Common Criteria Security Target

For

Citrix XenDesktop 4 Platinum edition

Version 1-0   17 August 2010

Summary of Amendments

Version 1-0 17 August 2010

First public release.

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® XenDesktop™ 4 Platinum edition product.

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

The Sponsor and Developer for the EAL2 evaluation is Citrix Systems Inc.

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 Final, 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 Final, July 2009.

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

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

Developer documentation

[CCECG] Common Criteria Evaluated Configuration Guide for Citrix XenDesktop 4
Platinum edition, version 1.0, document code: August 12 2010 10:09:00

Other

[FIPS140-2] Federal Information Processing Standards Publication
Security Requirements for Cryptographic Modules
FIPS PUB 140-2, NIST, 25 May 2001

0.5 Significant Assumptions

None

0.6 Outstanding Issues

None

0.7 Abbreviations

Acronym	Meaning
DCOM	Distributed Component Object Model
DDC	Desktop Delivery Controller
DSC	Delivery Services Console
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
ICA	Independent Computing Architecture
IMA	Independent Management Architecture
OSP	Organisational Security Policy
PP	Protection Profile
PSC	Presentation Server Console
PVS	Provisioning Server

Acronym	Meaning
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
SSL	Secure Sockets Layer
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
VDA	Virtual Desktop Agent
WCF	Windows Communication Foundation
WI	Web Interface

0.8 Glossary

Term	Meaning
Access permissions for virtual desktops	configuration data within the TOE which determines which virtual desktops each desktop user is permitted to access.
Assurance	grounds for confidence that a TOE meets the SFRs [CC1]
Citrix online plug-in	installed on user devices, this enables direct ICA connections from user devices to virtual desktops. Although it can be used as a plug-in to a Citrix framework, in the evaluated configuration it is used standalone.
Configdata	configuration data within the TOE; which includes Access permissions for virtual desktops, Virtual desktop configuration data and Endpoint data access control policy. See section 3.1.
Delivery Services Console	provides the administration interface to the Desktop Delivery Controller for managing access permissions for virtual desktops and virtual desktop configuration data.
Desktop Delivery Controller	authenticates administrators and desktop users, manages the assembly of desktop users' virtual desktop environments and brokers connections between desktop users and their virtual desktops.
Desktop Group	an administrative grouping of desktops of a similar type. Users can be given permissions to access one or more desktop groups, but in the evaluated configuration each user is given access to only a single desktop group.
Domain-joined (user) device	a domain-joined user device is a PC that is registered with the domain controller as a member of the Windows network domain that contains the TOE server components (i.e. the PC is a domain member).
Endpoint data access control policy	configuration data within the TOE defining a centrally administered policy which determines whether or not a virtual desktop user can access User Device resources from within a virtual desktop: specifically clipboard, local drives, USB devices.

Term	Meaning
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]
ICA File	a file used with the Independent Computing Architecture, which contains configuration information enabling a client to connect to a server.
Independent Computing Architecture	a presentation services protocol, used to present input (keystrokes, mouse clicks etc.) to the virtual desktop for processing and to return output (display, audio etc.) to the User Device.
Independent Management Architecture	a server-to-server infrastructure that provides robust, secure, and scalable tools for managing any size server farm. Among other features, IMA enables centralised platform-independent management, an ODBC-compliant data store, and management products that plug into a management console.
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.
Non-domain-joined (user) device	a non-domain-joined user device is a PC that is not registered with the domain controller as a member of the Windows network domain that contains the TOE server components (i.e. the PC is not a domain member).
Object	a passive entity in the TOE, that contains or receives information, and upon which subjects perform operations. [CC1]
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]
Presentation Server Console	provides the administration interface to the Desktop Delivery Controller for managing Endpoint data access control policy.
Protection Profile	an implementation-independent statement of security needs for a TOE type. [CC1]
Provisioning	providing the configuration required for virtual desktops.
Secure Sockets Layer	an open, non-proprietary protocol that provides data encryption, server authentication, message integrity and optional client authentication for a TCP/IP connection.
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]

Term	Meaning
Security Functional Requirement	a translation of the security objectives for the TOE into a standardised language. [CC1]
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]
Subject	an active entity in the TOE that performs operations on objects. [CC1]
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	the latest, standardised, version of SSL, providing server authentication, data stream encryption and message integrity checks.
TSF Data	data created by and for the TOE, that might affect the operation of the TOE. [CC1]
User Data	data created by and for the user, that does not affect the operation of the TSF. [CC1]
User Device	a device (in the evaluated configuration this will be a PC running Windows) used by a desktop user to gain access to their virtual desktops.
Userdata	user data within the TOE. See section 3.1.
Virtual Desktop	a desktop operating system running on a virtual machine on a virtualised server, personalised for a desktop user.
Virtual Desktop Agent	installed on virtual desktops, this enables direct ICA connections between the virtual desktop and users' User Devices.
Virtual desktop configuration data	configuration data within the TOE which determines the configuration and characteristics of each virtual desktop.
VM Host	a server providing the virtual machines on which the virtual desktops are running.
Web Interface	a server providing an interface for desktop users to authenticate themselves, in order to gain access to their virtual desktops.
XenAPI	the API for managing XenServer installations, i.e. for remotely configuring and controlling domains running on hosts in a XenServer pool.
XenServer	the Citrix server virtualisation product (used in the XenDesktop evaluated configuration).

Contents

Figures / Tables

1. ST Introduction

In this section, the introduction to the ST is provided.

1.1 ST and TOE Reference Identification

TOE Reference:	XenDesktop 4 Platinum edition
ST Reference:	CIN2-ST-0001
ST Version:	1-0
ST Date:	17 August 2010
Assurance Level:	EAL2 augmented by ALC_FLR.2 Flaw Reporting Procedures
ST Author:	SiVenture

1.2 TOE Overview

1.2.1 Usage and major features of the TOE

Citrix XenDesktop 4 Platinum edition (hereinafter referred to as XenDesktop) is a desktop virtualisation product that centralises and delivers Microsoft Windows XP or Vista virtual desktops as a service to users anywhere. Virtual desktops are dynamically assembled on demand, providing users with pristine, yet personalised, desktops each time they log on. This ensures that performance never degrades, while the high speed delivery protocol provides unparalleled responsiveness over any network. XenDesktop delivers a high definition user experience over any connection, including high latency wide area networks.

The open architecture of XenDesktop offers choice and flexibility of virtualisation platform and User Devices. XenDesktop integrates with server virtualisation products including Citrix XenServer and works out-of-the-box with desktop appliances from every major thin client vendor. Users can also access their virtual desktops from most common client devices, including Windows, Mac OS, and Linux. This means that there is no vendor lock-in for virtualisation or User Devices. [See section 1.4.3 for details of the evaluated configuration]

Unlike other desktop virtualisation alternatives, XenDesktop simplifies desktop lifecycle management by using a single image to deliver personalised desktops to users and enables administrators to manage service levels with built-in desktop performance monitoring. The entire desktop lifecycle is managed in one location, simplifying desktop provisioning, patching, security, and updates.

Although the desktops are virtual, running on remote servers, the user experience is equivalent to that of a local Windows desktop. From the user’s perspective, logging on to a virtual desktop is the same as logging on to a local desktop. Users enter their credentials once and are connected to their desktops.

Citrix XenDesktop provides the following key security features:

- **Authentication of desktop users**. Desktop users are authenticated before access is granted to virtual desktops. Multifactor authentication can be enabled and enforced for secure tokens and smart card authentication to Windows XP desktops. Once authenticated, desktop users are provided with a reliable connection to a pristine virtual desktop that incorporates their personal settings and applications, regardless of the User Device or location.
- **Authenticated administrators**. Only authenticated administrators can use the access management facilities.
- **Access Management**. Administrators can assign desktop users to virtual desktops, and manage the connections to the virtual desktops. Provisioning new users is simply a matter of creating an Active Directory user account and associating the account with a standard desktop image.
- **Control over use of User Device resources**. Centralised control policies, set by administrators, determine whether desktop users can access local User Device resources such as the clipboard, local drives, or USB devices, from their virtual desktop.
- **Secure communications**. High performance, standards-based encrypted transmissions are used for communications between server components, and between User Device and server components.

1.2.2 TOE Type

Desktop Virtualisation.

