



IA Claims Document (ICD)

Pointsec

**Pointsec for PC
Enterprise Workplace Edition**

Version 5.2.2

CCT Mark Certificate Number: 2006/04/0008

CCT Mark Award expires on: 25 April 2008

Vendor Address:

Pointsec Mobile Technologies Ltd
Rosemary House
Lanwades Business Park
Newmarket CB8 7PW

Vendor Website: <http://www.pointsec.com>

Vendor Email: sales@pointsec.com

Vendor Telephone Number: +44 (0) 1494 616092

1 Introduction

1.1 Background

This document states the Information Assurance (IA) claims made by Pointsec Ltd. in regard to the suitability of Pointsec™ for PC for use by the UK Public Sector in the enforcement of mandatory access control over laptops, desktops and workstations.

1.2 Objectives

The objectives of this ICD are twofold:

- 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 product description and contains all the information related to the security of the product;
- Section 3 details the claims that are made.

2 Product/Service Description

2.1 Product Identification

Product Name: *Pointsec™ for PC Enterprise Workplace Edition*

Version Number: 5.2.2

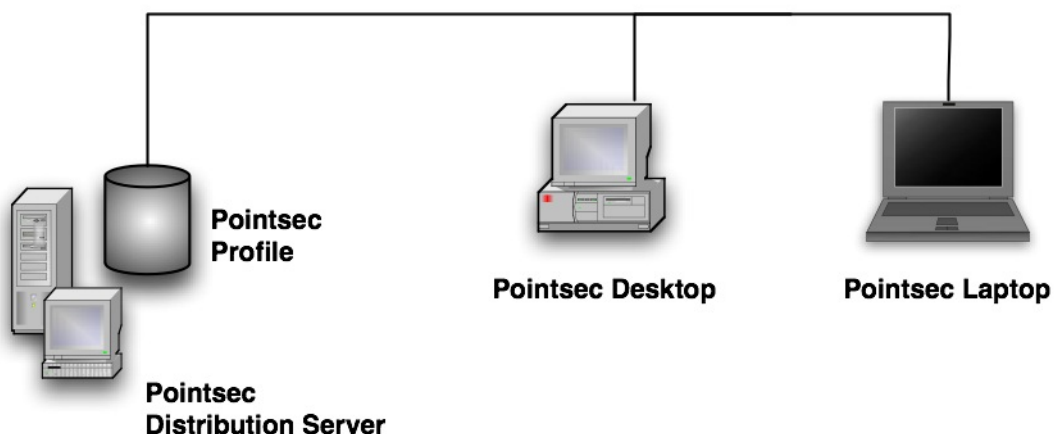
Platforms: *Windows XP Professional Edition SP2.*

2.2 Product/Service overview

2.2.1 Security Architecture

Pointsec™ for PC is a centrally administered, whole disk encryption and mandatory access control product for use on computers (laptops, desktops, or workstations) running Microsoft Windows 2000 or XP operating systems¹. Mandatory access control is provided at the startup of the computer, prior to the loading of the operating system. A successful authentication is required before the operating system is allowed to boot. Multiple user authentication mechanisms are supported, including fixed passwords, dynamic/challenge-response authentication, smart cards, and remote help.

Within the installed environment, workstations and laptops fitted with Pointsec™ for PC communicate with a Pointsec™ Distribution Server (see below), which provides them with a central point for storage and access to installation files, recovery files, update profiles, and software updates. Authorised individuals are able to utilise this server to install and configure Pointsec™-fitted workstations, delegate authorisation throughout the network of such workstations, modify the software for local conditions, and assign the properties and authorisation of individual users by using profiles.



All security related files (profiles, central log files, and recovery files) are encrypted by the Pointsec™ for PC software on the workstation, before they are stored on the server. Access to the server itself is configured appropriately to the server type.

Pointsec™ for PC supports the following security functions:

- **Access Control:** Secures desktops, workstations, and laptops from

¹ The CCTM testing and therefore certification relate solely to the environment used for the test, i.e. Windows XP Professional Edition SP2.

unauthorised access, using the combination of boot protection and full hard disk encryption. The product enforces access control for each disk partition by employing hard disk encryption, ensuring that unauthorised users are unable to access information on an encrypted device, either from available files, erased files, or temporary files.

