



CCT MARK IA CLAIMS DOCUMENT (ICD)

Tru Data Integrity

TruSeal
Version 2.0

VENDOR DETAILS
Tru Data Integrity Limited
Acorn House Oaks Business Park Oaks Lane Barnsley S71 1HT United Kingdom
Telephone Number: +44 (0) 870 251 7100
Vendor Website: www.tru-dataintegrity.com
Vendor Contact Email: j.wearing@singlepoint-dataservices.co.uk / d.pilfold@tru-dataintegrity.com

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/Service Identification	4
2.2	Product Overview	4
2.2.1	Security architecture	6
2.2.2	Hardware requirements	8
2.2.3	Software requirements	8
2.2.4	Out of Scope	8
2.3	Usage assumptions	8
2.3.1	Assets	8
2.3.2	Threat scenario	9
2.3.2.1	Expected operational environment	9
2.3.2.2	Organisational security policies	9
2.3.2.3	Security requirements on the environment	10
3	Security Claims for the IS Product or IS Service	10
3.1	Claims Statements	11
3.2	Existing assurance certificates	13
	Annex A Glossary of Terms	14

1 Introduction

1.1 **Background**

This document outlines the Information Assurance (IA) claims made by Tru Data Integrity Limited (a wholly owned subsidiary of Singlepoint Holdings Ltd) in regard to the suitability of TruSeal for use by the UK Public Sector for the secure sealing of digital files to evidential standards.

1.2 **Objectives**

1.2.1 The objectives of this Information Assurance Claims Document (ICD) are to provide:

- A description of TruSeal and the expected environment including identification of any perceived threats and requirements upon the environment; and
- A statement of claims for TruSeal that will provide a countermeasure against the threats identified and thus tested against as part of the CCT Mark scheme.

1.3 **Purpose of Document**

1.3.1 This document is the Information Assurance Claims Document (ICD) for TruSeal Version 2.0.

1.3.2 This ICD is the baseline document for the CCT Mark Claims Test of the TruSeal version 2.0 product.

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 Truseal version 2.0 and all the information related to the security of Truseal version 2.0.
- Section 3 details the security functionality claims that are being made.
- Section 4 details the Test Approach
- Annex A contains glossary of terms
- Annex B contains the marketing statement
- Annex C contains the effort estimates.

2 Product/Service Description

2.1 Product/Service Identification

Product Name: TruSeal

Version: Version 2.0

Platforms (for Products):

TruSeal Management Server (TMS)	Client Administrator	Client
Sun Solaris V240Z (Hardware)	Windows XP (SP2)	Windows XP (SP2)
Solaris 10	Internet Explorer (IE6)	MS office 2003 for plug-ins
		Java 1.6.0.20
NB :Supported authentication method (LDAP Kerberos native Windows OS,)		

2.2 Product Overview

General

TruSeal seals –digital files such as .doc, .htm, .mdb, .xls, .ppt, .html, .tif, .rtf, .mpeg and jpeg and thereby ensures the contents of that digital file to evidential standards, i.e. what the contents were when the file was sealed, together with information on who sealed the file.

TruSeal technology has been designed to meet the requirements of BIP0008 in providing the **who**, **what** and **when**, of any digital transaction to Legal Admissibility and Evidential Weight of Information standards. (However, use of the product does not infer compliance with the standard).

The **who** is derived from the client’s existing Logical Access methodology or email account details e.g. j.smith@anycompany.co.uk. The client is “anycompany” and “j.smith” is an authorised user within the client company. These details are recorded in the TruSeal Seal Record. The **what** is derived from obtaining a digital fingerprint of the transaction by applying a hashing algorithm (SHA 256) to the transaction. This provides a unique hash value, which is retained as part of the TruSeal Seal Record.

The **when** is derived from four internationally recognised time sources (UTC) which timestamps the TruSeal Seal Record.

When combined, the TruSeal Seal Record provides proof that a file with a given and unique hash value, was sealed by "j.smith" employed by "anycompany" at a given point in time. The identity and content are "frozen" in time. Each TruSeal Seal Record is stored on the TruSeal secure server. The original digital file does not leave the client's machine: only the unique hash value and associated data is stored on the TruSeal server. This guarantees confidentiality of content for customers – TruSeal never sends the data beyond their control.

