Common Criteria Security Target

for

Citrix XenDesktop 7.15 LTSR Platinum Edition and Citrix XenApp 7.15 LTSR Platinum Edition

Version 1-0

0. Preface

0.1 Objectives of Document

This document presents the Common Criteria (CC) Security Target (ST) to express the security and evaluation requirements for the Citrix XenDesktop 7.15 LTSR Platinum Edition and Citrix XenApp 7.15 LTSR Platinum Edition products.

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

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

0.2 Scope of Document

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

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

0.3 Intended Readership

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

0.4 Related Documents

Common Criteria[1]

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model, CCMB-2012-09-001, Version 3.1 Revision 5, April 2017.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security Functional Components,

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

CCMB-2012-09-002, Version 3.1 Revision 5, April 2017.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security Assurance Components, CCMB-2012-09-003, Version 3.1 Revision 5, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, CCMB-2012-09-004, Version 3.1, Revision 5, April 2017.

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

0.5 Significant Assumptions

None

0.6 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
ICA	Independent Computing Architecture
LAN	Local Area Network
OSP	Organisational Security Policy
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

0.7 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.
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 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 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]

Term	Meaning
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]
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]

Term	Meaning
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]
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.

Term	Meaning
Virtual Desktop	a desktop operating system running on a virtual machine on a virtualised server, personalised for a desktop user.
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

1. ST Introduction 10
  1.1 ST and TOE Reference Identification 10
  1.2 TOE Overview 10
    1.2.1 Usage and major features of the TOE 10
    1.2.2 TOE Type 11
    1.2.3 Required non-TOE hardware/software/firmware 12
  1.3 TOE Description 13
  1.4 TOE Boundaries 15
    1.4.1 Physical Boundary 15
    1.4.2 Logical Boundary 16
    1.4.3 Features and functions not evaluated 17
2. CC Conformance 20
3. Security Problem Definition 21
  3.1 Assets 21
  3.2 Users and Subjects 21
  3.3 Threats 22
    3.3.1 Attacks on the TOE 22
  3.4 Organisational Security Policies 22
  3.5 Assumptions 23
4. Security Objectives 24
  4.1 Security Objectives for the TOE 24
  4.2 Security Objectives for the Environment 25
    4.2.1 Security Objectives for the Technical Environment 25
    4.2.2 Security Objectives for the Procedural Environment 26
  4.3 SPD/Objectives Rationale 27
    4.3.1 T.Attack_DesktopOrApp 28
    4.3.2 T.Attack_Userdata 28
    4.3.3 T.Access_DesktopOrApp 28
    4.3.4 T.Access_Userdata 29
    4.3.5 T.Intercept 30
    4.3.6 T.Spoof 30
    4.3.7 T.Attack_Configdata 30
    4.3.8 P.Restrictions 31
    4.3.9 A.Physical 31
    4.3.10 A.Config_Endpoint 31
    4.3.11 A.Operations_Security 31
    4.3.12 A.VM_Host 31
    4.3.13 A.Third_Party_SW 31
5. IT Security Requirements 32
  5.1 Conventions 32
  5.2 Security Functional Requirements 32
    5.2.1 Authentication 32
      5.2.1.1 FIA_ATD.1/User User attribute definition 32
      5.2.1.2 FIA_UID.2/User User identification before any action 32
    5.2.2 Authorisation 33
      5.2.2.1 FMT_SMR.1/Authorise Security management roles 33
      5.2.2.2 FMT_SMF.1/Authorise Specification of management functions 33
      5.2.2.3 FDP_ACC.1/Application Subset access control 34
      5.2.2.4 FDP_ACF.1/Application Security attribute based access control 34
      5.2.2.5 FMT_MSA.1/Application Management of Security Attributes 34
      5.2.2.6 FMT_MSA.3/Application Static attribute initialisation 35
      5.2.2.7 FDP_ACC.1/Desktop Subset access control 35
      5.2.2.8 FDP_ACF.1/Desktop Security attribute based access control 35
      5.2.2.9 FMT_MSA.1/Desktop Management of security attributes 35