1.2.3 Required non-TOE hardware/software/firmware

For the Web Interface including the Web Interface Management Console, a server is required with the following software:

- Microsoft Windows Server 2003, 32-bit Edition, Enterprise Edition, R2, SP2
- Microsoft .NET Framework 3.5, SP1
- Microsoft Internet Information Server (IIS) 6.0
- Microsoft ASP.NET 2.0
- Microsoft Visual J# 2.0 Second Edition Redistributable Package

For the Desktop Delivery Controller (DDC) including the Delivery Services Console, Presentation Server Console and License Server, a server is required with the following software:

- Microsoft Windows Server 2003, 32-bit Edition, Enterprise Edition, R2, SP2
- Microsoft .NET Framework 3.5, SP1

- Java Runtime Environment (JRE) 1.6.0_20
- Microsoft Internet Information Server (IIS) 6.0
- Microsoft ASP.NET 2.0

The DDC requires a Data store with the following software:

- Microsoft SQL Server 2005 SP2
- Microsoft Windows Server 2003, 32-bit Edition, Enterprise Edition, R2, SP2

A User Device will be a PC with the following software:

- For domain-joined User Devices: Microsoft Windows XP Professional SP3
- For non-domain-joined User Devices:
  - Microsoft Windows Vista Ultimate SP1, or
  - Windows XP Professional SP3, or
  - Windows Server 2003 R2 SP2

Each Virtual desktop will require the following software:

- Microsoft Windows:
  - Microsoft Windows Vista 32-bit Ultimate SP1, or
  - Windows XP Professional 32-bit SP3

The virtual desktops will be provided on the hosting infrastructure, which requires at least one server running:

- Citrix XenServer 5.6, Platinum Edition

Access to the domain controller is required, which will be a Microsoft server in the environment running:

- Microsoft Active Directory Server in native mode

1.3 TOE Description

Citrix XenDesktop provides a complete virtual desktop delivery system by integrating several distributed components with advanced configuration tools that simplify the creation and real-time management of the virtual desktop infrastructure.

The core components of XenDesktop (illustrated in Figure 1) are:

- **Desktop Delivery Controller**. Installed on servers in the data centre, the controller requires that desktop users are authenticated, manages the assembly of desktop users' virtual desktop environments, and brokers connections between desktop users and their virtual desktops. It controls the state of the desktops, starting and stopping them based on demand and administrative configuration.

- **Virtual Desktop Agent**. Installed on virtual desktops, the agent enables direct ICA (Independent Computing Architecture) connections between the virtual desktop and the desktop user's User Device.
- **Citrix online plug-in**. Installed on user devices, the Citrix online plug-in enables direct ICA connections from user devices to virtual desktops.
- **Web Interface**. Installed on a server in the data centre, Web Interface is used to give authorised desktop users access through the Web or intranet to the virtual desktops that they are authorised to use. Desktop users log on to Web Interface using an Internet browser and are given the ICA file that the Citrix online plug-in needs to connect to the Virtual Desktop Agent for access to an authorised virtual desktop.
- **Web Interface Management Console**. This provides an administration interface to Web Interface, making use of Windows authentication for administrators. It provides administrators with functions to manage the configuration of Web Interface, including setting the desktop user authentication method. This is installed on the Web Interface server.
- **Delivery Services Console**. This provides an administration interface to the Desktop Delivery Controller, making use of Windows authentication for administrators. It provides administrators with a number of functions, to manage the configuration of virtual desktops and manage desktop users' access permissions for virtual desktops. This is installed on the Desktop Delivery Controller.
- **Presentation Server Console**. This provides an administration interface to the Desktop Delivery Controller, making use of Windows authentication for administrators. It provides administrators with a function to manage the Endpoint data access control policy. This is installed on the Desktop Delivery Controller.
- **Data Store**. This stores the Configdata managed by the administrators with the Delivery Services Console and Presentation Server Console, including the Endpoint data access control policy, configuration of virtual desktops, desktop users' access permissions for virtual desktops and access permissions for administrators.

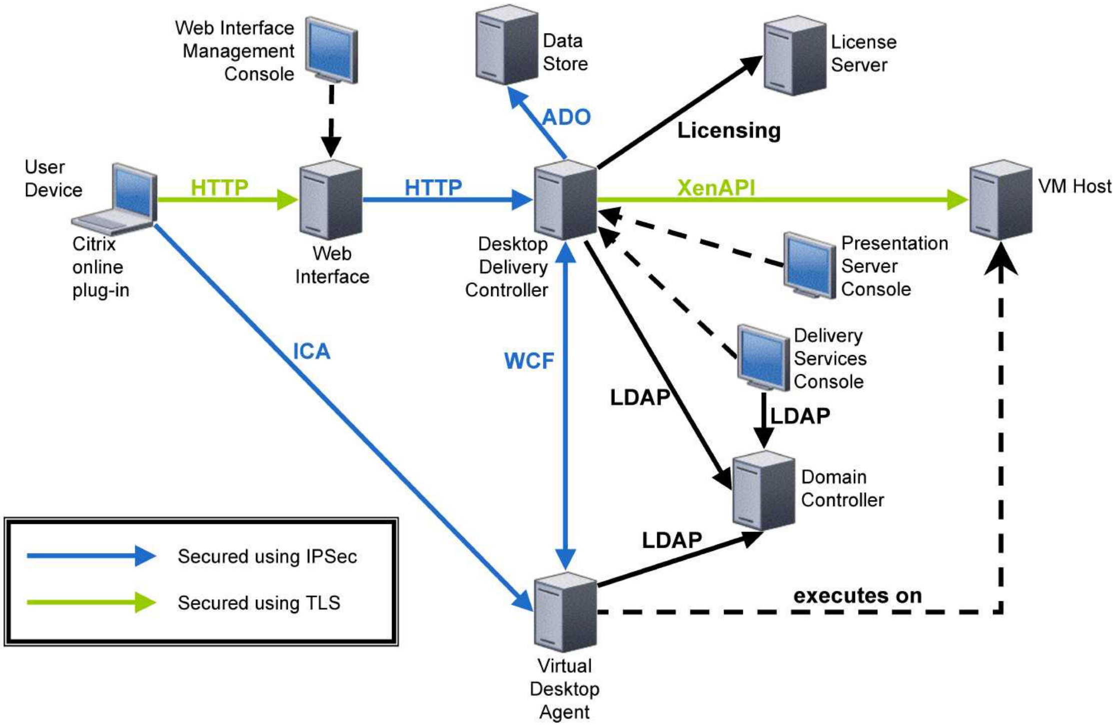

Figure 1: XenDesktop Components

The interactions between the components, to provide a virtual desktop to a desktop user, are as follows (and illustrated in Figure 2):

1. The user's access permissions are configured by the administrator via the Delivery Services Console. The authentication method (either username/password or smartcard/PIN) accepted by Web Interface is configured using the Web Interface Management Console.

2. A desktop user connects to Web Interface to establish a session; depending on configuration this may be via a web browser (in the case of a non-domain-joined user device) or using the Citrix online plug-in (in the case of a domain-joined user device). If the user device is domain-joined, the desktop user's identity will already have been authenticated during the Microsoft Windows logon process, in which case their identity is made available to Web Interface. If the user device is non-domain-joined, they are presented with a dialog box by Web Interface in order to login. If the Web Interface has been configured to accept username and password the desktop user enters their credentials, which are sent as a standard HTTP request protected by TLS. If the Web Interface has been configured to use Smartcard authentication then the user will be prompted to insert their smartcard and enter their PIN.

3. The Web Interface reads the desktop user's credential information and passes it to the Desktop Delivery Controller.

4. The Desktop Delivery Controller requests the Domain Controller to authenticate the desktop user's credentials and retrieves from the data store a list of desktops to which the desktop user's access permissions allow access and informs Web Interface. In the

evaluated configuration each desktop user belongs to only one virtual desktop group, however in other configurations a choice of desktop groups may be available to the desktop user.

5. Web Interface generates an HTML page containing a hyperlink for each desktop in the list received from the Desktop Delivery Controller. In the evaluated configuration each desktop user belongs to only one virtual desktop group, and hence there would be only one hyperlink on the HTML page.

6. The desktop user clicks one of the hyperlinks in the HTML page. The web browser (or Citrix online plug-in) sends a request to the Web Interface to retrieve the ICA file for the selected desktop. In the evaluated configuration each desktop user belongs to only one virtual desktop group and the desktop user would click the only hyperlink on the page.

7. Web Interface contacts the Desktop Delivery Controller requesting an authentication ticket for the desktop user.

8. The Desktop Delivery Controller allocates a virtual desktop from the pool of available desktops (if any).

9. If there is no available desktop, the Desktop Delivery Controller checks with the license server to confirm that there is an available license and, if so, starts a new desktop and allocates it to the desktop user.

10. The Desktop Delivery Controller generates and returns an authentication ticket to Web Interface along with the IP address of the Virtual Desktop Agent that will provide the virtual desktop allocated for the desktop user.

11. The Desktop Delivery Controller also instructs the appropriate Virtual Desktop Agent to prepare to receive a connection request.

