Security Target

for

Citrix Presentation Server 4.0

For Windows®

Reference: ST/T488

July 2005

Version: 1.0

This document has been prepared on behalf of:

Citrix Systems, Inc
851 West Cypress Creek Road
Fort Lauderdale, FL 33309
USA

Prepared by:

BT
Sentinel House
Harvest Crescent
Ancells Park, Fleet
Hampshire, GU51 2UZ
UK

DOCUMENT CONTROL

DOCUMENT TITLE	Security Target for Citrix Presentation Server 4.0 for Windows

Version	Date	Description
0.1	November 2004	Initial internal draft
0.2	December 2004	Incorporates Citrix comments Note that the following two issues are unresolved: 1 The addition of Kerberos changes to the sequence of interactions in section 2.2 2 The exact wording of the RIP claim (sep in relation to paged memory)
0.3	December 2004	Updated to address issues in 0.2.
0.4	January 2005	First release to evaluators.
0.5	February 2005	2nd Release to evaluators - updated to remove Kerberos authentication
0.6	April 2005	Updated to reflect the change of name to Citrix Presentation Server 4.0 and address EOR1
0.7	May 2005	Updated to clarify TOE scope and environment
0.8	June 2005	Update to clarify Client Drive mapping
1.0	July 2005	Final Issue

Contents

REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation, Version 2.2, January 2004 (aligned with ISO 15408)

GLOSSARY AND TERMS

Administrator	A person working on behalf of the owner of the publishing system owner, who is responsible for administering access of users to applications (and associated data). It is the administrator's responsibility to configure the system (both Presentation Server and Windows) such that access is allowed as intended. An administrator must be authenticated to become an authorised administrator. Authorised administrators can make use of administration tools to configure the system and manage users (the administration tools are not within the scope of the TOE). Administrators access applications in the same way as users (they are a subset of users), but can set their own access permissions, while operating as an administrator, to allow access to any application available. Administrators have physical access to the server component of the TOE.
Authorised Administrator	An authorised user who is an administrator.
CC	Common Criteria for Information Technology Security Evaluation
Authorised User	An end user who has been successfully authenticated.
Citrix XML Service	A Windows service that provides an HTTP interface to the ICA browser. It uses TCP packets that allow connections across most firewalls. This service will also be used to generate Web Interface tickets that are used for ICA Client authentication.
Citrix ICA Client	Citrix software that enables users to connect to Presentation servers from a variety of client devices. The TOE is split essentially into client and server components. The ICA Client connects users to the main presentation server functionality run on the server. The ICA Client component may be run on a PC, PDA and many other end systems. The client does little processing of the applications and does not store application data (other than cached data to ease access).
ICA	Independent Computing Architecture – a presentation services protocol for Microsoft Windows
ICA Protocol	The protocol that ICA clients use to present input (keystrokes, mouse clicks, etc) to Presentation Servers for processing.

	Presentation Servers use it to format application output (display, audio, etc) and return it to the client device.
IMA	The Independent Management Architecture (IMA) is an intelligent interface between the server-side subsystems, and between the server components and components of the operating system, such as the persistent data store. It resolves queries and requests relating to user authentication, enumeration, resolution and session management.
IT	Information Technology
IPSec	IP Security (IPSec) is a set of standard extensions to the Internet Protocol (IP) that provides authenticated and encrypted communications with data integrity and replay protection.
Object	An entity within the TSC that contains or receives information and upon which subjects perform actions.
Published Applications	These are the applications that administrators can configure to be accessible by authorised users. The definition also includes data and resources associated with a given application (e.g. data defining the initial configuration or appearance of an application). Different authorised users may have access to different sets of applications.
Permitted Published Applications	The set of published applications to which an authorised user has been granted access.
Person	Any human entity (e.g. attacker, user) that may attempt to access the TOE. To qualify as a user' the person must be recognisable by the TOE.
Secure Gateway server	A Windows service that runs on a Windows 2000 server, functioning as an TLS gateway between ICA clients and a server farm.
Secure Ticket Authority (STA) server	This server accepts requests for Secure Gateway tickets. The request data will include a Presentation Server address. A random ticket will be generated and returned. This server will also accept requests for server addresses that have been stored based on the ticket representing the address.
Server	The TOE is split essentially into client and server components. Applications are run on the server.
Server Farm	A Server farm is a group of Presentation Servers that can be

	managed as a single entity. To an authorised user this would appear as a set of published applications.
ST	Security Target
Subject	An entity within the TSC that causes operations to be performed.
TLS	Secure Sockets Layer (SSL) is an open, nonproprietary protocol that provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. Transport Layer Security (TLS) is the latest, standardized version of the SSL protocol. TLS is an open standard and like SSL, TLS provides server authentication, encryption of the data stream, and message integrity checks. For the TOE, only use of TLS is within scope.
TOE	Target of Evaluation
TSF	TOE Security Functions
TSC	TOE Scope of Control
User	An 'end user' of the system. This is a person who connects from some client component of the TOE. They do not have physical access to the server component. A person who has the potential to become an authorised user. They have a valid identity recognised by the TOE. To become an authorised user they must be successfully authenticated.

1 Introduction to the Security Target

1.1 Security Target Identification

Document Title	Security Target for Citrix Presentation Server 4.0 for Windows.
Version	V 1.0
Owner	Citrix Systems, Inc.
Originator	BT
TOE	Citrix Presentation Server 4.0 for Windows[1]
CC Version	2.2, January 2004 with CCIMB final interpretations at as October 2004 [CC]
Assurance Level	EAL2 augmented by ALC_FLR.2 Flaw Reporting Procedures.

1.2 Security Target Overview

This document describes the security features of the Citrix Presentation Server 4.0 (including Web Interface and Secure Gateway).

This Security Target includes the definition of the TOE, its scope and dependencies. It also lists the security requirements to be evaluated and how these are satisfied by the functionality of the TOE and/or associated policies.

The TOE provides users with secure access to applications. This access can be from a range of devices over any network connection including Internet, LAN, WAN, dial-up or wireless connection.

1.3 CC Conformance Claim

This TOE makes the following conformance claims with respect to [CC]:

- Part 2 extended
- Part 3 conformant EAL2 augmented, resulting from the selection of ALC_FLR.2 – Flaw Reporting Procedures.

[1] The TOE consists of a number of components as detailed in section 2.4.

2 TOE Description

2.1 Overview

The TOE provides users with secure access to applications and information. This access can be from a range of devices over any network connection including Internet, LAN, WAN, dial-up or wireless connection.

The set of Citrix solutions is formed by the following components.

2.1.1 Citrix Presentation Server

Citrix Presentation Server allows multiple users to log on and run applications in separate, protected sessions on the same server. The Presentation Server is installed on servers with a Windows 2003 operating system. These servers install and *publish* the applications that are to be deployed on the Presentation Servers. Examples of such applications are word processors, spreadsheets, and resource planning applications such as SAP and Peoplesoft, or any other custom applications.

Servers can be grouped together to form a *server farm.* A server farm is a group of Presentation Servers that is managed as a single entity. Server farms provide a flexible and robust way of deploying applications to users.

2.1.2 ICA Clients—for Secure, Remote Access to Applications

ICA Clients exchange information between a user's client device and the published application resources on the Presentation Server. The ICA Client software is available for a range of different devices and platforms. Keystrokes, mouse clicks and screen updates are sent between the server and the client. All this traffic is encrypted to provide confidentiality and integrity. Published applications run entirely on the server. To the user of the client device it appears as if the software is running locally.

Because applications run on the server and not on the client device, users can connect from any platform. The TOE is secured using the Transport Layer Security (TLS) protocol. TLS provides server authentication, encryption of the data stream and message integrity checks and enables secure delivery of an application within a LAN, WAN or across the Internet.

ICA Clients support client drive mapping, such that drives on client computers appear as network objects in Windows, making them available to applications.

If configured by an administrator, users are permitted to transfer information between a published application and a client windows clipboard.

Both the Client Drive mapping functionality and the ability to transfer information between a published application and a client windows clipboard can be enabled or disabled by the administrator. This functionality can either be controlled at a global

level or on the basis of users or groups of users. Only the ability to control this functionality globally is included within the scope of the evaluation.

In evaluated configurations users will with run a TLS-enabled Web browser (Internet Explorer) and the ICA Win32 Client.

Note that the TOE makes use of operating system calls to provide TLS, and does not itself implement the protocol.

2.1.3 Web Interface

Web Interface is used to give authorised users access to published applications and information through the Web or intranet. Users log on to Web Interface using an Internet browser, and see links to the applications that they are authorised to run (permitted published applications).

Web Interface dynamically creates an HTML page for the server farm for each authorised user. After logging in, the user sees a Web page that includes all the applications and resources in the server farm configured for that user. When the user selects an application from that Web page, Web Interface generates the ICA file that the client needs to connect to the Presentation Server via the Secure Gateway.

2.1.4 Secure Gateway

Secure Gateway is used in combination with Web Interface to securely transport data over the Internet using standards-based security technology (e.g. TLS, FIPS 140 certified cryptography, IPSec). It permits users authenticated by Web Interface to access resources on an internal network and provides a link between two encrypted data tunnels (TLS and IPSec protocols provided by the operating system) for client-server communications.