5.2.2.10 FMT_MSA.3/Desktop Static attribute initialisation 36
5.2.2.11 FDP_ACC.1/Resources Subset access control 36
5.2.2.12 FDP_ACF.1/Resources Security attribute based access control 36
5.2.2.13 FMT_MSA.1/Resources Management of security attributes 37
5.2.2.14 FMT_MSA.3/Resources Static attribute initialisation 37
5.2.3 Communications 38
5.2.3.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection 38
5.3 Security Assurance Requirements 38
5.4 Objectives/SFRs Rationale 40
5.4.1 O.Auth_User 40
5.4.2 O.Auth_Server 40
5.4.3 O.Desktop 40
5.4.4 O.Application 41
5.4.5 O.Secure_Setup_Data 41
5.4.6 O.Secure_User_Data 41
5.4.7 O.Config_Access 41
5.4.8 O.Endpoint_Resource 42
5.5 SFR Dependencies Analysis 42
6. TOE Summary Specification 44
6.1 Administrator access control 44
6.2 Administration of virtual desktop and published application authorisation 44
6.3 Desktop user and Application user access control 45
6.4 User Device resource access control 46
6.5 Secure communications 46

Figures / Tables

Figure 1: XenDesktop and XenApp Components 13
Figure 2: TOE Physical boundary 15
Figure 3: Logical boundaries 17
Table 1: Threats/OSP/Assumptions addressed by Security Objectives 27
Table 2: Security Assurance Requirements 38
Table 3: Summary of Objectives/SFRs Rationale 40
Table 4: Analysis of SFR Dependencies 43
Table 5: Summary of SFRs satisfied by TOE Functions 44

1. ST Introduction

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

1.1 ST and TOE Reference Identification

TOE Reference:	Citrix XenDesktop 7.15 LTSR Platinum Edition and Citrix XenApp 7.15 LTSR Platinum Edition
ST Reference:	Citrix XenDesktop 7.15 LTSR Platinum Edition and Citrix XenApp 7.15 LTSR Platinum Edition Security Target
ST Version:	1-0
ST Date:	15 January 2018
Assurance Level:	EAL2 augmented by ALC_FLR.2 Flaw Reporting Procedures

1.2 TOE Overview

1.2.1 Usage and major features of the TOE

Citrix XenDesktop 7.15 LTSR Platinum Edition and Citrix XenApp 7.15 LTSR 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 2016 and personalised virtual desktops hosted on Microsoft Windows 10[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, Features and functions not evaluated.

The open architecture of XenDesktop and XenApp offers choice and flexibility of virtualisation platform and user devices. XenDesktop and XenApp integrate with various server virtualisation products. 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. This means that there is no vendor

[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.

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**. The TOE requires users to be authenticated before granting them access to virtual desktops and/or applications. 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.

1.2.2 TOE Type

Desktop and Application Virtualisation.

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

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 2016, Standard Edition
- Microsoft .NET Framework 4.6
- Microsoft Internet Information Server (IIS) 10.0
- Microsoft ASP.NET 4.6

Citrix License Server 11.14.

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

- Microsoft Windows Server 2016, Standard Edition
- Microsoft .NET Framework 4.6

The Delivery Controller requires a Database with the following software:

- Microsoft SQL Server 2016
- Microsoft Windows Server 2016, Standard Edition.

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

- Microsoft Windows 10 Enterprise, 64-bit.
- Microsoft Internet Explorer version 11.

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

- Microsoft Windows 10 Enterprise, 64-bit.
- Microsoft Internet Explorer version 11.

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

- Microsoft Windows Server 2016, Standard 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 2016 native mode.

