122-B

CERTIFICATION REPORT No. CRP256

Citrix XenDesktop
4 Platinum Edition
running on Microsoft Windows Server 2003 SP2

Issue 1.0

August 2010

CESG Certification Body
IACS Delivery Office, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT

The product detailed below has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the specified Common Criteria requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this report.			
Sponsor:	Citrix Systems Inc.	Developer:	Citrix Systems Inc.
Product and Version:	Citrix XenDesktop 4 Platinum Edition		
Platform:	Server components: Microsoft Windows Server 2003, 32-bit Edition, Enterprise Edition, R2, SP2. Domain-joined User Devices: Microsoft Windows XP Professional SP3. Non-domain-joined User Devices: Microsoft Windows Vista Ultimate SP1, or Windows XP Professional SP3, or Windows Server 2003 R2 SP2.		
Description:	Citrix XenDesktop 4 Platinum Edition is a desktop virtualisation product that centralises and delivers Microsoft Windows XP or Vista virtual desktops as a service to users.		
CC Version:	Version 3.1 Revision 3		
CC Part 2:	Extended	CC Part 3:	Conformant
EAL:	EAL 2 augmented by ALC_FLR.2		
PP Conformance:	None		
CLEF:	SiVenture		
CC Certificate:	CRP256	Date Certified:	20 August 2010

The evaluation was performed in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in UK Scheme Publication 01 [UKSP01] and 02 [UKSP02P1], [UKSP02P2]. The Scheme has established the CESG Certification Body, which is managed by CESG on behalf of Her Majesty's Government.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [ST], which prospective consumers are advised to read. To ensure that the Security Target gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 1 [CC1] and 3 [CC3], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been performed properly and that no *exploitable* vulnerabilities have been found in the evaluated configuration of the TOE. It is not an endorsement of the product.

ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement [CCRA] and, as such, this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement.

The judgements[1] contained in the certificate and in this report are those of the Qualified Certification Body which issued them and of the Evaluation Facility which performed the evaluation. There is no implication of acceptance by other Members of the Arrangement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed by a third party upon those judgements.

MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES

The SOGIS MRA logo which appears below confirms that the conformant certificate has been authorised by a Participant to this Agreement [MRA] and it is the Participant's statement that the certificate has been issued in accordance with the terms of this Agreement.

The judgments[1] contained in the certificate and this Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which carried out the evaluation. Use of the logo does not imply acceptance by other Participants of liability in respect of those judgments or for loss sustained as a result of reliance placed upon those judgments by a third party.

CCRA logo **CC logo** **SOGIS MRA logo**

[1] All judgements contained in this Certification Report are covered by the CCRA [CCRA] and the MRA [MRA].

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria (CC) security evaluation of Citrix XenDesktop 4 Platinum Edition to the Sponsor, Citrix Systems Inc, as summarised on page 2 'Certification Statement' of this report, and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

2. Prospective consumers are advised to read this report in conjunction with the Security Target [ST], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The following product completed evaluation to CC EAL2, augmented by ALC_FLR.2, on 13th August 2010:

- **Citrix XenDesktop 4 Platinum Edition**

It is abbreviated to 'XenDesktop' in this document.

4. The Developer was Citrix Systems Inc.

5. The evaluated configuration of this product is described in this report as the Target of Evaluation (TOE). Details of the TOE Scope, its assumed environment and the evaluated configuration are given in Chapter III 'Evaluated Configuration' of this report.

6. The TOE is a desktop virtualisation product that centralises and delivers Microsoft Windows XP or Vista virtual desktops as a service to users. Virtual desktops are dynamically assembled on demand, providing users with pristine[2], personalised desktops each time they log on. Although the desktops are virtual, running on remote servers, the user experience is equivalent to that of a local Windows desktop. From the user's perspective, logging on to a virtual desktop is the same as logging on to a local desktop. Users enter their credentials once and are connected to their desktops.

7. The scope of the "Citrix XenDesktop 4 Platinum Edition" TOE excludes some applications that are bundled in the "Citrix XenDesktop 4 Platinum Edition" product. Those excluded applications are listed in [ST] Section 1.4.3 (e.g. Citrix XenServer, Citrix XenApp, Citrix Access Gateway). In addition, the following features are not included in the scope of the evaluation:

a) Server-side and client-side application virtualisation is not included; only applications 'baked-in' to the virtual desktop image are included in the evaluation.