The sealing software is supplied either as a software application integrated into Microsoft Outlook, Word, Excel and PowerPoint, or as a Standalone Application.

The product includes a 'TruSeal Applet' which enables the full functionality of the claimed product.

TruSeal Engine

The TruSeal Engine is the Java application installed on the user's PC.

A separate user interface has been developed to provide the product's functionality independent (or outside) of any Microsoft Application.

The TruSeal Engine comprises:

- **Data Collection Module.** The component responsible for gathering all associated data for the Seal Record eg user and client details, title of document, local time, reason for sealing etc.
- **Hash Engine.** The component that applies the Hashing Algorithm to the content of the document. In this case, SHA 256.
- **Seal Record Generator.** This combines the inputs from the Data Collection Module and the Hash Engine to produce part of the Seal Record.
- When combined, the Hash Engine and Seal Record Generator provide a unique record, in a predetermined format, that can be associated with the data file.
- The TruSeal Engine then communicates all relevant data to the secure and central Seal Server. known as the TruSeal Management Server or **TMS**.

For the purpose of this claims test, the product will be tested on Windows XP Professional SP2 platform, Microsoft Office 2003, and Internet Explorer IE 6

2.2.1 **Security architecture**

The TruSeal product is offered as a managed service or as a deployed enterprise application. This ICD defines the claims as constant for both architectures. This ICD is concerned with the use of the product as an enterprise application, a separate CCTM assessment could be conducted for the managed service..

A typical installation is detailed in Figure 1 below.