If multi-factor authentication (MFA), such as smart cards, is required, appropriate readers and drivers are required on endpoints, and appropirate middleware is required to integrate the multi-factor authentication with the domain controller. The TOE relies on the operational environment to provide user authentication. This may take the form of passwords or supported multi-factor authentication, including smart cards, depending on the customer's environment and requirements.

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).

Testing was performed using the Citrix XenServer 7.1 Long Term Service Release (LTSR) hypervisor. Other hypervisors are supported but were not included in Common Criteria testing. A list of hypervisor versions supported for XenApp 7.15 LTSR and XenDesktop 7.15 LTSR is included in the *System requirement*s article in the XenApp and XenDesktop 7.15 LTSR product documentation available at https://docs.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.

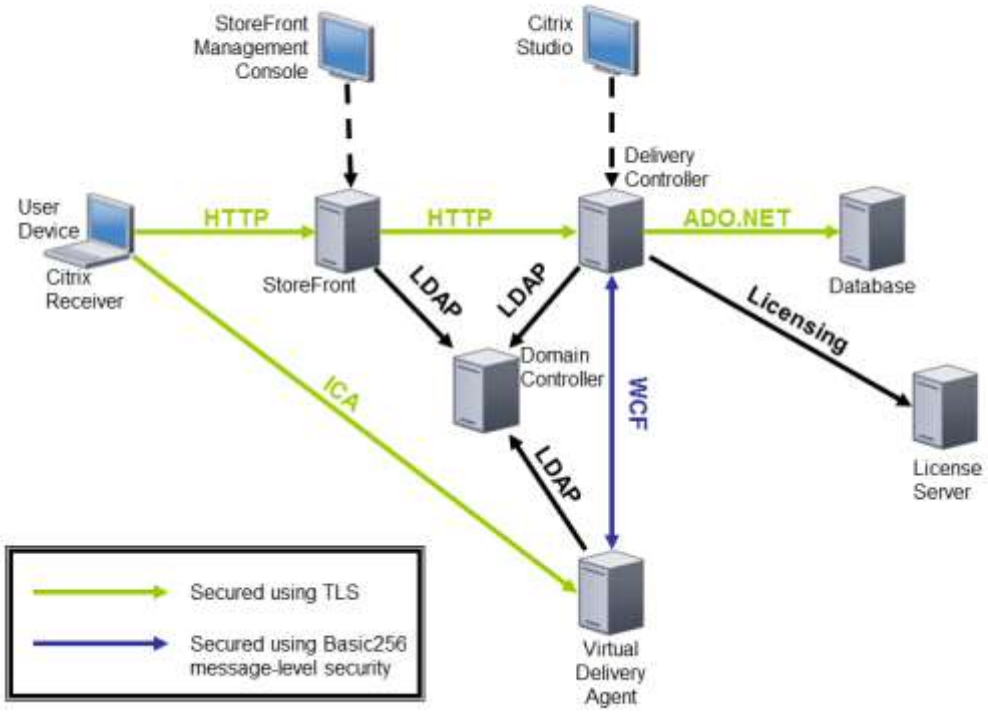

Figure 1: XenDesktop and XenApp Components

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.

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 2. 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.