2.1.5 Secure Ticket Authority (STA)

The Secure Ticket Authority is called when Web Interface receives a request for a Secure Gateway ticket. It generates and validates tickets for access to Presentation Server published applications. Users will connect with Secure Ticket Authority running on Microsoft Windows 2003 Server, Service Pack 1.

2.1.6 Smart Cards

Smart cards can be used to provide secure access to applications and data. The TOE can be configured to use smart cards to:

- Authenticate users to Presentation Servers[2]
- Authenticate users to Web Interface

The role of the TOE in this process is limited to the conveyance of authentication credentials from the smart card to the operating system, and reacting appropriately on receipt of a response from the operating system.

2.1.7 Firewalls

Firewalls are used to restrict access to the Presentation Server component to a specific port and, in some configurations (including the evaluated configuration), within the Presentation Server component to limit allowed protocols and connections. These firewalls are not in the scope of the evaluation.

2.2 Evaluated Deployment

A variety of configurations are possible using these components. The TOE comprises the sample deployment as described below. All other configurations are out of scope of the evaluation.

The deployment uses the Secure Gateway to provide TLS encryption between a TLS-enabled ICA Client and a secure application server (the TOE makes use of Windows TLS encryption functions, which are not themselves part of the TOE). Communication also occurs between a Web Browser and Web Server (the HTTP communication is encrypted). Communication within the Server Component is secured using IPSec, again, provided by Windows.

In this case the 'Client Component' of the TOE is an ICA Client and Web Browser. The 'Server Component' of the TOE is composed of the server running the Secure Gateway, the Secure Web Server, the server running the Web Interface, the server running the Secure Ticket Authority, the ICA server component and the Citrix XML service. The Web Browser and the Secure Web Server are trusted third party software (and are excluded from the scope of the TOE).

The interactions between the various components are as follows:

1 An ICA client device user uses a web browser to view the Web Interface Login page. If the Web Interface has been configured to use username and password the user enters user credentials which are sent as a standard HTTPS request. If the Web Interface has been configured to use Smartcard

[2] Authentication to published applications is also supported by Citrix Presentation Servers, but not within the scope of this evaluation.

authentication then the user will be prompted to enter their smartcard.

2 The web server reads the user's information and uses Web Interface to forward the information to the Citrix XML Service.

3 The Citrix XML Service retrieves a list of applications that the user can access. These applications comprise the user's application set and are configured by the administrator.

4 The Secure Web Server uses Web Interface to generate an HTML page containing hyperlinks to the applications in the user's application set.

5 The user initiates the next step by clicking one of the hyperlinks in the HTML page. The web browser sends a request to the web server to retrieve the ICA file for the selected application. The web server passes the request to Web Interface.

6 The Web Interface contacts the Citrix XML Service again, requesting information about the least-busy server in the server farm.

7 The Citrix XML Service locates the least-busy server hosting the selected application and requests an authentication ticket from the ICA server for the current user. The Citrix XML Service on the least-busy server accepts this request, generates an authentication ticket and returns the authentication ticket to the (primary) Citrix XML service. Note - authentication tickets are only applicable to username/password login.

8 The (primary) Citrix XML Service returns the IP address of the least-busy server and authentication ticket to Web Interface.

9 The Web Interface contacts the Secure Ticket Authority and requests a Secure Gateway ticket. The ICA Server address will be included in the request.

10 The Secure Ticket Authority stores the request data and returns a Secure Gateway ticket to the Web Interface.

11 The Web Interface sends a customized ICA file via the Secure Web Server to the web browser that contains the authentication ticket and Secure Gateway ticket.

12 The web browser receives the ICA file and passes it to the ICA Client.

13 The ICA Client receives the ICA file and connects to the Secure Gateway. This connection makes use of TLS to ensure data confidentiality and integrity is maintained. The confidentiality and integrity of information of the user's machine is protected by authentication of the (least busy) server through the use of TLS.

14 The ICA Client sends the Secure Gateway the Authentication Ticket and Secure Gateway ticket data.

15 The Secure Gateway contacts the Secure Ticket Authority server and sends it the Secure Gateway Ticket

16 The Secure Ticket Authority returns the stored IP address of the ICA Server that contains the application.

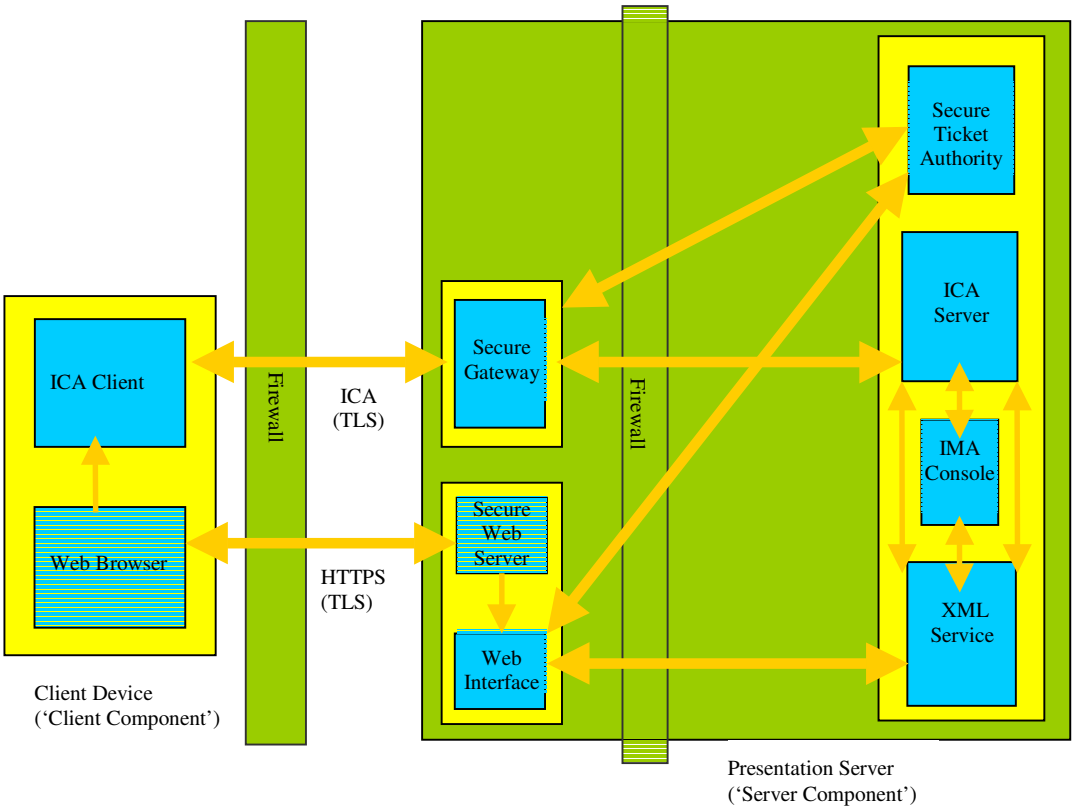
17 The Secure Gateway initiates an ICA session with the least-busy Presentation server according to

the IP address received from the Secure Ticket Authority.

18 If the Presentation server has been configured to use Smartcard Authentication then the user will be prompted to enter the smartcard in order to authenticate to the server,

19 If the Presentation server has not been configured to use Smartcard Authentication the Presentation server authenticates using the Authentication ticket data as the credentials.

18 The Secure Gateway forwards all ICA traffic between the Presentation server and the ICA Client.



Notes to diagram:

a) The Web Browser, Secure Web Server and the HTTPS connection between them are not part of the TOE.

b) The Secure Gateway resides on the server running the Secure Gateway.

c) The Secure Web Server and Web Interface reside on the server running the Web Interface.

d) The Secure Ticket Authority, ICA Server, IMA Console and XML Service reside on the Presentation Server.

2.3 TOE Installation Requirements

2.3.1 Citrix Presentation Server Requirements

Citrix Presentation Server 4.0 is supported on Microsoft Windows 2003 Server with Terminal Services, Service Pack 1 (or later) and Microsoft Internet Information Services version 6.0 installed. The Terminal Services component must be installed before installing the Presentation Server. Install Terminal Services in Application Server mode.

In addition, in the evaluated configuration, two further software components need to be installed on the Primary Presentation Server. Microsoft SQL Server 2000 Desktop Engine with Service Pack 3 (MSDE) must be installed as the data store and the MetaFrame Access Suite License Server must be installed in order to successfully license the product. These two components form part of the environment for the TOE.

The hardware platform should be a 550MHz, or faster, Pentium-compatible processor with 256MB of RAM and a 2GB hard disk.

2.3.2 Requirements for the Web Interface server

The Web Interface is supported on Microsoft Windows 2003 Server, Service Pack 1 (or later), with Microsoft Internet Information Services version 6.0 and the Microsoft .NET Framework (including Visual J# .NET v1.1) installed.

The hardware platform should be a 550MHz, or faster, Pentium-compatible processor with 256MB of RAM and a 2GB hard disk.

