Common Criteria Security Target

for

Citrix XenDesktop 7.6 Platinum Edition and Citrix XenApp 7.6 Platinum Edition

Version 1-0 2 March 2015

Summary of Amendments

Version	Date	Notes
1-0	2 March 2015	First definitive 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 Citrix XenDesktop 7.6 Platinum Edition and Citrix XenApp 7.6 Platinum Edition products.

The products are designed and manufactured by Citrix Systems, Inc. (http://www.citrix.com/).

The Sponsor and Developer for the EAL2 evaluations 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-2012-09-001, Version 3.1 Revision 4, September 2012.

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

[CC2] Common Criteria for Information Technology Security Evaluation,
Part 2: Security Functional Components,
CCMB-2012-09-002, Version 3.1 Revision 4, September 2012.

[CC3] Common Criteria for Information Technology Security Evaluation,
Part 3: Security Assurance Components,
CCMB-2012-09-003, Version 3.1 Revision 4, September 2012.

[CEM] Common Methodology for Information Technology Security Evaluation,
Evaluation Methodology,
CCMB-2012-09-004, Version 3.1, Revision 4, September 2012.

Note: the 3 separate parts of Common Criteria are also referred to collectively as "[CC]".

Developer documentation

[CCECG] Common Criteria Evaluated Configuration Guide for Citrix XenApp 7.6 Platinum Edition and XenDesktop 7.6 Platinum Edition, 27 February 2015, document code: 2/27/2015 14:17:44

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
AES	Advanced Encryption Standard
DDC	Delivery Controller (the leading 'D' is present for historical reasons and to avoid potential confusion with 'Domain Controller')
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standards
ICA	Independent Computing Architecture
LAN	Local Area Network
OSP	Organisational Security Policy

Acronym	Meaning
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
VDA	Virtual Delivery Agent
WCF	Windows Communication Foundation

0.8 Glossary

Term	Meaning
Access permissions for virtual desktops	configuration data within the TOE which determines which virtual desktops each user is permitted to access.
Access permissions for (published) applications	configuration data within the TOE which determines which published applications each user is permitted to access (cf. Permitted Published Applications (q.v.)).
Assurance	grounds for confidence that a TOE meets the SFRs [CC1]
Catalog	a collection of machines of the same Machine Type. Catalogs are managed as a single entity. Desktops or servers from more than one catalog can be allocated to a delivery group.
Citrix Receiver	installed on user devices, this is a client that provides direct ICA connections to server or desktop Virtual Delivery Agents. Although this is a Citrix framework that supports various plug-ins, in the evaluated configuration it will only be used with the Citrix Online Plug-in.
Citrix Studio	provides the administration interface to the Delivery Controller for managing access permissions for virtual desktops, virtual desktop configuration data, published applications, published application configuration data (permitted published applications for each application user) and Endpoint data access control policy.
Configdata	configuration data within the TOE; which includes access permissions for virtual desktops and published applcations, Virtual Desktop configuration data and Endpoint data access control policy. See section 3.1.
Controller	Delivery Controller (q.v.)
Delivery Controller	authenticates administrators and users, manages the assembly of users' virtual desktop and application environments and brokers connections between users and their virtual desktops and applications. In Citrix documentation often identified simply as the Controller.
Delivery Group	an administrative grouping of machines to supply desktops

Term	Meaning
	and/or applications that are allocated to users or groups of users. Machines from one or more catalogs are used to create the delivery group. Users can be given permissions to access one or more delivery groups, but in the evaluated configuration each user is given access to only a single desktop delivery group and a single application delivery group.
Domain pass-through	a means of authentication in which single sign-on is provided using the domain credentials (either smartcard and PIN, or username and password) used to log on to a domain-joined client running Citrix Receiver.
Endpoint data access control policy	a set of rules, configured within the TOE, which determine whether or not a user can access User Device resources from within a virtual desktop or published application: specifically clipboard, local drives, USB devices; used in conjunction with input evidence values to determine specific settings for any particular virtual desktop.
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 and published applications for processing and to return output (display, audio etc.) to the Citrix Receiver running on the client.
License Server	a server that issues licenses for Citrix products.
Machine Type	defines the machine type (desktop or server OS) as well as a number of other properties relating to how machines in a catalog are provisioned, allocated and managed. In the evaluated configuration only manually provisioned machine types will be used. The manually provisioned machine type enables the use of XenDesktop and XenApp to manage and deliver user desktops and applications that have already been migrated to VMs in the data centre. In the evaluated configuration, only static pre-assigned desktop machines are used, which means that each user is assigned a specific virtual desktop by an administrator, and the user receives this virtual desktop at each logon.
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]

Term	Meaning
Permitted Published Applications	The set of published applications to which an authorised User has been granted access. (See also Published Applications)
Protection Profile	an implementation-independent statement of security needs for a TOE type. [CC1]
Provisioning	act of creating new virtual desktops and/or published applications, including the operating system image for the desktops and related configuration.
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).
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], describing the desired security behaviour expected of a Target of Evaluation (TOE) [CC2].
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]
Site	a collection of Catalogs, Delivery Groups, Published Applications, virtual desktops and Configdata that are defined, managed and accessed via the same Delivery Controller, and which are stored within a common, shared database. In the evaluated configuration, there will only be a single application delivery group and a single desktop delivery group defined in the site.
StoreFront	a server that provides a user with an interface to an self-service store which allows them to subscribe to and launch their chosen apps and desktops following authentication.
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]

Term	Meaning
Transport Layer Security	an open, non-proprietary, standardised 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]
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 user to gain access to their virtual desktops or published applications.
Userdata	user data within the TOE. See section 3.1.
Virtual Delivery Agent	installed on virtual desktops and servers running Microsoft Remote Desktop Services, this enables direct ICA connections between the virtual desktop or published applications running on the server and users' User Devices.
Virtual Desktop	a desktop operating system running on a virtual machine on a virtualised server, personalised for a desktop user. (Note that only virtual desktops running on desktop Virtual Delivery Agents are included in the scope of the evaluation; desktops running on *server* Virtual Delivery Agents are excluded.)
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 and virtual applications are running.

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:	Citrix XenDesktop 7.6 Platinum Edition and Citrix XenApp 7.6 Platinum Edition
ST Reference:	CN11-ST-0001
ST Version:	1-0
ST Date:	2 March 2015
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 Citrix XenDesktop 7.6 Platinum Edition and Citrix XenApp 7.6 Platinum Edition (hereinafter referred to as “XenDesktop” and “XenApp” respectively) are virtualisation products that centralise and deliver Microsoft Windows virtual desktops and/or applications as a service to users anywhere. Applications hosted on Microsoft Windows Server 2012 and personalised virtual desktops hosted on Microsoft Windows 7[2] can be run on demand each time they log on. This ensures that performance never degrades, while the high speed delivery protocol provides unparalleled responsiveness over any network. XenDesktop and XenApp deliver a high definition user experience over any connection, including high latency wide area networks.