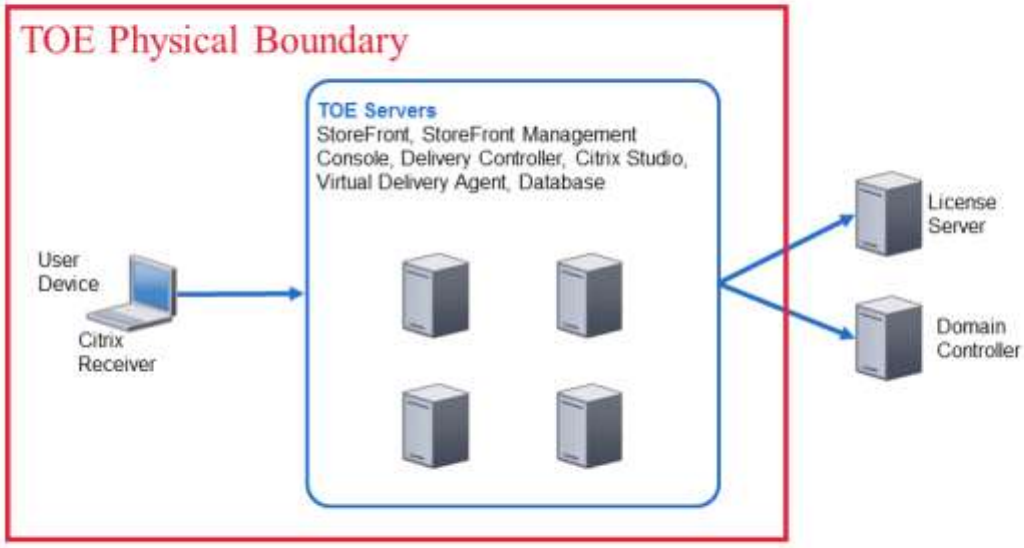

Figure 2: TOE Physical boundary

Developer documentation

- Common Criteria Evaluated Configuration Guide for Citrix XenDesktop 7.15 LTSR Platinum Edition and Citrix XenApp 7.15 LTSR Platinum Edition, 11 January 2018 **[CCECG]**

- Common Critera-specific documentation is provided at https://www.citrix.com/security in the Common Criteria section.

- Citrix product documentation is provided at https://docs.citrix.com/.

While administrators are expected to make use of the online documentation as a whole, the following sections of the online documentation are specifically relevant to the evaluated configuration:

For documentation about:	**From the left menu on docs.citrix.com, navigate to:**
Licensing	XenApp and XenDesktop > Licensing > Licensing 11.14
Citrix Receiver for Windows	Citrix Receiver > Receiver for Windows > Citrix Receiver for Windows 4.9 LTSR
StoreFront	XenApp and XenDesktop > StoreFront > StoreFront 3.12
XenApp and XenDesktop Version 7.15 LTSR	XenApp and XenDesktop > XenApp and XenDesktop 7.15 Long Term Service Release

1.4.2 Logical Boundary

XenDesktop and XenApp are offered in various editions that provide different features. The evaluated TOE consists of Citrix XenDesktop 7.15 LTSR Platinum Edition and Citrix XenApp 7.15 LTSR Platinum Edition, including:

- Delivery Controller 7.15.0.15097
- Citrix Studio 7.15.0.93
- StoreFront (including StoreFront Management Console) 3.12.0.17
- Virtual Delivery Agent 7.15.0.15097
- Citrix Receiver 4.9.0.2539 with Online Plug-in 14.9.0.2539

Customers download all components from the Citrix web site (https://www.citrix.com) in accordance with the detailed delivery information provided in **[CCECG]** section "Download and Verify the Installation Media."

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

The Citrix Receiver runs on the User Device and virtual desktops[4], while the other components run on servers (in a variety of possible configurations). The logical boundaries

[4] 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
(This footnote continues on the next page)

of the TOE are illustrated below in Figure 3, where elements shown shaded are components of the TOE.

