Common Criteria Security Target

For

XenApp 6.0 for Windows Server 2008 R2 – Platinum Edition

Version 1-0 7 February 2011

Summary of Amendments

Version 1-0 7 February 2011

First released version.

0. Preface

0.1 Objectives of Document

This document presents the Common Criteria (CC) Security Target (ST) to express the security and evaluation requirements for the Citrix® XenApp 6.0 for Windows Server 2008 R2 – Platinum Edition product.

The product is designed and manufactured by Citrix Systems Inc. (http://www.citrix.com/).

The Sponsor and Developer for the evaluation is Citrix Systems Inc. and the assurance level is EAL2 (augmented with ALC_FLR.2).

0.2 Scope of Document

The scope of the Security Target within the development and evaluation process is described in the Common Criteria for Information Technology Security Evaluation [CC]. In particular, a Security Target defines the IT security requirements of an identified TOE and specifies the functional and assurance security measures offered by that TOE to meet stated requirements [CC1, Section C.1].

Security Functional Requirements (SFRs), as defined in [CC2], are the basis for the TOE IT security functional requirements expressed in this Security Target. These requirements describe the desired security behaviour expected of a TOE and are intended to meet the security objectives as stated in this Security Target. Security Functional Requirements express security requirements intended to counter threats in the assumed operating environment of the TOE, and cover any identified organisational security policies and assumptions.

0.3 Intended Readership

The target audience of this ST are consumers, developers, certifiers and evaluators of the TOE; additional information can be found in [CC1, Section 6.2].

0.4 Related Documents

Common Criteria[1]

[CC1] Common Criteria for Information Technology Security Evaluation,
Part 1: Introduction and General Model,
CCMB-2009-07-001, Version 3.1 Revision 3, July 2009.

[1] For details see http://www.commoncriteriaportal.org/

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2: Security Functional Components,
CCMB-2009-07-002, Version 3.1 Revision 3, July 2009.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Components,
CCMB-2009-07-003, Version 3.1 Revision 3, July 2009.

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
CCMB-2009-07-004, Version 3.1, Revision 3, July 2009.

Developer documentation

[CCECG] Common Criteria Evaluated Configuration Guide for Citrix XenApp 6.0 for Windows Server 2008 R2, Document code: February 9 2011 16:28:33

0.5 Significant Assumptions

None.

0.6 Outstanding Issues

The following issues are awaiting resolution:

None.

0.7 Abbreviations

Acronym	Meaning
AD	Active Directory
CC	Common Criteria for Information Technology Security Evaluation
EAL	Evaluation Assurance Level
ICA	Independent Computing Architecture
IMA	Independent Management Architecture
IT	Information Technology
MMC	Microsoft Management Console
OSP	Organisational Security Policy
PIN	Personal Identification Number
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy

Acronym	Meaning
SFR	Security Functional Requirement
SG	Secure Gateway
SID	Security Identifier
SSO	Single Sign-On
ST	Security Target
STA	Secure Ticket Authority
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
WI	Web Interface

0.8 Glossary

Term	Meaning
Administrator	A person working on behalf of the application 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 XenApp and Windows) such that access is allowed as intended. Administrators can make use of administration tools to configure the system and manage Users. Administrators have physical access to the server component of the TOE.
Assurance	Grounds for confidence that a TOE meets the SFRs [CC1]
Clipboard Transfer	The transfer of data using cut, copy and paste operations, between a XenApp application session and the local Windows clipboard on an endpoint device connected to that application session.
Delivery Services Console	The Delivery Services Console (DSC) provides the administration interface to the XenApp Server, providing administrators with a number of management functions. The DSC is used to set up and monitor servers, Server Farms, published resources, and sessions.
Endpoint device	A device used by a user to gain access to their permitted published applications. The evaluated configuration of XenApp defines the endpoint device to be a PC as described in section 1.4.4.1.
Evaluation Assurance Level	An assurance package, consisting of assurance requirements drawn from CC Part 3, representing a point on the CC predefined assurance scale. [CC1]

Term	Meaning
ICA Protocol	The protocol that the Online Plug-in uses to present input (keystrokes, mouse clicks, etc) to XenApp for processing. ICA Servers use it to format application output (display, audio, etc) and return it to the endpoint device.
ICA Server	The ICA Server runs published applications and makes them available to authorised users (via the Online Plug-in on the user's endpoint device) in application sessions. ICA Servers can be grouped to form Server Farms.
IMA	IMA provides an intelligent interface between the XenApp server-side subsystems, and between the server components and components of the operating system. It resolves queries and requests relating to user authentication, enumeration, resolution and session management. IMA is a part of an ICA Server, and includes the Data Collector.
IPSec	A set of standard extensions to the Internet Protocol that provides authenticated and encrypted communications with data integrity and replay protection.
License Server	A server that validates licenses for Citrix products.
Online Plug-In	The Online Plug-in (formerly known as the ICA Client) allows the user access to published applications on an ICA Server, as if they were running locally. It sends inputs from the keyboard, mouse, etc on an endpoint device and receives screen updates from the ICA Server. (In the TOE, this is the 'Online Plug-in – web' version of the Online Plug-in.)
Operational Environment	The environment in which the TOE is operated. [CC1]
Organisational Security Policy	A set of security rules, procedures, or guidelines imposed (or presumed to be imposed) now and/or in the future by an actual or hypothetical organisation in the operational environment. [CC1]
Permitted Published Applications	The set of published applications to which an authorised User has been granted access. (See also Published Applications)
Personal Identification Number	The data used to authenticate the holder of a smartcard to that card when using smartcard login.
Protection Profile	An implementation-independent statement of security needs for a TOE type. [CC1]
Published Applications	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 (see Permitted Published Applications).
Secure Gateway	The Secure Gateway is used to establish authenticated connections between Online Plug-ins and ICA Servers, and provides secure channels that protect confidentiality and integrity of data sent between Online Plug-ins and ICA Servers.

Term	Meaning
Secure Ticket Authority	The Secure Ticket Authority generates and validates tickets that allow an Online Plug-in to gain access to an ICA Server (via the Secure Gateway) to run a published application for a particular authenticated user.
Security Assurance Requirement	A description of how assurance is to be gained that the TOE meets the SFRs. [CC1]
Security Attribute	A property of subjects, users (including external IT products), objects, information, sessions and/or resources that is used in defining the SFRs and whose values are used in enforcing the SFRs. [CC1]
Security Function Policy	A set of rules describing specific security behaviour enforced by the TSF and expressible as a set of SFRs. [CC1]
Security Functional Requirement	A translation of the security objectives for the TOE into a standardised language. [CC1]
Security Identifier	A unique value that is used to identify a security principal (such as a user) or security group in Windows operating systems.
Security Objective	A statement of intent to counter identified threats and/or satisfy identified organisation security policies and/or assumptions. [CC1]
Security Target	An implementation-dependent statement of security needs for a specific identified TOE. [CC1]
Server Farm	A Server Farm is a group of ICA Servers that can be managed as a single entity, and provides a load balancing capability.
Single Sign-On Component	A component providing additional functionality that can be used in conjunction with other XenApp components to provide a single sign-on and application password management capability. There are no claims relating to the SSO functionality in the scope of evaluation, but the evaluated configuration includes the presence of this component.
Target of Evaluation	A set of software, firmware and/or hardware possibly accompanied by guidance. [CC1]
TOE Security Functionality	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the SFRs. [CC1]
Transport Layer Security (TLS)	A protocol providing server authentication, data stream encryption and message integrity checks for a TCP/IP connection.
TSF Data	Data created by and for the TOE, that might affect the operation of the TOE. [CC1]
Web Interface	A server component providing an interface for Users to authenticate themselves, in order to gain access to their permitted published applications.
Web Interface Management Console	A console interface that allows administration activities at the Web Interface. This component can be used to configure the type of authentication required for users (username/password or smartcard/PIN).

Term	Meaning
XenApp Server	A collection of one or more of the following components running on one or more physical servers: Secure Ticket Authority, ICA Server (including IMA), DSC, XML Service.
XML Service	The XML Service is used by the Web Interface to retrieve the list of permitted published applications for a user, and the identity of the least loaded server (on which to run a selected application for a user).

Table of Contents

Figures / Tables

1. ST Introduction

1.1 ST and TOE Reference Identification

TOE Reference:	XenApp 6.0 for Windows Server 2008 R2 – Platinum Edition
ST Reference:	CIN4-ST-0001
ST Version:	1-0
ST Date:	7 February 2011
Assurance Level:	EAL2 augmented with ALC_FLR.2 Flaw Reporting Procedures
ST Author:	SiVenture

1.2 TOE Overview

1.2.1 Usage and major features of the TOE

The TOE is Citrix® XenApp 6.0 for Windows Server 2008 R2 – Platinum Edition (abbreviated in this document to "XenApp").

