusted Client 2.3 Administration Guide, version 1, 18 September 2008

[14] Trusted Client 2.3 User Guide, version 1, 18 September 2008

[15] Becrypt Trusted Client EAL2 Evaluation Technical Report 1.0, October 2009

A.2 Abbreviations

ACA	Australasian Certification Authority
AES	Advanced Encryption Standard
AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CCMB	Common Criteria Maintenance Board
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
SSL	Secure Socket Layer
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
USB	Universal Serial Bus
VPN	Virtual Private Network