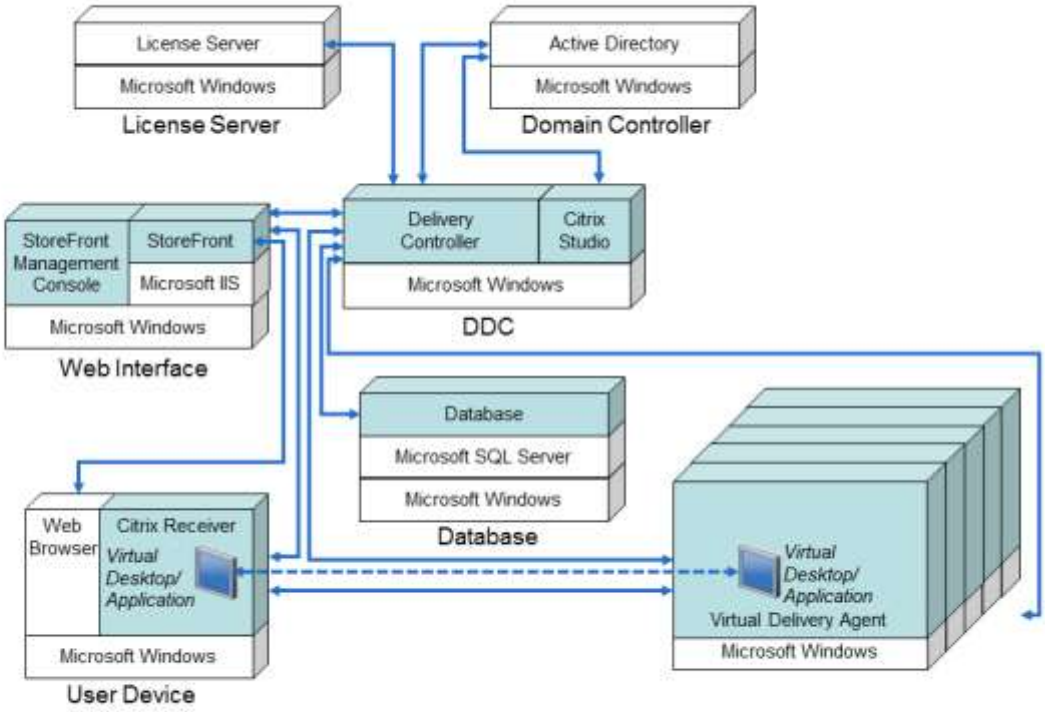

Figure 3: Logical boundaries

1.4.3 Features and functions not evaluated

The Citrix XenServer hypervisor was used in the environment for testing, but is not part of the TOE and is therefore not included in this evaluation. (Various other hypervisors are supported, please see section 1.2.3 for additional information.)

The following Citrix components should not be installed and are therefore not evaluated:

- 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;

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 3.

- Citrix Profile Management – high performance user personalisation method, not used in the evaluated configuration;
- Citrix NetScaler SD-WAN – accelerator for improved performance on wide area networks, not used in the evaluated configuration;
- 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 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.

The following features of XenDesktop and XenApp are disallowed in the evaluated configuration and are therefore not evaluated:

- Application delivery methods other than XenApp published apps, also known as server-based hosted applications;
- Desktop delivery methods other than VDI desktops;
- Desktop delivery groups of the *random* type;
- The capability for users to belong to multiple desktop delivery groups;
- The capability for desktop users to be assigned multiple desktops in a desktop delivery group;
- The capability for users to belong to multiple application delivery groups;
- Delegated administrator roles other than full administrators;
- Control of local peripheral support using individual and group policy (only global policy is used);
- The ability for administrators to automatically create virtual desktops and servers using Machine Creation Services;
- Power management of virtual machines via the Delivery Controller;
- The use of multiple Delivery Controllers;
- Connection leasing and use of Zones with Local Host Cache;
- Disconnected sessions;
- Non-brokered sessions;
- Streaming applications using AppV;
- The ability for administrators to deploy Personal vDisks for users and deliver applications using AppV and AppDisks;
- The ability for users to access their personal office PC remotely from Citrix Receiver using the Remote PC Access feature;

- The recording, archiving and playback of the on-screen activity of a user session hosted on a Server or Desktop VDA using the Session Recording feature; and,
- Use of the Federated Authentication Service to support SAML-based logon to StoreFront, and the use of unauthenticated (anonymous) delivery groups and StoreFront stores.

Any VM Host used to provide virtual desktops or published applications is outside the scope of the TOE (see OE.Config_VM_Host in section 4.2.1).