When used in the full XenDesktop configuration, the TOE gives access to both virtual desktops and published applications. When used in the XenApp configuration, the TOE gives access only to published applications. Note that the evaluated configuration of the product is defined in [CCECG], and specific limitations to the scope of the TOE are listed in section 1.4.3.

The open architecture of XenDesktop and XenApp offers choice and flexibility of virtualisation platform and User Devices. XenDesktop and XenApp integrate with server

[2] Note that only virtual desktops running on desktop Virtual Delivery Agents are included in the scope of the evaluation; desktops running on *server* Virtual Delivery Agents are excluded.

virtualisation products including Citrix XenServer and cloud-based delivery via Amazon EC2 and Citrix CloudPlatform. XenDesktop works out-of-the-box with desktop appliances from every major thin client vendor. Users can also access their virtual desktops and published applications from most common client devices, including Windows, Mac OS, and Linux desktops as well as smartphones and tablets. This means that there is no vendor lock-in for virtualisation or User Devices[3]. (See sections 1.2.3, 1.4.3 and [CCECG] for details of the evaluated configuration)

XenDesktop simplifies desktop lifecycle management by enabling administrators to manage service levels with built-in desktop performance monitoring, and to deliver applications separately to the underlying desktop image using virtualisation. The entire desktop and application lifecycle is managed in one location, simplifying desktop provisioning, patching, security, and updates.

Although the desktops and applications 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 and applications.

XenDesktop and XenApp provide the following key security features:

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

[3] Although XenDesktop supports many different user devices only Microsoft Windows user devices are included in the evaluated configuration

1.2.2 TOE Type

Desktop and Application Virtualisation.

1.2.3 Required non-TOE hardware/software/firmware

For Citrix StoreFront including the StoreFront Management Console, a server is required with the following software:

- Microsoft Windows Server 2012, Datacenter Edition
- Microsoft .NET Framework 4.5.1
- Microsoft Internet Information Server (IIS) 8.0
- Microsoft ASP.NET 4.5.

For the License Server, a server is required with the following software:

- Microsoft Windows Server 2012, Datacenter Edition

For the Delivery Controller including Citrix Studio, a server is required with the following software:

- Microsoft Windows Server 2012, Datacenter Edition
- Microsoft .NET Framework 4.5

The Delivery Controller requires a Database with the following software:

- Microsoft SQL Server 2012
- Microsoft Windows Server 2012, Datacenter Edition.

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

- Microsoft Windows 7 Ultimate 64-bit.

Each Desktop Virtual Delivery Agent for the virtual desktop will require the following software (used in XenDesktop only):

- Microsoft Windows 7 Ultimate 64-bit.

Each Server Virtual Delivery Agent for the virtual applications will require the following software:

- Microsoft Windows Server 2012, Datacenter Edition.

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

- Microsoft Active Directory Server in Windows Server 2012 native mode.

The TOE also requires the use of a hypervisor on the Delivery Controller, creating and maintaining a virtual machine for each virtual desktop. The only requirement placed on the hypervisor by this Security Target is that the selected hypervisor should meet A.VM_Host (see section 3.5) and OE.Config_VM_Host (see section 4.2.1). The list of supported hypervisors is regularly updated and can be found at http://support.citrix.com.

1.3 TOE Description

XenDesktop and XenApp provide a complete virtual desktop and/or application delivery system by integrating several distributed components with advanced configuration tools that simplify the creation and real-time management of the virtual desktop infrastructure and published applications hosted on servers running Remote Desktop Services.

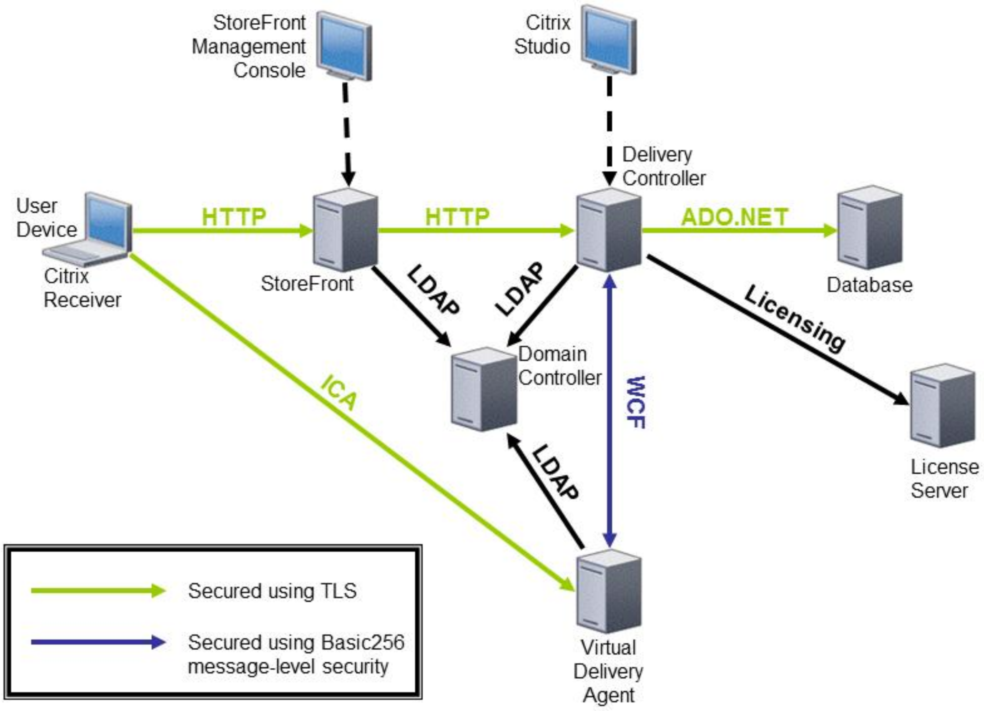

Figure 1: XenDesktop and XenApp Components

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

- **Delivery Controller**. Installed on servers in the data centre, the controller requires that users are authenticated, manages the assembly of virtual desktop environments and servers hosting published applications, and brokers connections between users and their virtual desktops and applications.
- **Virtual Delivery Agent**. Installed on virtual desktops and servers hosting published applications, the agent enables direct ICA (Independent Computing Architecture)

connections between the virtual desktop and servers hosting published applications and the end user's User Device.