XenApp provides users (endpoint device users) with secure access to applications and information, allowing multiple users to log on and run applications in separate, protected sessions. Applications (word processors, spreadsheets or any other type of application) are made available to users in a process known as 'publishing' the applications, which is carried out by XenApp Administrators. The published applications that are available to a user (the user's "permitted published applications") are assigned on the basis of user identity.

Users access their permitted published applications (and associated data) via an Online Plug-in that resides on their local endpoint device. Keystrokes, mouse clicks and screen updates relating to the application sessions open in the Online Plug-in are sent between the user's endpoint device and the remote ICA Server on which the published application runs. To the user of the endpoint device it appears as if the application is running locally on their endpoint device.

Because applications run on the server and not on the endpoint device, users can connect from any platform[2]. Communication between the endpoint and server components is secured

[2] The endpoint device included in the evaluated configuration is defined in section 1.4.4.1.

using the Transport Layer Security (TLS) protocol. TLS provides server authentication, encryption of the data stream and message integrity checks, and thus enables secure delivery of an application within a LAN, WAN or across the Internet.

Client drive mapping can be enabled by an administrator, such that data storage devices on an endpoint device appear as network objects in Windows, making them available to the user's permitted published applications. If configured by an administrator, users are permitted to transfer information between a published application and a Windows clipboard on the client ('clipboard transfer').

XenApp provides the following security features:

- Authentication of users: endpoint device users are authenticated before access is granted to published applications. Authentication can be by username/password or by smartcard/PIN.

- User Access Control: XenApp administrators can assign user access to published applications. This is achieved by associating a user's Active Directory account with published applications.

- Control over use of endpoint device resources: centralised control policies, set by a XenApp administrator, determine whether an endpoint device user can access local endpoint device resources such as clipboard transfer and local storage devices (through client drive mapping).

- Secure communications: high performance, standards-based encrypted transmissions are used for communications between server components (IPSec) and between the endpoint device and server components (TLS).

The TOE is described in more detail in section 1.3.

1.2.2 TOE Type

XenApp is an access control system which provides remote, secure access to applications and information, allowing multiple users to run applications in separate, protected sessions.

1.3 TOE Description

The XenApp TOE is shown diagrammatically in Figure 1 below.

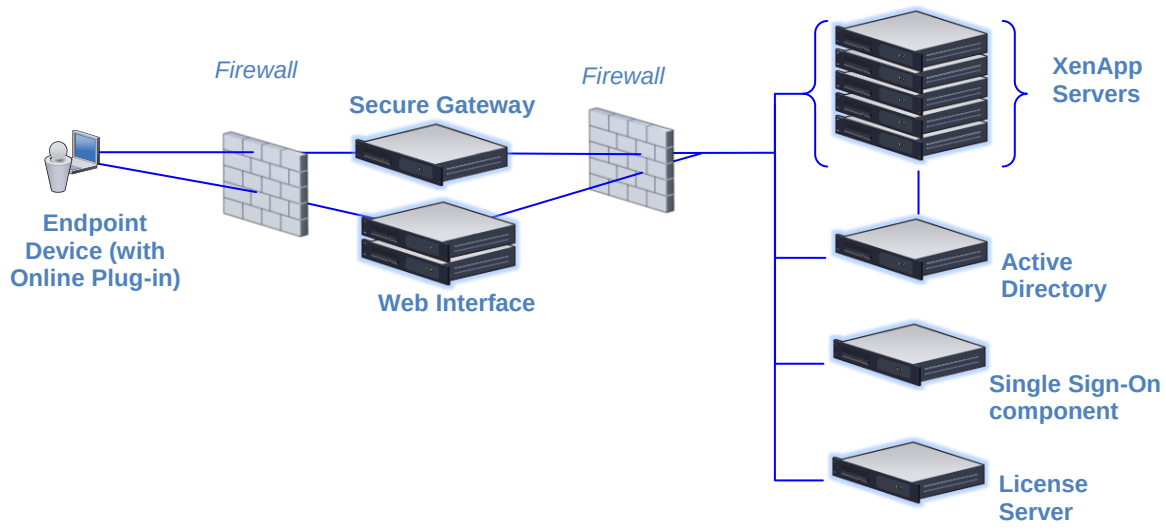

Figure 1: Deployment diagram of the TOE

The TOE comprises the following configuration of XenApp:

- A physical deployment of all the XenApp Server version 6.0 components[3] (ICA Server, XML Service and Secure Ticket Authority, with Hotfixes XA600W2K8R2X64002 & XA600W2K8R2X64021 (as described in [CCECG]), including at least two physical instances of the ICA Server component operating as a Server Farm
- Secure Gateway version 3.2
- Web Interface version 5.4
- Online Plug-in[4] version 12.1.

The evaluated configuration uses the Secure Gateway to provide an encrypted channel[5] between an Online Plug-in and the ICA Server on which its application session is running (the TOE invokes FIPS 140-2 validated Windows functions to provide the cryptographic

[3] The versions of the components in a XenApp Server is defined by the version number of the TOE as a whole (i.e. version 6.0). However, the three components identified in the list below (Secure Gateway, Web Interface, and Online Plug-in) are also available with their own separate version numbers. Hence, for clarity the version numbers of these items included in the TOE are given here.

[4] Note that this is the 'Online Plug-in – web' version of the Online Plug-in, which gives access to applications from a web interface. A version of the Online Plug-in giving access from either a web interface or a desktop is also available from Citrix, but is not the version used in the TOE.

[5] As can be seen in Figure 2, this channel is in fact in two parts: the Online Plug-in communicates with the Secure Gateway using TLS, and the Secure Gateway communicates with the ICA Server using IPSec.

functions for this secure channel; these Windows functions are not themselves part of the TOE). Communication also occurs between a Web Browser and Web Server (the communication is encrypted using HTTPS over TLS). Communication within the Server Component is secured using IPSec provided by Windows.

The evaluated configuration also includes operation of the TOE either with or without the use of the Single Sign-On/Password Management (v4.8) feature, although there are no claims relating to the Single Sign-On/Password Management functionality in the scope of evaluation.

The License Server is required for operation of the TOE, but is not itself part of the TOE, and is not in the scope of evaluation.

The logical components of the TOE are shown in Figure 2, and each component is described in more detail in sections 1.3.1-1.3.3 below. The way that the components interact in order to offer published applications to a user is then described in section 1.3.4. Figure 2 also shows physical boundaries for some of the components. As noted above, XenApp Server components may be distributed in various ways across physical servers. However, the Online Plug-in and web browser are both located on the same endpoint device, and separate physical servers must be used to host the Secure Gateway and the combination of web server, Web Interface and the Web Interface Management console.