2.3.3 Requirements for the Secure Gateway server

The Secure Gateway is supported on Microsoft Windows 2003 Server, Service Pack 1 (or later).

The hardware platform should be a 550MHz, or faster, Pentium-compatible processor with 256MB of RAM and a 2GB hard disk.

2.3.4 Requirements for the ICA Client

The ICA Client is supported on Microsoft Windows XP, Service Pack 2 (or later), with Internet Explorer version 6.0 SP2 installed.

The hardware platform should be a 233MHz, or faster, Pentium-compatible processor with 256MB of RAM and a 2GB hard disk.

2.3.5 Supported Hardware

Details of the hardware supported for Windows 2003 can be found on Microsoft's Server Catalog at http://www.microsoft.com/windows/catalog/server/.

Details of the hardware supported for Windows XP can be found on Microsoft's catalog at http://www.microsoft.com/windows/catalog/.

2.4 Scope of Evaluation

The Target of Evaluation (TOE) will be the following configuration of the Citrix Presentation Server 4.0 for Windows[3]:

- Two Citrix Presentation Servers[4] (comprising ICA Server, IMA Console, XML Service and STA Service), operating as a minimal server farm.
- Web Interface version 4.1.
- Secure Gateway version 3.0.
- ICA Client version 9.0.

[3] Citrix Presentation Server is available in three tailored solutions. The Enterprise Edition is the subject of this evaluation. The advanced edition and standard edition exclude some functionality that has no relevance to this security target. A single binary is supplied to all users, and access to functionality is controlled by licence.

[4] The Citrix Presentation Server 4.0 was previously referred to as the Citrix Metaframe Presentation Server. This is still reflected on the administrative interfaces and guidance documentation.

3 Security Environment

3.1 Introduction

This section provides the statement of the TOE security environment, which identifies and explains all:

- known and presumed threats countered by either the TOE or by the security environment;
- organisational security policies with which the TOE must comply;
- assumptions about the secure usage of the TOE, including physical, personnel and connectivity aspects.

3.2 Threats

This section identifies the threats to the IT assets against which protection is required by the TOE or by the security environment.

3.2.1 Assets

- Access to published applications and their data. This includes the fact that published applications should be *available* to an authorised user.
- Data in transit across a network between the client and servers, and between servers.
- User applications and data on the client. A user will wish to have assets held on the client protected from malicious/accidental damage from (say) a **non-authentic** server. Here 'applications' may be anything belonging to the user, and is distinct from 'published applications'.
- Server Hardware

3.2.2 Threat agent

The following are threat agents for the TOE:

(Unauthorised) Person	An attacker who has **not** been granted access to the TOE.
Authorised user	An attacker who has been granted access to the TOE. In this case, the threat would come from an authenticated user attempting access not granted to them.

Third Party Software	Non-TOE Software, which may introduce threats such as viruses.

3.2.3 Threats countered by the TOE

The following specific threats are countered by the TOE (in some cases with support from the environment):

T.AUTHENTIC	Communication channels may be unreliable, or may be intercepted, such that users of the TOE may incorrectly believe they are accessing the TOE when they are not. This may lead on compromise of data in transit or stored on the client.
T.ACCESS1	A person may gain unauthorised access to data or applications (including residual data on the client). This 'person' would be either an agent totally unknown to the TOE or an unauthorised user of the system.
T.ACCESS2	An authorised user may gain unauthorised access to data or published applications.
T.MOD_CONF	An attacker or authorised user may modify a user's configuration. This covers: • modification of the user's set of *permitted* published applications • modification of configuration data associated with a user.
T.MISDIRECT	An attacker may use malicious software to redirect communication between client and server to another server.
T.AVAIL	An authorised user may not be able to launch an application that is in their permitted published application set.

3.2.4 Threats countered by the Operating Environment

The following threats are required to be countered by technical and/or non-technical measures in the IT environment:

T.MOD_HW_SERVER	Unauthorised persons may gain access to server component hardware.

T.MOD_HW_CLIENT	Unauthorised persons may gain access to client component hardware.

3.3 Organisational Security Policies

OSP.CRYPTO	Cryptographic functions shall be validated to FIPS 140-1 Level 1 or FIPS 140-2 Level 1.[5]

3.4 Assumptions

A.TRUSTADMIN	Administrators are trustworthy.
A.USER_ PASSWORDS	Users will not disclose their passwords to others.
A.THIRD_PARTY_ SW	Trusted third party software is operating correctly and securely. Trusted third party software is defined as: • Microsoft Internet Information Server (IIS) (the secure Web Server) • Web Browsers used to connect • Microsoft Terminal Services (used on the client side) • Windows Server 2003 (including Active Directory) • Firewall software (Note: This, in fact, includes Firewall hardware too).
A.PUBLISHED_ CONFIG	The TOE will be configured such that only applications can be published. It will be configured such that the following cannot be published: • Desktop (other than for administrators) • Content.
A.APP_ INTERFERE	Published applications are trusted not to interfere with each other and not to undermine the user configuration.
A.APP_CONFIG	All published applications will be configured such that it is not possible to 'break out' of them, and hence gain direct access to operating system functions or other applications.

[5] Referred to generally in the ST as FIPS140 Level 1.

A.SMARTCARD	Where a smart card is used, it will be tamper resistant and maintain the confidentiality and integrity private keys contained within it.

4 Security Objectives

4.1 TOE Security Objectives

4.1.1 IT Security Objectives

The specific IT security objectives are as follows:

OT.AUTHENTIC_ SERVER	Presentation Server components must authenticate themselves to client components before communication of sensitive data.
OT.AUTHENTIC_ CLIENT	Users must be successfully identified and authenticated before being granted access to published applications and their data.
OT.CONF_CLIENT	The confidentiality of user data situated on the TOE client component must be maintained.
OT.INTEG_CLIENT	The integrity of user data situated on the TOE client component must be maintained.
OT.CONF	The confidentiality of data associated with published applications must be maintained during processing and transmission between client and server components.
OT.INTEG	The integrity of data associated with published applications must be maintained during processing and transmission.
OT.CUT_PASTE	An administrator must be able to control the ability of authorised users to cut, copy and paste information between published applications and a client Windows clipboard.
OT.DRIVES	An administrator must be able to control the ability of authorised users, through published applications to access local drives on the client machine.
OT.GATE_ALLOW	The Secure Gateway must allow only traffic that is directed to Presentation servers.
OT.SECURE_ENCRYP TION	Secure encryption modules used must be FIPS140-1 or FIPS 140-2 compliant. Note: This objective will be met through correct use of services provided by a correctly configured operating system.

OT.APPS_AVAIL	Authorised users must have access to their sets of permitted published applications. Note: The intention of the objective is primarily to ensure authorised users have published applications available to them. The restriction of an authorised user to only his permitted published set is covered elsewhere.

4.2 Environment Security Objectives

4.2.1 IT environment security objectives

The following IT security objectives are to be satisfied by the environment:

OE.OS_CONFIG_ SERVER	The operating systems of the server components must be securely configured, including appropriate file protection. Note: This includes the files that define user access to permitted published applications.
OE.OS_CONFIG_ CLIENT	The client component operating system must be securely configured, including appropriate file protection.
OE.SERVER_THIRD_ PARTY_SW	Trusted third party software must be securely configured. Trusted third party software is defined as: • Microsoft Internet Information Server (IIS) (the secure Web Server) • Web Browsers used to connect • Microsoft Windows (including Terminal Services) • Firewall software.
OE.MALWARE_PROT ECT	Client devices must have virus and other malware protection installed that is configured to be secure and effective.
OE.SECURE_ ENCRYPTION	Secure encryption modules used to provide IPSec and TLS must be FIPS140-1 or FIPS 140-2 compliant. Note – This means that the Operating System must be configured such that only FIPS140 implemented algorithms are used.

OE.SESSION_KEYS	Cryptographic session keys must be securely administered and protected from disclosure. Note – Session keys are managed entirely by the Operating System as part of the TLS implementation. The TOE does not import or process keys.
OE.LIMIT_AUTH	The Windows operating system must control the number of authentication failures permitted before a server account is disabled.
OE.PASSWORD_ SETUP	The Windows operating system must be used to authenticate the user to the Presentation Server component. This must be configured to an appropriate level of security for its intended use.
OE.IPSEC	All communication on the server component uses the configured protocol between the following servers: • Server running the Web Interface • Server running the Secure Gateway • All Presentation servers This is accomplished by the Administrator setting these servers to use the IPSec protocol.
OE.MEMORY	The Windows XP operating system on the client must ensure that contents of the volatile memory used by a client session are not available to other processes when that client session is complete.

4.2.2 Non-IT environment security objectives

Non-IT environment security objectives are to be satisfied without imposing technical requirements on the TOE. That is, they will not require the implementation of functions in the TOE hardware and/or software. Thus they will be implemented largely through procedural or administrative measures.

OE.TRUSTED_ OPS	Administration and configuration data must accessible only by Administrators.