[2] 'Pristine' here means 'in original condition, clean, unspoilt'. For example, following disconnection, the memory is erased, preventing any residual data from a desktop user remaining in the memory of the virtual desktop after that user has logged out, to ensure that the data cannot be recovered by a different user.

b) Smart card support for desktop user authentication is included in the evaluation, but tokens are not.

c) Administrators can enable/disable local peripheral support either as a global control policy or for individual users and groups of users; only the facility for applying a global control policy is included in the evaluation.

d) Desktop appliances and client devices other than Windows PCs are not included as User Devices in the evaluation.

e) The capability for Desktop users to belong to multiple desktop groups is not included, i.e. a Desktop user can only use a virtual desktop from one desktop group.

8. An overview of the TOE and its product architecture can be found in Chapter IV 'Product Architecture' of this report. Configuration requirements are specified in [ST] Section 1.2.3.

Security Claims

9. The Security Target [ST] fully specifies the TOE's Security Objectives, the Threats / Organisational Security Policies (OSPs) which these Objectives meet and the Security Functional Requirements (SFRs) that elaborate the Objectives. Most of the SFRs are taken from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products. For explicitly stated SFRs see [ST] Section 5.

10. The TOE security policies are detailed in [ST]. The OSPs that must be met are specified in [ST] Section 3.4.

11. The environmental assumptions related to the operating environment are detailed in Chapter III (in 'Environmental Requirements') of this report.

Evaluation Conduct

12. The CESG Certification Body monitored the evaluation which was performed by the SiVenture Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [ST]. The results of this work, completed in August 2010, were reported in the Evaluation Technical Report [ETR]. The CESG Certification Body raised comments on [ETR]; those comments were satisfactorily answered by the Evaluators ([ETRSup1], [ETRSup2]).

Conclusions and Recommendations

13. The conclusions of the CESG Certification Body are summarised on page 2 'Certification Statement' of this report.

14. Prospective consumers of Citrix XenDesktop 4 Platinum Edition should understand the specific scope of the certification by reading this report in conjunction with the Security Target [ST]. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that the SFRs and the evaluated

configuration match their identified requirements, and to give due consideration to the recommendations and caveats of this report.

15. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration. Chapter II 'TOE Security Guidance' of this report includes a number of recommendations regarding the secure receipt, installation, configuration and operation of the TOE.

16. In addition, the Evaluators' comment and recommendation is as follows:

a) All guidance necessary to determine that the TOE has been securely delivered, and to securely install and operate the TOE, is provided in or referenced from Common Criteria Evaluated Configuration Guide [CCECG], which is available for download from the Common Criteria link from the Citrix Security webpage https://www.citrix.com/security.

Disclaimers

17. This report is only valid for the evaluated TOE. This is specified in Chapter III 'Evaluated Configuration' of this report.

18. Certification is not a guarantee of freedom from security vulnerabilities. There remains a small probability (smaller with higher Evaluation Assurance Levels) that exploitable vulnerabilities may be discovered after an evaluation has been completed. This report reflects the CESG Certification Body's view at the time of certification.

19. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the ETR was issued and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

20. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE. However, note that unevaluated patching will invalidate the certification of the TOE, unless the TOE has undergone a formal re-certification or is covered under an approved Assurance Continuity process by a CCRA certificate-authorising Scheme.

21. All product or company names used in this report are for identification purposes only and may be trademarks of their respective owners.

II. TOE SECURITY GUIDANCE

Introduction

22. The following sections provide guidance of particular relevance to purchasers of the TOE.

Delivery

23. On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and check that the security of the TOE has not been compromised in delivery.

24. [CCECG] sections "Verification of Installation Media" and "Secure Delivery of Common Criteria Documentation" direct the consumer to:

a) Inspect the received media kit, ensuring it is shrink wrapped with a label detailing the Tracing Number and stating "Citrix XenDesktop 4.0 Media Kit – Multi Language", and that the box is labelled "Citrix XenDesktopTM 4" with the part number 120-0032.

b) Open the media kit and verify it contains the DVD labelled "Citrix XenDesktop Domain Delivery Controller v4 English", with part number 745-0101. In the kit, this is the only DVD required for installing the TOE. It includes the Client On-line Plug-in (COP).

c) Download the TOE related documentation from the Citrix website using HTTPS.