12. Web Interface sends an ICA file containing the authentication ticket as a reply to the desktop user's request. This is delivered to the Citrix online plug-in on the desktop user’s User Device.

13. The Citrix online plug-in receives the ICA file and uses it to send a connection request to the Virtual Desktop Agent, including the authentication ticket.

14. The Virtual Desktop Agent asks the Desktop Delivery Controller to confirm that the correct authentication ticket has been supplied within the time limit. If so the Desktop Delivery Controller returns the desktop user’s credentials to the Virtual Desktop Agent.

15. If the Desktop Delivery Controller has validated the authentication ticket and returned the desktop user’s credentials, the Virtual Desktop Agent establishes the session using the credentials to logon to the virtual desktop; it provides access to enable the desktop user’s Citrix online plug-in to present the desktop user with the virtual desktop.

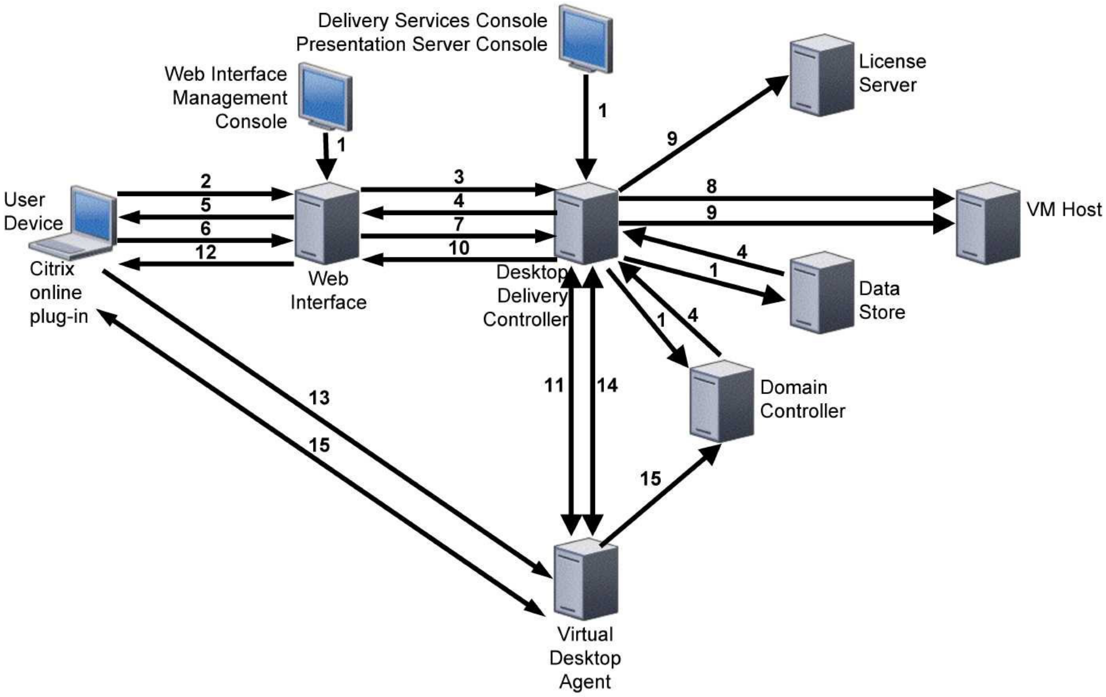

Figure 2: Interactions between components

1.4 TOE Boundaries

1.4.1 Physical Boundary

The physical boundary of the TOE encompasses the TOE Server components and the TOE Client component, as illustrated in Figure 3. The TOE Server components comprise the Desktop Delivery Controller (including the Delivery Services Console and Presentation Server Console), the Web Interface, the Data store, the VM Host and the Virtual Desktop Agents. The TOE Client component is the Citrix online plug-in running on a User Device.

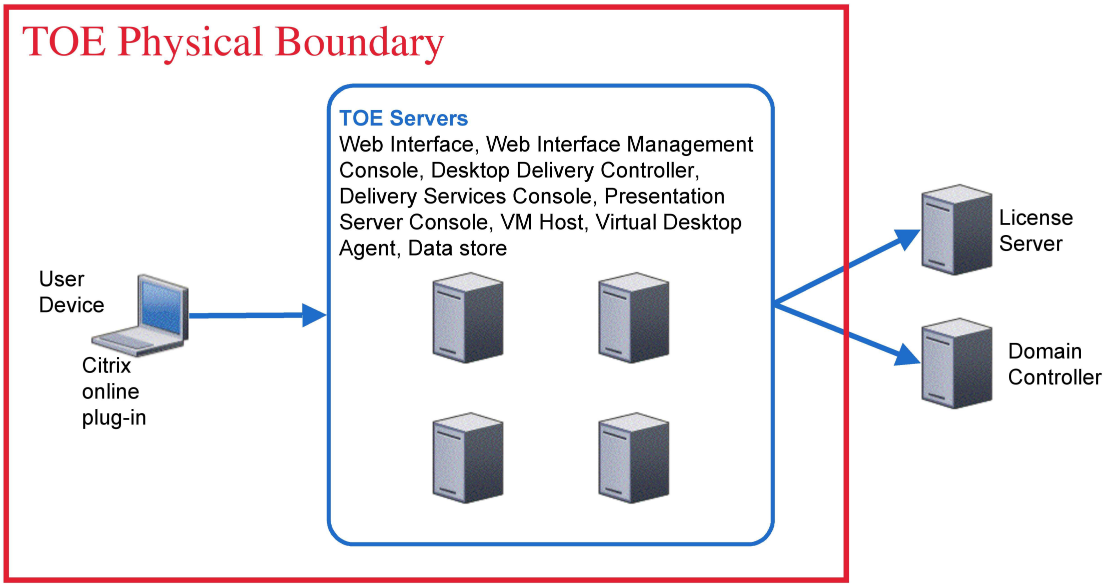
TOE Physical Boundary
TOE Servers
Web Interface, Web Interface Management Console, Desktop Delivery Controller, Delivery Services Console, Presentation Server Console, VM Host, Virtual Desktop Agent, Data store
User Device
Citrix online plug-in
License Server
Domain Controller

Figure 3: TOE Physical boundary

1.4.2 Logical Boundary

Citrix XenDesktop is offered in various editions that provide different features. The evaluated TOE consists of the following:

Citrix XenDesktop 4 Platinum Edition, including

- Desktop Delivery Controller v4.0,
- Delivery Services Console v3.0,
- Presentation Server Console v4.5,
- Web Interface (including Web Interface Management Console) v5.2,
- Virtual Desktop Agent v4.0,
- Citrix online plug-in v11.2

These are all (apart from the Citrix online plug-in in the case of a non-domain-joined User Device) required to belong to the same Active Directory domain, as are all desktop users and administrators.

The Citrix online plug-in runs on the User Device, while the other components run on servers (in a variety of possible configurations). The logical boundaries of the TOE are illustrated below in Figure 4, where elements shown shaded are components of the TOE.