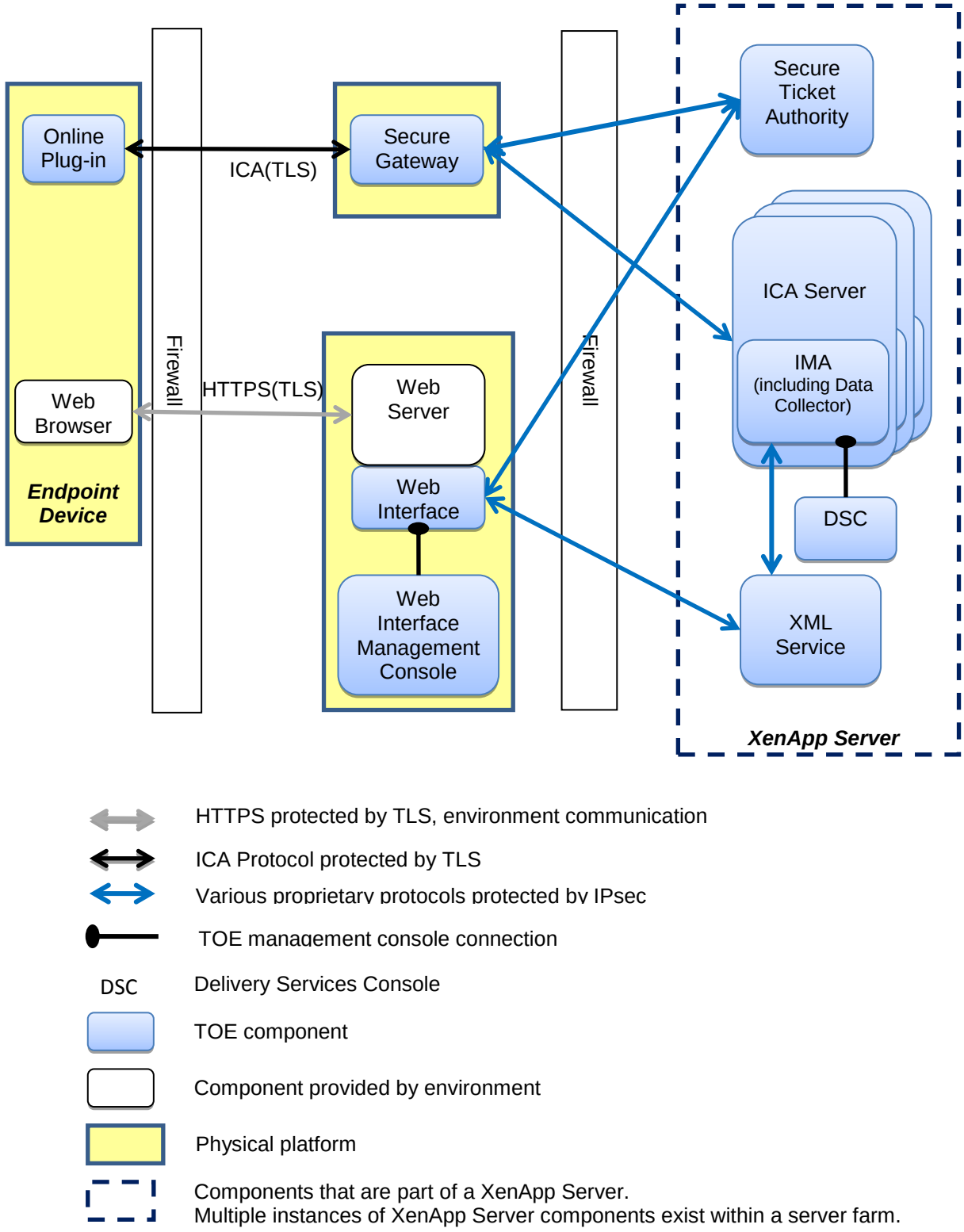

Figure 2: TOE logical structure

1.3.1 Endpoint Device Components

1.3.1.1 Online Plug-in

The Online Plug-in allows the user access to published applications on an ICA Server, as if they were running locally (note that this is the 'Online Plug-in – web' version of the Online Plug-in). The Online Plug-in intercepts and sends key strokes, mouse clicks, etc. from the local operating system and communicates them to the ICA Server. It receives screen updates in return, which it passes to the local operating system for display. Traffic between the Online Plug-in and the ICA Server (which travels via the Secure Gateway) is encrypted to protect confidentiality and integrity.

1.3.1.2 Endpoint Web Browser

The presence of a third party web browser is required on the endpoint device (in the evaluated configuration, Internet Explorer version 8.0 is used), which provides the communications channel to the Web Interface. Users access a list of their permitted applications from within their web browser, and click on links to launch published applications.

1.3.2 Server Components

1.3.2.1 ICA Server

The ICA Server is the XenApp component that runs published applications and may exist as one or more instances on one or more physical servers[6]. The ICA Server runs on the Windows Server operating system. XenApp Administrators install and publish the applications that are to be deployed by an ICA Server.

ICA Servers can be grouped together to form a Server Farm. A Server Farm is a group of ICA Servers that is managed as a single entity. Server Farms provide a flexible and robust way of deploying applications to users, allowing applications to be run on the least loaded server at the time of the access request.

1.3.2.2 Web Interface

The Web Interface gives users access to published applications. A user logs on to Web Interface using a web browser, and is presented with a dynamically created web page containing a list of links to the applications that they are authorised to launch (the user's permitted published applications). When the user selects an application from the Web page, the Web Interface generates the ICA file that the Online Plug-in on the endpoint device needs to connect to the ICA Server via the Secure Gateway.

[6] Each instance of the ICA Server runs on a separate physical server; a physical server hosts at most one ICA Server.

1.3.2.3 Web Server

The Web Server is used to communicate information about a user from the endpoint device web browser for use in authenticating the user and generating a web page showing a user's permitted published applications. The web server is a third-party component (in the evaluated configuration, Microsoft IIS is used).

1.3.2.4 Secure Gateway

The Secure Gateway permits users authenticated by Web Interface to access resources on an internal network and provides a link between two encrypted data tunnels (using TLS and IPSec protocols that invoke FIPS140-2 validated cryptographic functions provided by the operating system) for client-server communications.

1.3.2.5 Secure Ticket Authority (STA)

The Secure Ticket Authority generates and validates tickets that allow an Online Plug-in to gain access through the Secure Gateway to an ICA Server to run a published application for a particular authenticated user. The STA is called first by Web Interface to request an STA ticket for the least loaded ICA Server when a user has selected an application from the list of permitted published applications. The Online Plug-in, having received the STA ticket, presents it to the Secure Gateway with a request to connect to the specified published application. The Secure Gateway then sends the ticket to the STA for validation before initiating a session on the least-loaded ICA Server associated with the ticket.

1.3.2.6 XML Service

The XML Service is used by the Web Interface to retrieve the list of permitted published applications for a user, and the identity of the least loaded server (on which to run a selected application for a user), both of which are obtained by the XML Service from IMA.

1.3.2.7 IMA (including Data Collector)

IMA acts as an intelligent interface between the XenApp Server components of the TOE, and between the XenApp Server components and components of the Windows operating system. It is involved with authentication, session management and connections across the network. IMA contains the Data Collector, which is a dynamic data store containing frequently-updated data (such as server loading, which identifies the least-loaded server at any point), and also contains a persistent data store containing more static information (such as the list of published applications).

IMA locates the least-loaded ICA Server hosting a requested application and requests and communicates the logon ticket that is associated with a user. The logon ticket is used for identification and authentication of that user during subsequent communication between the endpoint device and the ICA Server.

1.3.2.8 Delivery Services Console (DSC)

The Delivery Services Console (DSC) provides the administration interface to a XenApp Server farm (via IMA), presenting administrators with a number of management functions. An administrator uses the Delivery Services Console to monitor and manage:

- configuration data
- available published applications
- users' access permissions for published applications
- central control policies for clipboard transfer and client drive mapping
- general server, Server Farms and user session details.

Client drive mapping and clipboard transfer policies for each individual endpoint user are controlled by administrators. When enabled by an administrator, client drive mapping can be further controlled (i.e. allowed or prevented) by each individual endpoint user for their own sessions.

The DSC is a snap-in to the Microsoft Management Console.

1.3.2.9 Web Interface Management Console

Web Interface Management is a console interface that allows administration activities at the Web Interface. This component can be used by administrators to configure the type of authentication required for users to the Web Interface (username/password or smartcard/PIN).

The Web Interface management console resides on the same physical server as the Web Interface, and is a snap-in to the Microsoft Management Console.

1.3.3 Other Components

1.3.3.1 Smartcards

Smartcards can be used to provide secure access to published applications and data. The TOE can be configured to use smartcards to:

- Authenticate users to Web Interface
- Authenticate users to XenApp.

The role of the TOE in this process is limited to conveying requests and responses between the smartcard and the operating system (including user authentication credentials collected and sent to the smartcard), and reacting appropriately to the authentication result from the operating system.

1.3.3.2 Firewalls

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

1.3.4 Component Interaction

The interactions between the various components are as follows (see Figure 2 for an illustration of the interactions involved and how the various communications paths are protected):

1 An endpoint user uses a web browser to view the Web Interface Login page. If the Web Interface has been configured to use username and password authentication, then the user enters their credentials, which are sent as a standard HTTPS POST request. If the Web Interface has been configured to use smartcard authentication then the user will be prompted to enter their smartcard PIN.

2 The Web Interface reads the user's information and passes it to the XML Service for validation if the Web Interface has been configured to use username and password for authentication. If the Web Interface has been configured to use smartcard authentication then the web server validates the user's smartcard credentials using TLS with client authentication and identifies the associated AD user account. In both the smartcard and username/password cases, the list of SIDs representing the AD user account is passed back from the operating system to the Web Interface and is used to request a list of applications from the XML Service.

3 The XML Service retrieves a list of applications that the user can access and returns it to the Web Interface. These applications comprise the user's permitted published application set and are configured by the administrator.

4 Web Interface uses the web server to send back a web 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 web 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 IMA via the XML Service, requesting information about the least-loaded server in the Server Farm (which IMA requests from the Data Collector). IMA returns the IP address of the least loaded ICA Server.

7 The Web Interface requests a logon ticket from the least-loaded server via the XML Service. The selected server generates a logon ticket and returns the logon ticket to the Web Interface via the XML Service. Note - logon tickets are only generated and used for username/password login (i.e. they are not applicable to smartcard login).

8 The Web Interface contacts the Secure Ticket Authority and requests an STA ticket. The least-loaded ICA Server IP address is included in the request.

9 The Secure Ticket Authority stores the request data, then generates and returns an STA ticket to the Web Interface.

10 The Web Interface sends a customized ICA file via the web server to the web browser that contains the Secure Gateway fully-qualified domain name, logon ticket (if applicable) and STA ticket.