Installation and Guidance Documentation

25. The TOE is supplied on a set of installation media, used to install the components identified in [ST] Section 1.4.2. Administering XenDesktop [XD_ADMIN] recommends an appropriate sequence for installation, reflecting dependencies of components, whereas [CCECG] includes guidance on installing and configuring the TOE for the evaluated configuration.

26. The Installation and Secure Configuration documentation is as follows:

a) Administering XenDesktop [OP];

b) Common Criteria Evaluated Configuration Guide for Citrix XenDesktop 4 Platinum Edition [CCECG];

c) Citrix Licensing 11.6.1 (License Server 11.6.1) [LS];

d) Online Plug-in 11.2 for Windows [OP];

e) Web Interface 5.2 [WI].

27. The User Guide and Administration Guide documentation is as follows:

a) [CCECG] Appendix A "Operational Guidance for XenDesktop Administrators";

b) [CCECG] Appendix B, "Operational Guidance for XenDesktop Users".

III. EVALUATED CONFIGURATION

TOE Identification

28. The TOE is Citrix XenDesktop 4 Platinum Edition, which consists of:

a) Desktop Delivery Controller (DDC) v4.0;

b) Delivery Services Console (DSC) v3.0;

c) Presentation Server Console (PSC) v4.5;

d) Web Interface (WI) (including Web Interface Management Console (WIMC)) v5.2;

e) Virtual Desktop Agent (VDA) v4.0;

f) Citrix Online Plug-in (COP) v11.2.

TOE Documentation

29. The relevant guidance documentation for the evaluated configuration is identified in Chapter II (in 'Installation and Guidance Documentation') of this report.

TOE Scope

30. The TOE Scope is defined in the Security Target [ST] Sections 1.4.1 and 1.4.2. Functionality that is outside the TOE Scope is defined in [ST] Section 1.4.3. It should be noted that the capability for Desktop users to belong to multiple desktop groups is not included, i.e. a Desktop user can only use a virtual desktop from one desktop group.

TOE Configuration

31. The evaluated configuration of the TOE is defined in [ST] Section 1.4 and [CCECG].

32. The physical boundary of the TOE encompasses the TOE Server components and the TOE Client component, as illustrated in Figure 1 below:

a) The TOE Server components comprise the Desktop Delivery Controller (including the Delivery Services Console and Presentation Server Console), the Web Interface, the Data store, the VM Host and the Virtual Desktop Agents.

b) The TOE Client component is the Citrix online plug-in running on a User Device.