- **Citrix Receiver**. Installed on user devices, the Citrix Receiver enables direct ICA connections from user devices to virtual desktops and published applications.
- **StoreFront**. Installed on a server in the data centre, StoreFront is used to give authorised users access through the Web or intranet to the virtual desktops and applications that they are authorised to use. Users log on to StoreFront using an Internet browser and are given the ICA file that the Citrix Receiver needs to connect to the Virtual Delivery Agent for access to an authorised virtual desktop or application. StoreFront is also accessed from an Internet browser running within the virtual desktop to launch virtual applications the user is authorised to access.
- **StoreFront Management Console**. This provides an administration interface to StoreFront, making use of Windows authentication for administrators. It provides administrators with functions to manage the configuration of StoreFront, including setting the user authentication method. This is installed on the StoreFront server.
- **Citrix Studio**. This provides an administration interface to the 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 applications, manage users' access permissions for virtual desktops and applications and to manage the Endpoint data access control policy. This is installed on the Delivery Controller.
- **Database**. This stores the Configdata managed by the administrators with the Citrix Studio, including the Endpoint data access control policy, configuration of virtual desktops, desktop users' access permissions for virtual desktops, lists of permitted published applications, and access permissions for administrators, as well as data used by the Delivery Controller to manage virtual desktops, users and sessions.

The product configuration in this ST is an internal deployment with no external access: the clients and servers are expected to be running within a LAN.

The interactions between the components, to provide a virtual desktop and applications to a user, are as follows (and illustrated in Figure 2). Note that when accessing published applications (as opposed to virtual desktops) then the user's access may be either direct from running Citrix Receiver or a browser on the User Device, or else established via a 'double hop'. In the case of a double hop connection the User first connects via Citrix Receiver or a browser on the User Device to that user's virtual desktop, and then starts Citrix Receiver on this virtual desktop and uses it to connect from the virtual desktop to a published application. In a double hop the steps below apply to each of the hops.

1. The user’s access permissions for virtual desktops and applications[4] are configured by the administrator via Citrix Studio. The authentication method (either username/password, smartcard or domain pass-through) accepted by StoreFront is configured using the StoreFront Management Console.

2. A user connects to StoreFront to establish a session in one of the following ways:

   - via a web browser running on an End User device (when launching a published application or virtual desktop directly)

   - via Citrix Receiver running on an End User device (when launching a published application or virtual desktop directly)

   - via Citrix Receiver running on a virtual desktop (when launching a published application on the second hop of a double-hop connection (see also footnote 7)).

   If StoreFront has been configured to use the domain pass-through authentication method, the user’s identity will already have been authenticated during the Microsoft Windows logon process, in which case their identity is made available to StoreFront. If StoreFront has been configured to accept username and password, the user enters their credentials, which are sent as a standard HTTP request protected by TLS.

3. StoreFront requests the Domain Controller to authenticate the user’s credentials.

4. StoreFront reads the user’s AD user account information and passes it to the Delivery Controller.

5. The Delivery Controller retrieves from the Database a list of desktops and applications to which the user’s access permissions allow access and informs StoreFront. In the case of a user running in the XenApp configuration (i.e. with a license for XenApp but not for XenDesktop), only the permitted published applications are available; users running in the XenDesktop configuration (i.e. with a license for XenDesktop) may have both permitted published applications and virtual desktops. In the evaluated configuration each desktop user belongs to only one Desktop Delivery Group/Application Delivery Group and may only have one virtual desktop assigned to them, however in other configurations a choice of virtual desktops may be available to the desktop user.

6. StoreFront returns the list of available resources. If the connection to StoreFront was made using a web browser then these resources are displayed as a web page containing a hyperlink for each available resource in the list received from the Delivery Controller. If the connection to StoreFront was made from running Citrix Receiver then these resources are displayed in the Windows Start menu.

[4] The virtual desktops and published applications available will depend on the configuration of the product. In the XenApp configuration virtual desktops will not be available, whereas in the XenDesktop configuration both applications and virtual desktops are available.

7. The web browser or Citrix Receiver (depending on the launch mechanism used in the previous step) sends a request to StoreFront to retrieve the ICA file for the selected desktop or application.

8. StoreFront contacts the Delivery Controller requesting access to the requested virtual desktop or published application. StoreFront also requests a ticket[5] for the user.

9. The Delivery Controller allocates an appropriate virtual desktop from the available desktops or an appropriate server which has the requested application available (if any).

10. The Delivery Controller instructs the appropriate Virtual Delivery Agent to prepare to receive a connection request[6]. The Delivery Controller generates a ticket and includes it in the request to the Virtual Delivery Agent. If this is a username/password launch (i.e. domain pass-through is not in use) the Delivery Controller also sends the user credentials to the Virtual Delivery Agent where they are temporarily stored and associated with the ticket.

11. The Delivery Controller returns the ticket to StoreFront along with the network address of the Virtual Delivery Agent that will provide the virtual desktop or application allocated for the user.

12. StoreFront sends an ICA file containing the ticket along with the network address of the Virtual Delivery Agent as a reply to the user's request. This is delivered to the Citrix Receiver on the User Device, or a Citrix Receiver running within a virtual desktop.

13. The Citrix Receiver receives the ICA file and uses it to send a connection request to the Virtual Delivery Agent, including the ticket and (optionally) user credentials if domain pass-through authentication is in use.

14. The Virtual Delivery Agent first verifies that the correct ticket has been supplied within the time limit, and then looks up the associated user credentials (if username/password authentication is in use).

[5] The tickets used for explicit username/password and for single sign-on (also known as ‘domain pass-through’) are in fact slightly different. The username/password ticket is called an ‘authentication ticket’ and that for domain pass-through is called a ‘launch reference ticket’. Both are similar in that they contain an expiry time, are limited to one-time use, and are passed back and stored in the ICA file; the difference is that the launch reference ticket is not associated with specific user credentials (because a launch reference ticket is used in a domain pass-through scenario where the user credentials are re-supplied by Citrix Receiver when it connects to the Virtual Delivery Agent). For the username/password case both tickets are used, but domain pass through uses only the launch reference ticket.

[6] Communications between the DDC and VDA are not protected by TLS, but by WCF message-level security. This uses XML-based WS-Security mechanisms to provide HMAC and encryption for the message contents together with Kerberos-based authentication. This is provided by the Basic256 ciphersuite as specified in FCO_SCO.1/WCF and FCS_ECA.1/FIPS_Enh.

15. The Virtual Delivery Agent requests the Delivery Controller to confirm the licensing details with the license server and validate that the user is authorised to access the requested virtual desktop or published application.

16. The Virtual Delivery Agent establishes the virtual desktop or Remote Desktop Services session for the application using the user credentials to logon; it provides access to enable the user's Citrix Receiver to present the user with the virtual desktop or published application.