11 The web browser receives the ICA file and passes it to the Online Plug-in.

12 The Online Plug-in 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 on the user's machine is protected by authentication of the Secure Gateway through the use of TLS.

13 The Online Plug-in sends the Secure Gateway the STA ticket.

14 The Secure Gateway contacts the Secure Ticket Authority server and gives it the STA ticket.

15 The Secure Ticket Authority validates the STA ticket and returns the stored IP address of the ICA Server that contains the requested application.

16 The Secure Gateway initiates an ICA session with the least-loaded ICA Server according to the IP address received from the Secure Ticket Authority. If the ICA 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. If the ICA Server has not been configured to use smartcard authentication, then the ICA Server authenticates the user using the logon ticket data as the credentials.

17 The Secure Gateway forwards all ICA traffic between the ICA Server and the Online Plug-in.

1.4 TOE Boundaries

1.4.1 Physical Boundary

The physical boundary of the TOE is defined by the physical boundaries around each of the physical components on which the TOE components shown in Figure 2 are installed, and therefore encompasses:

- The Endpoint Device, containing the Online Plug-in
- A physical server hosting the Secure Gateway
- A physical server hosting the Web Interface (and the Web Interface management console)

- A number of physical servers hosting the XenApp Server components; these may be distributed across physical servers in various ways (guidance on appropriate distribution of the components is given in [CCECG]).

1.4.2 Logical Boundary

The logical boundary is shown by the smaller blue boxes in Figure 2 (the yellow boxes surrounding these components indicate separate physical server/client platforms on which these logical components are installed). It should be noted that while the (endpoint device) Web Browser and (server) web server lie within the physical boundary of the TOE because they are installed on the same client and server platforms as some TOE components, they do not form part of the logical boundary of the TOE.

1.4.3 Summary of items out of scope of the TOE

The items out of scope of the TOE include the Microsoft components on which Citrix XenApp components are installed as detailed in section 1.4.4.

XenApp 6.0 Platinum Edition includes licenses entitling the use of a number of products and components. In the evaluated configuration only the following components are in scope:

- XenApp Server
- Online Plug-in (note that this is the 'Online Plug-in – web' version of the Online Plug-in)
- Secure Gateway
- Web Interface.

The four components listed above provide the functionality identified in section 1.2.1. The evaluated configuration also includes operation either with or without the use of the Single Sign-On feature, although there are no claims relating to the Single Sign-On functionality in the scope of evaluation. All other products and components supplied as part of the Platinum Edition (including, for example, the Access Gateway product and SmartAuditor component, and including other versions of the Online Plug-in), and hence all additional functionality supplied by these other products and components, are out of scope.

The evaluated configuration covers only the publishing of applications; streaming of applications, VM-hosted applications, and publishing of desktops or other content[7] is excluded from the evaluated configuration.

[7] Publishing content refers to the addition of content URLs (i.e. URLs linked to items other than XenApp published applications) to the list of permitted published applications that is presented to a XenApp user by Web Interface (cf. steps 3-4 in section 1.3.4)

1.4.4 Required non-TOE hardware/software/firmware

The context for the lists of non-TOE items given below can be found in section 1.3.

As shown in the deployment configuration in Figure 1, the following non-TOE items are required:

- Firewalls
- Active Directory
- Citrix License Server.

Other requirements for non-TOE software are identified for each of the TOE components below.

1.4.4.1 Endpoint device

The endpoint device is a PC with one of the following operating systems:

- Microsoft Windows 7, Ultimate edition, 32 & 64-bit versions
- Microsoft Windows Vista SP1, Ultimate edition, 32 & 64-bit versions

In evaluated configurations Endpoint users will run a TLS-enabled web browser (i.e. Internet Explorer 8.0) – this is not included in the TOE.

1.4.4.2 XenApp Server TOE Requirements

The term "XenApp Server" indicates a physical server containing one or more of the following components of XenApp:

- ICA Server (including IMA)
- Delivery Services Console
- XML Service
- Secure Ticket Authority.

For the purposes of this Security Target, the TOE is characterised in terms of these logical component roles, which may be deployed across physical servers in a variety of ways. Guidance on appropriate physical deployments is given in [CCECG].

In the evaluated configuration, the Single Sign-On component (shown in Figure 1 and discussed in sections 1.3 and 1.4.3) will be present on one of the XenApp physical servers.

In the evaluated configuration, a XenApp Server requires a physical server running Microsoft Windows Server 2008 R2 (Enterprise edition, 64-bit) and Microsoft IIS 7.5. Two further software components need to be installed on the ICA Server in the evaluated configuration:

Microsoft SQL Server 2008 Express Edition is installed as the data store (the product also supports other editions), and the Citrix Access Suite License Server must be installed in order to successfully license the product. These four components form part of the environment for the TOE.

1.4.4.3 Secure Gateway

In the evaluated configuration, the Secure Gateway requires a physical server running Microsoft Windows Server 2008 R2 (Enterprise edition, 64-bit).

1.4.4.4 Web Interface

In the evaluated configuration, the Web Interface requires the following software:

- Microsoft Windows Server 2008 R2 (Enterprise edition, 64-bit)
- Microsoft IIS 7.5.

2. CC Conformance

As defined by the references [CC1], [CC2] and [CC3], this TOE conforms to the requirements of Common Criteria v3.1, Revision 3. The methodology applied for the evaluation is defined in [CEM].

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of EAL2, augmented with ALC_FLR.2.

This ST does not claim conformance to any PPs.

3. Security Problem Definition

3.1 Assets

The assets to be protected by the TOE are as follows:

Published Applications	The published applications made available by the TOE. Protection of confidentiality and integrity is required.
Published Application Data	Application data in transit between the Online Plug-in (on the endpoint device) and the ICA Server that hosts the relevant application session. Protection of confidentiality and integrity is required.
Application Transfer Data	Application data that may be transferred between the ICA Server and a connected endpoint device during an application session, by means of clipboard transfer or client drive mapping[8]. Protection of confidentiality is required, in the sense that such data transfers (in either direction) should only be possible if an administrator has configured the global policy to allow the transfer[9].
Configuration Data	Configuration data, whether stored or in transit between the endpoint device and server components, and between server components (comprising the Secure Gateway, Web Interface, Web Interface Management, and XenApp Server components). This data is used to control user sessions (e.g. logon tickets, STA tickets, lists of permitted published applications, identification and authentication data). Protection of confidentiality and integrity is required.

3.2 Users and Subjects

The following define the users and IT systems. The subjects are interpreted as those processes representing the defined users and external systems.

[8] The property being protected for this asset is the ability to move data between the application session in an ICA Server and resources on the endpoint client. If such a transfer takes place then the same data will at some point also be considered as Published Application Data (i.e. while it is in transit on a communication channel).

[9] Protection against transfers from the endpoint device to the application session on the ICA Server could also be viewed as an integrity requirement (protecting the ICA Server). Whether viewed as confidentiality or integrity however, the underlying requirement for the TOE (as is described in OSP.Endpoint_Resource) is to provide the ability for an administrator to control the ability to transfer data between endpoint device resources and an application session.

Endpoint User	A user who has been granted access to the TOE. An endpoint user would access applications through an endpoint device.
Administrator	An administrator manages users' access to published applications. An administrator is responsible for the configuration of the components of the TOE and the operational environment, and is likely to have physical access to the TOE server components.
Endpoint device	A device used by a user to gain access to the TOE. It consists of a PC, laptop, PDA or similar desktop appliance. To enable access, the endpoint will be running the Client component of the TOE.

Endpoint User and Administrator are of course *roles*, and some individuals may be able to act in both roles. However, in the remainder of this document the term "user" refers to an Endpoint User. The Administrator and Endpoint User roles are disjoint: individuals operating in an Administrator role only carry out administration actions and do not connect to published applications.

3.3 Threats

The TOE (in some cases with the support of the operational environment) is intended to address the following threats.

T.Attack_Application	An attacker may gain access to published applications or published application data.
T.Access_Application	An endpoint user may gain unauthorised access to published applications or published application data.
T.Intercept	An attacker may intercept communication channels. This may lead to compromise of published application data or configuration data (including a user's authentication credentials).
T.Spoof	An attacker may cause communications between an endpoint and a server to be redirected, such that users of the TOE may incorrectly believe they are accessing the TOE when they are not. This may lead to compromise of published applications, published application data, or configuration data (including a user's authentication credentials).
T.Attack_Configdata	An attacker or endpoint user may make unauthorised modifications to configuration data.

3.4 Organizational Security Policies

OSP.Crypto	Cryptographic functions shall be validated to FIPS 140-2 level 1.
OSP.Endpoint_Resource	In order to limit the potential exposure of application transfer data, an administrator must be able to control: • the ability to cut, copy and paste clipboard data between a XenApp application session and the endpoint device clipboard • the ability to access local drives (including USB drives) on the endpoint device.