OE.SERVER_ PHYSICAL	Server hardware running the following must be physically protected: • Server running the Secure Gateway • Server running the Web Interface • Presentation Server.
OE.CLIENT_ PHYSICAL	Users will handle their client devices in a secure and responsible manner.
OE.CLIENT_TPSW	Client devices must have only trusted third party software installed. This software must be configured securely.
OE.CERTIFICATES	Cryptographic certificates must be accessible only by administrators. They must be obtained and maintained securely. This needs to be done at product installation and as determined by the relevant certification authority thereafter.

5 IT Security Requirements

5.1 TOE Security Functional Requirements

The TOE security functional requirements are presented in this section. The following table summarises those security requirements. Completed operations are shown in *italics*. Iteration is indicated by use of (n) following the component designator, where n is the number of the iteration.

All components are taken from Part 2 of the CC apart from FTP_ITC.2, which is an extended component that has been closely modelled on FTP_ITC.1. This component is needed to express the requirement for authentication between the client and the secure gateway. This requirement could not easily be expressed using any existing component.

Functional Components	
	Cryptographic operation
FCS_COP.1(1)[6] Cryptographic operation	FCS_COP.1.1 - The TSF shall perform [*encryption of traffic between client and server components*] in accordance with the specified cryptographic algorithm [*3DES, as defined by the ciphersuite RSA_WITH_3DES_EDE_CBC_SHA in the TLS specification in RFC 2246*] and cryptographic key sizes [*168 bit*[7]] that meet the following: • [*FIPS140, Level 1*] Note: RSA_WITH_3DES_EDE_CBC_SHA has the following attributes: • Key Exchange = RSA • Cipher algorithm =3DES_EDE_CBC • Hash algorithm = SHA Further details can be found at "http://www.faqs.org/rfcs/rfc2246.html"

[6] This requirement is met partially by the TOE and partially by the operating system in the environment. The TOE shall be configured to make use of encryption services that meet the standards, and shall ensure that such services are used.

[7] Both TLS and SSL use 3DES with three keys (a total of 168) bits. However, the *effective* key length

Functional Components	
	Internal Data Transfer Protection
FDP_ITT.1 Basic Internal Transfer Protection	FDP_ITT.1.1 - The TSF shall enforce the [*access control SFP*] to prevent the [*disclosure and modification*] of data associated with applications when it is transmitted between separated parts of the TOE. Notes - The Internet is considered to be an 'internal channel' of the TOE, given that the TOE is providing encrypted protection of traffic. Here the SFR relates to the use of TLS between the client and the secure gateway server. The SFR is repeated in the section on requirements for the IT environment to address the use of IPSEC within the server component.
	Security Management Roles
FMT_SMR.1 Security Roles	FMT_SMR.1.1 - The TSF shall maintain the roles [*user and administrator*]. FMT_SMR.1.2 - The TSF shall be able to associate users with roles.
	Specification of Management Functions
FMT_SMF.1[8] Specification of Management Functions	FMT_SMF.1.1 - The TSF shall be capable of performing the following security management functions: *a) Administration of user access rights* *b) Publishing of applications* *c) Enabling/disabling cut and paste* *d) Enabling / disabling client drive mapping.*

is significantly less than this. This is because SSL and TLS generate a random 48-byte "pre-master secret". This pre-master secret is divided up among a pair of 3DES session keys, plus a pair of MAC integrity keys and a pair of initialization vectors. The effect is to reduce the random input to each 3DES session key to about 112 bits; SSL and TLS then expand this to 168 bits.

[8] Note that this family was added to CC 2.1 by CCIMB Interpretation 065

Functional Components	
	Management of Security Attributes
FMT_MSA.1 Management of Security Attributes	FMT_MSA.1.1 - The TSF shall enforce the [*access control SFP*] to restrict the ability to [*add*, *change and delete*] the security attributes:[*a) users' permitted published applications* *b) users' configuration data]* to *[authorised administrators.]*
FMT_MSA.3 Static Attribute Initialisation	FMT_MSA.3.1 - The TSF shall enforce the [*access control SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP. FMT_MSA.3.2 – The TSF shall allow the [*authorised administrator*] to specify alternative initial values to override the default values when an object or information is created.
	Management of functions in TSF
FMT_MOF.1(1) Management of security functions behaviour	FMT_MOF.1.1(1) - The TSF shall restrict the ability to [*disable, enable*] the function [*cut and paste*] to [*the authorised administrator*].
FMT_MOF.1 (2) Management of security functions behaviour	FMT_MOF.1.1(2) – The TSF shall restrict the ability to [*disable, enable*] the function [*client drive mapping*] to [*the authorised administrator*].
	Access Control Policy
FDP_ACC.1 Subset access control	FDP-ACC.1.1 - The TSF shall enforce [*access control SFP*] on [*a) applications* *b) application data*

Functional Components	
	c) users' configuration data *d) mapped client drives].*
FDP_ACF.1 Security attribute based access control	FDP-ACF.1.1 - The TSF shall enforce [*access control SFP*] to objects based on [*user identity and user access permissions].* FDP-ACF.1.2 - The TSF shall enforce the following rules to determine if an operation among controlled subjects and objects is allowed: *[Applications shall be accessible by a user if:* • *The application is published,* • *The user is authorised, and* • *The user's access permissions allow access.* *Users shall be permitted to cut and paste application data between a published application and a Windows client clipboard if the function has been enabled by the authorised administrator.* *Client drives shall be accessible to a published application if:* • *The function has been enabled by the authorised administrator, and* • *The user has permitted the access*[9]*.* FDP-ACF.1.3 - The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*No rules].* FDP-ACF.1.4 - The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*Access by a user to applications that are not permitted published applications shall be denied].*

[9] The Windows XP access permissions must also allow the user access to the client drives. This is controlled by the client operating system and is outside the scope of control of the TOE.

Functional Components	
FPT_ITT.1 Basic Internal TSF Data Transfer Protection	FPT_ITT.1.1 - The TSF shall protect TSF data from [*disclosure and modification*] when it is transmitted between separated parts of the TOE. Notes: This is intended to cover TSF data traffic used during authentication and subsequent communication. Additionally, it protects TSF data by ensuring that secure authentication of the end point of the communication path between client and server occurs. Here the SFR relates to the use of TLS between the client and the secure gateway server. The SFR is repeated in the section on requirements for the IT environment to address the use of IPSEC within the server component.
	Reference Mediation
FPT_RVM.1 Non-bypassability of the TSP	FPT_RVM.1.1 - The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSF is allowed to proceed Note: The fact that the TOE must ensure TLS protocol is not bypassed during communication between the client and server is included by this SFR.
	Identification and Authentication
FIA_ATD.1 User Attribute Definition	FIA_ATD.1.1 - The TSF shall maintain the following list of security attributes belonging to individual users:[*Access permissions for permitted published applications]*.
FIA_UAU.2[10] User Authentication before any action	FIA_UAU.2.1 - The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

[10] Implicit within this is the requirement for the operating system to protect authentication credentials against unauthorised disclosure.

Functional Components	
FIA_UID.2 User Identification before any action	FIA_UID.2.1 - The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
FTP_ITC.2[11] Client-server trusted channel	FTP_ITC.2.1 The TSF shall provide a communication channel between [*the ICA client and the secure gateway*] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure. FTP_ITC.2.2 The TSF shall permit [*the ICA client*] to initiate communication via the trusted channel. FTP_ITC.2.3 The TSF shall initiate communication via the trusted channel for [*authentication of the server and all communication*]

Table 5-1 Functional Requirements for the TOE

5.2 IT Environment Security Functional Requirements

The security functional requirements for the IT environment are presented in this section. The following table identifies those security requirements.

Functional Components	
	Cryptographic Key Management
FCS_CKM.1 Cryptographic key generation	FCS_CKM.1.1 – The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [*FIPS 186-2 Appendix 3 Section 3.3 SHS random number generator*] and specified cryptographic key sizes [*168 bit*] that meet the following: • [*FIPS140, Level 1*].

[11] Note that this is an extended component.

Functional Components	
FCS_CKM.2(1) Cryptographic key distribution	FCS_CKM.2.1 – The TSF shall distribute cryptographic keys in accordance with a specified key distribution method [RSA, *as defined by the ciphersuite RSA_WITH_3DES_CBC_SHA in the TLS specification in RFC 2246*] that meets the following: • [*FIPS140, Level 1*].
FCS_CKM.2(2) Cryptographic key distribution	FCS_CKM.2.1 – The TSF shall distribute cryptographic keys in accordance with a specified key distribution method [OAKLEY, *as defined by IPSec in RFC 2412*] that meets the following: [*FIPS140, Level 1*].
FCS_CKM.4(1) Cryptographic key destruction	FCS_CKM.4.1 – The TSF shall destroy cryptographic keys in accordance with a specified key destruction method [TLS - *Microsoft Schannel key destruction method*] that meets the following: • [*FIPS140, Level 1*].
FCS_CKM.4(2) Cryptographic key destruction	FCS_CKM.4.1 – The TSF shall destroy cryptographic keys in accordance with a specified key destruction method [IPSec - *Microsoft IPSec key destruction method*] that meets the following: [*FIPS140, Level 1*].
	Cryptographic operation
FCS_COP.1(1) Cryptographic operation	FCS_COP.1.1 - The TSF shall perform [*encryption of traffic between client and server components*] in accordance with the specified cryptographic algorithm [3DES as defined by the ciphersuite *RSA_WITH_3DES_EDE_CBC_SHA in the TLS specification in RFC 2246*] and cryptographic key sizes [*168 bit*] that meet the following: • [*FIPS140-2, Level 1*].