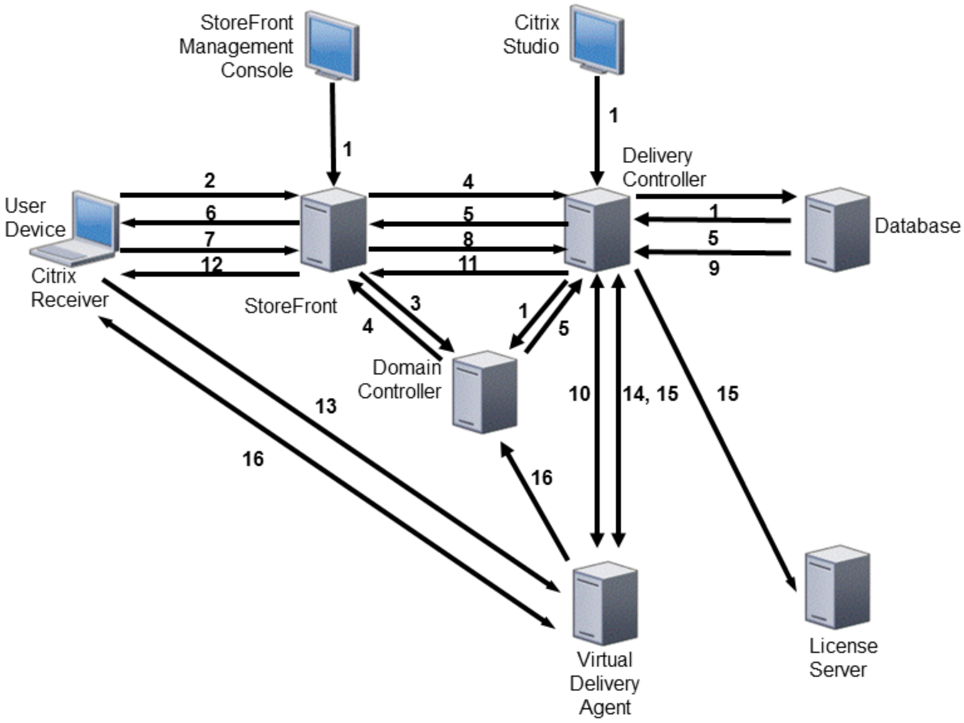

Figure 2: Interactions between components

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 Delivery Controller (including Citrix Studio), StoreFront (including StoreFront Management Console), the Database and the Virtual Delivery Agents. The TOE Client component is the Citrix Receiver running on a User Device or Desktop Virtual Delivery Agent.

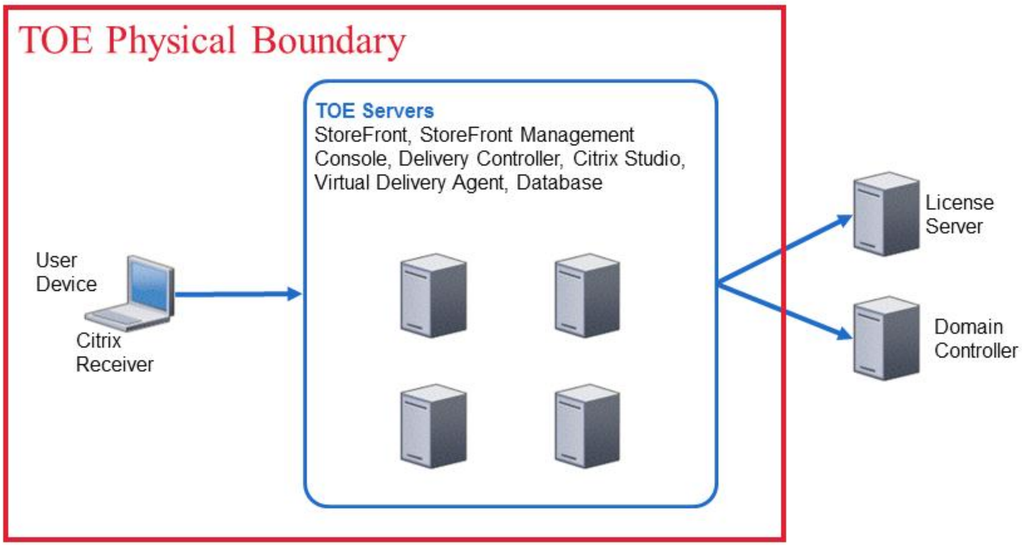
TOE Physical Boundary
TOE Servers
StoreFront, StoreFront Management Console, Delivery Controller, Citrix Studio, Virtual Delivery Agent, Database
User Device
Citrix Receiver
License Server
Domain Controller

Figure 3: TOE Physical boundary

1.4.2 Logical Boundary

XenDesktop and XenApp are offered in various editions that provide different features. The evaluated TOE consists of the following:

Citrix XenDesktop 7.6 Platinum Edition and Citrix XenApp 7.6 Platinum Edition , including

- Delivery Controller v7.6.0.5026
- Citrix Studio v7.6.0.5026
- StoreFront (including StoreFront Management Console) v2.6.0.5031
- Virtual Delivery Agent v7.6.0.5026
- Citrix Receiver v4.2.0.10 with Online Plug-in v14.2.0.10
- Desktop Lock v14.2.0.10 (only applicable to XenDesktop).

These are all required to belong to the same Active Directory domain, as are all users and administrators.

In addition, the evaluated configuration guidance document [CCECG] forms part of the TOE.

The Citrix Receiver runs on the User Device and virtual desktops[7], 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.

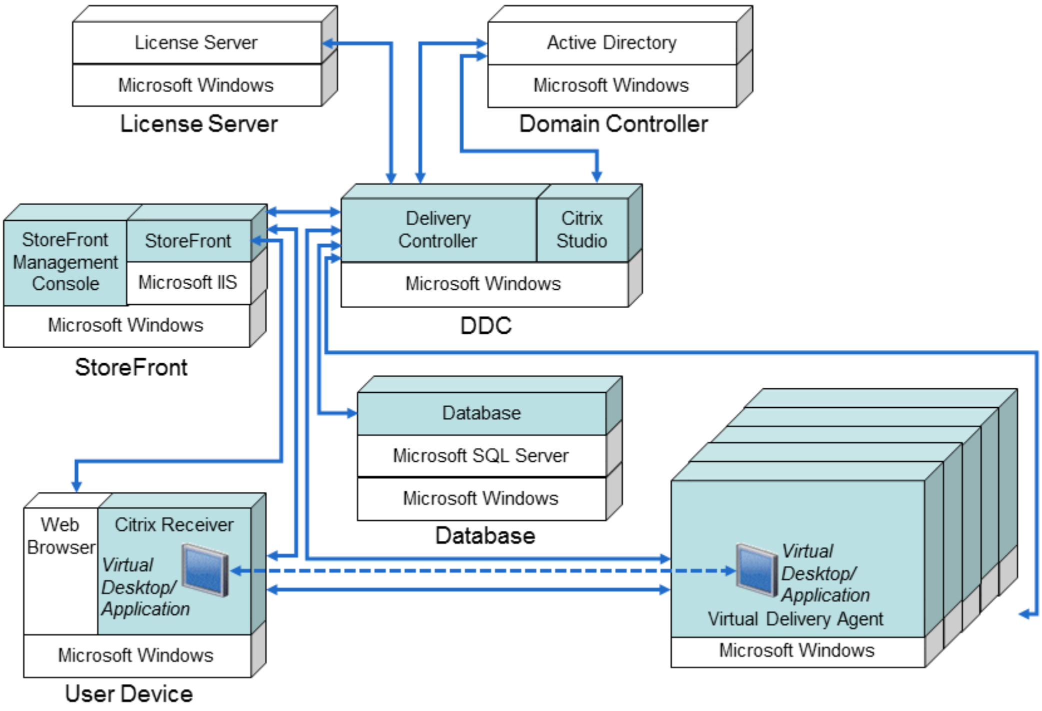

Figure 4: Logical boundaries

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 XenDesktop and XenApp integrate, 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 and XenApp Platinum Edition:

[7] Note that when making a double hop connection to start a published application session then the Citrix Receiver is run on the User Device to start the virtual desktop session in the first hop, and another instance of the Citrix Receiver is then run from within the virtual desktop in the Virtual Delivery Agent on the second hop. To avoid excessive complexity in the diagram, this second instance of the Citrix Receiver is not shown in Figure 4.