3.5 Assumptions

A.Physical	TOE servers are installed in an environment such that only administrators can gain physical access to the TOE servers.
A.Config_Endpoint	The endpoint device operating system is securely configured, including appropriate file and registry protection, according to [CCECG] and any additional requirements that may arise from the risks in a specific user's deployment environment.
A.Operations_Security	Where keys and other secret data are generated and stored outside the TOE, they are managed in accordance with the level of risk.
A.Third_Party_SW	Trusted third party software is operating correctly and securely. Trusted third party software is defined as: • Microsoft IIS • Web Browsers used to connect • Windows Server (including Active Directory) • SQL Server • Firewall software.
A.Published_Desktop	Administrators will not publish the Desktop or other Content[10]
A.Application	Administrators will ensure that applications are published and configured such that they do not act in a malicious manner. Specifically, published applications will not

[10] See footnote 7.

maliciously interact with other applications nor will they maliciously affect published application data or configuration data. This includes maintaining the security state of the published applications according to the user's risk environment (e.g. by applying relevant patches). It shall not be possible to 'break out' of applications, and hence gain direct access to operating system functions or other applications.

4. Security Objectives

4.1 Security Objectives for the TOE

O.Auth_User	Endpoint users must be successfully identified and authenticated before being granted access to the published applications (and their associated published application data).
O.Auth_Server	TOE server components must authenticate themselves to client endpoints before communication of sensitive data.
O.Application	Users must be granted access only to applications for which they have been authorised.
O.Secure_Data_Transmission	The confidentiality and integrity of both published application data and configuration data, must be maintained during transmission (i) between pairs of TOE server components (ii) between the Secure Gateway and the Online Plug-in on an endpoint device (iii) between the web browser on an endpoint device and the web server.
Application note	The requirements of O.Secure_Data_Transmission are linked to other requirements as follows: • OE.IPSec requires the deployed configuration to use IPSec between pairs of TOE server components (to achieve (i) above). OE.Encryption ensures the use of FIPS140-2 validated cryptographic functions when providing IPSec (and is a requirement on the environment because the IPSec protocol implementation and its cryptographic functions are provided by Windows) • O.TLS-TOE requires the TOE to use TLS between the Secure Gateway and Online Plug-ins (to achieve (ii) above). O.Use_FIPS ensures that, when TLS is implemented by the TOE for this link, the TSF invokes the relevant cryptographic functions in Windows in accordance with their FIPS140-2 validation • OE.TLS-Config requires the TOE deployment to be configured so that the client web browser and the web

	server use TLS. OE.Encryption ensures the use of FIPS140-2 validated cryptographic functions when using TLS (and, as noted for the use of IPSec above, is a requirement on the environment because the TLS protocol implementation and its cryptographic functions are provided by Windows[11]).
O.TLS-TOE	The TOE shall ensure that all communication between the Online Plug-in and the Secure Gateway uses the TLS protocol.
O.Endpoint_Resource	In order to limit the potential exposure of application transfer data, an administrator must be able to control: • the ability to cut, copy and paste clipboard data between a XenApp application session and the endpoint device clipboard • the ability to access local drives (including USB drives) on the endpoint device.
O.Use_FIPS	TOE components must invoke FIPS 140-2 level 1 validated cryptographic functions in accordance with the conditions of the validation.
O.Config_Apps	The published applications must only be configurable by administrators.
Application note	Published applications must be configured by administrators such that it is not possible for users to 'break out' of the application to gain access to the underlying operating system of the ICA Server on which the application is running.

4.2 Security Objectives for the Environment

The following objectives relate to the server components of the TOE:

OE.Config_Server	The operating systems of the server components must be securely configured according to [CCECG], including appropriate file protection, and any additional requirements that may arise from the risks in a specific user's deployment environment.

[11] Note: the TOE implements the TLS protocol for the link between Online Plug-in and Secure Gateway, and uses FIPS 140-2 validated cryptographic functions provided by the Windows cryptographic API to do so. The link between the web browser on an endpoint device and the web server uses the Windows implementation of TLS, which also makes use of FIPS 140-2 validated cryptographic functions,

OE.Config_TP_SW	Trusted third party software must be securely configured according to [CCECG], and any additional requirements that may arise from the risks in a specific user's deployment environment. Trusted third party software is defined as: • Microsoft IIS • Web Browsers used to connect • Windows Server (including Active Directory) • SQL Server Express • Firewall software.
OE.Published_Desktop	Only applications may be published; desktops and other content must not be published and hence available to endpoint users.
OE.Application	Applications must be published and configured such that they do not act in a malicious manner. The published applications must not maliciously interact with other applications nor maliciously affect published application data or configuration data. This includes maintaining the security state of the published applications according to the user's risk environment (e.g. by applying relevant patches). Also they must be configured so that it shall not be possible to 'break out' of applications, and hence gain direct access to operating system functions or other applications.
OE.Authenticate	Endpoint users must be authenticated by the underlying operating system on the relevant platform. Authentication requirements in the operating system shall be configured according to [CCECG] and the risks in the operational environment.
OE.Server_Physical	The operational environment shall ensure that only administrators are able to gain physical access to the TOE servers.
OE.Admin_Users	Configuration data on server components must be accessible only to authorised administrators.

The following objectives relate to the endpoint devices:

OE.Config_Endpoint	The endpoint device operating system must be securely configured, including appropriate file protection and registry protection, according to [CCECG] and any additional requirements that may arise from the risks in a specific user's deployment environment.
Application note	Implementing the access controls on endpoint devices will be based on the risk environment in which they are deployed,

	and may include guidance given to users on maintaining the security of their endpoint device.
OE.Endpoint_TP_SW	Endpoints must have only trusted third party software installed. This software must be configured securely according to the risks in the operational environment.

The following objectives relate to connectivity between components of the TOE:

OE.IPSec	The administrator shall ensure that all communication between the TOE server components uses the IPSec protocol configured as in [CCECG].
OE.TLS-Config	The administrator shall ensure that all communication between the web browser in the endpoint device and the web server uses the TLS protocol configured as in [CCECG].
OE.Encryption	Secure cryptographic functions used to provide IPSec and TLS must be FIPS 140-2 level 1 compliant.
Application note	This means that the software in the environment used by the TOE must be configured such that only FIPS140-2 level 1 validated algorithms are used.
OE.Operations_Security	Any keys and other secret data that are generated and stored outside the TOE must be managed in accordance with the level of risk.

4.3 Security Objectives Rationale

The following table provides a summary of the relationship between the security objectives and the security problem definition.

Threat/ OSP/ Assumption / Security Objectives	T.Attack_Application	T.Access_ Application	T.Intercept	T.Spoof	T.Attack_Configdata	OSP.Crypto	OSP.Endpoint_Resource	A.Physical	A.Config_Endpoint	A.Operations_Security	A.Third_Party_SW	A.Published_Desktop	A.Application
O.Auth_User	X	X			X								
O.Auth_Server				X									
O.Application	X	X											
O.Secure_Data_Transmission	X		X		X								
O.TLS-TOE		X	X	X	X								
O.Endpoint_Resource							X						
O.Use_FIPS						X							
O.Config_Apps		X											
OE.Config_Server	X	X		X	X								
OE.Config_TP_SW	X	X		X	X						X		
OE.Published_Desktop												X	
OE.Application													X
OE.IPSec		X	X		X								
OE.Authenticate	X	X			X								
OE.Config_Endpoint	X	X		X	X				X				
OE.TLS-Config		X	X	X	X								
OE.Encryption						X							
OE.Operations_Security										X			
OE.Server_Physical								X					
OE.Endpoint_TP_SW				X							X		
OE.Admin_Users					X								

Table 1 Threats/OSP/Assumptions addressed by Security Objectives

4.3.1 T.Attack_Application

Published applications and published application data are protected against attacker access by the authentication of users (O.Auth_User and OE.Authenticate) and the use of access controls that limit a user to their list of permitted published applications (O.Application). The communication channels used for application access are protected by channel encryption (O.Secure_Data_Transmission).

The environment provides further protection of the assets by ensuring that the TOE components are securely configured according to the risk environment (OE.Config_Server, OE.Config_TP_SW, and OE.Config_Endpoint).

4.3.2 T.Access_Application

Published applications and published application data are protected against unauthorised access from endpoint users by the authentication of users (O.Auth_User and OE.Authenticate), and by the use of access controls that limit a user to their list of permitted published applications (O.Application) which can only be set by an administrator (O.Config_Apps).

The environment provides further protection of the assets by ensuring that the TOE components are securely configured according to the risk environment (OE.Config_Server, OE.Config_TP_SW, and OE.Config_Endpoint), and that the communications in the environment are protected from unauthorised access by authentic users who may have greater access to the TOE than more general attackers (O.TLS-TOE, OE.IPSec and OE.TLS-Config).