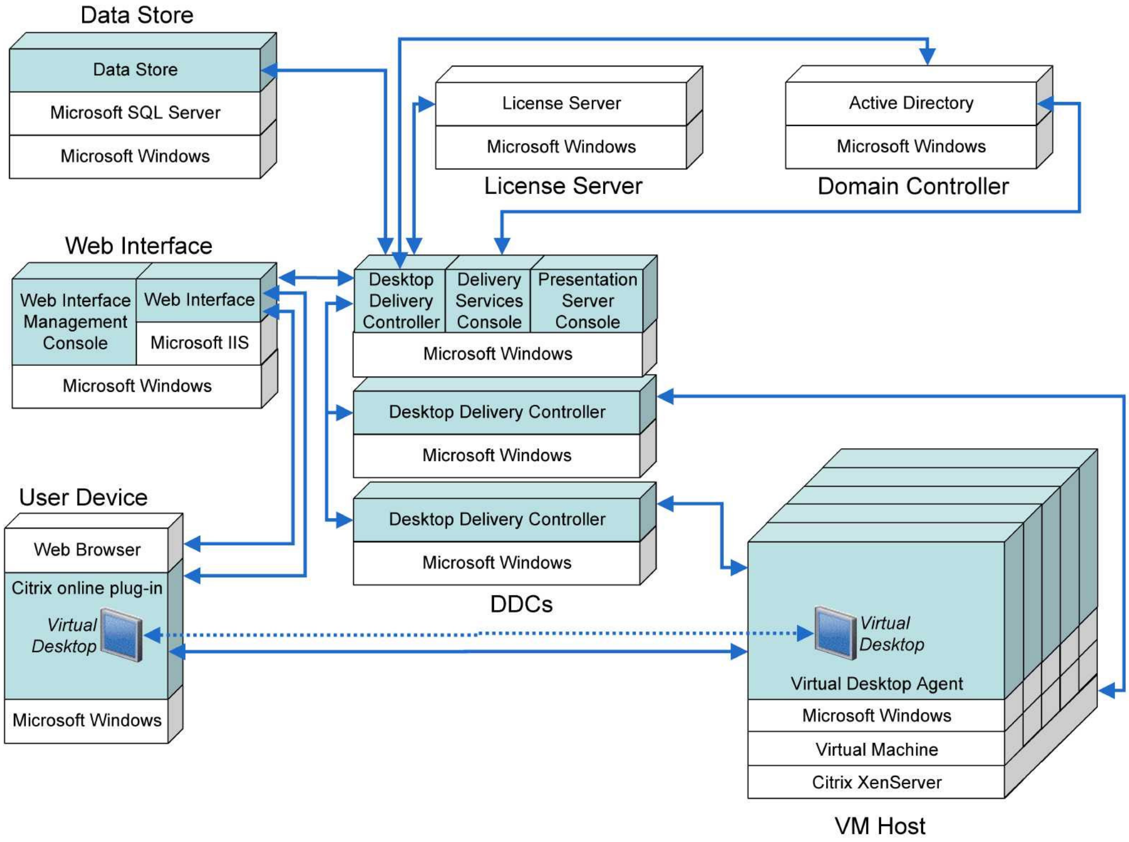

Figure 4: Logical boundaries

1.4.3 Summary of items out of scope of the TOE

The items out of scope of the TOE include the Microsoft components with which Citrix XenDesktop integrates, as detailed in section 1.2.3.

Also out of scope of the TOE are the following Citrix components which are included in XenDesktop Platinum Edition:

- Citrix XenServer – hypervisor, used in the environment of the evaluated configuration to provide the hosting for the virtual desktops;
- Citrix XenApp for Virtual Desktops – offers application virtualisation, not used in the evaluated configuration;
- Citrix Access Gateway – offers secure remote access, not used in the evaluated configuration;
- Citrix Provisioning Services– optimises provisioning of virtual desktops, not used in the evaluated configuration;
- Citrix Workflow Studio – graphical interface for workflow composition, not used in the evaluated configuration;

- Citrix Profile Management – high performance user personalisation method, not used in the evaluated configuration;
- Citrix EdgeSight for Endpoints – centralised performance monitoring and management of User Devices, not used in the evaluated configuration;
- Citrix Repeater – accelerator for improved performance on wide area networks, not used in the evaluated configuration;
- Citrix GoToAssist – remote user support, not used in the evaluated configuration;
- Citrix EasyCall – voice communications, not used in the evaluated configuration.

As a result, certain features of XenDesktop are not included in the scope of the evaluation:

- Server-side and client-side application virtualisation is not included; only applications 'baked-in' to the virtual desktop image are included in the evaluation;
- Smart card support for desktop user authentication is included in the evaluation, but tokens are not;
- Administrators can enable/disable local peripheral support either as a global control policy or for individual users and groups of users; only the facility for applying a global control policy is included in the evaluation;
- Desktop appliances and client devices other than Windows PCs are not included as User Devices in the evaluation;
- The capability for Desktop users to belong to multiple desktop groups is not included, a Desktop user can only use a virtual desktop from one desktop group.

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 for Parts 1, 2 and 3. The methodology applied for the evaluation is defined in [CEM].

This Security Target is Part 2 extended, Part 3 conformant. The assurance level is EAL2 augmented by ALC_FLR.2 Flaw Reporting Procedures.

The extended components, defined in section 5, are:

- FCS_ECA.1 Conformance with External Cryptographic Accreditation;
- FCO_SCO.1 Secure Channel Operation.

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:

Desktop

A virtual desktop. Protection requirements are for confidentiality and integrity.

Userdata

User data in transit across a network between the User Device and servers, and between servers. Protection requirements are for confidentiality and integrity.

The following asset is introduced as a result of using the TOE:

Configdata

Data generated by an administrator during configuration and management of the TOE. This includes desktop users' access permissions for virtual desktops; virtual desktop configuration data; and setup data exchanged between server components and with the client component during the establishment of a virtual desktop for provision to a desktop user. Protection requirements are for confidentiality and integrity.

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.

Desktop user

A user who has been granted access to the TOE. A desktop user would access virtual desktops through a User Device.

Administrator

An administrator manages users' access to virtual desktops. 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

A User Device used by a desktop user to gain access to the TOE. It consists of a PC. To enable access, the User Device will be running the Client component of the TOE.

3.3 Threats

3.3.1 Attacks on the TOE

The following items detail threats which the TOE (in some cases with the support of the operational environment) is intended to address:

T.Attack_Desktop An attacker may gain access to a virtual desktop.

T.Attack_Userdata An attacker may gain access to Userdata.

T.Access_Desktop A desktop user may gain unauthorised access to a virtual desktop.

T.Access_Userdata A desktop user may gain unauthorised access to another desktop user's Userdata.

T.Intercept An attacker may intercept communication channels. This may lead to compromise of users' authentication credentials, other Userdata, or Configdata in transit.

T.Spoof An attacker may cause communications between a User Device 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 users' authentication credentials.

T.Attack_Configdata An attacker or desktop user may modify Configdata.

3.4 Organisational Security Policies

OSP.Crypto Cryptographic functions shall be validated to FIPS 140-2 Level 1.

3.5 Assumptions

A.Physical It is assumed that TOE servers are installed in a physically secure location that can only be accessed by authorised administrators.

A.Config_Endpoint The User Device operating system is securely configured, including appropriate file protection. In particular, a non-administrative user should not have access to facilities to edit the User Device registry.

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.VM_Host The VM Host software is operating correctly and securely.

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
- Microsoft Terminal Services

- Windows Server 2003 (including Active Directory)

4. Security Objectives

4.1 Security Objectives for the TOE

O.Auth_User

Desktop users and administrators must be successfully identified and authenticated before being granted access to the TOE.

O.Auth_Server

TOE server components must authenticate themselves to User Devices and other servers before communication of Userdata or Configdata.

O.Desktop

Desktop users must be granted access only to virtual desktops for which they have been authorised.

O.Secure_Setup_Data

The confidentiality and integrity of data required for setup and assignment of a virtual desktop must be maintained during processing and transmission between servers.

O.Secure_User_Data

The confidentiality and integrity of Userdata being processed on the virtual desktop must be maintained.

O.Use_FIPS

TOE components must invoke FIPS 140-2 level 1 validated cryptographic functions in accordance with the conditions of the validation.

O.Virtualised_Memory

The contents of the memory used by the Virtual Desktop Agent to run the virtual desktop during a desktop user's session must not be available to other processes when that user's session is complete.

O.Config_Desktop

The virtual desktop must only be configurable by administrators.

Application note

Virtual desktops must be configured by administrators such that it is not possible for users to gain access to the underlying operating system or hardware on which the Virtual Desktop Agent is running.

O.Endpoint_Resource

An administrator must be able to control the use of User Device resources by authorised desktop users. This includes the ability to cut, copy and paste information between a virtual desktop and a User Device operating system clipboard; access, from a virtual desktop, to local drives on the User Device; access, from a virtual desktop, to local USB devices on the User Device.

4.2 Security Objectives for the Environment

4.2.1 Security Objectives for the Technical Environment

The following technical 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.

OE.Config_VM_Host

VM Host software must be securely configured.

OE.Config_TP_SW

Trusted third party software must be securely configured according to [CCECG]. Trusted third party software is defined as:

- Microsoft IIS (the secure Web Server)
- Microsoft Windows (including Terminal Services)

OE.Authenticate

Desktop users and administrators must be authenticated by the underlying operating system on the relevant platform. Authentication requirements in the operating system shall be configured according to the risks in the operational environment.

OE.IPSec

All communication between the TOE servers (apart from communications between the Desktop Delivery Controller and the VM Host), and between Virtual Desktop Agents and User Device Citrix online plug-ins, uses the configured IPSec protocol. This is accomplished by the administrator setting these servers to use the IPSec protocol.

OE.TLS

All communication between the Web Interface and the User Device (web browser or Citrix online plug-in), and between the Desktop Delivery Controller and the VM Host, uses the configured TLS protocol.

The following technical objectives relate to the User Devices:

OE.Config_Endpoint

The User Device operating system must be securely configured according to [CCECG], including appropriate file protection.

Application note

User Devices must be configured such that desktop user authentication credentials and user data are not left in memory after the user has logged out from their virtual desktop.

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

OE.Encryption

Secure encryption modules 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.

4.2.2 Security Objectives for the Procedural Environment

OE.Server_Physical The operational environment shall provide physical protection to the TOE servers to ensure only administrators are able to gain physical access to the servers.