- Citrix XenServer – an enterprise-class virtual machine infrastructure solution that creates the foundation for delivering virtual desktops
- Citrix NetScaler 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 Profile Management – high performance user personalisation method, not used in the evaluated configuration;
- Citrix CloudBridge – accelerator for improved performance on wide area networks, not used in the evaluated configuration;
- Citrix CloudPlatform - a unified cloud management platform (powered by Apache CloudStack) that combines the best cloud foundation for private enterprise workloads with the Amazon-style scale, elasticity and operational efficiency of cloud workloads.
- Citrix Desktop Director – provides the help desk with a single console to monitor, troubleshoot and fix virtual desktops, not used in the evaluated configuration;
- Citrix XenClient – high-performance, bare-metal hypervisor that divides the physical resources of a User Device and enables multiple operating systems to run side-by-side securely in complete isolation, not used in the evaluated configuration.
- Citrix XenMobile – a comprehensive solution to manage mobile devices, apps and data, and allowing users to access all of their mobile, SaaS and Windows apps from a unified corporate app store, not used in the evaluated configuration.
- Citrix AppDNA - reduces the time, cost and risk for OS migration and virtualization technology adoptions by automating application compatibility and overall application migration, not used in the evaluated configuration.

In addition, certain features of XenDesktop and XenApp are not included in the scope of the evaluation:

- Only one application delivery method is included in the evaluation: XenApp published apps, also known as server-based hosted applications. These are applications hosted from a Windows server to a Windows desktop. All other application delivery methods are excluded from the evaluation.
- Only one desktop delivery method is included in the evaluation: VDI desktops. These are virtual applications each running a Windows desktop operating system, rather than running in a shared, server-based environment. These virtual desktops are delivered to physical Windows desktop machines. All other desktop deliver methods are excluded from the evaluation.
- All desktop delivery groups in the evaluation deliver desktops of the *static* type, meaning each user connects to the same desktop each time. Desktops of the *random* type are not included in the evaluation. Furthermore, administrators must pre-assign a user to each desktop, rather than allowing the desktop to be assigned to a user on first use.

- Each user in the evaluated configuration can only use one virtual desktop from one desktop delivery group. The capability for users to belong to multiple desktop delivery groups is not included in the evaluation; nor is the capability for desktop users to be assigned multiple desktops in a desktop delivery group.
- In the evaluated configuration each user is given access to only a single application delivery group. The capability for users to belong to multiple application delivery groups is not included in the evaluation.
- Only Full Administrators are included in the evaluation; other delegated administrator roles are excluded.
- Administrators can enable/disable local peripheral support either as a global data access control policy or for individual users and groups of users; only the facility for applying a global data access 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 ability for administrators to automatically create virtual desktops and servers using Machine Creation Services is not included; only virtual desktops of type ‘existing’ created explicitly by an administrator, will be included in the evaluation
- Because only virtual machines of the *existing* type are included, power management of virtual machines via the Delivery Controller is not included in the evaluation.
- Connection leasing is not included in the evaluation.
- Streaming applications using AppV is not included in the evaluation.
- The ability for administrators to deploy Personal vDisks for users and stream applications using AppV is not included
- The ability for users to access their personal office PC remotely from Citrix Receiver using the Remote PC Access feature is not included.

Any VM Host used to provide virtual desktops or published applications is not included in the scope of the TOE (see OE.Config_VM_Host in section 4.2.1).

2. CC Conformance

As defined by the references [CC1], [CC2] and [CC3], this TOE conforms to the requirements of Common Criteria v3.1, Revision 4 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.

Published Applications

The published applications made available by the TOE. 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; lists of permitted published applications; 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.

Application User

A user who has been granted access to published applications via the TOE. An Application User accesses virtual applications through a client known as an Endpoint.

Desktop User

A user who has been granted access to virtual desktops via the TOE. The user accesses their virtual desktop through a client known as an Endpoint.

Administrator

An administrator manages users' access to virtual desktops and 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 A client used to gain access to a virtual desktop or published application. It consists of either a User Device running on a PC or a virtual machine running a Desktop Virtual Delivery Agent. To enable access, the Endpoint 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_DesktopOrApp An attacker may gain unauthorised access to a virtual desktop or published application.

T.Attack_Userdata An attacker may gain unauthorised access to Userdata.

T.Access_DesktopOrApp A desktop user or application user may gain unauthorised access to a virtual desktop or published application (i.e. to a virtual desktop that is not their own or to a published application that they have not been given permission to access).

T.Access_Userdata A desktop user or application user may gain unauthorised access to another 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 Userdata or users' authentication credentials.

T.Attack_Configdata An attacker, application user 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 Endpoint 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 provides certified virtual machine isolation and 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 Windows (including Active Directory)
- Microsoft SQL Server
- Microsoft .NET Framework 4.5.1
- Microsoft ASP.NET 4.5.

This shall include administrators ensuring that applications are published and configured such that it is not possible for users to gain access to the underlying operating system or hardware on which the Virtual Delivery Agent is running, other than in the context of an unprivileged user account, or other applications. The security state of the published applications should also be maintained according to the user’s risk environment (e.g. by applying relevant patches).

4. Security Objectives

4.1 Security Objectives for the TOE

O.Auth_User 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 Each application user and desktop user must be granted access only to the virtual desktop for which they have been authorised.

O.Application Each application user and desktop user must be granted access only to applications 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 or published application 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 or in a published application 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.Config_Access The virtual desktops and published applications must only be configurable by administrators.

Application note Virtual Desktops and published applications 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 Delivery Agent is running, other than in the context of an unprivileged user account.

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

Application note In the evaluated configuration a published application session using a double hop connection via a first hop that connects to a virtual desktop will only be able to map client drives from the User Device, and not any other client drives that may be available on the virtual desktop from the first hop.

Where access to a User Device resource has been rejected by a user on the first hop of a double hop connection to a published application, then access cannot be made over the second hop. (Although the user may accept the access on the second hop, it will fail when the prohibition is reached on the first hop).

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.

This includes ensuring that the contents of the memory used by the Virtual Delivery Agent to run the virtual desktop during a user’s session are not available to other processes when that user’s session has ended (this is achieved in the evaluated configuration by maintaining the assignment between each virtual desktop and its user, so that the user is always connected to the same persistent desktop).