4.3.3 T.Intercept

The threat of interception of communication channels is countered by the use of protected communication channels. The TOE is required to protect confidentiality of communications between pairs of TOE server components, and between the Secure Gateway and the Online Plug-in on an endpoint device (O.Secure_Data_Transmision), noting that the endpoint device must be correctly configured to use cryptographic functions in a suitably secure manner (O.TLS-TOE and OE.IPSec). In addition, the web browser connection to the web server is required to use TLS (OE.TLS-Config).

4.3.4 T.Spoof

The redirection threat is countered firstly by requiring authentication of server components before transmission of sensitive data (O.Auth_Server), and by ensuring that TLS is appropriately used for the communications between an endpoint and both the Secure Gateway and the web server (O.TLS-TOE and OE.TLS-Config). This is supported by ensuring that the endpoints, server components and trusted third-party software are securely configured (OE.Config_Endpoint, OE.Config_Server, OE.Config_TP_SW and OE.Endpoint_TP_SW).

4.3.5 T.Attack_Configdata

The ability of an attacker or endpoint user to make unauthorised modifications to configuration data is prevented by the combination of user authentication (O.Auth_User and OE.Authenticate) and a requirement to limit access to configuration data on servers to administrators (OE.Admin_Users). This is further enforced by protection of communication channels (O.Secure_Data_Transmision), supported by appropriate configuration of the relevant hardware and software (OE.Config_Server, OE.Config_TP_SW and OE.Config_Endpoint,) and appropriate use of protocols that protect the data on the channels (O.TLS-TOE, OE.IPSec and OE.TLS-Config).

4.3.6 OSP.Crypto

This policy requirement is met directly by requiring that cryptographic functions are FIPS140-2 level 1 compliant (OE.Encryption) and that the TOE uses these functions in accordance with their validation (O.Use_FIPS).

4.3.7 OSP.Endpoint_Resource

This policy requirement is met directly by O.Endpoint_Resource.

4.3.8 A.Physical

The assumption of physical security of TOE servers is met directly by OE.Server_Physical.

4.3.9 A.Config_Endpoint

This assumption is met directly by OE.Config_Endpoint.

4.3.10 A.Operations_Security

This assumption is met directly by OE.Operations_Security.

4.3.11 A.Third_Party_SW

This assumption is met directly by a combination of the requirement for secure configuration of third-party software in OE.Config_TP_SW and the requirement for secure configuration of software installed on the endpoint (and limitation of that software to trusted software) in OE.Endpoint_TP_SW.

4.3.12 A.Published_Desktop

This assumption is met directly by OE.Published_Desktop.

4.3.13 A.Application

This assumption is met directly by OE.Application.

5. Extended Component Definition

This chapter defines components that are not drawn from [CC2].

5.1 Extended Security Requirement

There are two security requirements defined for this TOE for which extended components are required as no applicable requirement is provided in [CC2].

5.1.1 Conformance with External Cryptographic Accreditation

The family FCS_ECA describes a requirement for the TOE to provide certain cryptographic functionality in accordance with the conditions of an external accreditation[12], such as a Common Criteria evaluation or a national cryptographic programme (e.g. FIPS 140 validation in USA & Canada, or CAPS in the UK). This might typically be used where the TSF uses a third-party software or hardware item to provide the functionality, and therefore does not implement the cryptographic functionality within the TSF, but should be shown to use the item in accordance with the conditions of its accreditation[13].

Family behaviour

This family defines a requirement for the TOE to implement certain functionality in accordance with an external cryptographic accreditation.

Component levelling:

FCS_ECA: Conformance with External Cryptographic Accreditation	1

The statement of functionality must give enough detail that it can be directly matched to corresponding functions of the external cryptographic module that has successfully gained accreditation against the quoted cryptographic standard(s): for example, the cryptographic operations, together with the specific algorithms or key sizes; in addition, objects or channels

[12] While 'accreditation' is used here it is intended to be understood as a generic term to encompass validation, certification or approval as used variously by different schemes and accreditation bodies.

[13] For example, if the TSF used a FIPS 140 validated cryptographic module, but makes use of a non-FIPS approved algorithm, then this would be outside the scope of the accreditation.

to which the cryptographic functionality applies may be identified.

Other relevant information about the scope or applicability of the accreditation to the use of the functionality in the TOE may be identified in the optional annotations.

The identification of the external cryptographic module must be sufficiently precise so that, in the evaluated configuration, it can be directly matched to an accreditation of the relevant cryptographic functionality during the course of the evaluation (e.g. by reference to a specific certificate).

The list of cryptographic standards with optional annotations must be such that it can be determined that the stated cryptographic functionality used in the evaluated configuration is consistent with the accreditation of the external cryptographic module (e.g. that the external cryptographic module is being used in an approved mode).

Evidence (e.g. an accreditation report or a certificate) that the external cryptographic module has gained accreditation against the quoted standard for the listed functionality shall be provided to the evaluator. A cryptographic security policy may form part of this demonstration, depending on whether the external cryptographic standard requires one to be produced for accreditation.

None of the assignments in FCS_ECA.1 may be completed with 'None'.

Management: FCS_ECA.1

There are no management activities foreseen.

Audit: FCS_ECA.1

There are no auditable events foreseen.

5.1.1.1 FCS_ECA.1 Conformance with External Cryptographic Accreditation

Hierarchical to: No other components.

Dependencies: No dependencies.

FCS_ECA.1.1 The TOE shall invoke [assignment: *statement of cryptographic functionality*] using [assignment: *identification of external cryptographic module*] in accordance with the conditions of the external accreditation of this functionality against [assignment:

list of external cryptographic standards with optional annotations].

5.1.2 Secure Channel Operation

This family describes a requirement for operation of a trusted channel for the transmission of data between the TSF and other components.

Family behaviour

This family defines requirements for the creation and use of a trusted channel between components, at least one of which is part of the TSF, for the performance of security critical operations.

Component levelling:

FCO_SCO.1 requires that a secure channel can be set between two elements, at least one of which is part of the TSF (the other may be outside the TSF, provided that the TSF can control the security level on the channel, and ensure that it is used for the required communications). The characteristic that determines when the channel is used may be the communication of particular data, the execution of a particular function or operation, the endpoints involved in the communication or another specified characteristic.

Only the assignment in FCO_SCO.1.3 may be completed with 'None'; all other assignments require identification of an element or characteristic as appropriate.

Management: FCO_SCO.1

The following actions could be considered for the management functions in FMT:

a. Configuring the actions that require the secure channel, if supported.

Audit: FCO_SCO.1

There are no auditable events foreseen.

5.1.2.1 FCO_SCO.1 Secure Channel Operation

Hierarchical to: No other components

Dependencies: None

FCO_SCO.1.1 The TSF shall use a communication channel between [assignment: *pairs of elements, with at least one element being a part of the TSF*] that is logically distinct from other communication channels and provides assured identification of [assignment: *list of one or more end points whose identity is assured*] and protection of the channel data from [selection: *modification, disclosure*].

FCO_SCO.1.2 The TSF shall permit [assignment: *list of the elements that can initiate the communication*] to initiate communication via the communication channel.

FCO_SCO.1.3 The TSF shall ensure that the communication channel meets the following additional requirements for security: [assignment: *list of the requirements in terms of protocol, key lengths, or other properties*]

FCO_SCO.1.4 The TSF shall use the communication channel for [assignment: *characteristic for which a trusted channel is required*].

6. IT Security Requirements

6.1 Conventions

The following conventions are used to denote the completion of operations:

- ~~Strikethrough~~ indicates text removed as a refinement and underlined text indicates additional text provided as a refinement.
- [**Bold text within square brackets**] indicates the completion of an assignment.
- [*Italicised text within square brackets*] indicates the completion of a selection.

6.2 Security Functional Requirements

The operation of the TOE is considered under three functional groupings for the purposes of the specification of the security functional requirements. These are:

- Authentication
- Authorisation
- Communications

The individual security functional requirements are specified in the sections below. The term 'user' should be understood to relate to only endpoint users (users of endpoint devices), and not to administrators.

6.2.1 Authentication

The SFRs in this section are concerned with enforcing access control to ensure that only authenticated endpoint users are granted access to the permitted published applications and their data. The TOE is instrumental in enforcing authentication of endpoint users by prompting the endpoint user to enter their authentication credentials, then passing the credentials to the IT environment (Active Directory) for validation, and acting on the response received[14].

[14] Note that TOE administrators are authenticated by the underlying operating system, and are not prompted by the TOE to enter their credentials.

6.2.1.1 FIA_ATD.1/User User Attribute Definition

FIA_ATD.1.1/User The TSF shall maintain the following list of security attributes belonging to individual users: [**Access permissions for permitted published applications**].

