



#becrypt

## CCTM IA CLAIMS DOCUMENT (ICD)

### BeCrypt

<b>Trusted Client Platform</b>
<b>Version 3.0</b>

<b>VENDOR DETAILS</b>	<b>TEST LABORATORY DETAILS</b>
BeCrypt Limited	Sogeti UK Ltd
Wyvols Court Swallowfield Berkshire RG7 1WY United Kingdom	1-9 Memel Street London EC1Y 0UT United Kingdom
Telephone Number: +44(0) 845 838 2050	Telephone Number: +44(0) 207 148 900
Email: info@becrypt.com	Email: ian.mcewen@sogeti.com
Website: www.becrypt.com	Website: www.sogeti.co.uk

<b>CERTIFICATE DETAILS</b>	
CCTM Certificate Number	2009/09/0051
CCTM Awarded on	2 <sup>nd</sup> September 2009
CCTM Award Expires on	1 <sup>st</sup> September 2011
ICD Issue Date	2 <sup>nd</sup> September 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 DESCRIPTION.....	4
2.1	Product Identification.....	4
2.2	Product 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.....	12
Annex A	GLOSSARY OF TERMS .....	13
Annex B	Marketing Statement .....	15

# 1 INTRODUCTION

## 1.1 Background

This document outlines the IA claims made by “*BeCrypt Ltd.*” in regard to the suitability of “*Trusted Client Platform*” for use by the UK Public Sector for a self contained mobile computing platform for PCs.

## 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 Trusted Client Platform V3.0 product

1.3.2 This ICD is the baseline document for the CCTM Claims Test of Trusted Client Platform V3.0.

## 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 Trusted Client Platform v3.0 and all the information related to the security of Trusted Client Platform v3.0.
- Section 3 details the security functionality claims that are being made.

## 2 IS PRODUCT DESCRIPTION

### 2.1 Product Identification

Product Name: Trusted Client Platform

Version: 3.0

Platforms:

Administration/Installation	Client (Host)
Windows XP (SP3)	x86 PC platforms with Intel processor that allow booting from USB devices.  NB: The product implements a Linux operating system

### 2.2 Product Overview

Trusted Client Platform is a computing environment that can be run on unmanaged computers. This gives organisations the capability to provide their personnel with a cost effective and managed remote working solution.

Features of the software include:

- Self-contained portable computing environment that runs from a bootable USB device;
- Data at rest on the USB stick is protected by industry standard encryption, AES with a 128-bit encryption key [FIPS 140-2].
- Password authentication is required to access the Trusted Client environment;
- The Trusted Client environment provides isolation between itself and the host platform by ensuring that data cannot be exchanged between the host PC and Trusted Client.
- Allows the administrator to build custom security policies with regards to password authentication and controlling network access;
- The installer applications can be run on a standalone machine

### 2.2.1 Security architecture

BeCrypt's Trusted Client Platform is a secure mobile computing environment that allows users to work securely on unmanaged computers.

Trusted Client Platform allows the administrator to create a custom-built environment; this includes setting strong passwords; controlling network access and IP destination filtering; and disabling access to local hard drive storage.

Security offered by Trusted Client Platform may be summarised as:

- **Can be run on unmanaged computers** The Trusted Client Platform can be securely run on unmanaged computers that are bootable via a USB flash drive. Isolation is maintained between the Trusted Client Platform and host PC preventing data leakage between them.
- **Fixed Disk Access** The product provides a modified Linux kernel which does not have drivers for external media, thus preventing the mounting of any external storage media such as CD/DVD, floppy disks, internal or external HDD, flash drives and firewire devices etc.
- **User Authentication** The user must authenticate to the Trusted Client Platform (either by password or smart card) every time the Trusted Client Platform is booted or the screen locked using functionality provided by the product. Policies can be set up to;
  - Define password format and number of unsuccessful attempts before the device is locked.
  - Force password change and user name change on first boot of the Trusted Client Platform.
- **Smartcard Support** The product supports dual factor user authentication using Gemalto .Net smart cards.
- **Device Recovery** The Trusted client platform supports an optional device recovery process via the use of an administrator recovery console, should the device become locked following unsuccessful authentication attempts. Upon failure of the authentication attempts a challenge code is presented to the user. The user must then take this code to an administrator who has access to a recovery console, who can then generate a response code to be entered into the locked device to recover the password.
- **Data encryption** Data held on the Trusted Client Platform remains encrypted. The data on the device is decrypted to the

RAM of the host computer when users have successfully authenticated themselves.

- **Personal Firewall** The Trusted Client Platform can be configured to provide client IP destination control.
- **Centrally Provisioned** Trusted Client devices can be centrally provisioned by an authorised administrator. Operational and User policy are set at the time of device creation and cannot be modified by the user at run time.
- **Download Control** Trusted client can work with a secure VPN to provide gateway security and download controls. The device can additionally be set to use non-persistent volatile memory so that data cannot be transported on the device.