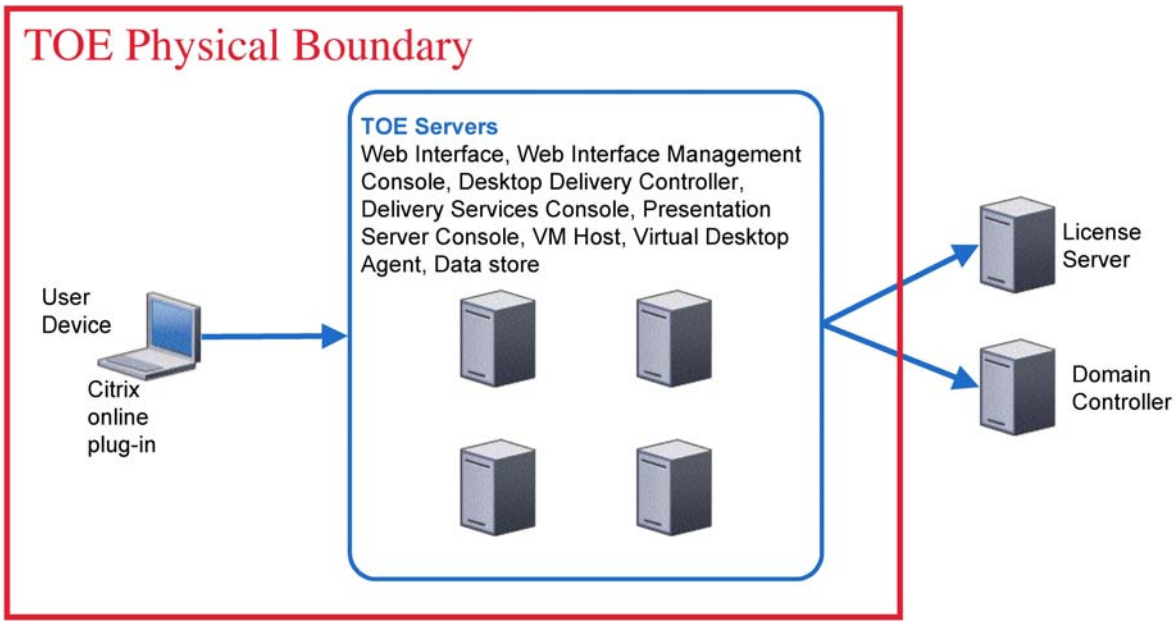

Figure 1 - TOE Physical Boundary

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

34. The Citrix online plug-in runs on the User Device, while the other components run on servers (in a variety of possible configurations). The logical boundaries of the TOE are illustrated below in Figure 2, where elements shown shaded are components of the TOE.