OE.Endpoint_TP_SW User Devices must have only trusted third party software installed. This software must be configured securely according to the risks in the operational environment.

OE.Admin_Users Configdata stored outside the TOE, such as in the datastore, must be accessible only by administrators.

4.3 SPD/Objectives Rationale

The following table provides a summary of the relationship between the security objectives and the security problem definition. The rationale is provided in the sections that follow.

Threat/ OSP/ Assumption Security Objectives	T.Attack_Desktop	T.Attack_Userdata	T.Access_Desktop	T_Access_Userdata	T.Intercept	T.Spoof	T.Attack_Configdata	OSP.Crypto	A.Physical	A.Config_Endpoint	A.Operations_Security	A.VM_Host	A.Third_Party_SW
O.Auth_User	X	X					X						
O.Auth_Server					X	X							
O.Desktop			X	X									
O.Secure_Setup_Data			X		X		X						
O.Secure_User_Data		X		X									
O.Use_FIPS								X					
O.Virtualised_Memory		X	X	X									
O.Config_Desktop		X	X	X									
O.Endpoint_Resource		X		X									
OE.Config_Server	X	X	X	X		X	X						
OE.Config_VM_Host	X	X	X	X		X						X	
OE.Config_TP_SW	X	X	X	X		X	X						X
OE.Authenticate	X	X		X			X						
OE.IPSec		X		X	X		X						
OE.TLS		X		X	X	X							
OE.Config_Endpoint	X	X		X		X				X			
OE.Encryption		X		X			X	X					
OE.Operations_Security											X		
OE.Server_Physical									X				
OE.Endpoint_TP_SW						X							X
OE.Admin_Users			X				X						

Table 1: Threats/OSP/Assumptions addressed by Security Objectives

4.3.1 T.Attack_Desktop

Attackers are prevented from gaining access to a virtual desktop by a combination of TOE and environment objectives to apply identification and authentication.

O.Auth_User and OE.Authenticate ensure that only identified and authenticated desktop users and administrators are granted access to the TOE.

OE.Config_Server ensures that the servers have been set up properly, while OE.Config_VM_Host and OE.Config_TP_SW ensure that potentially privileged programs do not undermine security.

OE.Config_Endpoint ensures that the User Devices have been set up properly and that authentication credentials are not left in the User Device memory to be retrieved by an attacker.

4.3.2 T.Attack_Userdata

Attackers are prevented from gaining access to Userdata by a combination of TOE and environment objectives to apply authentication, authorisation, confidentiality and integrity.

O.Auth_User and OE.Authenticate ensure that only identified and authenticated desktop users and administrators are granted access to the TOE.

OE.TLS, OE.IPSec and OE.Encryption ensure the confidentiality of Userdata, including authentication credentials, during login and establishment of a virtual desktop.

O.Secure_User_Data, ensures the confidentiality and integrity of Userdata being processed on a virtual desktop.

O.Config_Desktop ensures that the virtual desktops have been set up properly, while O.Virtualised_Memory ensures that Userdata are not left in the virtual desktop memory after a user has logged out of the virtual desktop.

OE.Config_Server ensures that the servers have been set up properly, while OE.Config_VM_Host and OE.Config_TP_SW ensure that potentially privileged programs do not undermine security.

O.Endpoint_Resource ensures that users can only use the clipboard and devices attached to the User Device when authorised.

OE.Config_Endpoint ensures that the User Devices have been set up properly and that authentication credentials and other Userdata are not left in the User Device memory to be retrieved by an attacker.

4.3.3 T.Access_Desktop

Users are prevented from gaining unauthorised access to a virtual desktop by a combination of TOE and environment objectives to apply authorisation, confidentiality and integrity.

O.Desktop ensures that a virtual desktop is only available to an authorised desktop user. OE.Admin_Users ensures that only administrators have access to Configdata and thus the ability to authorise users' access to a virtual desktop. O.Secure_Setup_Data ensures the confidentiality and integrity of the setup and assignment data for the virtual desktop on the servers.

O.Config_Desktop ensures that the virtual desktops have been set up properly, while O.Virtualised_Memory ensures that Userdata are not left in the virtual desktop memory after a user has logged out of the virtual desktop.

OE.Config_Server ensures that the servers have been set up properly, while OE.Config_VM_Host and OE.Config_TP_SW ensure that potentially privileged programs do not undermine security.

4.3.4 T.Access_Userdata

Desktop users are prevented from gaining unauthorised access to another desktop user's Userdata by a combination of TOE and environment objectives to apply authentication, authorisation, confidentiality and integrity.

O.Desktop ensures that a virtual desktop is only available to a desktop user authorised to have access.

OE.TLS, OE.IPSec and OE.Encryption ensure the confidentiality of Userdata, including authentication credentials, during login and establishment of a virtual desktop.

O.Secure_User_Data, ensures the confidentiality and integrity of Userdata being processed on a virtual desktop.

O.Config_Desktop ensures that the virtual desktops have been set up properly, while O.Virtualised_Memory ensures that Userdata are not left in the virtual desktop memory after a user has logged out of the virtual desktop.

OE.Config_Server ensures that the servers have been set up properly, while OE.Config_VM_Host and OE.Config_TP_SW ensure that potentially privileged programs do not undermine security.

O.Endpoint_Resource ensures that users can only use the clipboard and devices attached to the User Device when authorised.

OE.Config_Endpoint ensures that the User Devices have been set up properly and that authentication credentials and other Userdata are not left in the User Device memory to be retrieved by an attacker.

4.3.5 T.Intercept

Attackers are prevented from intercepting communications channels by a combination of TOE and environment objectives to apply authentication, confidentiality and integrity.

O.Auth_Server ensures that servers authenticate themselves to clients and other servers before communicating Userdata or Configdata. O.Secure_Setup_Data ensures the confidentiality and integrity of the setup and assignment data for the virtual desktop during transmission between servers.

OE.TLS ensures the confidentiality and integrity of communications between the User Device browser and the web interface during login and establishment of the virtual desktop, and between the Desktop Delivery Controller and the VMHost. OE.IPSec ensures the confidentiality and integrity of communications between the User Device and the virtual desktop.

4.3.6 T.Spoof

Attackers are prevented from redirecting communications between a User Device and a server to a spoof server by a combination of TOE and environment objectives to apply authentication, confidentiality and integrity.

O.Auth_Server and OE.TLS ensure that servers authenticate themselves to clients before communicating Userdata such as authentication credentials.

OE.Config_Server ensures that the servers have been set up properly, while OE.Config_VM_Host and OE.Config_TP_SW ensure that potentially privileged programs do not undermine security.

OE.Config_Endpoint and OE.Endpoint_TP_SW ensure that the User Devices have been set up properly.

4.3.7 T.Attack_Configdata

Attackers and desktop users are prevented from modifying Configdata by a combination of TOE and environment objectives to apply authentication, authorisation, confidentiality and integrity.

O.Auth_User and OE.Authenticate ensure that only identified and authenticated desktop users and administrators are granted access to the TOE.

OE.Admin_Users ensures that only administrators have access to Configdata. O.Secure_Setup_Data, OE.IPSec and OE.Encryption ensure the confidentiality and integrity of the Configdata on the servers and when transmitted between servers.

OE.Config_Server ensures that the servers have been set up properly, while OE.Config_TP_SW ensures that potentially privileged programs do not undermine security.

4.3.8 OSP.Crypto

The OSP.Crypto Organisation Security Policy to use FIPS 140-2 Level 1 cryptographic functions is addressed by the environment objective OE.Encryption which ensures that the servers are configured to use FIPS 140-2 Level 1 validated algorithm implementations, and the TOE objective O.Use_FIPS which ensures that the TOE components invoke the cryptographic functions in accordance with the conditions of the validation.

4.3.9 A.Physical

The assumption that TOE servers are installed in physically secure locations is addressed by the environment objective OE.Server_Physical which ensures that servers are physically protected and only accessible by administrators.

4.3.10 A.Config_Endpoint

The assumption that User Device operating systems are securely configured with appropriate access permissions is met by the environment objective OE.Config_Endpoint which ensures that the User Device is securely configured including the file protection.

4.3.11 A.Operations_Security

The assumption that secret data outside the TOE is managed appropriately, is met by environment objective OE.Operations_Security which ensures that keys and other secret data generated and stored outside the TOE are managed in accordance with the level of risk.

4.3.12 A.VM_Host

The assumption that the VM Host software is operating correctly and securely is met by the environment objective OE.Config_VM_Host which ensures that the VM Host software is securely configured.

4.3.13 A.Third_Party_SW

The assumption that third party software is operating correctly and securely is met by the environment objectives OE.Config_TP_SW which ensures that trusted third party software is securely configured, and OE.Endpoint_TP_SW which ensures that only securely configured trusted third party software is installed on the User Devices.

