



## CCT MARK IA CLAIMS DOCUMENT (ICD)

BeCrypt

<b>Trusted Client Platform</b>
<b>Version 1.2.1.7</b>

<b>VENDOR DETAILS</b>
BeCrypt Limited Wyvols Court Swallowfield Berkshire RG7 1WY United Kingdom
Telephone Number: +44(0) 845 838 2050
Vendor Website: <a href="http://www.becrypt.com">www.becrypt.com</a>
Vendor Contact Email: <a href="mailto:info@becrypt.com">info@becrypt.com</a>

<b>CERTIFICATE DETAILS</b>	
CCT Mark Certificate Number	2007 09 0027
CCT Mark Award Expires on	26 <sup>th</sup> September 2009
ICD Issue Date	27 <sup>th</sup> September 2007

## 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	PRODUCT/SERVICE DESCRIPTION	4
2.1	Product Identification	4
2.2	Product/Service Overview	4
2.2.1	Security Architecture	5
2.2.2	Hardware Requirements	6
2.2.3	Software Requirements	6
2.3	Usage assumptions	7
2.3.1	Assets	7
2.3.2	Threat Scenario	7
2.3.3	Expected Operational Environment	8
2.3.4	Organisational Security Policies	8
2.3.5	Security Requirements on the Environment	8
3	SECURITY CLAIMS FOR THE IA PRODUCT/SERVICE	10
3.1	Claims Statements	10
3.2	Existing Assurance Certificates	11
4	ANNEX A Glossary of terms	12
5	ANNEX B Marketing Statement	14

## 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

The objectives of this ICD are to provide:

- To provide a basis for the CSIA Claims Tested Mark (CCTM) scheme assessment of the product; and
- To 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

The purpose of this ICD is to agree:

- A statement of the security objectives for the product;
- A list of the security claims made for the product;
- A statement of the marketing claims to be made about the product on successful CCTM certification;

The document also sets out the additional information required to agree the scope and process of testing, including:

- A description of the assumed operational threat environment for the product;
- A description of the test approach and test environment.

### 1.4 Structure

The structure of this ICD is as follows:

- Section 1 (this section) contains the introductory material.
- Section 2 contains the “Trusted Client Platform” description and contains all the information related to the security of “Trusted Client Platform”.
- Section 3 details the claims that are made.

## 2 PRODUCT/SERVICE DESCRIPTION

### 2.1 Product Identification

Product Name: Trusted Client Platform

Version: 1.2.1.7

Platforms:

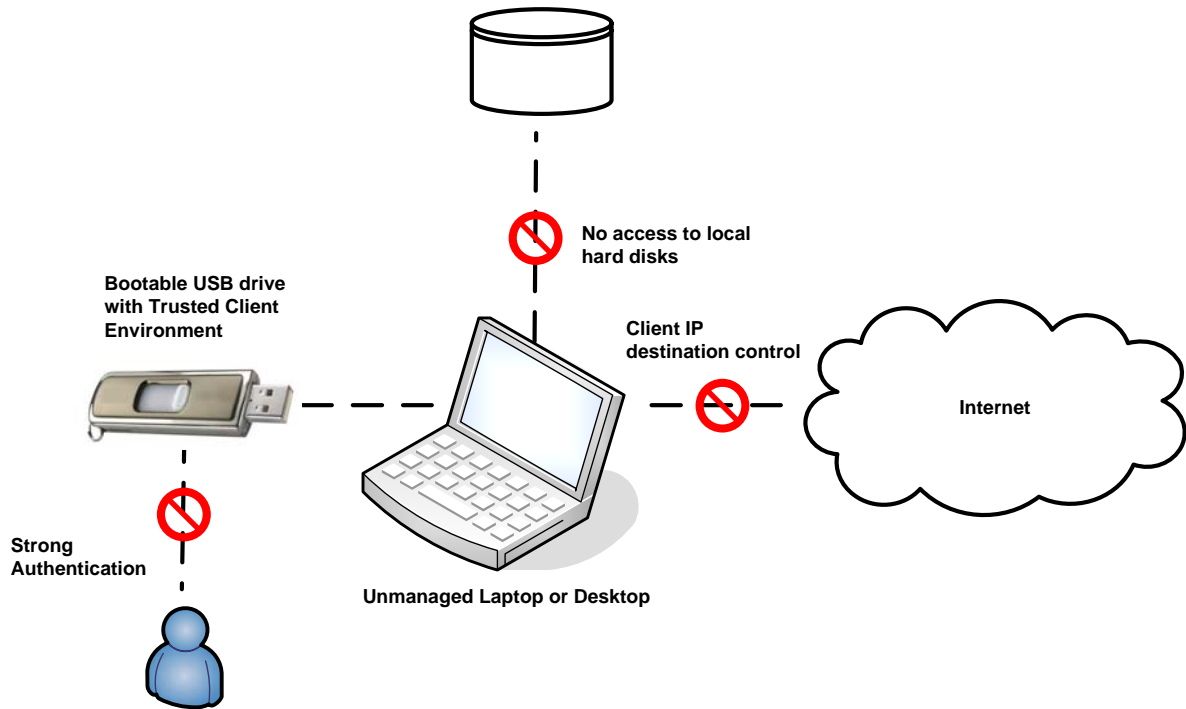
Administration/Installation	Client (Host)
Windows XP (SP2)	x86 PC platforms with Intel processor that allow booting from USB devices.  NB: The product implements its own mini-OS based on a Linux distribution.