2. CC Conformance

This ST supports the following conformance claims:

- CC Version 3.1 Revision 5,
- CC Part 2 conformant,
- CC Part 3 conformant, and,
- Evaluation Assurance Level (EAL) 2 augmented by ALC_FLR.2 Flaw Reporting Procedures.

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

P.Restrictions	The TOE shall prevent the following actions by users when configured to do so by an administrator in order to meet the TOE customer's security requirements: • 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; and,
- Access to User Device USB devices from virtual desktops.

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	Data (including keys) generated, processed, and stored outside the TOE is managed in accordance with the level of risk. This includes the application of appropriate controls to prevent the use of cameras and smart phones to photograph screens, and disabling screen capture and print screen functions on endpoints if required by the TOE customer.
A.VM_Host	The VM Host software provides virtual machine isolation and is operating correctly and securely.
A.Third_Party_SW	Trusted third-party software is operating correctly and securely. 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.Config_Access	The virtual desktops and published applications must only be configurable by trusted 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.

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]. 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. This includes authentication using the domain controller in the environment and any two-factor authentication used by the TOE customer such as smart cards.
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. This is provided by the Windows operating system cryptograhic modules.

OE.Encryption	Communications between the DDC and VDA are not protected by TLS, but by WCF message-level security. This is provided by the Windows operating system cryptographic module. It uses XML-based WS-Security mechanisms to provide HMAC and encryption for the message contents together with Kerberos-based authentication.

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 and other security best practices.
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. If required, endpoint functionality such as screen capture and screen print must be disabled so that users can not bypass controls on data movement between published desktops/applications and their local endpoint.

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

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	P.Restrictions	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.Config_Access		X	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		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.

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.

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 and OE.Encryption ensure 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 P.Restrictions

Restrictions are in place to control whether TOE facilitates moving data between published applications and virtual desktops and the user's endpoint.

O.Endpoint_Resource ensures that users can only use the clipboard and devices attached to the Endpoint when authorised. This controls cut and paste and moving files between the published desktop or application and the endpoint.

O.Config_Access ensures that the virtual desktops and published applications have been set up properly.

OE.Config_Endpoint ensures that the security of TOE will not be compromised by the security of the endpoint.

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 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. IT Security Requirements

5.1 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.

5.2 Security Functional Requirements

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

- Authentication
- Authorisation
- Communications

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.

5.2.1 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.

5.2.1.1 FIA_ATD.1/User User attribute definition

FIA_ATD.1.1/User	The TSF shall maintain the following list of security attributes belonging to individual users: [**id, group membership**].

5.2.1.2 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.

5.2.2 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.

5.2.2.1 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.

5.2.2.2 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.

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.

5.2.2.3 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].**

5.2.2.4 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: [

subject (**user) security attribute: id, group membership**

object (application) security attributes: security permissions].

FDP_ACF.1.2/Application The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**An application shall be accessible by a user only if security permissions for the delivery group to which the application is assigned explicitly grant the user id or the user group the access required.**]

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**].

5.2.2.5 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) User id

b) User group,

c) Security permissions]

to [**administrators**].

5.2.2.6 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.

Application note Administrators are instructed by [CCECG] to always select the correct options to establish a restrictive configuration.

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.

5.2.2.7 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**].

5.2.2.8 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: [

subject (**user) security attribute: id**

object (desktop) security attribute: security permissions].

FDP_ACF.1.2/Desktop The TSF shall enforce the following rules to determine if an operation among controlled subjects and objects is allowed: [Security permissions explicitly grant the user id the access required.]

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].**

5.2.2.9 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: [

- **User id**
- **Security permissions**]

to [**administrators**].

5.2.2.10 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 policy.

Application note Administrators are instructed by [CCECG] to always select the correct options to establish a restrictive configuration.

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.

5.2.2.11 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; and,**
- **access to endpoint-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.

5.2.2.12 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: [

subject (user) security attribute: none

object (application or virtual desktop) security attribute: endpoint data access permissions].