OE.Config_VM_Host

VM Host software must be securely configured. The deployment must provision a VM Host that provides suitable virtual machine isolation since this is relied upon to effect separation of user's virtual desktops in the XenDesktop security architecture. The VM Host should therefore be a hypervisor certified against a security target that includes the separation of virtual machines (including virtual memory, virtual disk and networking).

OE.Config_TP_SW

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

- Microsoft IIS
- Web Browsers used to connect
- Microsoft Windows (including Active Directory)
- Microsoft SQL Server
- Microsoft .NET Framework 4.5.1

- Microsoft ASP.NET 4.5.

Published applications 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 Delivery Agent is running, other than in the context of an unprivileged user account, or other applications.

OE.Authenticate

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.TLS

All communication between the TOE Servers, between Virtual Delivery Agents and User Device Citrix Receivers, and between StoreFront and the User Device (web browser), uses the configured TLS protocol.

The following technical objectives relate to the User Devices:

OE.Config_Endpoint

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

Application note

Endpoints must be configured such that user authentication credentials and user data are not available after the user has logged out from their virtual desktop. Users should also log out of their Windows session on the User Device after logging 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 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 Endpoints 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 database, 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_DesktopOrApp	T.Attack_Userdata	T.Access_DesktopOrApp	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.Application			X	X									
O.Secure_Setup_Data			X		X		X						
O.Secure_User_Data		X		X									
O.Use_FIPS								X					
O.Config_Access		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.TLS		X		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_DesktopOrApp

Attackers are prevented from gaining access to a virtual desktop or published application 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, application 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 Endpoints have been set up properly and that authentication credentials are not left in the Endpoint 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, application users and administrators are granted access to the TOE.

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

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

O.Config_Access ensures that the virtual desktops and published applications have been set up properly, while OE.Config_Server ensures that any content of the virtual desktop memory is reserved for that user after the user has logged out of the virtual desktop.

OE.Config_Server also 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 Endpoint when authorised.

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

4.3.3 T.Access_DesktopOrApp

Users are prevented from gaining unauthorised access to a virtual desktop or published application 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 desktop user who has been specifially authorised for access to the relevant desktop. O.Application similarly ensures that a published application is only available to an application user who has been specifically authorised for access to the relevant application (as recorded in the Configdata). OE.Admin_Users ensures that only administrators have access to Configdata and thus the ability to authorise users' access to a virtual desktop or published application. O.Secure_Setup_Data ensures the confidentiality and integrity of the setup and assignment data for virtual desktops and published applications on the servers.

O.Config_Access ensures that the virtual desktops and published applications have been set up properly, while OE.Config_Server ensures that any content of the virtual desktop memory is reserved for that user after the user has logged out of the virtual desktop.

OE.Config_Server also 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 and application users are prevented from gaining unauthorised access to another 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. O.Application similarly ensures that a published application is only available to an application user who has been specifically authorised for access to the relevant application (as recorded in the Configdata). OE.Authenticate ensures that the underlying operating system performs the required authenticaiton on which to base access decisions.

OE.TLS and OE.Encryption ensure the confidentiality of Userdata, including authentication credentials, during login and establishment of a virtual desktop or access to a published application.

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

O.Config_Access ensures that the virtual desktops and published applications have been set up properly, while OE.Config_Server ensures that any content of the virtual desktop memory is reserved for that user after the user has logged out of the virtual desktop.

OE.Config_Server also 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 Endpoint when authorised.

OE.Config_Endpoint ensures that the Endpoints have been set up properly and that authentication credentials and other Userdata are not available to be used 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 and published applications during transmission between servers.

OE.TLS ensures the confidentiality and integrity of communications between the User Device browser and StoreFront during login and establishment of the virtual desktop or access to a published application, and also 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 Endpoints have been set up properly.

4.3.7 T.Attack_Configdata

Attackers, application users 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, application 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.TLS 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 Endpoint 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 VM Host software is operating correctly and securely, and uses a hypervisor certified to provide VM separation, is met by the environment objective OE.Config_VM_Host, which ensures that these requirements are met.

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[8], 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[9].

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.

[8] 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.

[9] 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 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. Unless stated otherwise, the term 'user' should be understood to relate to desktop users, published application 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/published applications.

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 application users and desktop users: [**access permissions for published applications; 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.

Application note — The user identification requirement applies to administrators, as well as to application users and desktop users.

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.

Application note — The user authentication requirement applies to administrators, as well as to application users and desktop users.

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 application users for access to published applications, 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, application 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: [

- **Definition of published applications**
- **Administration of access permissions for published applications**
- **Allocation of administrator role to users**
- **Administration of access permissions for virtual desktops**
- **Administration of virtual desktop configuration data**
- **Administration of Endpoint data access control policy.**]

Application note — Adminstration of virtual desktop configuration data includes assigning each desktop machine to a single desktop user, in which the administrator pre-allocates a dedicated virtual desktop to each desktop user (and virtual desktops are therefore not shared between different desktop users). In the evaluated configuration each desktop delivery group may contain many desktops each of which is assigned to a single user. An application delivery group may contain many applications each of which may be accessed by one or more users/groups. In the evaluated configuration each desktop user will belong to one application delivery group and one desktop delivery group. Similarly, each application user will belong to a single application delivery group.

Administration of the Endpoint data access control policy consists of enabling or disabling the following functions for published applications and virtual desktops:

- cut and paste between a client clipboard and the clipboard in a published application or virtual desktop;
- client drive mapping in a published application or virtual desktop;
- access to User Device USB devices from virtual desktops.

A USB *storage* device may be accessed through client drive mapping or through general USB device access (subject to configuration). General USB device access is available from virtual desktops but not from within published applications. Hence within a published application a USB storage device can only be made available using client drive mapping: there is no general USB device access available from within 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 [**application 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 identity, access permissions for applications**].

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 is authorised to access a delivery group that provides 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.

Application note The default values are restrictive in that a new user defaults to no access to published applications. .

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 In the evaluated configuration, only a single application delivery group is defined, and a user can only access published applications after they have been given access to this application delivery group. Action is required from an adminstrator in order to grant a user access to the application delivery group (it is not granted by default). [CCECG] notes that to avoid unintended access being granted, access should be granted *directly* to a user, rather than by allocating the user to a group that has access.

6.2.2.7 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**].

6.2.2.8 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].**

6.2.2.9 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**].

6.2.2.10 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.

Application note The administrator is required (see [CCECG]) to set the virtual desktop configuration data to assign each virtual desktop to a single user.

6.2.2.11 FDP_ACC.1/Resources Subset access control

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

- **transfer of user data between the Endpoint clipboard and a published application or virtual desktop clipboard**
- **access to mapped client drives from a published application or virtual desktop**
- **access to attached USB devices from a virtual desktop**].