#### 2.2.2 Hardware requirements

- x86 based computers with Intel processor
- USB flash drive with 63 sectors per track, supporting sector size of 512 bytes and a minimum of 512 MB of storage. The USB device should also have a unique serial number.

#### 2.2.3 Software requirements

- *Trusted Client Platform V3.0*
- *OS environment based on a Linux Distribution*
- *Windows XP SP3.*

#### 2.2.4 Out of Scope

The cryptographic algorithms used in Trusted Client Platform V3.0 are not tested under the CCTM Scheme.

The product allows compatibility with the BeCrypt Removable Media Product to provide secure management of removable storage within the organisation. However this will be out of scope for the purposes of this claims test.

Trusted Client Platform allows compatibility with BeCrypt Protect Manager to provide a central management resource for BeCrypt modules. However, for the purposes of this assignment this product is out of scope.

The product operates on a wide variety of host PC platforms; however, for the purposes of this claims test only Windows XP SP3 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 will be used. AMD based processors are out of scope for this assessment.

In the real world the product can 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.

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, other than for the purposes of secure VPN testing (claim 004), is considered to be out of scope.

Trusted Client Platform supports the restriction of internet access to approved IP destinations. Any sub-protocol of the IP protocol suite including TCP, UDP and ICMP can be allowed or filtered. However for the purposes of this assessment only TCP will be tested all others are out of scope.

The use of the Trusted Client Platform 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 sensitive data and IPR at IL1 or IL2 on the USB flash drive that could pose a risk or threat to an organisation or individual if lost or stolen or copied or transferred onto an unauthorised host PC or device.

### **2.3.2 Threat scenario**

Threats to assets which are countered are:

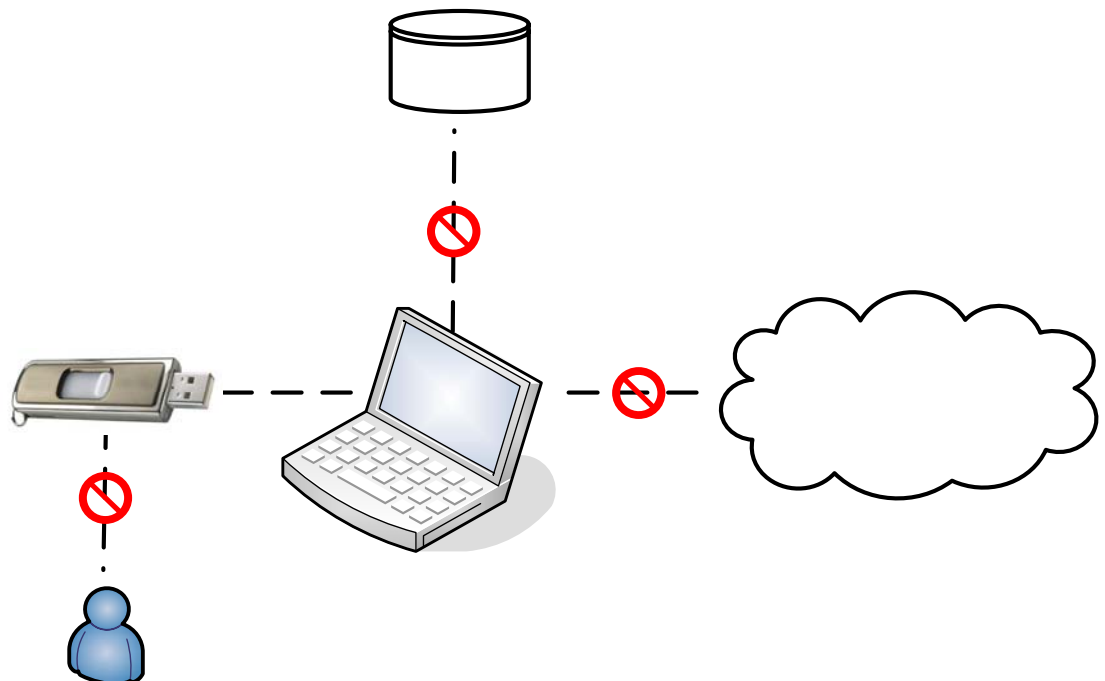
- Unauthorised access to sensitive data held on the USB flash drive;
- Inappropriate data transfer through mounting the local hard drives on an unauthorised host PC;
- Inappropriate data transfer via network connection from the Trusted Client Platform to unauthorised devices.

- Risk to the business from viruses or malicious software being introduced into the corporate network.
- Lost or Stolen USB flash drives - In the statistical likelihood that devices are lost or stolen with all government, corporate, customer and partner information held on it.

### 2.3.2.1 Expected operational environment

The expected operational environment consists of:

A bootable trusted environment that may be run on standard USB bootable computers supporting Intel based processors (as detailed in section 2.1 of this ICD, a typical configuration is shown below).



**Figure 1 - Typical Operational environment.**

Trusted Client Platform supports one user account per protected device and consists of a lightweight Operating System, a web browser and optional additional components (such as SSL VPN, thin client).