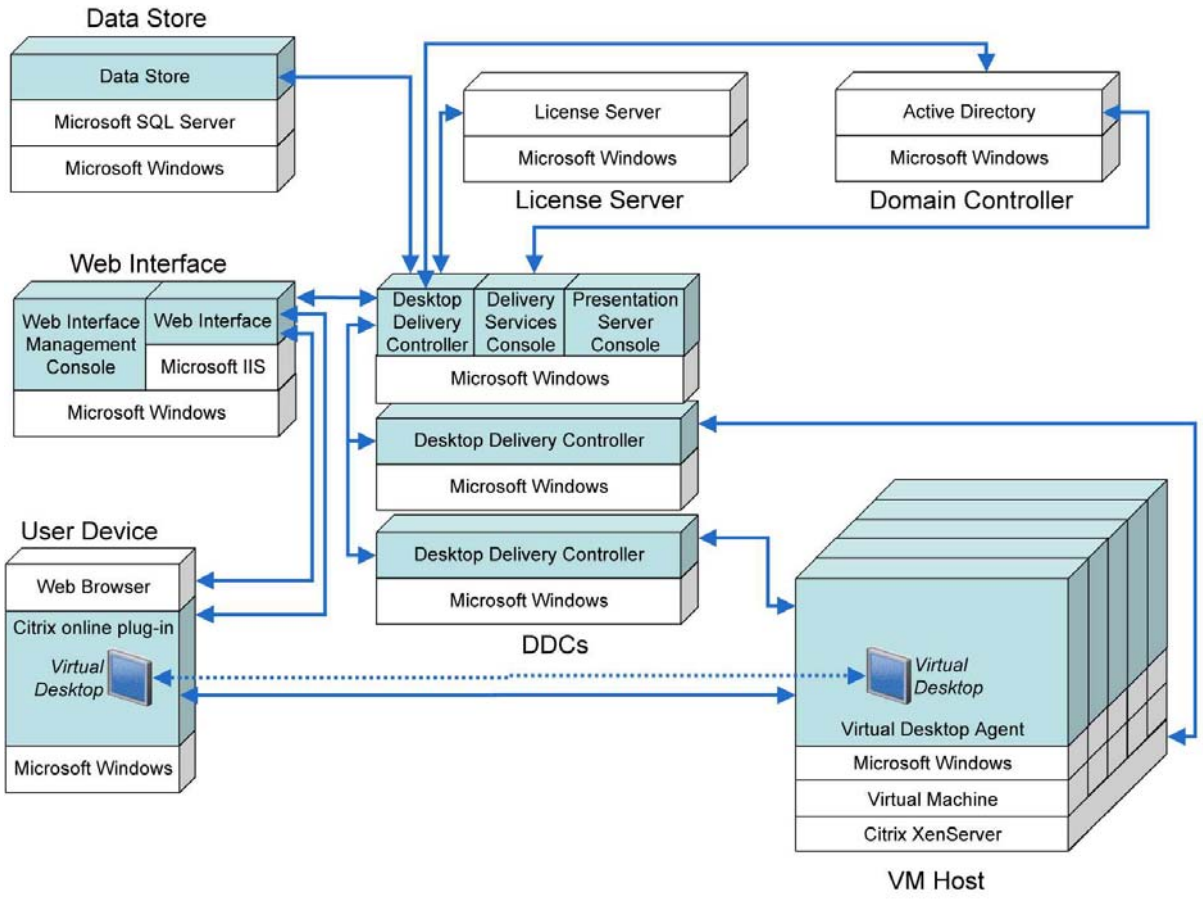

Figure 2 – TOE Logical Boundaries

Environmental Requirements

35. The environmental assumptions for the TOE are stated in [ST] Section 3.5.

36. The environmental IT configuration is detailed in [ST] Section 1.2.3 and [CCECG].

37. The environmental IT configuration is as follows:

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

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

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

- Microsoft Windows Server 2003, 32-bit Edition, Enterprise Edition, R2, SP2;
- Microsoft .NET Framework 3.5, SP1;
- Java Runtime Environment (JRE) 1.6.0_20;
- Microsoft Internet Information Server (IIS) 6.0;
- Microsoft ASP.NET 2.0.

c) The DDC requires a Data store with the following software:

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

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

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

e) Each Virtual desktop will require the following software:

- Microsoft Windows Vista 32-bit Ultimate SP1; or
- Windows XP Professional 32-bit SP3.

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

- Citrix XenServer 5.6, Platinum Edition

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

- Microsoft Active Directory Server in native mode.

Test Configuration

38. The Developer's environment is configured according to [CCECG], which the evaluators confirmed is consistent with [ST] Sections 1.4 and 1.2.3.

39. The Evaluators used the same configuration for their testing as that used by the Developer. The only exception to this was during the course of re-running one of the developer's test cases:

a) in this instance, Wireshark was installed onto the Web Interface machine directly, instead of being installed on a separate laptop;

b) the Evaluators determined that this change had no impact on the TOE or on the functionality being tested.

40. The following server components were provided for evaluator testing:

a) DDC running Delivery Services Console, Presentation Server Console, Web Interface and License Server;

b) VM Hosting infrastructure, to be comprised of single XenServer 5.6 host;

c) Domain Controller, running Microsoft Active Directory Server.

41. The following virtual desktops were made available:

a) Microsoft Windows Vista 32-bit Enterprise;

b) Windows XP Professional 32-bit SP3.

42. Two User Device PCs were provided:

a) For domain-joined User Device: Microsoft Windows XP Professional SP3;

b) For non-domain-joined User Device: Windows Vista SP1.

IV. PRODUCT ARCHITECTURE

Introduction

43. This Chapter gives an overview of the main TOE architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration' of this report.

Product Description and Architecture

44. The architecture of the TOE is described in [ST] Sections 1.3 and 1.4.2. XenDesktop provides a complete virtual desktop delivery system, by integrating several distributed components with advanced configuration tools that simplify the creation and real-time management of the virtual desktop infrastructure. The core components of XenDesktop are illustrated in Figure 3 below.