6.2.1.2 FIA_UID.2/User User Identification before any action

FIA_UID.2.1/User The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.1.3 FIA_UAU.2/User User Authentication before any action

FIA_UAU.2.1/User The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.2 Authorisation

The SFRs in this section are concerned with providing the administrator with the means to authorise endpoint users for access to published applications (and associated data) and to limit the operations they are able to perform.

6.2.2.1 FMT_SMR.1/Authorise Security Roles

FMT_SMR.1.1/Authorise The TSF shall maintain the roles [**endpoint user, administrator**].

FMT_SMR.1.2/Authorise The TSF shall be able to associate users with roles.

6.2.2.2 FMT_SMF.1/Authorise Specification of Management Functions

FMT_SMF.1.1/Authorise The TSF shall be capable of performing the following security management functions:[

- **Definition of published applications**
- **Definition of user access permissions for published applications**
- **Setting endpoint device access control policy**]

Application note Administration of endpoint device access control policy consists of enabling or disabling the following functions when accessing published applications:

- Clipboard transfer (cut, copy and paste between endpoint device and clipboards of ICA Servers running published applications);
- Endpoint device client drive mapping from published applications.

6.2.2.3 FDP_ACC.1/Application Subset access control

FDP_ACC.1.1/Application The TSF shall enforce the [**Application Access Policy**] on [**users attempting access to a published application].**

6.2.2.4 FDP_ACF.1/Application Security attribute based access control

FDP_ACF.1.1/Application

The TSF shall enforce the [**Application Access Policy**] to objects based on the following: [**user access permissions**].

FDP_ACF.1.2/Application

The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

An application shall be accessible by a user only if

- **The application is published, and**
- **The user's access permissions allow access to that application**.]

FDP_ACF.1.3/Application

The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**None**].

FDP_ACF.1.4/Application

The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**None**].

6.2.2.5 FMT_MSA.1/Application Management of Security Attributes

FMT_MSA.1.1/Application The TSF shall enforce the [**Application Access Policy**] to restrict the ability to [*modify*] the security attributes: [

a) published applications;

b) **Users' access permissions for published applications**]

to [**administrators**].

6.2.2.6 FMT_MSA.3/Application Static attribute initialisation

FMT_MSA.3.1/Application The TSF shall enforce the [**Application Access Policy**] to provide [*restrictive*] default values for security attributes that are used to enforce the ~~SFP~~ policy.

FMT_MSA.3.2/Application The TSF shall allow the [**administrator**] to specify alternative initial values to override the default values when an object or information is created.

Application note The default values are restrictive in that when a new application is published then the TOE ensures that by default no users will have access to it.

6.2.2.7 FDP_ACC.1/Resource Subset access control

FDP_ACC.1.1/Resource The TSF shall enforce the [**Resource Access Policy**] on [**endpoint users' use of the following operations:**

- **Clipboard transfer: transfer of user data between the endpoint clipboard and the clipboard of the ICA Server running the published application on behalf of that user**
- **Client drive mapping: access to mapped client drives from the application session (on the relevant ICA Server) for that user].**

Application note The mapped client drives include USB drives at the endpoint device.

6.2.2.8 FDP_ACF.1/Resource Security attribute based access control

FDP_ACF.1.1/Resource The TSF shall enforce the [**Resource access SFP**] to objects based on the following: [**endpoint user identity and user access permissions**].

FDP_ACF.1.2/Resource The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

- **An endpoint user shall be permitted to cut, copy and paste application data between a published application and a Windows clipboard on their endpoint device only if clipboard transfer has been enabled for that user by the administrator.**
- **Drives on an endpoint device shall be accessible to a published application in use by the endpoint user only if client drive mapping has been enabled by the administrator for that user, and the user has permitted the access].**

FDP_ACF.1.3/Resource The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**None**].

FDP_ACF.1.4/Resource The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**None**].

Application note If the Administrator has enabled client drive mapping then an endpoint user may configure their session to allow or prevent this operation.

6.2.2.9 FMT_MSA.3/Resource Static attribute initialisation

FMT_MSA.3.1/Resource The TSF shall enforce the [**Resource Access Policy**] to provide [*restrictive*] default values for security attributes that are used to enforce the ~~SFP~~ policy.

Application note The default values are restrictive in that, although the defaults may be configured differently during installation, the clipboard transfer and client drive mapping device access functions will default to disabled following installation of the evaluated configuration.

FMT_MSA.3.2/Resource The TSF shall allow the [**administrator**] to specify alternative initial values to override the default values when an object or information is created.

6.2.2.10 FMT_MOF.1/Resource Management of security functions behaviour

FMT_MOF.1.1/Resource The TSF shall restrict the ability to [*disable, enable*] the functions [**clipboard transfer, client drive mapping**] to [**administrators**].

6.2.3 Communications

The SFRs in this section are concerned with protecting data that is being communicated between separate components of the TOE.

6.2.3.1 FCO_SCO.1/Client Secure Channel Operation

FCO_SCO.1.1/Client The TSF shall use a communication channel between [**the endpoint Online Plug-in and the Secure Gateway**] that is logically distinct from other communication channels and provides assured identification of [**the Secure Gateway**] and protection of the channel data from [*modification, disclosure*].

FCO_SCO.1.2/Client The TSF shall permit [**the endpoint Online Plug-in**] to initiate communication via the communication channel.

FCO_SCO.1.3/Client The TSF shall ensure that the communication channel meets the following additional requirements for security: [**use of TLS in accordance with FIPS140 validation of the underlying cryptographic functions**].

FCO_SCO.1.4/Client The TSF shall use the communication channel for [**all traffic between the endpoint Online Plug-in and the Secure Gateway**].

Note: no management actions of the sort identified in the definition of the family in section 5.1.2 are required in the TOE since there is no administrator choice of the actions that require the secure channel. The use of the secure channel is a static requirement of the evaluated configuration.

6.2.3.2 FCS_ECA.1/Client Conformance with external cryptographic accreditation

FCS_ECA.1.1/Client The TOE shall invoke [

encryption of traffic between the endpoint Online Plug-in and the Secure Gateway using

- **Triple-DES as defined by the ciphersuite TLS_RSA_WITH_3DES_EDE_CBC_SHA, or**
- **AES as defined by the ciphersuite RSA_WITH_AES_128_CBC_SHA, or**
- **AES as defined by the ciphersuite RSA_WITH_AES_256_CBC_SHA**]

using [**Microsoft Enhanced Cryptographic Provider**] in accordance with the conditions of the external accreditation of this functionality against [**FIPS140-2**].

Application note

The accreditation of the Microsoft Enhanced Cryptographic Provider against FIPS140-2 is documented in the following certificate(s):

Windows Server 2008 R2 Enhanced Cryptographic Provider (RSAENH) – Certificate #1337.

Windows 7 Enhanced Cryptographic Provider (RSAENH) – Certificate #1330.

Windows Vista SP1 Enhanced Cryptographic Provider (RSAENH) – Certificate #1002.

6.3 Security Assurance Requirements

The security assurance requirements are drawn from [CC3] and represent EAL2, with the addition of ALC_FLR.2 Flaw Reporting Procedures. The assurance components are identified in the table below.

Assurance Class	**Assurance Components**
Security Target (ASE)	ST introduction (ASE_INT.1)
	Conformance claims (ASE_CCL.1)
	Security problem definition (ASE_SPD.1)
	Security objectives (ASE_OBJ.2)
	Extended components definition (ASE_ECD.1)
	Derived security requirements (ASE_REQ.2)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Security architecture description (ADV_ARC.1)
	Security-enforcing functional specification (ADV_FSP.2)
	Basic design (ADV_TDS.1)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)

Assurance Class	Assurance Components
	Preparative procedures (AGD_PRE.1)
Life cycle support (ALC)	Use of a CM System (ALC_CMC.2)
	Parts of the TOE CM coverage (ALC_CMS.2)
	Delivery procedures (ALC_DEL.1)
	Flaw reporting procedures (ALC_FLR.2)
Tests (ATE)	Evidence of coverage (ATE_COV.1)
	Functional testing (ATE_FUN.1)
	Independent testing – sample (ATE_IND.2)
Vulnerability assessment (AVA)	Vulnerability analysis (AVA_VAN.2)

Table 2 Security Assurance Requirements

The selection of EAL2 is consistent with the assurance levels commonly used for commercial products of this sort, and the augmentation with ALC_FLR.2 provides additional confidence for users that there is a process for reporting and addressing any vulnerabilities that might be subsequently discovered in the product, and hence that its security will be maintained over time.

6.4 Security Requirements Rationale

The following table provides a summary of the relationship between the security objectives and the security functional requirements (including the extended components).