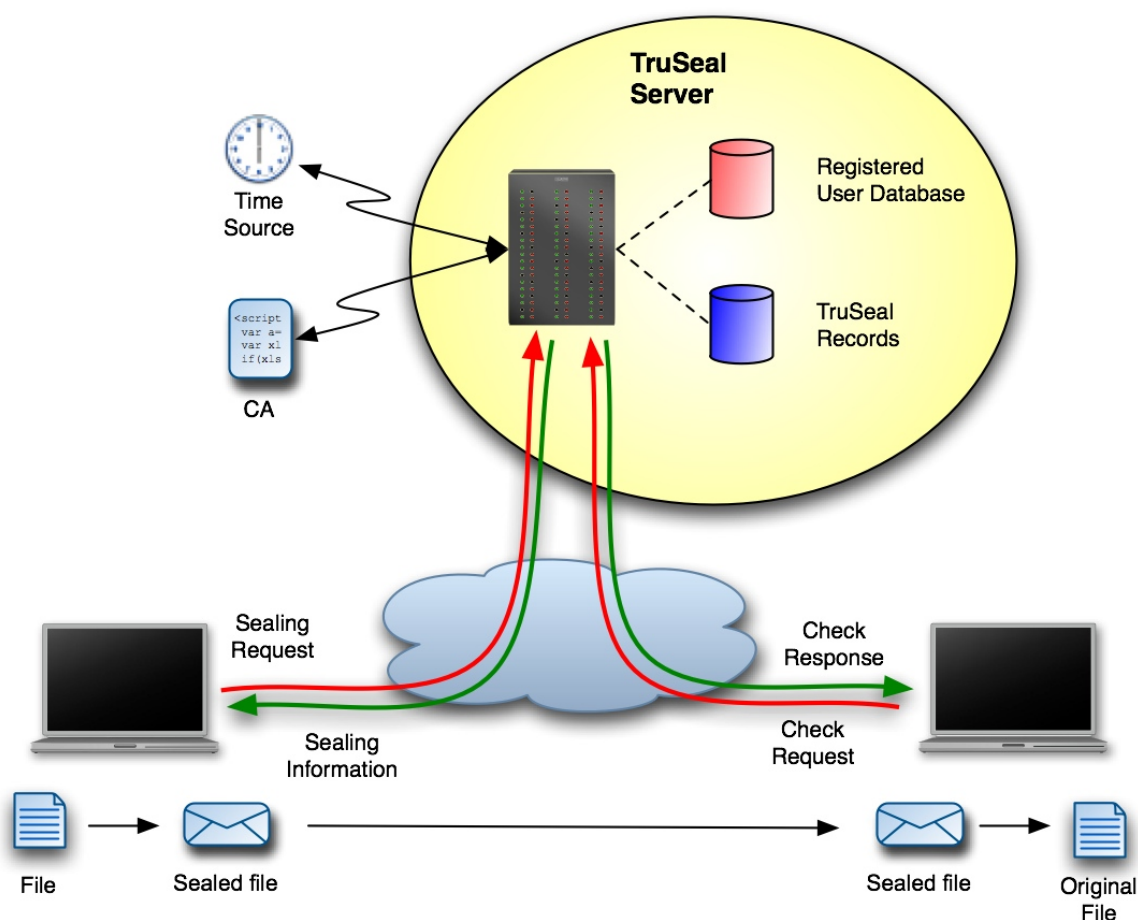


Figure 1. TruSeal in the MS Outlook application.

A registered user creates an email. There are three options:

1. The user may opt to Seal and Send the email with no attachments. This action just seals the email content and metadata.
2. The user may opt to add attachments and seal the email content and attachments by the Seal and Send function. This seals the email content and the attached files with their associated metadata within a single seal.

3. The user may opt to seal the attachments individually using the MS Office or Standalone Application and then attach them to the email. This approach ensures the integrity of each of the attached files separately from the email. A sub-option enables the user to attach the files to the email and then chose to either Seal and Send the email (the email content and the sealed attached files and all associated metadata are then sealed within a further single seal) or not seal the email (only the attachments are sealed).

The MS Office application has been developed to seal file types provided within this Microsoft application. The sealing functionality has been integrated into the respective Office programs. File extensions would include .doc, .htm, .mdb, .xls, .ppt, .html, .tif, .rtf, .mpeg and jpeg

The TruSeal Engine communicates with the TruSeal Server where a timestamp is applied, the user and/or client organization is verified as a registered user and the TruSeal Record is archived. Part of the TruSeal record is then returned to the customer's machine, where a .tru file is created by applying the TruSeal to the original file. The .tru file contains both the original digital file and part of the Seal Record. The .tru file is then sent to the recipient as an attachment in the email.

The recipient may then simply extract the original file. However, the recipient may also validate the contents of the sealed file by securely accessing the TruSeal Record on the server, or against a file stored on a local system.

In an enterprise application configuration, the TruSeal server is locally managed, as is the database of registered users.

TruSeal in the Microsoft Windows and Office applications.

TruSeal has been designed and developed to seal a data file. To facilitate this two further applications are available to meet client needs. Both work in similar fashions.

TruSeal for Microsoft Windows: This is a desktop version enabling the user to "drag and drop" or load any data file, folder or directory into the sealing application.

TruSeal for Microsoft Office: This application is embedded in the standard MS Office programs and adds additional toolbar buttons. The user creates the file in the normal manner using the MS Office 2003 program of choice. Sealing is facilitated using the Seal button, Validation and Extraction of another TruSeal sealed data file can be achieved using the appropriate buttons provided.

Any data file sealed by either of these TruSeal applications can then be communicated to other parties via email (MS Outlook version, described above) or any other method enabling file attachment. Any TruSealed data file can be stored on the user's desktop or central

server or managed within the client's document management system

2.2.2 **Hardware requirements**

The sealing software requires a minimum of: 50 MB of client disk storage on the user PC. A resident Java Runtime Environment is required on the user PC, this requires a further 15MB of disk space however, this is normally shipped with the computer.

The Managed version requires a minimum of a single TruSeal Server and a single Security Manager server

2.2.3 **Software requirements**

The Java Runtime Environment (JRE v1.4 or 1.5) is required to support the TruSeal application. The TruSeal installer determines whether Java is installed and automatically downloads Java from the website if it is required.

2.2.4 **Out of Scope**

The nature and strength of the hashing algorithm used to seal files is outside the scope of CCTM testing.

The product is designed to operate on any Windows platform. However the claims made here relate only to a Windows XP Professional SP2 platform, Microsoft Office 2003, and Internet Explorer IE 6

The Command Line version of the TruSeal Engine which enables integration with existing workflow process software applications is outside the scope of this Claims Document.