### 2.2 Product/Service 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 197].
- 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;
- Can be installed and configured on a standalone machine



**Figure 1. High Level Functional Overview**

### 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 that by default prevents the mounting of fixed disks within a host computer and other external storage media (such as CD/DVD, floppy disks, external HDD, flash drives, SD, CF)
- **Password protection** The user is authenticated by password every time the Trusted Client Platform is booted. A policy can be set up to

define password format and number of unsuccessful attempts before the device is locked.

- **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.
- **Network Address Filtering** The Trusted Client Platform can be configured to provide client IP destination control.

### **2.2.2 Hardware Requirements**

- x86 based computers with Intel processor fitted with a USB host controller and capable of supporting MSC (Mass Storage Class) / UMS (USB Mass Storage) devices.
- USB flash drive (UFD) with a minimum of 512 MB of storage.

### **2.2.3 Software Requirements**

- Trusted Client Platform version 1.2.1.7
- Mini-OS environment based on a Linux distribution.
- Windows XP SP2

### **2.2.4 Out of Scope for Claims Testing**

The following will not form part of the Claims testing.

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 will be 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 will be used, AMD based processors are out of scope for this assessment.

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.

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 supports the restriction of internet access to approved IP destinations using UDP. However for the purposes of this assessment this is considered to be out of scope.

Use of the Trusted Client Platform on Intel based Apple Mac systems is deemed to be out of scope for this assessment.

## **2.3 Usage assumptions**

### **2.3.1 Assets**

Assets to be protected include: any sensitive data and IPR 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**

The Trusted Client Platform product is designed to counter the following threats:

- 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.

### **2.3.3 Expected Operational Environment**

#### Operational Environment

- Trusted Client Platform operates on standard USB bootable computers supporting either Intel or AMD based processors.
- Trusted Client Platform supports one user account per protected device.
- Adhere to corporate compliance issues (ISO 27001, SOX, BASLE II, DPA) and US legal requirements - Senate Bill 1386 and Assembly Bill 700, effective July 1, 2003.

### **2.3.4 Organisational Security Policies**

Trusted Client Platform is designed to work in line with an organisations security policy. 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.

### **2.3.5 Security Requirements on the Environment**

Users and Administrators must observe conventional good security practices as per their organisations security policies when using Trusted Client Platform, including:

- using strong passwords and not writing passwords down.
- changing passwords on a regular basis.
- not sharing credentials between users or Administrators.
- not sharing the Trusted Client Platform USB flash drive between users or Administrators.
- 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 driver should be removed from the host computer and stored securely by the user when the system

is not being used.

Only Administrators with Trusted Client Platform 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;
- mount the host computers local hard drives;
- modify client IP destinations.

### 3 SECURITY CLAIMS FOR THE IA PRODUCT/SERVICE

#### 3.1 Claims Statements

Ref	Claim
	<b>Encryption</b>
001	The USB flash drive containing the Trusted Client Platform remains encrypted.
002	Following successful password entry, the Linux 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 approved IP destination addresses with approved ports and protocols (TCP) on standard DHCP/DNS networks.
004	The product provides a modified Linux kernel that prevents the mounting of fixed disks and other external storage media (such as CD/DVD, floppy disc, external HDD, flash drives, SD, CF) within a host computer.
	<b>Identification and Authentication</b>
005	Successful user authentication is required to access the Trusted Client Platform whenever a host computer is booted from it.
006	The product 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).
	<b>Management</b>
007	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> </ul>
008	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

### **3.2 Existing Assurance Certificates**

Advanced Encryption Standard (AES, FIPS 197): Certificate #247

**4 ANNEX A****Glossary of terms**

<b>Terms</b>	<b>Definitions</b>
CCT Mark	CSIA Claims Tested Mark
CSIA	Central Sponsor for Information Assurance
ICD	Information Assurance Claims Document
OS	Operating System
PC	Personal Computer
SP	Service Pack
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.
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.
Administrator	These accounts have Trusted Client Platform and Windows system administrative privileges. Administrators can perform operational, administrative and maintenance tasks using Trusted Client Platform management utilities.
Removable Media	External storage devices which can be used to easily move data between computers with the right readers.
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 flash drive	USB flash drives are flash memory data storage devices integrated with a USB (universal serial bus) interface. They are typically small, lightweight, removable and rewritable
AES	Advanced Encryption Standard is a block cipher adopted as an encryption standard by the U.S. government
IPR	Intellectual Property Rights
SOX	The Sarbanes-Oxley Act of 2002 is a controversial United States federal law passed in response to a number of major corporate and accounting scandals. The Act covers issues such as auditor independence, corporate governance and enhanced financial disclosure.
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.
FIPS	Federal Information Processing Standard
CD	Compact Disc
DVD	Digital Video(Versatile) Disc an optical disc storage media format that can be used for data storage.
SD	Or SD card, Secure Digital card, flash memory card format used for data storage.

CF	Compact Flash, a solid state memory technology.
HDD	Hard Disk Drive
Flash Memory	Non-volatile computer memory that can be electrically erased and re-programmed.
ISO 27001	ISO 27001 is a formal standard against which organizations may seek independent certification of their Information Security Management Systems (meaning their frameworks to design, implement, manage, maintain and enforce information security processes and controls systematically and consistently throughout the organizations).
DPA	The Data Protection Act (DPA) is a United Kingdom Act of Parliament. It defines a legal basis for the handling in the UK of information relating to living people.

**5 ANNEX B****Marketing Statement**

BeCrypt™ Trusted Client Platform is a secure portable computing environment that can be used on unmanaged and unsecured computers. 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.