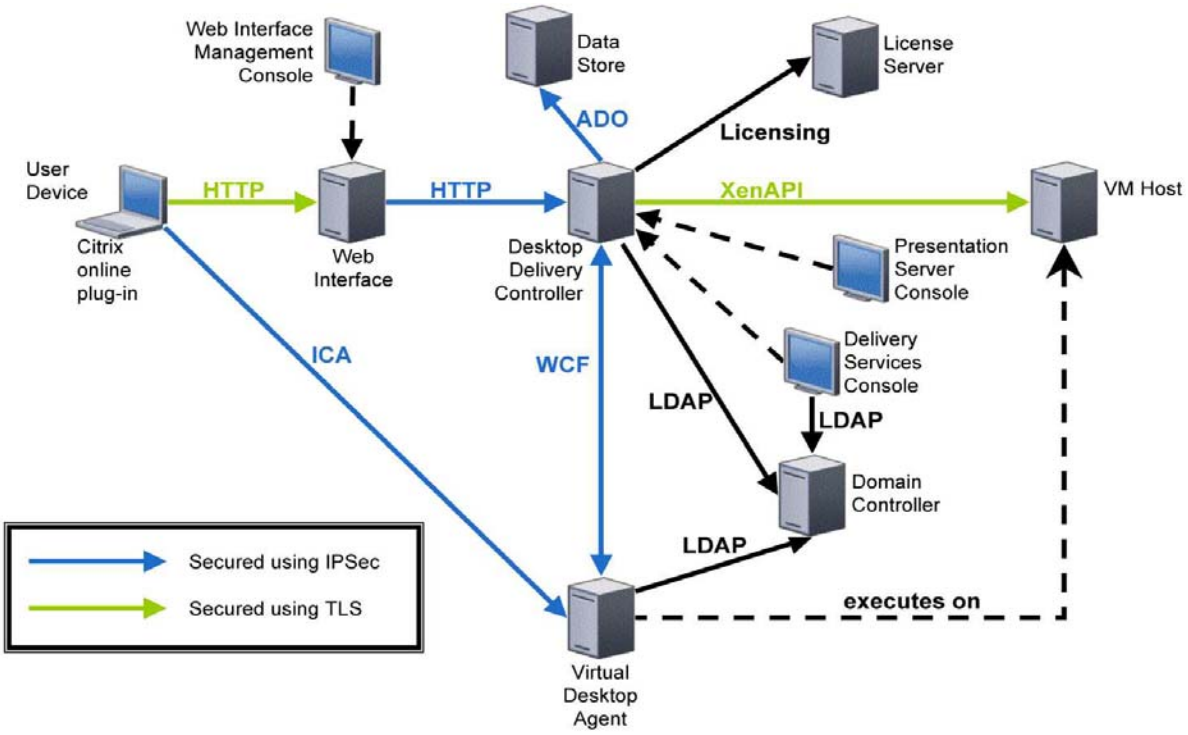

Figure 3 - XenDesktop Components

TOE Design Subsystems

45. The TOE subsystems, and their security features/functionality, are as follows:

a) The Citrix on-line plug-in - Installed on user devices, the Citrix online plug-in enables direct Independent Computing Architecture (ICA) connections from user devices to virtual desktops.

b) Web Interface - Installed on a server in the data centre, Web Interface is used to give authorised desktop users access through the Web or intranet to the virtual desktops that they are authorised to use. Desktop users log on to Web Interface using an Internet browser and are given the ICA file that the Citrix online plug-in needs to connect to the Virtual Desktop Agent for access to an authorised virtual desktop.

c) Web Interface Management Console - This provides an administration interface to Web Interface, making use of Windows authentication for administrators. It provides administrators with functions to manage the configuration of Web Interface, including setting the desktop user authentication method. This is installed on the Web Interface server.

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

e) Datastore - This stores the Configdata managed by the administrators with the Delivery Services Console and Presentation Server Console, including the Endpoint data access control policy, configuration of virtual desktops, desktop users' access permissions for virtual desktops and access permissions for administrators.

f) Delivery Services Console - This provides an administration interface to the Desktop Delivery Controller, making use of Windows authentication for administrators. It provides administrators with a number of functions, to manage the configuration of virtual desktops and manage desktop users' access permissions for virtual desktops. This is installed on the Desktop Delivery Controller.

g) Presentation Server Console - This provides an administration interface to the Desktop Delivery Controller, making use of Windows authentication for administrators. It provides administrators with a function to manage the Endpoint data access control policy. This is installed on the Desktop Delivery Controller.

h) Virtual Desktop Agent - Installed on virtual desktops, the agent enables direct ICA (Independent Computing Architecture) connections between the virtual desktop and the desktop user's User Device.

TOE Dependencies

46. The TOE dependencies on the IT environment are identified in Chapter III 'Environmental Requirements' of this document.