- **Identification and authentication:** The product provides a suite of five authentication mechanisms, enabling authorised individuals to assign appropriate authentication requirements for the intended environment. Users authenticate to the system using one of the following mechanisms: fixed password (username/password), smart card (username/smart card/PIN), dynamic authentication (username/token/challenge-response), Remote Help authentication (username/phone identification/challenge/Admin response) and Windows Password Change (username/new password/old password). Remote Help is divided into two types, one-time login and remote password change. These provide a way to authorise a user to login when the normal authentication process cannot be performed, such as when the user forgets their smart card, or a fixed password has been forgotten. Windows Password is a special login sequence that occurs when passwords are synchronised between Windows and the Pointsec™ for PC software. For added security, the computer must be restarted after three consecutive failed authentication attempts by any authentication mechanism.
- **Security Management:** Pointsec™ for PC provides a number of interfaces to manage the configuration and implementation of the various policies enforced by the product. Security management includes managing the following items: authentication data, group memberships, audit data, and cryptographic functions.
- **Self-Protection:** Pointsec™ for PC implements a set of security mechanisms to ensure that other security functions such as access control cannot be bypassed and that the security functions themselves cannot be tampered with. Additionally, mechanisms such as cryptographic self-tests have been implemented to ensure that important cryptographic functions are always operating correctly.
- **Auditing:** The product collects audit data and provides an interface for authorised individuals to review audit logs. Audit information generated by the product includes date and time of the event, user ID that caused the event to be generated, computer where the event occurred, and other event specific data. The product also restricts log access to authorised users.
- **Cryptographic Support:** The product's cryptographic functionality is based upon code that has been certified as meeting the requirements of FIPS 140-1 Level 1. Cryptographic keys are generated, accessed, protected, and destroyed in accordance with requirements defined by FIPS 140-1 Level 1. For the purposes of this ICD no claims are made relating to the strength, implementation or algorithms associated with the encryption functions.
- **Fault Tolerance:** When a workstation with Pointsec™ for PC installed loses contact with the Pointsec™ Distribution Server, the Pointsec™ for PC software provides authorised administrative account holders with the capability to identify an additional three Pointsec™ Distribution Servers for redundancy.
- **Trusted Path:** The product provides a mechanism to ensure that users are communicating directly with the product during initial authentication.
- **Initial Encryption.** Pointsec™ for PC will continue to provide access to the PC during the encryption process, thereby avoiding locking out expensive resources.

2.2.2 Hardware Requirements

X86 type processors with 15Mb of local disk space. The installed environment also requires a network connection to an appropriate Distribution Server.

2.2.3 Software Requirements

Pointsec™ for PC 5.2.2 will run on Windows 2000 or Windows XP platforms².

The Pointsec™ Distribution Server could be a Windows NT/2000 server, Novell Netware with the Netware client installed locally, a Linux server running SAMBA or a Sun Solaris server with PC-NFS installed on the client.

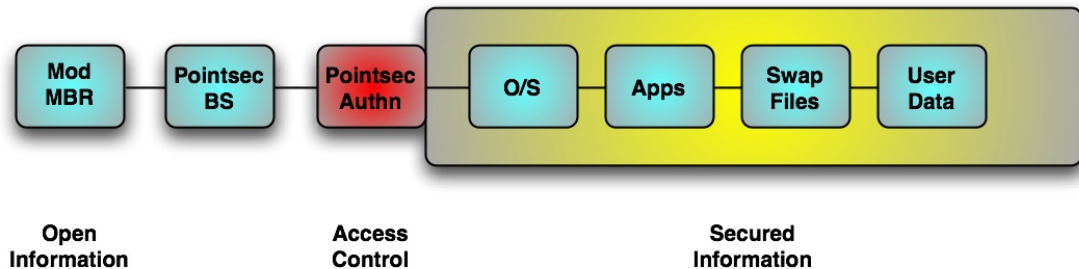
2.2.4 Out of Scope for Claims Testing

The claims will be tested on a platform running Windows XP Professional, with Service Pack 2. Although the product will run on other platforms, these are out of scope for the claims testing.

2.3 Usage Assumptions

2.3.1 Assets

The Pointsec™ for PC product provides full hard drive encryption; therefore in comparison to the use of file level encryption, the product protects not just user data areas but also the workstation operating system, applications loaded onto the workstation, and all operating system working areas such as swap files. The situation is summarised in the diagram below:



2.3.2 Threat Scenario

The product is designed to counter the following threats:

- An unauthorised user with physical access may remove a system's hard drive to subvert authentication mechanisms allowing them to gain unauthorised access to information contained on the hard drive.
- An unauthorised user with physical access may subvert the system's normal boot process allowing them to access information assets contained on the system.
- An authorised user of the product may access information without having permission from the person who owns, or is responsible for, the information.
- An unauthorised user may eavesdrop on communications between separate parts of the product or network, allowing them to gain

²The CCTM testing and therefore certification relate solely to the environment used for the test, i.e. Windows XP Professional Edition SP2.

unauthorised access to information.