Functional Components	
FCS_COP.1(2) Cryptographic operation	FCS_COP.1.1 - The TSF shall perform [*encryption of traffic between machines within the server component*] in accordance with the specified cryptographic algorithm [3DES as defined *in the IPSec specification in RFC 2451*] and cryptographic key sizes [*168 bit*] that meet the following: [*FIPS140-2, Level 1*].
	Internal Data Transfer Protection
FDP_ITT.1 Basic Internal Transfer Protection	FDP_ITT.1.1 - The TSF shall enforce the [*access control SFP*] to prevent the [*disclosure and modification*] of data associated with applications when it is transmitted between physically-separated parts of the TOE.
FPT_AMT.1 Abstract Machine Testing	FPT_AMT.1.1 The TSF shall run a suite of tests [*during initial start-up, at the request of an authorised user*] to demonstrate the correct operation of the security assumptions provided by the abstract machine that underlies the TSF.[12]
FPT_ITT.1 Basic Internal TSF Data Transfer Protection	FPT_ITT.1.1 - The TSF shall protect TSF data from [*disclosure and modification*] when it is transmitted between separated parts of the TOE. Note: This is intended to cover user data traffic used during authentication and subsequent communication. Additionally, it protects user data by ensuring that secure authentication of the end point of the communication path between client and server occurs.
FDP_RIP.1 Subset residual information protection	FDP_RIP.1.1 – The TSF shall ensure that any previous information content of a resource is made unavailable upon the [*deallocation of the resource from*] the following objects: [Windows client volatile memory].

[12] This security functional requirements FPT_AMT.1 and FPT_TST.1 are to be met through provision of anti-virus software.

Functional Components	
FPT_TST.1 TSF Testing	FPT_TST.1.1 - The TSF shall run a suite of self tests [*during initial start-up, at the request of the authorised user*] to demonstrate the correct operation of [*the TSF*]. FPT_TST.1.2 – The TSF shall provide authorised users with the capability to verify the integrity of [*TSF data*]. FPT_TST.1.3 – The TSF shall provide authorised users with the capability to verify the integrity of stored TSF executable code.
	Identification and Authentication
FIA_UAU.2 User Authentication before any action	FIA_UAU.2.1 - The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
FIA_UID.2 User Identification before any action	FIA_UID.2.1 - The TSF shall require each user to identify itself before allowing any other TSF-mediated actions on behalf of that user.
FIA_AFL.1 Authentication Failure Handling	FIA_AFL.1.1 - The TSF shall detect when [*an administrator configurable positive integer within* [*the range of values supported by the underlying operating system*]] unsuccessful authentication attempts occur related to [*user authentication*]. FIA_AFL.1.2 – When the defined number of unsuccessful authentication attempts has been met or surpassed, the TSF shall [*display "access denied" and not display a list of applications*]. Note - This applies to the server component only. Client component authentication is carried out by the Operating System and is not configured by the server component administrator.

Functional Components	
	Domain Separation
FPT_SEP.1 TSF Domain Separation	FPT_SEP.1.1 – The TSF shall maintain a security domain for its own execution that protects it from interference and tampering from untrusted subjects. FPT_SEP.1.2 – The TSF shall enforce separation between the security domains of subjects in the TSC.
	Security Management
FMT_MSA.2 Secure Security Attributes	FMT_MSA.2.1 – The TSF shall ensure that only secure values are accepted for security attributes. Note: This SFR is present to cover the handling of encryption keys.

Table 5-2: IT Environmental Security Functional Requirements

5.3 TOE Security Assurance Requirements

The security assurance requirements are taken from Part 3 of the CC and are those that comprise the EAL2 assurance package, with the addition of ALC_FLR.2 Flaw Reporting Procedures). The assurance components are identified in the following table.

Assurance Class	Assurance Components	
Configuration management	ACM_CAP.2	Configuration items
Delivery and operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation and start-up procedures

Assurance Class	Assurance Components	
Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Guidance documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Flaw Remediation	ALC_FLR.2	Flaw Reporting Procedures
Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
Vulnerability assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 5-3: Assurance Requirements: EAL2+

Further information on these assurance components can be found in [CC] Part 3.

5.4 Strength of Function Claim

A Strength of Function (SoF) claim of SoF-BASIC is made for the TOE.

Note: The Windows operating system provides the function that authenticates users. This is out of scope of the TOE, so there are no mechanisms requiring assessment.

6 TOE Summary Specification

6.1 TOE Security Functions

This section describes the security functions provided by the TOE to meet the security functional requirements specified for the TOE in Section 5.1.

F1 – User Authentication

A user will be authorised to access the XML Service or to launch an application on the ICA Server only if the user identity and password or smartcard and smartcard PIN, supplied by the user are valid.

F2 – User Access

An authorised user will be allowed access to a published application only if the published application is a member of the user's set of permitted published applications.

F3 – Membership of user's permitted application set

An application is a member of the set of permitted published applications for a given user only if an administrator has published the application and has set the access permission list to allow that.

F4 – Inter-Component Encryption

All data transmitted between client and server components is encrypted using the TLS protocol. The TOE performs the following encryption:

- RSA_WITH_3DES_EDE_CBC_SHA, which has the following attributes:
    - Key Exchange = RSA
    - Cipher algorithm =3DES_EDE_CBC
    - Hash algorithm = SHA

This is carried out by calls to the Microsoft Cryptographic Service Providers (CSPs) and associated crypto algorithms associated with Windows 2003 CryptoAPI to encrypt/decrypt communication between client and server. The cipher algorithm 3DES_EDE_CBC performs encryption of traffic between client and server components. The cipher algorithm 3DES_EDE_CBC specifies TripleDES in Encrypt-Decrypt-Encrypt mode with Cipher-Block Chaining. The size of the TripleDES key is 168 bits.

Further details can be found at http://www.ietf.org/rfc/rfc2246.txt.

F5 – Secure authentication mechanism

The TLS mechanism will ensure that client components are able to identify server components as authentic. Further details can be found at http://www.faqs.org/rfcs/rfc2246.html and http://support.microsoft.com/

F6 – Availability of permitted published applications

Following authentication, authorised users are provided with access to all of their permitted published applications.

F7 – Cut and Paste

When the function is enabled by the authorised administrator, users may cut, copy and paste information between a published application and a Windows clipboard on the client.[13]

F8 – Client Drive Mapping

When the function is enabled by the authorised administrator; a published application, if permitted by the user, may access the local drives on the client machine.[14]

6.2 Assurance Measures

Deliverables will be produced to comply with the Common Criteria security assurance requirements for EAL2, with the addition of ALC_FLR.2 (Flaw Reporting Procedures).

---

[13] The Cut and Paste functionality can be enabled / disabled either globally (for all users) or on the basis of individual users or user groups. Only the global enable / disable is included within the scope of the evaluation.

[14] The Client Drive mapping functionality can be enabled / disabled either globally (for all users) or on the basis of individual users or user groups. Only the global enable / disable is included within the scope of the evaluation.

It should be noted that a Client user can allow an application no access, full access or read access to the local drives. This setting applies to all users of the client machine and can be changed at any time by a different logged on user.

7 Protection Profiles Claims

There are no Protection Profile Claims.

8 Rationale

8.1 Introduction

This section identifies the rationale for the adequacy of the security functional requirements and the security assurance requirements in addressing the threats and meeting the objectives of the TOE.

8.2 Security Objectives for the TOE and Environment Rationale

The following table demonstrates how the objectives of the TOE and the TOE environment counter the threats identified in Section 3.2.1.

Note that all assumptions are axiomatic and hence not shown in this table. It would be possible to restate each one as an objective for the environment, and provide a one to one mapping for these, but this step has been omitted for clarity. There are no policies to consider.