Security Objectives **SFRs**	**O.Auth_User**	**O.Auth_Server**	**O.Application**	**O.Secure_Data_Transmission**	**O.TLS-TOE**	**O.Endpoint_Resource**	**O.Use_FIPS**	**O.Config_Apps**
FIA_ATD.1/User			X					
FIA_UID.2/User	X							
FIA_UAU.2/User	X							
FMT_SMR.1/Authorise			X			X		X
FMT_SMF.1/Authorise			X			X		X
FDP_ACC.1/Application			X					
FDP_ACF.1/Application			X					
FMT_MSA.1/Application			X					X
FMT_MSA.3/Application			X					X
FDP_ACC.1/Resource						X		
FDP_ACF.1/Resource						X		
FMT_MSA.3/Resource						X		
FMT_MOF.1/Resource						X		
FCO_SCO.1/Client		X		X	X			
FCS_ECA.1/Client							X	
SARs								
Guidance documents (AGD)				X				

Table 3 Summary of Objectives/SFRs Rationale

6.4.1 O.Auth_User

The objective of identifying and authenticating endpoint users is realised directly by FIA_UID.2/User and FIA_UAU.2/User.

6.4.2 O.Auth_Server

The objective of authenticating the Secure Gateway server component to endpoints is realised by the use of a secure channel in FCO_SCO.1/Client.

6.4.3 O.Application

The objective of limiting access by a user to the applications authorised for that user is realised primarily by the requirement to maintain access permissions in FIA_ATD.1/User and the access control policy in FDP_ACC.1/Application and FDP_ACF.1/Application. The secure management of these access controls is realised by FMT_SMR.1/Authorise (to ensure recognition of endpoint user and administrator roles), FMT_SMF.1/Authorise (to define the ability to administer permitted published applications), FMT_MSA.1/Application (restricting the ability to administer permitted published applications to administrators), and FMT_MSA.3/Application (to set restrictive defaults on user access to newly published applications).

6.4.4 O.Secure_Data_Transmission

The protection of confidentiality and integrity of published application data and configuration data in transit is realised by FCO_SCO.1/Client and by guidance documentation (AGD) which requires the configuration of the TOE (according to [CCECG]) to use TLS and IPSec based on FIPS 140 validated cryptographic functions.

6.4.5 O.TLS-TOE

The implementation of TLS by the TOE is realised by FCO_SCO.1/Client.

6.4.6 O.Endpoint_Resource

Control over application transfer data is realised primarily by the policy over availability of clipboard transfer and client drive mapping in FDP_ACC.1/Resource and FDP_ACF.1/Resource. The secure management of these access controls is realised by FMT_MSA.3/Resource (to set restrictive defaults on clipboard transfer and client drive mapping), FMT_SMR.1/Authorise (to ensure recognition of endpoint user and administrator roles), and a combination of FMT_SMF.1/Authorise and FMT_MOF.1/Resource (which both ensure that only administrators can enable and disable these functions).

6.4.7 O.Use_FIPS

This objective is directly realised by FCS_ECA.1/Client.

6.4.8 O.Config_Apps

The objective of limiting the configuration of published applications to administrators is realised by FMT_SMR.1/Authorise (to ensure recognition of endpoint user and administrator roles), FMT_SMF.1/Authorise (to define the ability to administer permitted published applications), FMT_MSA.1/Application (restricting the ability to administer permitted

published applications to administrators), and FMT_MSA.3/Application (to set restrictive defaults on user access to newly published applications).

6.4.9 SFR Dependencies Analysis

The dependencies between SFRs implemented by the TOE are addressed as follows.

SFR	Dependencies	Rationale Statement
FIA_ATD.1/User	None	
FIA_UID.2/User	None	
FIA_UAU.2/User	FIA_UID.1	Met by FIA_UID.2/User
FMT_SMR.1/Authorise	FIA_UID.1	Met by FIA_UID.2/User
FMT_SMF.1/Authorise	None	
FDP_ACC.1/Application	FDP_ACF.1	FDP_ACF.1/Application
FDP_ACF.1/Application	FDP_ACC.1	Met by FDP_ACC.1/Application
	FMT_MSA.3	Met by FMT_MSA.3/Application.
FMT_MSA.1/Application	[FDP_ACC.1 or FDP_IFC.1]	Met by FDP_ACC.1/Application
	FMT_SMR.1	Met by FMT_SMR.1/Authorise
	FMT_SMF.1	Met by FMT_SMF.1/Authorise
FMT_MSA.3/Application	FMT_MSA.1	Met by FMT_MSA.1/Application
	FMT_SMR.1	Met by FMT_SMR.1/Authorise
FDP_ACC.1/Resource	FDP_ACF.1	FDP_ACF.1/Resource
FDP_ACF.1/Resource	FDP_ACC.1	Met by FDP_ACC.1/Resource
	FMT_MSA.3	Met by FMT_MSA.3/Resource.
FMT_MSA.3/Resource	FMT_MSA.1	The dependency on FMT_MSA.1 for security attribute modification is not necessary here: it is addressed under FMT_MOF.1/Resource instead.
	FMT_SMR.1	Met by FMT_SMR.1/Authorise

SFR	Dependencies	Rationale Statement
FMT_MOF.1/Resource	FMT_SMR.1	Met by FMT_SMR.1/Authorise
	FMT_SMF.1	Met by FMT_SMF.1/Authorise
FCO_SCO.1/Client	None	
FCS_ECA.1/Client	None	

Table 4 Analysis of SFR dependencies

7. TOE Summary Specification

The following sections describe how the TOE provides the security functional requirements described in section 6.2 above.

TOE Functions / SFRs	User Authentication	User Access Control	Membership of user's permitted application set	Inter-Component Authentication and Encryption	Clipboard Transfer	Client Drive Mapping
FIA_ATD.1/User		X	X			
FIA_UID.2/User	X					
FIA_UAU.2/User	X					
FMT_SMR.1/Authorise			X		X	X
FMT_SMF.1/Authorise			X		X	X
FDP_ACC.1/Application		X	X			
FDP_ACF.1/Application		X	X			
FMT_MSA.1/Application		X	X			
FMT_MSA.3/Application			X			
FDP_ACC.1/Resource					X	X
FDP_ACF.1/Resource					X	X
FMT_MSA.3/Resource					X	X
FMT_MOF.1/Resource					X	X
FCO_SCO.1/Client				X		
FCS_ECA.1/Client				X		

Table 5 Summary of SFRs satisfied by TOE Functions

7.1 User Authentication

An endpoint user will be allowed to launch an application on the ICA Server only after the user has been authenticated by supplying a valid user identity and password or smartcard and smartcard PIN.

This aspect of XenApp therefore implements FIA_UID.2/User and FIA_UAU.2/User.

7.2 User Access Control

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.

This aspect of XenApp therefore implements FIA_ATD.1/User, FDP_ACC.1/Application, FDP_ACF.1/Application, and FMT_MSA.1/Application.

7.3 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 access by that user.

This aspect of XenApp therefore implements FIA_ATD.1/User, FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FDP_ACC.1/Application, FDP_ACF.1/Application, FMT_MSA.1/Application and FMT_MSA.3/Application.

7.4 Inter-Component Authentication and Encryption

All data transmitted between endpoint device and server components are encrypted using the TLS protocol, the endpoint Online Plug-in having first performed authentication of the server component.

All data transmitted between server components are encrypted according to IPSec, having first performed authentication of both components.

Encryption/decryption of communication between endpoint device and server according to TLS is carried out by calls to the Microsoft Enhanced Cryptographic Provider using

- **Triple-DES as defined by the ciphersuite TLS_RSA_WITH_3DES_EDE_CBC_SHA, or**
- **AES as defined by the ciphersuite RSA_WITH_AES_128_CBC_SHA, or**
- **AES as defined by the ciphersuite RSA_WITH_AES_256_CBC_SHA**

in accordance with the conditions of their accreditation against FIPS140-2.

This aspect of XenApp therefore implements FCO_SCO.1/Client and FCS_ECA.1/Client. (Note also that guidance in [CCECG] ensures that the configuration uses TLS between web browser and web server, and IPSec between server components, also in accordance with FIPS 140-2 accreditation.)

7.5 Clipboard Transfer

When (and only when) clipboard transfer is enabled for a user by an administrator, users may cut, copy and paste information between a published application and a Windows clipboard on the endpoint device.

This aspect of XenApp therefore implements FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FDP_ACC.1/Resource, FDP_ACF.1/Resource, FMT_MSA.3/Resource and FMT_MOF.1/Resource.

7.6 Client Drive Mapping

When (and only when) client drive mapping is enabled for a user by an administrator, a published application may, if allowed by the user, access the local drives on the endpoint device.

This aspect of XenApp therefore implements FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FDP_ACC.1/Resource, FDP_ACF.1/Resource, FMT_MSA.3/Resource and FMT_MOF.1/Resource.

End of Document