5. Extended Component Definition

This Security Target uses two components defined as extensions to CC part 2.

5.1 Extended Security Requirements

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 (FCS_ECA)

The family FCS_ECA describes a requirement for the TOE to provide certain cryptographic functionality in accordance with the conditions of an external accreditation[2], 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[3].

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

Management: FCS_ECA.1

There are no management activities foreseen.

Audit: FCS_ECA.1

There are no auditable events foreseen.

[2] 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.

[3] 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.

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*].

Application note 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 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.

5.1.2 Secure Channel Operation (FCO_SCO)

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: No dependencies.

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 for 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 four functional groupings for the purposes of the specification of the security functional requirements. These are:

- Authentication
- Authorisation
- Communications
- Virtual Desktop

The individual security functional requirements are specified in the sections below. Unless stated otherwise, the term 'user' should be understood to relate to both desktop users and administrators.

6.2.1 Authentication

The SFRs in this section are concerned with enforcing access control to ensure that only authenticated users are granted access to the TOE and virtual desktops.

6.2.1.1 FIA_ATD.1/Desktop_user User attribute definition

FIA_ATD.1.1/Desktop_user The TSF shall maintain the following list of security attributes belonging to individual desktop users: [**access permissions for virtual desktops**].

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 desktop users for access to virtual desktops, and to limit the operations that the desktop users are able to perform.

6.2.2.1 FMT_SMR.1/Authorise Security management roles

FMT_SMR.1.1/Authorise The TSF shall maintain the roles [**desktop 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 management functions: [

- **Administration of access permissions for administrators**
- **Administration of access permissions for virtual desktops**
- **Administration of virtual desktop configuration data**
- **Administration of Endpoint data access control policy.**]

Application note Administration of Endpoint data access control policy consists of enabling or disabling the following functions for virtual desktops:

- cut and paste between User Device and virtual desktop clipboards;
- User Device client drive mapping;
- access to User Device USB devices from virtual desktops.

6.2.2.3 FDP_ACC.1/Desktop Subset access control

FDP_ACC.1.1/Desktop The TSF shall enforce the [**Desktop access policy**] on [**desktop users' access to virtual desktops**].

6.2.2.4 FDP_ACF.1/ Desktop Security attribute based access control

FDP_ACF.1.1/Desktop The TSF shall enforce the [**Desktop access policy**] to objects based on the following: [**user identity, access permissions for virtual desktops**].

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

Virtual desktops shall be accessible by a desktop user only if permitted by the user's access permissions for virtual desktops.]

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

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

6.2.2.5 FMT_MSA.1/Desktop Management of security attributes

FMT_MSA.1.1/Desktop The TSF shall enforce the [**Desktop access policy**] to restrict the ability to [*modify*] the security attributes: [

- **access permissions for virtual desktops**
- **virtual desktop configuration data**]

to [**administrators**].

6.2.2.6 FMT_MSA.3/Desktop Static attribute initialisation

FMT_MSA.3.1/Desktop The TSF shall enforce the [**Desktop 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 a new user defaults to no desktop access.

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

6.2.2.7 FDP_ACC.1/Resources Subset access control

FDP_ACC.1.1/Resources The TSF shall enforce the [**Resource access policy**] on [**desktop users' use of the following operations**

- **transfer of user data between the User Device clipboard and the virtual desktop clipboard**
- **access to mapped client drives from the virtual desktop**
- **access to attached USB devices from the virtual desktop**].

6.2.2.8 FDP_ACF.1/Resources Security attribute based access control

FDP_ACF.1.1/Resources The TSF shall enforce the [**Resource access policy**] to objects based on the following: [**Endpoint data access control policy**].

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

Desktop users shall be permitted to cut and paste data between a virtual desktop and an User Device operating system clipboard only if the cut and paste function has been enabled by the administrator.

User Device client drives shall be accessible to a virtual desktop only if:

- **The client drive mapping function has been enabled by the administrator, and**
- **The desktop user has also permitted the access.**

USB devices on a User Device shall be accessible to a virtual desktop only if:

- **The USB device access function has been enabled by the administrator, and**
- **The desktop user has also permitted the access.**]

Application note A USB storage device may also be accessed through client drive mapping, therefore to ensure that such a device cannot be accessed both client drive mapping and USB device access must be disabled.

The Endpoint data access control policy is applied to the virtual desktop at the launch of the desktop user's session and persists throughout that session. If the policy is subsequently changed, the change will not therefore be effective for any sessions that are already in progress.

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

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

6.2.2.9 FMT_MSA.3/Resources Static attribute initialisation

FMT_MSA.3.1/Resources 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 cut and paste, client drive mapping and USB device access functions will default to disabled following installation of the evaluation configuration.

FMT_MSA.3.2/Resources 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/Resources Management of security functions behaviour

FMT_MOF.1.1/Resources The TSF shall restrict the ability to [*disable, enable*] the functions [**cut and paste, client drive mapping, USB device access**] to [**the administrator**].

Application note The cut and paste, client drive mapping and USB device access functions can be separately enabled/disabled by an administrator either globally (for all desktop users), for groups of desktop users, or for individual desktop users. However, only the global enable/disable is included within the scope of the evaluation. Each Desktop user still has the opportunity to deny or permit access to local client drives or USB devices on their user device, if the administrator has enabled the functions globally.

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/Browser Secure channel operation

FCO_SCO.1.1/Browser The TSF shall use a communication channel between [**the User Device web browser and the Web Interface, and another between the Citrix online plug-in and the Web Interface**] that is logically distinct from other communication channels and provides assured identification of [**the Web Interface**] and protection of the channel data from [*modification, disclosure*].

FCO_SCO.1.2/Browser The TSF shall permit [**the User Device web browser and the Citrix online plug-in**] to initiate communication via the communication channel.

FCO_SCO.1.3/Browser The TSF shall ensure that the communication channel meets the following additional requirements for security: [**use of TLS in accordance with FIPS140-2 validation of the underlying cryptographic functions**].

FCO_SCO.1.4/Browser The TSF shall use the communication channel for [**all traffic between the User Device web browser and the Web Interface, and all traffic between the Citrix online plug-in and the Web Interface**].

Application note No management actions of the sort identified in the definition of the family in section 5 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 FCO_SCO.1/Desktop Secure channel operation

FCO_SCO.1.1/Desktop The TSF shall use a communication channel between [**the User Device Citrix online plug-in and the Virtual Desktop Agent**] that is logically distinct from other communication channels and provides assured identification of [**the User Device Citrix online plug-in and the Virtual Desktop Agent**] and protection of the channel data from [*modification*, *disclosure*].

FCO_SCO.1.2/Desktop The TSF shall permit [**the User Device Citrix online plug-in**] to initiate communication via the communication channel.

FCO_SCO.1.3/Desktop The TSF shall ensure that the communication channel meets the following additional requirements for security: [**use of IPSec in accordance with FIPS140-2 validation of the underlying cryptographic functions**].

FCO_SCO.1.4/Desktop The TSF shall use the communication channel for [**all traffic between the User Device Citrix online plug-in and the Virtual Desktop Agent**].

Application note No management actions of the sort identified in the definition of the family in section 5 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.

6.2.3.3 FCO_SCO.1/Server Secure channel operation

FCO_SCO.1.1/Server The TSF shall use a communication channel between [**pairs of TOE servers**] that is logically distinct from other communication channels and provides assured identification of [**each TOE server**] and protection of the channel data from [*modification*, *disclosure*].

FCO_SCO.1.2/Server The TSF shall permit [**TOE servers**] to initiate communication via the communication channel.

FCO_SCO.1.3/Server The TSF shall ensure that the communication channel meets the following additional requirements for security: [**use of IPSec in accordance with FIPS140-2 validation of the underlying cryptographic functions**].

FCO_SCO .1.4/Server The TSF shall use the communication channel for [**all traffic between TOE servers**].

Application note This does not include communications between the Desktop Delivery Controller and the VM Host which are addressed by the separate SFR FCO_SCO.1/VMHost defined below.

No management actions of the sort identified in the definition of the family in section 5 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.

6.2.3.4 FCO_SCO.1/VMHost Secure channel operation

FCO_SCO.1.1/VMHost The TSF shall use a communication channel between [**the Desktop Delivery Controller and the VM Host**] that is logically distinct from other communication channels and provides assured identification of [**the VM Host**] and protection of the channel data from [*modification*, *disclosure*].

FCO_SCO.1.2/VMHost The TSF shall permit [**the Desktop Delivery Controller**] to initiate communication via the communication channel.

FCO_SCO.1.3/VMHost The TSF shall ensure that the communication channel meets the following additional requirements for security: [**use of TLS in accordance with FIPS140-2 validation of the underlying cryptographic functions**].

