

CCT Mark Test Report Summary BeCrypt

Trusted Client Platform
Version 1.2.1.7

VENDOR DETAILS	TEST LABORATORY DETAILS
BeCrypt Limited	Vizuri Limited
Wyvols Court Swallowfield Berkshire RG7 1WY United Kingdom	1-9 Memel Street London EC1Y 0UT
Telephone Number: +44(0) 845 838 2050	Telephone Number: +44 (0) 207 014 8900

Test Report Summary Issue Date: 27th September 2007

Further details about the claims tested are included in the Information Assurance Claims Document (CCT Mark Certificate Number 2007/09/0027) published on the CCT Mark website (www.cctmark.gov.uk)

1 Test Result

- 1.1 The CSIA claims testing of the BeCrypt Trusted Client Platform ver.1.2.1.7 conducted by Vizuri Ltd. concluded that all 8 security claims made within the [ICD] are valid for this IA Product

2 References

- [ICD] IA Claims Document, Reference 100980_0001_2 dated 29th June 2007.
- [TLG] CSIA Claims Tested Mark Scheme Test Laboratory Guide Version 2.3.0, Published 4th May 2007
- [TCP1] Trusted Client version 1.2 Administration Guide published 28th June 2007
- [TCP2] Trusted Client version 1.2 User Guide published 21st June 2007
- [FIPSCERT] Advanced Encryption Standard (AES, FIPS 197): Certificate #247
(<http://csrc.nist.gov/cryptval/aes/aesval.html>)

3 Scope of Testing

- 3.1 The Trusted Client Platform version 1.2.1.7 Product was tested using the Generic Claims Test Method (as specified in the TLG) to assess the claims made in the [ICD].
- 3.2 The following features of the BeCrypt Trusted Client Platform were not tested under the CCT Mark scheme.

User Authentication is achieved through a SHA-256 [FIPS 180-2] hash of an arbitrary username and password. The nature and strength of the hashing algorithm is outside the scope of CCTM testing.

The product allows compatibility with the BeCrypt Removable Media Product to provide secure management of removable storage within the organisation. However this is out of scope for the purposes of this claims test. The product operates on a wide variety of host PC platforms; however, for the purposes of this claims test only Windows XP SP2 will be used.

Trusted Client Platform operates on standard USB bootable computers supporting either Intel or AMD based processors, however for the purposes of

this claims test only Intel based processors was used, AMD based processors are out of scope for this assessment.

Trusted Client Platform may be additionally configured to include third party software at the client request. However, for the purposes of this assessment, this configurability is considered to be out of scope.

Trusted Client Platform may be rolled out to install bases using standard software deployment tools. However the testing of the scalability of roll out forms no part of this assessment and is considered out of scope.

3.3 The product consists of:

Product: Trusted Client Platform

Version: 1.2.1.7

3.4 All tests were carried out in the Vizuri Secure Test Laboratory, located at 1-9 Memel Street, London.

3.5 The following platform combinations were used.

Administration/Installation	Client (Host)
Windows XP (SP2)	x86 PC platforms with Intel processor that allow booting from USB devices.

4 Ease of Use

4.1 Installation of the product was relatively straight forward. This process was aided by the Administration Guide [TCP1] listed at Section 2.2 of this document. It should be noted that creation of the Trusted Client device and the initial login time, on first use of the device, may be time consuming operations if USB1 devices and host computer ports are utilized. A note to Administrators will be added to the Test Report Summary detailing this. The installation of the product was performed by a Vizuri Tester.

The product provides support documents that give the user a guide of installation, configuration, functionalities and an overview of the product. There

is no online help embedded within the product; however, user may contact the Vendor for additional help:

The public email address for BeCrypt product support is 'support@becrypt.com'. The BeCrypt support team is also contactable by calling their switchboard on +44 (0) 1189-880277 and asking for Customer Support.

Once the product is properly configured and the device created, use of the product is straightforward, although there may be a small learning curve in user familiarization with the Linux GUI if they are more commonly used to the Windows operating system. Administration of the system is straight forward, the functionality of the Trusted Client Platform version 1.2.1.7 administration system is well displayed and navigation of the system is intuitive. Further assistance is supplied by the vendor's Customer Support team.

5 Quality of Guidance Documentation

5.1 All of the guidance documentation listed at 2 of this report was available from the outset of testing.

[TCP1] Trusted Client version 1.2 Administration Guide published 28th June 2007

This document is intended for the following different audience categories:

- Systems Administrators.
- Users of the product.

The document is divided into three main sections:

- About Trusted Client provides a good overview of the concepts of the Trusted Client product. It should be noted that it is stated here that the Trusted Client Platform may be configured to include third party software at the client request. This is outside the bounds of this assessment. A note should be added to the Out of Scope section of the Final ICD to this effect.
- Creating a Trusted client explains how to configure Trusted Client's security features and save the setup as a .tcs file, and how to write the configured Trusted Client to a USB device. It is generally well detailed and easy to understand.
- Using Trusted Client explains how to use a Trusted Client device with a temporary host and how to use Challenge-Response. Again, it is generally well detailed and easy to understand / follow.

The guide is supplied in compiled HTML format and is easily navigable via contents, Index, search and Favourites tabs and via internal selectable links within the main body of the text.

[TCP2] Trusted Client version 1.2 User Guide published 21st June 2007

This document is intended for the following different audience categories:

- Users of the product.

The document is broadly similar to the Administration Guide, without the information on configuration of the Trusted Client. It is supplied in the same format as the Administration Guide and is as easy to use and navigate.

6 Resistance to Publicly Known Vulnerabilities

- 6.1 A search of known vulnerability databases failed to yield any publicised A search of known vulnerability databases failed to yield any publicised weakness for the Trusted Client Platform version 1.2.1.7 product.

In addition to a vulnerability search for weaknesses in the product, a search for weaknesses within the underlying operating system was conducted. A number of publicised issues were found with the Operating Systems that the product supports, all of these had patches that were offered by Microsoft to fix these vulnerabilities. All patches were downloaded and applied to the machines in the test environment.

7 Validation of Existing Assurance Certificates

The entry on the NIST website states that 'the BeCrypt Crypto Library implements SHA 256 and AES algorithms for use within Becrypt's Product Set for Enterprise Data Security Solutions.'

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 CCT Mark Scheme and should not be taken as an endorsement or otherwise of the IS Product or Service.

9 Abbreviations

Terms	Definitions
CCT Mark	CSIA Claims Tested Mark
CSIA	Central Sponsor for Information Assurance
ICD	Information Assurance Claims Document
USB	Universal Serial Bus is a serial interface standard designed to allow peripherals to be connected using a single standardized interface socket
PC	Personal Computer
SP	Service Pack
Hash	A complex digital signature calculated to uniquely identify each executable file that can be run.
SHA	The SHA hash functions are five cryptographic hash functions designed by the National Security Agency (NSA) and published as a U.S. Federal Information Processing Standard. SHA stands for Secure Hash Algorithm
AES	Advanced Encryption Standard is a block cipher adopted as an encryption standard by the U.S. government
FIPS	Federal Information Processing Standard
TCP	Transmission Control Protocol – a transportation protocol that is one of the core protocols of the Internet protocol.
GUI	Graphical User Interface is a type of user interface which allows people to interact with a computer and computer-controlled devices which employ graphical icons.
.tcs	A file type recognized by the Trusted Client Platform administration and configuration software.