Threats / **Objectives**	T.AUTHENTIC	T.ACCESS1	T.ACCESS2	T.MOD_CONF	T.MISDIRECT	T.AVAIL	T.MOD_HW_Server	T.MOD_HW_Client	OSP.CRYPTO
OT.AUTHENTIC_SERVER	✓								
OT.AUTHENTIC_CLIENT		✓	X	✓					
OT.CONF_CLIENT		✓							
OT.INTEG_CLIENT		✓	X						
OT.CONF		✓	✓						
OT.INTEG		✓	✓						
OT.GATE_ALLOW	✓				✓	✓			
OT.CUT_PASTE			✓						
OT.DRIVES			✓						

Threats / **Objectives**	T.AUTHENTIC	T.ACCESS1	T.ACCESS2	T.MOD_CONF	T.MISDIRECT	T.AVAIL	T.MOD_HW_Server	T.MOD_HW_Client	OSP.CRYPTO
OT.SECURE_ENCRYPTION	X	X	X	X	X	X			✓
OT.APPS_AVAIL						✓			
OE.OS_CONFIG_SERVER	X	X	X	✓	✓	✓			
OE.OS_CONFIG_CLIENT	X	X	X	X	✓	X			
OE. SERVERTHIRDPARTYSW	X	X	X	X	X	X			
OE.CLIENT_TPSW	X	X	X	X	✓	X			
OE.MALWARE_PROTECT	X	X	X	X	✓	X			
OE.SECURE_ENCRYPTION	X	X	X	X	X	X			✓
OE.SESSION_KEYS	X	X	X	X	X	X			
OE.CERTIFICATES	X	X	X	X	X	X			
OE.LIMIT_AUTH		✓		X					
OE.PASSWORD_SETUP		✓							
OE.TRUSTED_OPS	X	X	X	X	X	X			
OE.SERVER_PHYSICAL	X	X	X	X	X	X	✓		
OE.CLIENT_PHYSICAL	X	X	X	X		X		✓	
OE.IPSEC	X	✓	✓	✓					✓
OE.MEMORY		✓							

Table 8-1 Objectives Rationale

Key:

X Indirect contribution to meeting a threat

✔ Direct contribution to meeting a threat

As can be seen from the table above, all threats and organisational security policies are met by at least one objective of, either the TOE or environment, as applicable. The coverage of the threats countered by the TOE is discussed in the subsections below.

With the exception of T.MOD_HW_Server and T.MOD_HW_Client, all of the threats require that certain objectives are met to ensure the configuration is secure. These are:

- OE.OS_CONFIG_SERVER – to ensure the server has been set up correctly;
- OE.OS_CONFIG_CLIENT – to ensure client devices have been set up correctly;
- OE.SERVER_THIRD_PARTY_SW, OE.CLIENT_TPSW, OE.MALWARE_PROTECT – to ensure that potentially privileged or malicious programs do not undermine security;
- OE.CERTIFICATES, OE.SESSION_KEYS – to ensure that cryptographic certificates provide the protection intended;
- OT.SECURE_ENCRYPTION, OE.SECURE_ENCRYPTION – to ensure that FIPS 140 compliant encryption modules are used;
- OE.TRUSTED_OPS – to ensure that administrators do not abuse their privileges;
- OE.SERVER_PHYSICAL – to ensure only authorised access to the Presentation servers occurs.

These mappings are shown as "X" in the above table. All objectives that play a more specific part in countering the threat are shown as " ✔ ". Additionally, described below are the objectives that meet specific threats.

T.AUTHENTIC

The use of TLS ensures that clients are able to be sure they are connected to a valid Presentation server (OT.Authentic_Server). OT.Gate_Allow ensures that traffic does not connect to non-Presentation servers (which are not part of the TOE).

T.ACCESS1

Unauthorised access to data (by an *unauthorised person*) is prevented by ensuring that only authorised users are able to authenticate themselves (OT.Authentic_Client and OE.Password_Setup) and that having done so all traffic is kept confidential (OT.Conf and OE.IPSEC). Data situated on client devices is also kept confidential (OT.Conf_Client). OE.Limit_Auth restricts the number of unsuccessful login attempts permitted.

OT.Integ maintains the integrity of data traffic between client and server and data situated on the server. The integrity of data situated on client devices is maintained by OT.Integ_Client.

OE.Memory ensures that the contents of the Windows client volatile memory are not available for other processes when a session is complete.

T.ACCESS2

Unauthorised access to data (by an *authorised user* of the system) is prevented by ensuring that authorised users are configured only to see those applications they should (OT.Conf), and that cut and paste, and client drive access operations only occur when authorised (OT.Cut_Paste and OT.Drives). The authentication mechanism ensures the correct application set access is mapped to a given user. Additionally, users must keep their password secure otherwise other users could impersonate them. OT.Integ maintains the integrity of data traffic between client and server and data situated on the server. OE.IPSEC maintains confidentiality of server traffic.

T.MOD_CONF

User configuration data is kept secure by the fact that the access permissions to permitted published applications (and the files defining that configuration data itself) are correctly set up (OE.OS_Config_Server) and that this will only be carried out and modifiable by administrators, who are authenticated (OT.Authentic_Client). OE.IPSEC maintains confidentiality of server traffic.

T.AVAIL

This threat is countered by the objective that the applications shall be available (OT.Apps_Avail). Additionally, the administrator must have correctly configured the permitted published applications so that the user has access to his set (OE.OS_Config_Server)

T.MISDIRECT

This threat is covered by an objective that the gateway enforce control over the destination address of client traffic (OT.Gate_Allow), together with objectives for control over the software on the client (OE.OS_Config_Client, OE.Client_TPSW and OE.MalwareProtect), and on the server (OE.OS_Config_Server).

T.MOD_HW_Server

This threat is countered by the objective that ensures physical protection of the server (OE_Server_Physical).

T.MOD_HW_Client

This threat is countered by the objective that ensures physical protection of the client (OE_Client_Physical).

OSP.CRYPTO

This organisational security policy is addressed by the TOE and environmental objectives that requires FIPS 140 approved cryptographic modules (OT.Secure_Encryption, OE.Secure_Encryption, OE.IPSEC).

8.3 Security Requirements Rationale

8.3.1 TOE security functional requirements are appropriate

The following table identifies which TOE SFRs satisfy the TOE Objectives defined in Section 4.1.1. The coverage of the objectives by the SFRs is discussed below.

Security Functional Requirements	FCS_COP.1(1)	FPT_RVM.1	FPT_ITT.1	FMT_SMR.1	FMT_SMF.1	FMT_MOF.1(1)	FMT_MOF.1(2)	FMT_MSA.1	FMT_MSA.3	FDP_ACC.1	FDP_ACF.1	FDP_ITT.1	FIA_ATD.1	FIA_UAU.2	FIA_UID.2	FTP_ITC.2
OT.AUTHENTIC_ SERVER	X	X	✓	X	X			X	X			✓				✓

Security Functional Requirements	FCS_COP.1(1)	FPT_RVM.1	FPT_ITT.1	FMT_SMR.1	FMT_SMF.1	FMT_MOF.1(1)	FMT_MOF.1(2)	FMT_MSA.1	FMT_MSA.3	FDP_ACC.1	FDP_ACF.1	FDP_ITT.1	FIA_ATD.1	FIA_UAU.2	FIA_UID.2	FTP_ITC.2
OT.AUTHENTIC_ CLIENT	X	X	X	X	X			X	X			X	✓	✓	✓	
OT.CONF_ CLIENT	X	X	✓	X	X			X	X			✓				
OT.INTEG_ CLIENT	X	X	✓	X	X			X	X			✓				
OT.CONF	X	X	✓	X	X			X	X	✓	✓	✓				
OT.INTEG	X	X	✓	X	X			X	X	✓	✓	✓				
OT.GATE_ALLO W	✓	X	X	X	X			X	X	✓	✓	X				
OT.CUTPASTE					✓	✓				✓	✓					
OT.DRIVES					✓		✓			✓	✓					
OT.SECURE_ENC RYPTION	✓	X	X	X	X			X	X			X				
OT.APPS_ AVAIL	X	X	X	✓	✓			✓	✓	✓	✓	X	✓			

Table 8-2 Mapping of TOE Objectives to TOE SFRs

All of the objectives require that certain SFRs are implemented correctly to ensure the TOE is secure. These are:

- FPT_RVM.1 – this SFR ensures that all and any security functionality of the TOE is invoked as required. As such, all objectives depend on it.
- FCS_COP.1(1) – this ensures that the cryptography used in the TOE is correctly implemented.
- FPT_ITT.1 and FDP_ITT.1 – These ensure that all TOE traffic is kept securely, whether that be within TOE components or between them.
- FMT_SMR.1, FMT_SMF.1, FMT_MSA.1, FMT_MSA.3 – The TOE will only be secure if the security management functions are correctly implemented. These allow different roles (User and Administrator) to be distinguished from each other and allow associated security attributes to be set.

These mappings are shown as "X" in the above table. All SFRs that satisfy objectives more specifically are shown as " ✔ ". Additionally, described below are the SFRs

that satisfy specific objectives.

OT.AuthenticServer

This objective is addressed by FTP_ITC.2, FPT_ITT.1 and FDP_ITT.1. The mechanism that ensures the end point of the communication path between client and server is authentic is, in fact, ensuring the server is authentic.

FTP_ITC.2 covers the authentication process. FDP_ITT.1 and FPT_ITT.1 cover protection against loss of confidentiality and availability for user and TSF specific data, respectively.

OT.AuthenticClient

This objective is addressed primarily by SFRs FIA_UAU.2 and FIA_UID.2, which ensure that users must be identified and authenticated before being able to use TOE functionality. This relies on FIA_ATD.1 being correctly implemented so that the identification and authentication will occur correctly.

OT.Conf_Client

The objective is addressed by FPT_ITT.1, FDP_ITT.1 and FDP_RIP.1. Confidentiality of data on the client machine is protected by ensuring that secure authentication of the endpoint of the communication path (the server component) occurs correctly. As long as client devices connect only to known secure servers, then they can trust that server won't break confidentiality of data on their client. Purging of volatile storage at the end of a user session also helps maintain this confidentiality.