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

1) **Users shall be permitted to cut and paste data between a published application or a virtual desktop and an endpoint operating system clipboard if the cut and paste function is enabled in the endpoint data access permissions.**

2) **Endpoint drives shall be accessible to a published application or a virtual desktop only if the client drive mapping function is enabled in the endpoint data access permissions.**

3) **USB devices on an endpoint shall be accessible to a virtual desktop only if the USB device access function is enabled in the endpiont data access permissions.]**

Application note Note that that endpoint data access permissions allowed in the evaluated configuration are global and therefore apply to all users. Individual and group permissions are disallowed in the evaluated configuration.

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].**

5.2.2.13 FMT_MSA.1/Resources Management of security attributes

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

- **endpoint data access permissions]**

to [**administrators**].

5.2.2.14 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 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.

5.2.3 Communications

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

5.2.3.1 FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1.1 The TSF shall protect TSF data from [**disclosure and modification]** when it is transmitted between separate parts of the TOE**.**

5.3 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**
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.

5.4 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	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.1/Resources	FMT_MSA.3/Resources	FPT_ITT.1
O.Auth_User		X															
O.Auth_Server																	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
O.Secure_User_Data																	X
O.Config_Access			X	X	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

5.4.1 O.Auth_User

This objective is addressed by FIA_UID.2/User which ensures that desktop users and administrators are successfully identified and authenticated before they can use the TOE functionality. (Authentication is provided in the OE by a domain controller.)

5.4.2 O.Auth_Server

This objective is addressed by FPT_ITT.1. This ensures the confidentiality, integrity and authenticity of TOE components for all communications between TOE servers, and between User Devices and TOE servers.

5.4.3 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.

5.4.4 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 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.

5.4.5 O.Secure_Setup_Data

This objective is addressed by FPT_ITT.1 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).

FPT_ITT.1 ensures 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.

5.4.6 O.Secure_User_Data

This objective is addressed by FPT_ITT.1 which ensures the confidentiality and integrity of communications between Citrix Receiver and the Virtual Delivery Agent, and the confidentiality and integrity of communications between TOE servers.

5.4.7 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), the Application access policy (FDP_ACC.1/Application, FDP_ACF.1/Application), and the Resource access policy (FMT_MSA.1/Resources, FMT_MSA.3/Resources).

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

5.4.8 O.Endpoint_Resource

This objective is addressed by security management functions (FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Resources, FMT_MSA.1/Resources, and 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, and FMT_MSA.3/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.

5.5 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	
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

SFR	Dependencies	Rationale
	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	Met by FMT_MSA.1/Resources
	FMT_SMR.1	Met by FMT_SMR.1/Authorise
	FMT_SMF.1	Met by FMT_SMF.1/Authorise
FPT_ITT.1	None	

Table 4: Analysis of SFR Dependencies

6. TOE Summary Specification

The table below provides a summary of the TOE functions that satisfy the security functional requirements described in section 5.2 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	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.1/Resources	FMT_MSA.3/Resources	FPT_ITT.1
Administrator access control		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					
User Device resource access control									X	X							
Secure communications																	X

Table 5: Summary of SFRs satisfied by TOE Functions

6.1 Administrator access control

Administrators are authenticated as part of their Windows login via the operating system and domain controller (see OE.Authentication). 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** requirement for administrators.

6.2 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.1/Resources, and FMT_MSA.3/Resources** security management requirements as well as the **FIA_ATD.1/User** attribute requirement.

6.3 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** requirement 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**).

6.4 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**).

6.5 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.

The TOE ensures that communications are protected by leveraging two Windows cryptographic modules in the environment. Server-side components of communication channels leverage the kernel mode cryptographic module. Client applications, including the web browser, use the user-mode DLL module.

These secure communications mechanisms satisfy the **FPT_ITT.1** requirements for integrity-protected and encrypted communication channels.

End of Document