- Internal configuration data or other trusted data (such as registry settings) may be tampered with by unauthorised users.
- Users may request access to resources and gain unauthorised access to information by using out-of-date authentication data, thereby releasing information to the subsequent user.
- Unauthorised users may tamper with audit data by gaining unauthorised access to the audit trail.
- An unauthorised user may perform unauthorised actions that go undetected.
- An unauthorised user may gain unauthorised access to the system and act as an administrator or an authorised user.
- A hostile entity masquerading as the IT system may receive unauthorised access to authentication data from authorised users who incorrectly believe they are communicating with the IT system during attempts by a user to initially logon.
- An unauthorised user may cause the modification of the security functions in the system (executable code), and thereby gain unauthorised access to system and user resources.

2.3.3 Expected Operational Environment

The Pointsec™ for PC encryption security software for laptops and PCs running Windows 2000 and XP operating systems is designed to be easily managed in large organisations, enabling them to enforce their security policy without interfering with users' productivity.

Business benefits of implementing Pointsec™ for PC include:

- With the Pointsec™ solution, only authorised users can gain access to information stored on mobile computing devices.
- Pointsec™'s user transparent encryption ensures enforceable, automatic mobile security practices — all data is protected without requiring user intervention.
- Pointsec™ enables widespread deployment of mobile devices without compromising security.
- With Pointsec™, you minimise financial losses and mitigate legal and regulatory risk associated with exposure of sensitive information.
- By showing that your organisation takes the necessary means to protect sensitive data, you create trust, which enhances brand value.

Pointsec™ for PC is easily managed and completely scalable, whether implementing 500, 5,000, or even 50,000 units.

2.3.4 Organisational Security Policies

Pointsec™ for PC enforces and/or supports the following components of organisational level security policies:

- All user information will be encrypted when stored on user PC's.
- Users of the system shall be held accountable for their security relevant actions pertaining to the system.

- The system must provide authorised individuals with utilities to effectively manage the security functions of the system.
- Only those users who have been authorised access to information within the system may access the system.
- The system must have the ability to protect system data in transmission between distributed parts of the protected system.
- The system must ensure that access control functions continue to operate if systems lose communications with central administration servers.

2.3.5 Security Requirements on the Environment

The following assumptions characterise the security requirements on the expected operational environment:

- There will be one or more competent individuals assigned to manage the implementation of the software and the security of the information it contains.
- The system administrative personnel are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the administration documentation.
- Authorised users and administration staff are trusted to follow the guidance provided for the secure operation of the product.
- Authorised users of workstations fitted with the product will keep all their authentication data private.
- The IT environment is required to provide a reliable time source to enable the product to timestamp audit records.
- The IT environment will provide a distribution server for the management of the Pointsec™ client software. This server provides installed PCs with a central point for storage of installation files, recovery files, update profiles, and software updates.
- Support and system management personnel maintain an independent database containing a list of authorised users along with unique authentication data (not related to the use of Pointsec™ for PC), that can be used to verify identity over a telephone connection (i.e. no video, only voice communications) for the purposes of providing Remote Help authentication to authorised users.

3 Security Claims for the IA Product or Service

3.1 Claims Statements

The table below sets out the claims for the Pointsec™ for PC product.

Ref.	Claim
001	The product will ensure that only authorised users gain access to the workstation and its resources by uniquely identifying all users and authenticating their claimed identity before granting access.
002	The product will control access to each logical partition on the workstation hard disk, using the confirmed user identity. The product provides the ability to limit each user's access.
003	The product will provide complete hard drive encryption to protect information assets on the workstation from unauthorised users that have gained physical access.
004	The product will allow administrators to effectively manage the product and its security functions, and will ensure that only authorised administrators are able to access such functionality.
005	When centrally administered, the product will record the security relevant actions of users and have the ability to associate each action with a unique user. The product will present this information in a readable format to authorised users and ensure that only authorised users are able to access this information.
006	The product will protect its own data and resources and will maintain a domain for its own execution that protects it from external interference or tampering.
007	The product will provide the capability to allow users to ensure they are communicating with the product during initial authentication and not with another entity impersonating the product.
008	The product provides the capability to protect system data in transmission between distributed parts of the Pointsec™ solution.
009	The product will continue to enforce access control policies if communications are lost with the central administration server.
010	The product provides a Single Sign On link following pre-boot authentication using the credentials required by the underlying operating system.
011	The product provides remote help (password reset) which does not require either the end user or product administrator to be network connected.
012	The product provides a secure method for system administrators to recover encrypted partitions back to clear text.
013	The product is capable of supporting up to 100 end user accounts.
014	The product provides two levels of administration with configurable privileges.
015	The product provides a simple mechanism to make policy changes post deployment.