OT.Integ_Client

The objective is addressed by FPT_ITT.1 and FDP_ITT.1. Integrity of data on the client machine is protected by ensuring that secure authentication of the endpoint of the communication path (the server component) occurs correctly. As long as client devices connect only to known secure servers, then they can trust that server won't break integrity of data on their client.

OT.Conf and OT.Integ

Both of these objectives are addressed through the correct implementation of all data transfer encryption (FPT_ITT.1 and FDP_ITT.1) and the access control policy (FDP_ACC.1 and FDP_ACF.1) to ensure data is kept confidential and not subject to modification.

OT.Apps_Avail

Access to permitted published applications will be available as long as users' security attributes are maintained correctly (FMT_SMR.1, FMT_SMF.1, FMT_MSA.1,

FMT_MSA.3, FIA_ATD.1) and the access control SFRs are in place (FDP_ACC.1 and FDP_ACF.1).

OT.Gate_Allow

This objective is addressed through requirements FDP_ACC.1 and FDP_ACF.1, which require access to applications other than those permitted to be denied, and through the requirement for traffic to be correctly encrypted (FCS_COP.1(1)).

OT.Cut_Paste

This objective is addressed through requirements FMT_MOF.1(1), FMT_SMF.1, FDP_ACC.1 and FDP_ACF.1, which require the ability to carry out cut and paste operations to be enabled by an authorised administrator.

OT.Drives

This objective is addressed through requirements FMT_MOF.1(2), FMT_SMF.1, FDP_ACC.1 and FDP_ACF.1, which require the ability to carry out client drive mapping operations to be enabled by an authorised administrator.

OT.Secure_Encryption

The objective for FIPS140 approved encryption is addressed through FCS_COP.1(1).

8.3.2 IT environment functional requirements are appropriate

The following table identifies which IT environment SFRs address the objectives for the IT environment defined in Section 4.2.1. The coverage of the objectives by the SFRs is discussed below. It should be noted that many of these objectives will be met through procedural and administrative measures, and as such there may be objectives that do not map to any of the included security functional requirements.

Security Functional Requirements	FDP_RIP.1	FCS_COP.1(1)	FCS_COP.1(2)	FCS_CKM.1	FCS_CKM.2(1)	FCS_CKM.2(2)	FCS_CKM.4(1)	FCS_CKM.4(2)	FIA_AFL.1	FIA_UID.2	FIA_UAU.2		FPT_AMT.1	FPT_SEP.1	FPT_TST.1	FMT_MSA.2
OE.OS_CONFIG_SERVER																✓
OE.OS_CONFIG_CLIENT																✓
OE.SERVER_THIRD_PARTY_SW																✓

Security Functional Requirements	FDP_RIP.1	FCS_COP.1(1)	FCS_COP.1(2)	FCS_CKM.1	FCS_CKM.2(1)	FCS_CKM.2(2)	FCS_CKM.4(1)	FCS_CKM.4(2)	FIA_AFL.1	FIA_UID.2	FIA_UAU.2		FPT_AMT.1	FPT_SEP.1	FPT_TST.1	FMT_MSA.2
OE.MALWARE_PROTECT													✓		✓	
OE.SECURE_ENCRYPTION		✓	✓	✓	✓	✓	✓	✓								
OE.SESSION_KEYS				✓	✓	✓	✓									
OE.LIMIT_AUTH									✓							
OE.PASSWORD_SETUP										✓	✓					
OE.IPSEC			✓	✓	✓	✓	✓	✓								
OE.MEMORY	✓															

Table 8-3 Mapping of IT environment objectives to IT environment SFRs

OE.OS_Config_Server, OE.OS_Config_Client and OE.Server_Third_Party_SW

These objectives relate to the need to configure the IT environment in a secure manner. This is partially supported by FMT_MSA.2, but is essentially reliant on sound administrative controls, rather than IT support.

OE.MALWARE_Protect

This objective requires the installation of specific third party software for virus and other malware protection. The security functional requirements for this software are addressed by FPT_AMT.1 and FPT_TST.1.

OE.Secure Encryption

The objective for FIPS140 approved encryption is addressed through FCS_COP.1(1), FCS_COP.1(2), FCS_CKM.1, FCS_CKM.2(1), FCS_CKM.2(2), FCS_CKM.4(1) and FCS_CKM.4(2).

OE.Session_Keys

This objective is addressed through requirements that deal with all aspects of the key

lifecycle (FCS_CKM.1, FCS_CKM.2(1), FCS_CKM.2(2), FCS_CKM.4(1) and FCS_CKM.4(2)).

OE.Limit_Auth

The objective to control unsuccessful authentication attempts is directly addressed by FIA_AFL.1.

OE.Password_Setup

This objective requires the use of operating system identification authentication functions as represented by FIA_UID.2 and FIA_UAU.2.

OE.IPSEC

This objective is addressed through the provision of encryption for traffic within the Presentation server component (FCS_COP.1(2)).

OE.MEMORY

This objective is addressed through the provision of Memory Object Reuse by the Client operating system (FDP_RIP.1).

8.3.3 Security Requirement dependencies are satisfied

TOE security functional requirements

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FCS_COP.1	FCS_ITC.1 or FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	Satisfied by provision of FCS_CKM.1, FCS_CKM.4 and FMT_MSA.2 in the IT environment. See table below.
FPT_RVM.1	None	Satisfied
FPT_ITT.1	None	Satisfied
FMT_SMR.1	FIA_UID.1	Satisfied by FIA_UID.2
FMT_SMF.1	None	Satisfied
FDP_ACC.1	FDP_ACF.1	Satisfied

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FDP-ACF.1	FDP_ACC.1, FMT_MSA.3	Satisfied
FDP_ITT.1	FDP_ACC.1 or FDP_IFC.1	Satisfied by FDP_ACC.1
FIA_ATD.1	None	Satisfied
FIA_UAU.2	FIA_UID.1	Satisfied by FIA_UID.2
FIA_UID.2	None	Satisfied
FMT_MOF.1(1)	FMT_SMF.1, FMT_SMR.1	Satisfied
FMT_MOF.1 (2)	FMT_SMF.1, FMT_SMR.1	Satisfied
FMT_MSA.1	FDP_ACC.1 or FDP_IFC.1, FMT_SMF.1, FMT_SMR.1	Satisfied
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	Satisfied
FTP_ITC.2	None	Satisfied

IT environment security functional requirements

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
FCS_CKM.1	FCS_CKM.2 or FCS_COP.1, FCS_CKM.4, FMT_MSA.2	Satisfied
FCS_CKM.2	FCS_ITC.1 or FCS_CKM.1, FCS_CKM.4, FMT_MSA.2	Satisfied
FCS_CKM.4	FCS_ITC.1 or FCS_CKM.1, FMT_MSA.2	Satisfied
FCS_COP.1	FCS_ITC.1 or FCS_CKM.1, FCS_CKM.4,	Satisfied

Functional Component	Dependencies	SFR(s) in Security Target meeting Dependencies
	FMT_MSA.2	
FDP_RIP.1	None	Satisfied
FIA_AFL.1	FIA_UAU.1	Satisfied by FIA_UAU.2
FIA_UID.2	None	Satisfied
FIA_UAU.2	FIA_UID.1	Satisfied by FIA_UAU.2
FMT_MSA.2	ADV_SPM.1, FDP_ACC.1 or FDP_IFC.1, FMT_MSA.1, FMT_SMR.1	Satisfied Note: FMT_MSA.2 is present to cover the handling of encryption keys. In this context the dependency on ADV_SPM.1 is not required, as 'secure values' are defined as those appropriate for the algorithm
FPT_AMT.1	None	Satisfied
FPT_SEP.1	None	Satisfied
FPT_TST.1	FPT_AMT.1	Satisfied

Table 8-3 Mapping of SFR Dependencies

8.3.4 Security Requirements are mutually supportive

The only interactions between the security requirements specified for the TOE are those which are identified in the CC Part 2 as dependencies between the SFRs. These dependencies are documented and demonstrated to be satisfied in Section 8.3.2. These interactions are specified in the CC Part 2, and are therefore mutually supportive

8.3.5 Security assurance requirements rationale

The assurance level EAL2 was selected as providing a moderate level of independently assured security, including confidence that the TOE will not be tampered with during delivery. This level of assurance should be sufficient to allow the TOE to be used to protect unclassified but sensitive information such as that found in government organisations. Such applications require evidence of third party functional and known vulnerability testing, good quality guidance documentation and a well specified external interface.

8.3.6 ST complies with the referenced PPs

This Security Target does not claim compliance with a Protection Profile.

8.4 IT security functions rationale

8.4.1 IT security functions are appropriate

The Table below provides a mapping of Section 6 IT functions to SFRs (Section 5.1).