The product supports the sealing of other digital file types however these are out of scope for claims testing and only the file types listed above will be tested.

The product may be optionally configured so that an extra level of authentication using X509 certificates generated and managed by Entrust Certification Authority may be implemented. The issuing and management of the certificates is out of scope for this assessment.

The MS Standalone Application has been developed to cover all other data file types including those produced by MS Offices programs. For the purpose of this claims test .doc, .htm, .mdb, .xls, .ppt, .html, .tif, .rtf, .mpeg and jpeg will be tested.

The functionality of the 'TruSeal Applet Lite' is out of scope for this assessment.

2.3 **Usage assumptions**

2.3.1 **Assets**

The primary asset to be protected is the integrity of corporate files. However, the product is intended to support the governance process within an organisation, and hence protect the organisation's legal and commercial position.

2.3.2 **Threat scenario**

Threats to assets which are countered by the product are listed below:

- T1** Post-facto amendments of email records to conceal an error, obtain commercial advantage or conceal the evidence of another misdemeanour.
- T2** Post-facto amendments of e.g. legal/commercial documentation, technical documentation or clinical information.
- T3** Files sent by one person purportedly on behalf of another.
- T4** Compromise of an organisation's legal position through the inadmissibility of evidence.
- T5** Compromise of an organisation's commercial position through not setting in place sufficient support for the governance and compliance processes.

2.3.2.1 **Expected operational environment**

In an enterprise application deployment, the TruSeal server is expected to be connected to a corporate network linking all users of the service. Where sealed documents are to be sent to external organizations, the TruSeal server must be externally accessible in order to provide the verification service to those external organisations.

2.3.2.2 **Organisational security policies**

The product is designed to support the following ISO/IEC 17799 recommendations (however, use of the product does not infer in any way compliance with the standard).

1. The risks to the organization's information and information processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.
2. Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.
3. Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.
4. Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

5. An access control policy should be established, documented, and reviewed based on business and security requirements for access.
6. Users should only be provided with access to the services that they have been specifically authorized to use.
7. Software, data, and other information requiring a high level of integrity, being made available on a publicly available system, should be protected by appropriate mechanisms, e.g. digital signatures.
8. All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.

In addition the product is designed to support policies developed from the British Standards Institute Codes of Practice on the subject of legal admissibility and evidential weight, in the areas of:

- **Authenticity**, trustworthiness, the ability to prove that the transaction was genuine.
- **Integrity**, the ability to retain the evidential properties of the transaction, in order to prove that the transaction has not been tampered with.
- **Availability**, the ability to recover the transaction in an intact and original form.

2.3.2.3 **Security requirements on the environment**

A trusted time source is required for the TruSeal server.

Where the TruSeal server is to be made externally accessible, an appropriate level of protection (e.g. a firewall) is recommended.

An existing authentication framework is required, so that users of the product are given a unique identity.

There will be one or more competent individuals assigned to manage the Implementation of the product and the security of the information it contains.

Those personnel are not careless, wilfully negligent, nor hostile, and will abide by the documented instructions.

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.

3 Security Claims for the IS Product or IS Service

The security claims made for the product in an enterprise application deployment are as follows:

3.1 Claims Statements

Ref	Claims Statement
	Sealing
001	The TruSeal Engine of the TruSeal product will generate a hash value for files submitted for sealing, and will pass the hash value to a nominated TruSeal server.
002	The TruSeal Engine will unambiguously associate the user ID with the hash value and a timestamp and the TruSeal Server will send a TruSeal Record to the client.
003	To avoid the possibility of a Seal becoming compromised, the TruSeal Validate process detects tampering of any three vital elements of a seal, namely; <ul style="list-style-type: none"> • The Digital Signature (i.e. the .p7m file) • The original file • The Seal evidence ID & timestamp.
004	On receipt of the TruSeal record, the client software will generate and correctly apply the seal to the original file, creating a .tru file for onward transmission.
005	The TruSeal Standalone Application provides the ability to seal whole folders and directories.
006	The TruSeal product is capable of sealing files of up to 2Gb in size.
007	The TruSeal product is capable of sealing digital file types such as .doc, .htm, .mdb, .xls, .ppt, .html, .tif, .rtf, .mpeg and jpeg
	Verification
008	The TruSeal software provides a means by which the original file may be recovered from the .tru file.
009	The TruSeal server provides a means by which the integrity of the received file may be confirmed by validating the .tru file against the TruSeal record held on the server.
010	The TruSeal product provides a means by which the user ID and time of sealing of the received file may be confirmed by validating the .tru file against the TruSeal record held on the server.
011	The TruSeal client software provides a means by which the integrity of a received file may be confirmed by validating the .tru file against a locally held sealed file.
012	The TruSeal client software provides a means by which the user ID and time of sealing of the received file may be confirmed by validating the .tru file against a locally held sealed file.
	Identification and Authentication
013	The product will ensure that Individuals successfully authenticate

Ref	Claims Statement
	themselves prior to being given access to sealing capabilities.
014	The TruSeal server maintains a database of registered users and protects the database against unauthorized access, modification, and deletion.
	Auditing
015	The TruSeal server maintains a database of all TruSeal records created by it, and protects the database against unauthorised access, amendment and deletion.
016	The TruSeal server maintains a record of sealing operations, and protects the record from unauthorised access, amendment and deletion.
	Access Control
017	Only registered users are provided with access to sealing capabilities.
	Application Integration
018	TruSeal Client tool plug-ins provides an interface of three icons Seal and Send, Verify & Extract integrated with Microsoft Office suite tools (Word, Excel, Access, PowerPoint), and with Microsoft Outlook.
019	The product provides an alternative Standalone Application which does not require integration with any other product.
	Fault Tolerance
020	If the TruSeal server is not available it will still be possible for a registered user to extract the original file from a <i>.tru</i> file.
	Management
021	The product will maintain a domain for its own execution, which ensures that configuration parameters and settings are protected against unauthorized amendment.
022	The product provides a means of centrally managing the user registration database.
023	The product supports two different levels of privilege: Regular Users and System Manager.
024	The product ensures that no access to administrative functions is possible before successful authentication as an authorised administrator.
025	The product provides facilities to allow an authorised administrator to query the number of seals created by an individual user, in a specified time period.
026	The product has been developed for the IA market by an ISO 9001 and ISO 27001 accredited company.

3.2 **Existing assurance certificates**

ISO 9001 certificate.

ISO 27001 certificate.

Annex A Glossary of Terms

Terms	Definitions
CA	Certificate Authority
CCT Mark	CSIA Claims Tested Mark
Digital File	A file stored electronically on a computer or storage device.
CSIA	Central Sponsor for Information Assurance
Hashing Algorithm	A mathematical algorithm used to generate a unique hash value from an input. Given the output, the input cannot be determined.
Hash Value	The output of a hashing algorithm.
ICD	Information Assurance Claims Document
JRE	Java Runtime Environment
JVM	Java Virtual Machine
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
OS	Operating System
PC	Personal Computer
Seal	A sealed digital file.
Seal Management System (SMS)	Refer to TruSeal server.
Seal Record	A record containing the who, what and when or a seal transaction, i.e. who sealed what at what time.
SP	Service Pack
Timestamp	A time applied to a file.
TruSeal Applet	Web-based version of the TruSeal, providing the full TruSeal capability through a web-browser.
TruSeal Applet Lite	Limited version of the TruSeal Applet, enabling any user to validate and extract digital files from a seal.
TruSeal Server	The computer upon which all Seal Records are stored.
URL	Uniform Resource Locator
UTC	Universal Time Constant
Win32	Microsoft Windows 32-bit Operating Systems

Annex B Marketing Statement

The Tru Data Integrity TruSeal product provides a solution to the question of what happens to information once it leaves the originator; the product provides a means of ensuring that copies of original data continue to hold evidential weight even once they have moved into the hands of third parties. The product delivers proof (in line with BIP0008) of integrity and origin, for legal and Information Integrity purposes, by sealing data and ensuring that the seal remains with all copies of data, regardless of ownership or location.