Application note A USB *storage* device may be accessed through client drive mapping or through general USB device access (subject to configuration). General USB device access is available from virtual desktops but not from within published applications. Hence within a published application a USB storage device can only be made available using client drive mapping: there is no general USB device access available from within published applications.

6.2.2.12 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: [

Application users and desktop users shall be permitted to cut and paste data between a published application and an Endpoint operating system clipboard, or between a virtual desktop and an Endpoint 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 published application or a virtual desktop only if:

- **The client drive mapping function has been enabled by the administrator, and**
- **The application/desktop user has not prevented 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 be accessed from a virtual desktop either as a USB device in its own right or through client drive mapping; therefore, if an administrator wishes to ensure that such a device cannot be accessed both client drive mapping and USB device access must be disabled. USB devices are not accessible from published applications, except that USB storage devices may be accessed through client drive mapping.

Note that clipboard transfer between a published application and a User Device clipboard that occurs over a double-hop in fact takes place as a pair of transfers between published application and virtual desktop and then between virtual desktop and User Device. Where there is no double-hop then the transfer is directly between the published application or virtual desktop and User Device clipboard.

In the evaluated configuration a published application session using a double hop connection via a first hop that connects to a virtual desktop will only be able to map client drives and USB devices from the User Device, and not any other resources that may be available on the virtual desktop from the first hop.

Where access to a User Device resource has been rejected by a user on the first hop of a double hop connection to a published application, then access cannot be made over the second hop.

Where a published application is accessed by executing Citrix Receiver then the client drives on the User Device are accessible for read and write by default. Where a published application is launched from a web browser, then the user is prompted as to whether they wish to make client drives on the User Device accessible. A virtual desktop will prompt for access to client drives on the User Device in either of these cases.

The Endpoint data access control policy is applied to the published application or virtual desktop at the launch of the 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 (in the case of a double hop connection this means that a change made in the first hop but before the second hop has been made will be applied to that second hop).

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].**

6.2.2.13 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.

6.2.2.14 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 an entire Site), for one or more Delivery Groups, or for groups of users and individual desktop users. However, only the global enable/disable is included within the scope of the evaluation. Each 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 **[web browser and StoreFront, or between Citrix Receiver and StoreFront]** that is logically distinct from other communication channels and provides assured identification of [**StoreFront**] and protection of the channel data from [*modification, disclosure*].

Application note The web browser or Citrix Receiver in this case may be executing on the User Device or on a virtual desktop.

FCO_SCO.1.2/Browser The TSF shall permit [**the web browser or Citrix Receiver**] 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 web browser and StoreFront, or between Citrix Receiver and StoreFront**].

Application note The use of the FIPS 140-2 validated TLS in FCO_SCO.1.3/Browser is also addressed by FCS_ECA.1/FIPS_Enh.

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.

The connection from a User Device web browser to StoreFront takes place in any direct connection to a virtual desktop or published application. A connection between Citrix Receiver in a virtual desktop and StoreFront exists only on the second hop of any double-hop connection that is made[10].

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 Citrix Receiver and the Virtual Delivery Agent**] that is logically distinct from other communication channels and provides assured identification of [**the Virtual Delivery Agent**] and protection of the channel data from [*modification, disclosure*].

FCO_SCO.1.2/Desktop The TSF shall permit [**the Citrix Receiver**] 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 TLS 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 Citrix Receiver and the Virtual Delivery 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.

Where published applications are accessed via Citrix Receiver running in a virtual desktop (the double-hop case) then the ICA channel between the the Citrix Receiver in the virtual desktop and the virtual application session (i.e. the second hop) is protected by TLS, and in addition any ICA channel communications between the virtual desktop and the Citrix Receiver in the physical User Device (i.e. the first hop) are similarly protected by TLS.

[10] The instance of the Citrix Receiver for the second hop connection is run from within the virtual desktop in the Virtual Delivery Agent. This represents an HTTP connection from a VDA to StoreFront that is conceptually the same as the first hop HTTP connection from the User Device to StoreFront, but which is not shown in Figure 1 to avoid excessive complexity in the diagram.

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 (excluding DDC-VDA communications)**] that is logically distinct from other communication channels and provides assured identification of [**the server end of each client-server TLS connection**] and protection of the channel data from [*modification*, *disclosure*].

FCO_SCO.1.2/Server The TSF shall permit [**TOE servers (excluding DDC-VDA communications)**] 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 TLS 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 (excluding DDC-VDA communications)**].

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.

Communications between the DDC and VDA are separately addressed by FCO_SCO.1/WCF.

6.2.3.4 FCO_SCO.1/WCF Secure channel operation

FCO_SCO.1.1/WCF The TSF shall use a communication channel between [**DDC and VDA**] that is logically distinct from other communication channels and provides assured identification of [**the non-initiating entity**] and protection of the channel data from [*modification*, *disclosure*].

FCO_SCO.1.2/WCF The TSF shall permit [**either DDC or VDA**] to initiate communication via the communication channel.

FCO_SCO.1.3/WCF The TSF shall ensure that the communication channel meets the following additional requirements for security: [**use of Basic256 ciphersuite for WCF message-level security in accordance with FIPS140-2 validation of the underlying cryptographic functions**].

FCO_SCO .1.4/WCF The TSF shall use the communication channel for [**all traffic between DDC and VDA**].

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.

In fact this SFR covers two channels: one initiated by the VDA in order to register with the DDC (which therefore authenticates the DDC to the VDA) and that continues subsequently to be used by the VDA to communicate status information to the DDC. The other channel is initiated by the DDC (which therefore authenticates the VDA to the DDC) for ongoing communication with the VDA.

6.2.3.5 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 StoreFront, and between the virtual desktop web browser and StoreFront using AES as defined by the ciphersuite TLS_RSA_WITH_AES_128_CBC_SHA in RFC 2246; and**

- **encryption of traffic between the User Device Citrix Receiver and the Virtual Delivery Agent using AES as defined by the ciphersuite TLS_RSA_WITH_AES_128_CBC_SHA in RFC 2246; and**

- **encryption of traffic between StoreFront and the Delivery Controller using AES as defined by the ciphersuite TLS_RSA_WITH_AES_128_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 ActiveX Data Objects for .NET (ADO.NET) with AES as defined by the ciphersuite TLS_RSA_WITH_AES_128_CBC_SHA in RFC 2246** using [**Microsoft Enhanced Cryptographic Provider**] in accordance with the conditions of the external accreditation of this functionality against [**FIPS140-2**].

Application note

The protocols for the various communication channels identified above, are shown on the XenDesktop Components diagram in Figure 1 earlier in this document.

The accreditation of the Microsoft Enhanced Cryptographic Provider against FIPS140-2 is documented in the following certificates:

Microsoft Windows 7 Ultimate – Certificate #1330
Microsoft Windows Server 2012 Datacenter Edition – Certificate #1894.