IT Function	Security Functional Requirement(s)
F1	FPT_RVM.1, FIA_UAU.2, FIA_UID.2, FIA_ATD.1
F2	FPT_RVM.1, FDP_ACC.1, FDP_ACF.1, FMT_SMR.1., FPT_ITT.1, FDP_ITT.1
F3	FPT_RVM.1, FMT_SMR.1, FMT_SMF.1, FIA_ATD.1., FMT_MSA.1, FMT_MSA.3, FDP_ACC.1., FDP_ACF.1
F4	FPT_RVM.1, FDP_ITT.1, FPT_ITT.1, FCS_COP.1(1)
F5	FPT_RVM.1, FDP_ITT.1, FPT_ITT.1, FTP_ITC.2
F6	FPT_RVM.1, FMT_SMR.1, FMT_SMF.1, FMT_MSA.1, FMT_MSA.3, FDP_ACC.1, FDP_ACF.1, FIA_ATD.1
F7	FMT_MOF.1(1), FMT_SMR.1, FMT_SMF.1, FDP_ACC.1, FDP_ACF.1
F8	FMT_MOF.1(2), FMT_SMR.1, FMT_SMF.1, FDP_ACC.1, FDP_ACF.1

Table 8-4 Mapping of IT Functions to SFRs

As can be seen by the table above all Security Functional Requirements of the TOE are fully provided by the IT security functions specified in the TOE Summary Specification.

Also demonstrated in Table 8-4, all IT Security Functions identified for the TOE in the TOE Summary Specification are required to meet the TOE Security Functional Requirements.

Note that FPT_RVM.1 ensures that all and any security functionality of the TOE is invoked as required. As such, all Security Functions map to it.

F1 – User Authentication

A user will be authorised to access the XML Service or to launch an application on the ICA Server only if the user identity and password or smartcard and smartcard PIN supplied by the user are valid.

FIA_UAU.2 and FIA_UID.2 ensure that users must be identified and authenticated before being able to use TOE functionality. FIA_ATD.1 ensures the security attributes are available to achieve this.

F2 - User Access

An authorised user will be allowed access to a published application only if the published application is a member of the user's set of permitted published applications

FDP_ACC.1 ensures that the access control policy is operated on applications. FDP_ACF.1 defines the rules regarding **when** access is allowed. Note that it is necessary for the TOE to recognise a **user** as distinct from an administrator. This is provided by FMT_SMR.1.

Additionally, FPT_ITT.1 and FDP_ITT.1 protect access to data since they provide correct implementation of data transfer encryption between the client and the secure gateway server, hence enforcing confidentiality and integrity.

F3 – Membership of user's permitted application set

An application is a member of the set of permitted published applications for a given user only if an administrator has published the application and has set the access permission list to allow that.

Implementation of this function is dependent upon administrators having the ability to publish applications and to manage the security attributes of users, specifically the ability to set access permissions to published applications. The SFRs associated with this are FMT_SMR.1, FMT_SMF.1 and FIA_ATD.1.

Once an administrator has used the TOE to set the access rights, the TOE must then implement a mechanism to enforce them. This is covered by FMT_MSA.1, FMT_MSA.3, FDP_ACC.1.

FDP_ACF.1 defines the rules regarding **what** access is allowed (Note: It also defines when access is allowed).

F4 – Inter-Component Encryption

All data transmitted between client and server components is encrypted using the TLS protocol.

This is carried out by calls to the Microsoft Cryptographic Service Providers (CSPs)

and associated crypto algorithms associated with Windows 2000 CryptoAPI to encrypt/decrypt communication between client and server. . The cipher algorithm 3DES_EDE_CBC performs encryption of traffic between client and server components. The cipher algorithm 3DES_EDE_CBC specifies TripleDES in Encrypt-Decrypt-Encrypt mode with Cipher-Block Chaining. The size of the TripleDES key is 168 bits.

Further details can be found at http://www.ietf.org/rfc/rfc2246.txt.

FDP_ITT.1 and FPT_ITT.1 map to this Security Function. FCS_COP.1 states what encryption methods will be implemented by the TOE.

The TOE performs the following encryption:

- RSA_WITH_3DES_EDE_CBC_SHA, which has the following attributes:
    - Key Exchange = RSA
    - Cipher algorithm =3DES_EDE_CBC
    - Hash algorithm = SHA

FCS_COP.1 states what encryption methods will be implemented by the TOE.

This is carried out by calls to the Microsoft Cryptographic Service Providers (CSPs) and associated crypto algorithms associated with Windows 2000 CryptoAPI to encrypt/decrypt communication between client and server.

Further details can be found at http://www.faqs.org/rfcs/rfc2246.html and http://support.microsoft.com/

F5 – Secure authentication mechanism

The TLS mechanism will ensure that client components are able to identify server components as authentic. Further details can be found at http://www.faqs.org/rfcs/rfc2246.html and http://support.microsoft.com/

This security function is mapped to by FTP_ITC.2, FPT_ITT.1 and FDP_ITT.1. FTP_ITC.2 is concerned directly with authentication. The other two SFRs require that the traffic on the link is not disclosed or modified, and the authenticated link helps to ensure this.

F6 – Availability of permitted published applications

Following authentication, authorised users are provided with access to all of their permitted published applications.

Note: The intent of this function is that authorised users will have applications available to them. However, it is not intended to be so strong that continued access is ensured – i.e. it's allowable for a server to become unavailable or an internet connection to be lost. Nor is any claim made regarding speed of connection or

processing. The restriction of an authorised user to only his permitted published set is covered in F2.

Access to permitted published applications will be available as long as users security attributes are maintained correctly (FMT_SMR.1, FMT_SMF.1, FMT_MSA.1, FMT_MSA.3, FIA_ATD.1) and the access control SFRs are in place (FDP_ACC.1 and FDP_ACF.1.).

F7 – Cut and Paste

When the function is enabled by the authorised administrator, users may cut and paste information between a published application and a Windows clipboard on the client.

The TOE provides a function to allow or disallow use of cut and paste between accessible applications and a Windows clipboard (FDP_ACC.1 and FDP_ACF.1). This function is under the control of the authorised administrator (FMT_MOF.1(1), FMT_SMF.1 and FMT_SMR.1).

F8 – Client Drive Mapping

When the function is enabled by the authorised administrator; a published application, if allowed by the user, may access the local drives on the client machine.

The TOE provides a function to allow or disallow use of Client Drive Mapping whereby a published application can access a client drive if permitted by the user (FDP_ACC.1 and FDP_ACF.1). Use of this function is controlled by the authorised administrator (FMT_MOF.1(2), FMT_SMF.1 and FMT_SMR.1).

8.4.2 IT security functions are mutually supportive

The mutually supportive nature of the IT security functions can be derived from the mutual support of the SFRs (demonstrated in Section 8.3.4), as each of the IT functions can be mapped to one or more SFRs, as demonstrated in Table 8-4.

8.4.3 Strength of Function claims are appropriate

The SoF claim made by the TOE is SOF-BASIC, which is defined in the CC Part 1 as “adequate protection against casual breaches of security”.

AVA_VLA.1, one of the assurance components from which the EAL2 assurance level is comprised, determines that “obvious vulnerabilities cannot be exploited in the intended environment of the TOE” (CC Part 3). Therefore, a SoF claim of SOF-BASIC demonstrates that the functions with an associated SoF would ensure that obvious vulnerabilities have been addressed.

Therefore, the claim of SOF-BASIC made by the TOE is viewed to be appropriate for this use.

8.4.4 Assurance measures satisfy assurance requirements

Table 8-5 Mapping of Assurance Measures to Assurance Requirements, below, provides a tracing of the Assurance Measures to the assurance requirements that they meet. From the table it can be seen that all assurance requirements trace to at least one assurance measure.

The assurance requirements identified in the table are those required to meet the CC assurance level EAL2, with the addition of ALC_FLR.2 (Flaw Reporting Procedures). As all assurance requirements are traced to at least one of the assurance measures, the identified assurance measures are sufficient to meet the assurance requirements. It is also asserted that the assurance measures have been produced with EAL2 in mind and as a consequence contains sufficient information to meet the assurance requirements of the TOE.

Assurance Measures (documentation)	Assurance Requirements Met by Assurance Measure	
Configuration Management Documentation	ACM_CAP.2	Configuration items
Delivery, Installation and generation Procedures	ADO_DEL.1	Delivery Procedures
	ADO_IGS.1	Installation, generation and start-up procedures
Functional Specification Documentation	ADV_FSP.1	Informal Functional Specification
High-Level Design Documentation	ADV_HLD.1	Descriptive high-level design
Flaw Remediation Documentation	ALC_FLR.2	Flaw reporting procedures
Correspondence Demonstration Document	ADV_RCR.1	Informal correspondence demonstration
Administrator Guidance Documentation	AGD_ADM.1	Administrator guidance
User Guidance Documentation	AGD_USR.1	User guidance

Assurance Measures (documentation)	Assurance Requirements Met by Assurance Measure	
Test Coverage Documentation	ATE_COV.1	Evidence of coverage
Test Plan and actual tests and Results	ATE_FUN.1	Functional testing
Independent Testing Resources	ATE_IND.2	Independent testing
Strength of Function Documentation	AVA_SOF.1	Strength of TOE security function evaluation
Vulnerability Assessment Analysis Documentation	AVA_VLA.1	Developer vulnerability analysis

Table 8-5 Mapping of Assurance Measures to Assurance Requirements