3.2 Existing Assurance Certificates

There are no existing assurance certificates relating to Pointsec™ for PC 5.2.2 (the version submitted for testing).

Annex A: Glossary of Terms

The following terminology is used in the ICD:

- **Administrator:** Accounts at this level have limited authority in the administration of the product (according to what has been defined in the system settings). The Administrator can add, remove, and change settings for specific users.
- **Authentication data:** Information used to verify the claimed identity of a user.
- **Authorised administrators:** A term used to encompass both the Administrator and System Administrator roles defined by the product.
- **Authorised users:** A term used to describe all users that interact with the product, that have a unique identifier. This includes the non-privileged set of users and all others within the Administrator and System Administrator groups.
- **Disk Partition:** A logical division of a hard disk. Each partition can be formatted for a different file system. A partition must be completely contained on one physical disk. The Master Boot Record for a physical disk can contain up to four entries for partitions, including one extended partition, which can be further subdivided into logical volumes, allowing for more than four partitions on one physical disk.
- **Disk Partition Access Control SFP:** An access control policy enforced by the product that defines rules for controlling access to disk partitions.
- **Dynamic authentication mechanism:** A challenge-response mechanism that supports single-use authentication. The product supports any password token that supports the x.9.9 security standard.
- **Fixed password authentication:** A normal password authentication mechanism. The product requires that passwords contain at least eight characters but no more than 31. The administrator can make changes to the default requirements for passwords.
- **Identity:** A representation uniquely identifying an authorised user.
- **One-time Login authentication:** An authentication mechanism whereby a user who normally authenticates with either a smart card or a dynamic token is granted temporary, one-time access to the product. See Remote Help authentication mechanisms.
- **Partition key (KP):** A symmetric encryption key that is used by the product to encrypt individual partitions on a hard drive.
- **PKCS#11:** Public Key Cryptography Standard dealing with mechanisms for one time password tokens.
- **Pointsec™ Distribution Server:** The central administration server for the product. System administrators are able to utilise this server to install and configure a network of Pointsec™-fitted workstations, delegate authorisation throughout the network, modify the software configuration for local conditions, and assign the properties and authorisation of individual users by using profiles.
- **Remote Help authentication mechanism:** A secondary authentication mechanism, only used in special circumstances, where the user requests login assistance from authorised personnel over the phone. This mechanism uses a challenge-response sequence that is read over the phone to provide the user authorisation for access to the workstation. There are two types of Remote Help, One-time login and Remote Password

Change. These mechanisms provide temporary authentication to a Pointsec™-fitted workstation when normal authentication is not possible.

- **Remote Password Change authentication:** This type of authentication allows a user to change a forgotten password during the login process with the help of authorised personnel over the phone. This is also the basis for remotely unlocking a locked user account.
- **Smart card authentication:** An authentication mechanism employed by the product that utilises smart cards to store credentials for the user that can only be accessed with a PIN, known only to the owner of the card.
- **System Administrator:** The highest authorisation level in the administration of the product. This role can: create and administer profiles, configure system settings, add and remove administrators and users, configure settings for administrators and users, and provide remote assistance to users who are locked out or have forgotten their passwords.
- **Users:** Any external user that interacts with the product.
- **User Database Access Control SFP:** An access control policy enforced by the product that defines rules for controlling access to the product's user database.

Annex B: Marketing Statement to be Used

Pointsec™ for PC combines enforceable mandatory access control and strong encryption to create an advanced enterprise security solution. This has been proven under the CSIA Claims Tested Scheme, on Windows XP Professional SP2. User credentials and confidential data remain private, enabling organisations and agencies to take advantage of today's mobile PC technology without compromising security. Pointsec™ for PC simplifies security procedures by providing users with a Single Sign-On to multiple operating systems.