Trusted Client Platform benefits the business by providing a secure flexible access method for remote working which may be run on unmanaged, untrusted platforms where the cost of dedicated laptops is inappropriate.

Trusted Client Platform may be centrally provisioned and rolled out scalable to the needs of the organisation.

#### 2.3.2.2 Organisational security policies

Trusted Client Platform is designed to work in line with an organisations security policy and can help meet corporate compliance issues (e.g. ISO 27001, SOX, BASLE II) and US legal requirements - Senate Bill 1386 and Assembly Bill 700, effective July 1, 2003). However, it should not be inferred that the use of the product constitutes compliance against any of these standards.

Policy can be applied at machine level as per the organisations requirements.

It provides a secure portable self-contained computing environment managed in adherence with the organisations security policy.

When deploying Trusted Client Platform, it is important to recognise the two operational roles supported by Trusted Client Platform, i.e., the Trusted Client Platform 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 Trusted Client Platform, including:

- Using strong passwords and appropriately protecting those passwords.
- Changing passwords on a regular basis.
- Not sharing credentials between users or Crypto Officers.
- Not sharing the Trusted Client Platform USB flash drive between users or Crypto Officers.

- Not leaving the Trusted Client Platform unattended whilst connected to host PC in environments that are unsecured. It is recommended that the trusted client platform USB device should be removed from the host computer and stored securely by the user when the system is not being used.

Only Crypto Officers with Trusted Client Platform Administrative Privileges may carry out configuration (operational policy and user policy), maintenance and recovery tasks.

### 3 CCTM CLAIMS FOR THE IS PRODUCT

#### 3.1 Claims Statements

Unique Reference	Claim Statements
	<b>Encryption</b>
001	The USB flash drive containing the Trusted Client Platform remains encrypted.
002	Following successful password entry, the Linux kernel operating system will be decrypted to RAM and executed.
	<b>Access Control</b>
003	Trusted Client Platform can be configured by an authorised Administrator to restrict Internet access to single route access only to IP destination addresses with approved ports and protocols (TCP) on standard DHCP/DNS network.
004	Trusted client can work with a secure VPN (e.g. Citrix and Juniper) to provide gateway security and download controls.
005	Trusted Client Platform provides a modified Linux kernel that prevents the mounting of fixed disks and other external storage media (such as CD/DVD, floppy disks, internal or external HDD, SD and CF flash drives and firewire devices) within a host computer.
	<b>Identification and Authentication</b>
006	Successful user authentication is required to access the Trusted Client Platform whenever a host computer is booted from it or if the screen is locked using functionality provided by the product.
007	Trusted Client Platform locks out the platform device after a password has been incorrectly entered in excess of the maximum number of password attempts set by an Administrator (3-20)
008	Trusted Client Platform supports dual factor user authentication using the Gemalto.net smartcard.
	<b>Management</b>
009	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 length (applies to user created passwords only)</li> <li>• Password format (applies to user created passwords only)</li> <li>• Maximum password attempts</li> <li>• Trusted Client Platform may be further configured to enforce password change on first boot.</li> </ul>
010	Trusted Client Platform may be configured to force user name change on first boot.
011	Trusted Client Platform provides a secure mechanism, via an authorised

	Administrator and the use of a BeCrypt Recovery console, to allow an authorised user to regain control of a locked platform device.
012	Trusted Client forces users to store data only for the live session. This prevents downloaded data persisting on the device between reboots or being transported using the device itself.
013	Trusted Client devices can be centrally provisioned by an authorised administrator. Operational and User policy are set at the time of device creation and cannot be modified by the user at run time.

### 3.2 Existing Assurance Certificates

Trusted Client Platform V3.0 product uses the Advanced Encryption Standard (AES) from the BeCrypt Cryptographic Library, which is certificated to FIPS140-2. The certificate may be found at;

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

## Annex A GLOSSARY OF TERMS

Terms	Definitions
Administrator	See Crypto Officer
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. This term and 'Administrator' are synonymous for the purposes of this ICD
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
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.
HDD	Hard Disk Drive
ICD	Information Assurance Claims Document
ICMP	Internet Control Message Protocol
IP	Internet Protocol
IPR	Intellectual Property Rights
OS	Operating System
PC	Personal Computer
RAM	Random Access Memory
Removable Media	External storage devices which can be used to easily move data between computers with the right readers.

SD	Or SD card, Secure Digital card, flash memory card format used for data storage.
SP	Service Pack
TCP	Transmission Control Protocol
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)
UDP	The User Datagram Protocol
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
VPN	Vitual Private Network

**Annex B Marketing Statement**

BeCrypt™ Trusted Client Platform V.3.0 is a secure portable computing environment that can be used on unmanaged and unsecured computers supporting Intel based processors. The platform is an enterprise security solution designed to ensure reduced operational risk by protecting information on bootable USB flash devices on which critical information could be compromised if lost or stolen. It is a solution that is easy to design, deploy and support in line with organisational security requirements. Implementation and ongoing management can be achieved with a low Total Cost of Ownership.