TOE Interfaces

47. The external TOE Security Functions Interface (TSFI) is shown in Figure 4 below.

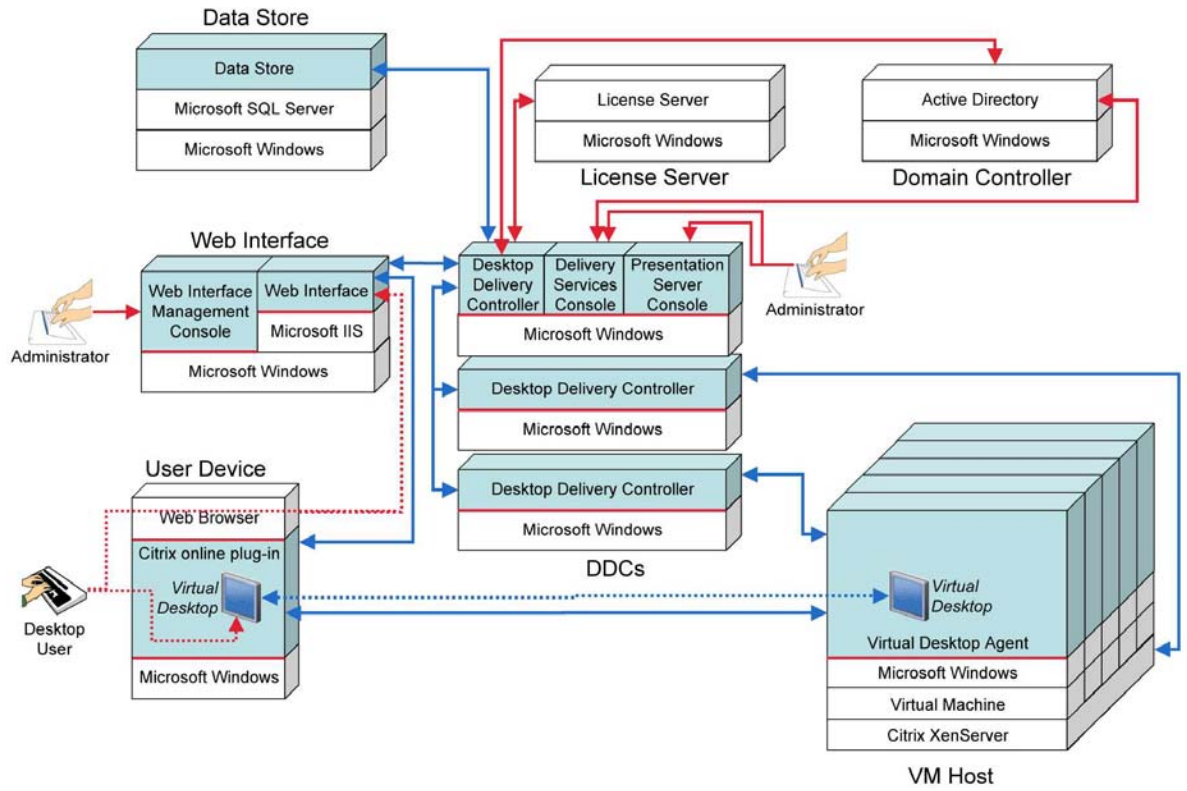

Figure 4 - Interfaces to XenDesktop and Between Components

48. In Figure 4, elements shown shaded are components of the TOE. Red lines represent interfaces into the TOE (i.e. user interfaces and interfaces with external components including the operating system). Blue lines between TOE components represent interfaces that are internal to the TOE (note however, that these are delivered through the underlying network mediated by the operating system). To avoid over-complicating this diagram, other interfaces that are entirely outside the TOE (for example, between a Desktop user and the operating system on their User Device, or between the operating system on each server and the domain controller) are not shown.

49. The interactions between the components, to provide a virtual desktop to a desktop user, are detailed in [ST] Section 1.3.

V. TOE TESTING

TOE Testing

50. The Developer's tests covered:

a) all SFRs;

b) all Security Functions (SFs);

c) the TSFI, as identified in Chapter IV (in 'TOE Interfaces') of this report.

51. The Developer carried out testing on all combinations of hardware as described in Chapter III (in 'Test Configuration') of this report.

52. The Evaluators repeated 6 of the Developer's manual test cases. The Evaluators confirmed the results were consistent with those reported by the Developer.

53. The Evaluators devised and ran 11 independent functional tests, different from those performed by the Developer. No anomalies were found.

54. The Evaluators also devised and ran 7 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

55. The Evaluators carried out testing on the hardware combination described in Chapter III (in 'Test Configuration') of this report.