FCO_SCO.1.4/VMHost The TSF shall use the communication channel for [**starting, restarting and stopping VMs executing Virtual Desktop Agents, and setting and retrieving status information**].

Application note The Desktop Delivery Controller in this case sends XenAPI commands to the VM Host (XenServer).

No management actions of the sort identified in the definition of the family in section 5 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.

6.2.3.5 FCS_ECA.1/FIPS_KM Conformance with external cryptographic accreditation

FCS_ECA.1.1/FIPS_KM The TOE shall invoke [

encryption of traffic between the User Device Citrix online plug-in and the Virtual Desktop Agent using IPSec with Triple-Des as defined by the ciphersuite DES-EDE3-CBC in RFC 2451]

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

Application note The accreditation of the Microsoft Kernel Mode Cryptographic Module against FIPS140-2 is documented in the following certificates:

Microsoft Windows XP Professional SP3 – Certificate #997.
Microsoft Windows Server 2003 – Certificate #405.
Microsoft Windows Server 2003 SP2 – Certificate #869.
Microsoft Windows Vista Ultimate – Certificate #891.
Microsoft Windows Vista Ultimate SP1 – Certificate #1000.

6.2.3.6 FCS_ECA.1/FIPS_Enh Conformance with external cryptographic accreditation

FCS_ECA.1.1/FIPS_Enh The TOE shall invoke [

- **encryption of traffic between the User Device web browser and the Web Interface using Triple-DES as defined by the ciphersuite TLS_RSA_WITH_3DES_EDE_CBC_SHA in RFC 2246, and**
- **encryption of traffic between the User Device citrix online plug-in and Web Interface using Triple-DES as defined by the ciphersuite TLS_RSA_WITH_3DES_EDE_CBC_SHA in RFC 2246, and**
- **encryption of traffic between the Desktop Delivery Controller and VM Host using Triple-DES as defined by the ciphersuite TLS_RSA_WITH_3DES_EDE_CBC_SHA in RFC 2246, and**
- **encryption of traffic between servers using the Windows Communication Framework (WCF) as defined by the ciphersuite Basic256, and**
- **encryption of traffic between servers using the Distributed Component Object Model (DCOM) and ActiveX Data Objects (ADO) with SSPI**]

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 certificates:

Microsoft Windows XP Professional SP3 – Certificate #989.
Microsoft Windows Server 2003 – Certificate #382.
Microsoft Windows Server 2003 SP2 – Certificate #1012.
Microsoft Windows Vista Ultimate – Certificate #893.
Microsoft Windows Vista Ultimate SP1 – Certificate #1002.

When using DCOM and ADO with SSPI the ciphersuite is not directly selectable, but SSPI is constrained to use only FIPS-compliant algorithms by the setting of group policy according to [CCECG].

6.2.4 Virtual Desktop

The SFR in this section is concerned with preventing any residual data from a desktop user remaining in the memory of the virtual desktop after that user has logged out, to ensure it cannot be recovered by a different user.

6.2.4.1 FDP_RIP.1/Desktop Subset residual information protection

FDP_RIP.1.1/Desktop 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: [**virtual desktop memory**].

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)
	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 Objectives/SFRs Rationale

The following table provides a summary of the relationship between the security objectives and the security functional requirements. The rationale is in the sections that follow.

SFRs Security Objectives	FIA_ATD.1/Desktop_user	FIA_UID.2/User	FIA_UAU.2/User	FMT_SMR.1/Authorise	FMT_SMF.1/Authorise	FDP_ACC.1/Desktop	FDP_ACF.1/Desktop	FMT_MSA.1/Desktop	FMT_MSA.3/Desktop	FDP_ACC.1/Resources	FDP_ACF.1/Resources	FMT_MSA.3/Resources	FMT_MOF.1/Resources	FCO_SCO.1/Browser	FCO_SCO.1/Desktop	FCO_SCO.1/Server	FCO_SCO.1/VMHost	FCS_ECA.1/FIPS_KM	FCS_ECA.1/FIPS_Enh	FDP_RIP.1/Desktop
O.Auth_User		X	X																	
O.Auth_Server														X	X	X	X			
O.Desktop	X			X	X	X	X	X	X											
O.Secure_Setup_Data				X	X			X	X							X	X			
O.Secure_User_Data										X	X				X	X		X	X	
O.Use_FIPS																		X	X	
O.Virtualised_Memory																				X
O.Config_Desktop				X	X	X	X	X	X											
O.Endpoint_Resource				X	X					X	X	X	X							

Table 3: Summary of Objectives/SFRs Rationale

6.4.1 O.Auth_User

This objective is addressed by FIA_UID.2/User and FIA_UAU.2/User, which ensure that desktop users and administrators are successfully identified and authenticated before they can use the TOE functionality.

6.4.2 O.Auth_Server

This objective is addressed by FCO_SCO.1/Browser, FCO_SCO.1/Desktop, FCO_SCO.1/Server and FCO_SCO.1/VMHost. These requirements ensure the confidentiality, integrity and authenticity of TOE components for all communications between TOE servers, and between User Devices and TOE servers.

6.4.3 O.Desktop

This objective is addressed by FIA_ATD.1/Desktop_user, in conjunction with the security management functions (FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Desktop, FMT_MSA.3/Desktop) and the Desktop access policy (FDP_ACC.1/Desktop, FDP_ACF.1/Desktop).

FIA_ATD.1/Desktop_user ensures that individual desktop users can be granted access permissions for virtual desktops, while FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Desktop and FMT_MSA.3/Desktop ensure that only administrators can manage the desktop users' access permissions.

The Desktop access policy (FDP_ACC.1/Desktop and FDP_ACF.1/Desktop) ensures that only desktop users with the correct access permissions can gain access to a virtual desktop.

6.4.4 O.Secure_Setup_Data

This objective is addressed by FCO_SCO.1/Server and FCO_SCO.1/VMHost, in conjunction with the security management functions (FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Desktop, FMT_MSA.3/Desktop).

FCO_SCO.1/Server ensures the confidentiality and integrity of communications between separate TOE servers to protect Configdata, FCO_SCO.1/VMHost ensures the confidentiality and integrity of communications between the Desktop Delivery Controller and the VM Host to protect Configdata, while FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Desktop and FMT_MSA.3/Desktop ensure that only administrators can manage Configdata.

6.4.5 O.Secure_User_Data

This objective is addressed by FCO_SCO.1/Desktop which ensures the confidentiality and integrity of communications between User Devices and the Virtual Desktop Agent, and FCO_SCO.1/Server which ensures the confidentiality and integrity of communications between TOE servers. The conformance requirements FCS_ECA.1/FIPS_KM and ECS_ECA.1/FIPS_Enh ensure that the cryptographic functions used to secure these communications are invoked in conformance with any conditions of the FIPS 140-2 level 1 validation of the cryptographic modules being used. The Resource access policy (FDP_ACC.1/Resources and FDP_ACF.1/Resources) controls access to Userdata on the User Device.

6.4.6 O.Use_FIPS

This objective is addressed by FCS_ECA.1/FIPS_KM and FCS_ECA.1/FIPS_Enh, which ensure that cryptographic functions are invoked in conformance with any conditions of the FIPS 140-2 level 1 validation of the cryptographic modules being used.

6.4.7 O.Virtualised_Memory

This objective is addressed by FDP_RIP.1/Desktop, which ensures that the contents of memory used by a virtual desktop are purged when the desktop user logs out.

6.4.8 O.Config_Desktop

This objective is addressed by the security management functions (FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Desktop, FMT_MSA.3/Desktop) and the Desktop access policy (FDP_ACC.1/Desktop, FDP_ACF.1/Desktop).

FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Desktop and FMT_MSA.3/Desktop ensure that only administrators can modify or delete virtual desktop configuration data.

The Desktop access policy (FDP_ACC.1/Desktop and FDP_ACF.1/Desktop) ensures that only administrators can gain access to virtual desktop configuration data.

6.4.9 O.Endpoint_Resource

This objective is addressed by FMT_MOF.1/Resources in conjunction with the security management functions (FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.3/Resources) and the Resource access policy (FDP_ACC.1/Resources, FDP_ACF.1/Resources).

FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.3/Resources and FMT_MOF.1/Resources ensure that only authorised administrators can enable or disable cut and paste, client drive mapping, and USB device access functions.

The Resource access policy (FDP_ACC.1/Resources and FDP_ACF.1/Resources) ensures that desktop users can only cut and paste data between a virtual desktop and the User Device operating system clipboard if the cut and paste function has been enabled by an administrator.