The client-side of the channel between the User Device Citrix Receiver and the Virtual Delivery Agent uses the Microsoft Enhanced Cryptographic Provider as noted above, but the server side of this channel uses the kernel-mode cryptographic provider as in FCS_ECA.1.1/FIPS_KM (see section 6.2.3.6).

6.2.3.6 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 Receiver and the Virtual Delivery Agent using AES as defined by the ciphersuite TLS_RSA_WITH_AES_128_CBC_SHA in RFC 2246]**

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 7 Ultimate – Certificate #1328
Microsoft Windows Server 2012 Datacenter Edition – Certificate #1891.

The client-side of the channel between the User Device Citrix Receiver and the Virtual Delivery Agent uses the Microsoft Enhanced Cryptographic Provider as in FCS_ECA.1.1/FIPS_Enh (see section 6.2.3.5), but the server side of this channel uses the kernel-mode cryptographic provider as in FCS_ECA.1.1/FIPS_KM above.

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/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	FDP_ACC.1/Application	FDP_ACF.1/Application	FMT_MSA.1/Application	FMT_MSA.3/Application	FMT_MSA.3/Resources	FMT_MOF.1/Resources	FCO_SCO.1/Browser	FCO_SCO.1/Desktop	FCO_SCO.1/Server	FCO_SCO.1/WCF	FCS_ECA.1/FIPS_Enh	FCS_ECA.1/FIPS_KM
O.Auth_User		X	X																				
O.Auth_Server																		X	X	X	X		
O.Desktop	X			X	X	X	X	X	X														
O.Application	X			X	X							X	X	X	X								
O.Secure_Setup_Data				X	X			X	X					X	X					X	X		
O.Secure_User_Data										X	X								X	X	X	X	X
O.Use_FIPS																						X	X
O.Config_Access				X	X	X	X	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/WCF. 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/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/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.Application

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

FIA_ATD.1/User ensures that individual application users can be granted access permissions for published applications, while FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Application and FMT_MSA.3/Application ensure that only administrators can manage the application users' access permissions.

The application access policy (FDP_ACC.1/Application and FDP_ACF.1/Application) ensures that only application users with the correct access permissions can gain access to a published application.

6.4.5 O.Secure_Setup_Data

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

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

6.4.6 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 Delivery Agent, and FCO_SCO.1/Server and FCO_SCO.1/WCF which ensure the confidentiality and integrity of communications between TOE servers. The conformance requirements FCS_ECA.1/FIPS_Enh and FCS_ECA.1/FIPS_KM 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.

6.4.7 O.Use_FIPS

This objective is addressed by FCS_ECA.1/FIPS_Enh and FCS_ECA.1/FIPS_KM, 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.

6.4.8 O.Config_Access

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 (FMT_MSA.1/Application, FMT_MSA.3/Application), the Desktop access policy (FDP_ACC.1/Desktop, FDP_ACF.1/Desktop), and the Application access policy (FDP_ACC.1/Application, FDP_ACF.1/Application).

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

The Desktop access policy (FDP_ACC.1/Desktop and FDP_ACF.1/Desktop) and Application access policy (FDP_ACC.1/Application and FDP_ACF.1/Application) ensure that only administrators can gain access to virtual desktop and published application 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/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/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/Application	FDP_ACF.1	Met by 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_MSA.3/Application	FMT_MSA.1	Met by FMT_MSA.1/Application
	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

SFR	**Dependencies**	**Rationale**
FCO_SCO.1/Browser	None	
FCO_SCO.1/Desktop	None	
FCO_SCO.1/Server	None	
FCO_SCO.1/WCF	None	
FCS_ECA.1/FIPS_Enh	None	
FCS_ECA.1/FIPS_KM	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/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	FDP_ACC.1/Application	FDP_ACF.1/Application	FMT_MSA.1/Application	FMT_MSA.3/Application	FMT_MSA.3/Resources	FMT_MOF.1/Resources	FCO_SCO.1/Browser	FCO_SCO.1/Desktop	FCO_SCO.1/Server	FCO_SCO.1/WCF	FCS_ECA.1/FIPS_Enh	FCS_ECA.1/FIPS_KM
Administrator access control		X	X																				
Administration of virtual desktop and published application authorisation	X			X	X			X	X					X	X	X	X						
Desktop user and Application user access control		X	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 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 and published application authorisation

The management of Configdata is performed by an administrator using Citrix Studio, in conjunction with the Delivery Controller which controls access, and the database 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;
- The list of published applications and access permissions for users to those applications (i.e. the list of permitted published applications);
- 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 administration mechanisms satisfy the **FMT_SMR.1/Authorise**, **FMT_SMF.1/Authorise**, **FMT_MSA.1/Desktop**, **FMT_MSA.1/Application**, **FMT_MSA.3/Desktop**, **FMT_MSA.3/Application**, **FMT_MSA.3/Resources** and **FMT_MOF.1/Resources** security management requirements as well as the **FIA_ATD.1/User** attribute requirement.

7.3 Desktop user and Application user access control

StoreFront provides the means for a user to log in to the TOE using a web browser or Citrix Receiver, in order to gain access to their virtual desktops and permitted published applications. StoreFront receives the user’s credentials, which may be username/password or multifactor authentication using a smart card. It forwards the credentials to the Delivery Controller for authentication by the domain controller. 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 Delivery Controller for authorisation to ensure that users are only granted access to virtual desktops and published applications for which they have the appropriate permission. Once a user’s access permission has been verified, the Delivery Controller assembles the user’s virtual desktop or published application environment using the virtual desktop configuration data or access permissions for published applications. The Delivery Controller starts the virtual desktop and generates a ticket which is passed to the Virtual Delivery Agent and, via StoreFront, to the user’s Citrix Receiver.

The Citrix Receiver in the user’s User Device uses the ticket to establish a session with the appropriate Virtual Delivery Agent. The Virtual Delivery Agent provides access to the virtual desktop and permitted published applications for the user. It authenticates the user before establishing the session, by confirming that the same ticket has been presented by the Citrix Receiver as that supplied by the Delivery Controller. (See also section 1.3 for additional description of the steps, interactions and data items involved.)

Once a user has logged out of a virtual desktop, the virtual desktop and its virtual machine are preserved and available only for that user.

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

7.4 User Device resource access control

Desktop users and application users 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 Receiver and the Virtual Delivery Agent. Only global enabling of the functions (i.e. applicable to the entire Site) 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 StoreFront and the User Device web browser is protected by TLS.

Communication between the Virtual Delivery Agent and the Citrix Receiver in the user's User Device is protected by Windows secure communications mechanisms, which are configured to use TLS for authentication, confidentiality and integrity.

Communication between the TOE servers is protected by Windows secure communications mechanisms, which are configured to use either TLS or Windows message-level security (as shown in Figure 1) 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/WCF** requirements for authenticated communication channels; they also satisfy the **FCS_ECA.1/FIPS_Enh** and **FCS_ECA.1/FIPS_KM** requirements for conformance with FIPS 140-2 Level 1 accreditation.

End of Document