56. The Evaluators finished running their penetration tests on 6th August 2010.

Vulnerability Analysis

57. The Evaluators' vulnerability analysis, which preceded penetration testing and was reported in [ETR], was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables.

58. The Microsoft workaround presented in Microsoft Security Advisory 977377 for the Transport Layer Security (TLS) renegotiation issue cannot be implemented in the evaluated configuration of the TOE, if smartcard authentication is required, as renegotiation of the TLS session is required to support client certificate authentication. The Evaluators concluded that this potential vulnerability is not exploitable in the TOE, and does not constitute a residual vulnerability in the TOE as, even if it is exploited, it cannot be used to undermine the security properties of the TOE.

Platform Issues

59. The platform on which the TOE is installed should meet the requirements specified in [ST] Section 1.2.3 and Chapter III (in 'Environmental Requirements') of this report.

VI. REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation (comprising Parts 1, 2, 3: [CC1], [CC2], [CC3]).

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1, Introduction and General Model, Common Criteria Maintenance Board, CCMB-2009-07-001, Version 3.1 R3, July 2009.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2, Security Functional Components, Common Criteria Maintenance Board, CCMB-2009-07-002, Version 3.1 R3, July 2009.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3, Security Assurance Components, Common Criteria Maintenance Board, CCMB-2009-07-003, Version 3.1 R3, July 2009.

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, Participants in the Arrangement Group, May 2000.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Common Criteria Maintenance Board, CCMB-2009-07-004, Version 3.1 R3, July 2009.

[CCECG] Common Criteria Evaluated Configuration Guide for Citrix XenDesktop 4 Platinum Edition, Citrix Systems Inc,, document code August 12 2010 10:09:00, Version 1.0, 12 August 2010.

[ETR] Evaluation Technical Report: Citrix XenDesktop 4 Platinum Edition, SiVenture CLEF, LFV/T005, CIN2-TR-0001, Version 1-0, 16 August 2010.

[ETRSup1] Review Form, containing Certifier Comments and Evaluator Responses, CESG Certification Body, CB/100818/LFV/T005, 18 August 2010, updated 20 August.

[ETRSup2] Review Form, containing Certifier Comments and Evaluator Responses, CESG Certification Body, CB/100820/LFV/T005, 20 August 2010, updated 20 August.

[LS] Citrix Licensing 11.6.1 (Licence Server 11.6.1),
Citrix Systems Inc.,
document code 19 July 2010 10:18:12, Version 0.9, 19 July 2010.

[MRA] Mutual Recognition Agreement of Information Technology Security Evaluation Certificates,
Management Committee,
Senior Officials Group – Information Systems Security (SOGIS),
Version 3.0, 8 January 2010 (effective April 2010).

[OP] Online Plug-in 11.2 for Windows,
Citrix Systems Inc.,
document code 19 July 2010 10:20:38, Version 0.9, 19 July 2010.

[ST] Common Criteria Security Target for Citrix XenDesktop 4 Platinum Edition,
Citrix Systems Inc,
CIN2-ST-0001, Version 1-0, 17 August 2010.

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.6, December 2009.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.3, December 2009.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.2, December 2009.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.4, December 2009.

[WI] Web Interface 5.2,
Citrix Systems Inc.,
document code 19 July 2010 10:17:17, Version 0.9, 19 July 2010.

[XD_ADMIN] Administering XenDesktop,
Citrix Systems Inc,
document code 19 July 2010 10:19:48, Version 0.9, 19 July 2010.

VII. ABBREVIATIONS

This list of abbreviations is specific to the TOE. It therefore excludes: general IT abbreviations (e.g. GUI, HTML, LAN, PC); standard CC abbreviations (e.g. TOE, TSF) covered in CC Part 1 [CC1]; and UK Scheme abbreviations (e.g. CESG, CLEF) covered in [UKSP00].

COP	Client Online Plug-in
DDC	Desktop Delivery Controller
DSC	Delivery Services Console
ICA	Independent Computing Architecture
PSC	Presentation Server Console
TLS	Transport Layer Security
VDA	Virtual Desktop Agent
WI	Web Interface
WIMC	WI Management Console

This page is intentionally blank.