The Resource access policy (FDP_ACC.1/Resources and FDP_ACF.1/Resources) ensures that desktop users can only access User Device client drives from the virtual desktop if the client drive mapping function has been enabled by an administrator and the user has permitted the access.

The Resource access policy (FDP_ACC.1/Resources and FDP_ACF.1/Resources) ensures that desktop users can only access USB devices on a User Device from the virtual desktop if the USB device access function has been enabled by an administrator and the user has permitted the access.

6.5 SFR Dependencies Analysis

The dependencies between SFRs implemented by the TOE are detailed in the table below.

SFR	Dependencies	Rationale
FIA_ATD.1/Desktop_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

SFR	Dependencies	Rationale
FMT_SMF.1/Authorise	None	
FDP_ACC.1/Desktop	FDP_ACF.1	Met by FDP_ACF.1/Desktop
FDP_ACF.1/Desktop	FDP_ACC.1	Met by FDP_ACC.1/Desktop
	FMT_MSA.3	Met by FMT_MSA.3/Desktop
FMT_MSA.1/Desktop	FDP_ACC.1 or FDP_IFC.1	Met by FDP_ACC.1/Desktop
	FMT_SMR.1	Met by FMT_SMR.1/Authorise
FMT_MSA.3/Desktop	FMT_MSA.1	Met by FMT_MSA.1/Desktop
	FMT_SMR.1	Met by FMT_SMR.1/Authorise
	FMT_SMF.1	Met by FMT_SMF.1/Authorise
FDP_ACC.1/Resources	FDP_ACF.1	Met by FDP_ACF.1/Resources
FDP_ACF.1/Resources	FDP_ACC.1	Met by FDP_ACC.1/Resources
	FMT_MSA.3	Met by FMT_MSA.3/ Resources
FMT_MSA.3/Resources	FMT_MSA.1	FMT_MSA.1 enforces management of security attributes, but FMT_MOF.1/Resources enforces management of the security attributes for the Resource access policy by managing the ability to enable/disable the resource access functions. Therefore this dependency is met by FMT_MOF.1/Resources.
	FMT_SMR.1	Met by FMT_SMR.1/Authorise
	FMT_SMF.1	Met by FMT_SMF.1/Authorise
FMT_MOF.1/Resources	FMT_SMR.1	Met by FMT_SMR.1/Authorise
	FMT_SMF.1	Met by FMT_SMF.1/Authorise
FCO_SCO.1/Browser	None	
FCO_SCO.1/Desktop	None	
FCO_SCO.1/Server	None	
FCO_SCO.1/VMHost	None	
FCS_ECA.1/FIPS_KM	None	
FCS_ECA.1/FIPS_Enh	None	
FDP_RIP.1/Desktop	None	

Table 4: Analysis of SFR Dependencies

7. TOE Summary Specification

The table below provides a summary of the TOE functions that satisfy the security functional requirements described in section 6.2 above. The following sections describe how the TOE functions satisfy the security functional requirements.

SFRs TOE Functions	FIA_ATD.1/Desktop_user	FIA_UID.2/User	FIA_UAU.2/User	FMT_SMR.1/Authorise	FMT_SMF.1/Authorise	FDP_ACC.1/Desktop	FDP_ACF.1/Desktop	FMT_MSA.1/Desktop	FMT_MSA.3/Desktop	FDP_ACC.1/Resources	FDP_ACF.1/Resources	FMT_MSA.3/Resources	FMT_MOF.1/Resources	FCO_SCO.1/Browser	FCO_SCO.1/Desktop	FCO_SCO.1/Server	FCO_SCO.1/VMHost	FCS_ECA.1/FIPS_KM	FCS_ECA.1/FIPS_Enh	FDP_RIP.1/Desktop
Administrator access control		X	X																	
Administration of virtual desktop authorisation	X			X	X			X	X			X	X							
Desktop user access control		X	X			X	X													X
User Device resource access control										X	X									
Secure communications														X	X	X	X	X	X	

Table 5: Summary of SFRs satisfied by TOE Functions

7.1 Administrator access control

Administrators must be registered with the domain controller and are identified and authenticated as part of their Windows login. The authenticated identity is used by the Desktop Delivery Controller for authorisation before access is provided for administrators to Configdata.

These administrator access control mechanisms satisfy the **FIA_UID.2/User** and **FIA_UAU.2/User** identification and authentication requirements for administrators.

7.2 Administration of virtual desktop authorisation

The management of Configdata is performed by an administrator using the Delivery Services Console and Presentation Server Console, in conjunction with the Desktop Delivery Controller which controls access, and the datastore wherein the Configdata is stored.

Only administrators are able to modify Configdata. Configdata includes:

- Access permissions for administrators, determining whether administrative users can access configdata;
- Access permissions for virtual desktops, determining which virtual desktops each user can access;
- Virtual desktop configuration data, determining the configuration and characteristics of each virtual desktop;
- Endpoint data access policy, defining a central control policy that determines whether or not the user of a virtual desktop can cut and paste data between virtual desktop and User Device clipboards, whether the user is permitted to access local drives from the virtual desktop, and whether the user is permitted to access User Device USB devices from the virtual desktop.

These virtual desktop authorisation administration mechanisms satisfy the **FMT_SMR.1/Authorise**, **FMT_SMF.1/Authorise**, **FMT_MSA.1/Desktop**, **FMT_MSA.3/Desktop**, **FMT_MSA.3/Resources** and **FMT_MOF.1/Resources** security management requirements as well as the **FIA_ATD.1/Desktop_user** attribute requirement.

7.3 Desktop user access control

The Web Interface provides the means for a desktop user to log in to the TOE using a web browser or Citrix online plug-in, in order to gain access to their virtual desktops. The Web Interface receives the user's credentials, which may be username/password or multifactor authentication using a smart card. It forwards the credentials to the Desktop Delivery Controller for authentication by the domain controller. Desktop users must be registered with the domain controller and are identified and authenticated as part of their Windows login.

The authenticated identity is used by the Desktop Delivery Controller for authorisation to ensure that users are only granted access to desktops for which they have the appropriate permission. Once a user's access permission has been verified, the Desktop Deliver Controller assembles the user's virtual desktop environment using the virtual desktop configuration data. The Desktop Delivery Controller starts the virtual desktop and generates an authentication ticket which is passed to the Virtual Desktop Agent and, via the Web Interface, to the user's Citrix online plug-in.

The Citrix online plug-in in the user's User Device uses the authentication ticket to establish a session with the appropriate Virtual Desktop Agent. The Virtual Desktop Agent provides access to the virtual desktop for the desktop user. It authenticates the user before establishing the session, by confirming that the same authentication ticket has been presented by the Citrix online plug-in as that supplied by the Desktop Delivery Controller.

Once a desktop user has logged out of a virtual desktop it is 'torn down' to ensure that a pristine virtual desktop is available for the next desktop user.

These desktop user access control mechanisms satisfy the **FIA_UID.2/User** and **FIA_UAU.2/User** identification and authentication requirements for desktop users, as well as the desktop access policy requirements (**FDP_ACC.1/Desktop** and **FDP_ACF.1/Desktop**).

Tearing down the virtual desktop satisfies the **FDP_RIP.1/Desktop** residual information requirement.

7.4 User Device resource access control

Desktop users that have been granted access to a virtual desktop can use User Device resources if an administrator has enabled the appropriate functions in the Endpoint data access control policy. This is enforced by the Citrix online plug-in and the Virtual Desktop Agent. Only global (i.e. for all users) enabling of the functions is included in the scope of the evaluation.

The User Device resource access control mechanisms satisfy the resource access policy requirements (**FDP_ACC.1/Resources** and **FDP_ACF.1/Resources**).

7.5 Secure communications

Communication between the Web Interface and the User Device web browser is protected by TLS.

Communication between the Desktop Delivery Controller and the VM Host is protected by TLS.

Communication between the Virtual Desktop Agent and the Citrix online plug-in in the user's User Device is protected by Windows secure communications mechanisms, which are configured to use IPSec protocols for authentication, confidentiality and integrity.

Communication between the TOE servers is protected by Windows secure communications mechanisms, which are configured to use IPSec protocols for authentication, confidentiality and integrity.

All secure communications mechanism are configured to use FIPS 140-2 Level 1 validated algorithm implementations provided by Microsoft Cryptographic modules, and the TOE components invoke the cryptographic functions in accordance with the conditions of the validation.

These secure communications mechanisms satisfy the **FCO_SCO.1/Browser**, **FCO_SCO.1/Desktop**, **FCO_SCO.1/Server** and **FCO_SCO.1/VMHost** requirements for authenticated communication channels; they also satisfy the **FCS_ECA.1/FIPS_KM** and **FCS_ECA.1/FIPS_Enh** requirements for conformance with FIPS 140-2 Level 1 accreditation.

End of Document