122

CERTIFICATION REPORT No. CRP271

Citrix XenDesktop
Version 5.6 Platinum Edition

Running on *Server Components*:
Microsoft Windows Server 2008 R2 SP1, Enterprise Edition, 64-bit
and *User Devices and VMs*:
Microsoft Windows 7 Ultimate SP1, 32-bit or 64-bit

Issue 1.0

November 2012

CESG Certification Body
AAS 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 Version 5.6 Platinum Edition		
Platform:	*Server Components*: Microsoft Windows Server 2008 R2 SP1, Enterprise Edition, 64-bit. *User Devices and VMs*: Microsoft Windows 7 Ultimate SP1, 32-bit or 64-bit.		
Description:	Citrix XenDesktop 5.6 Platinum Edition is a desktop virtualisation product that centralises and delivers Microsoft Windows 7 virtual desktops as a service to users anywhere.		
CC Version:	Version 3.1 Revision 3		
CC Part 2:	Extended	CC Part 3:	Conformant
EAL:	EAL2 Augmented by ALC_FLR.2		
PP Conformance:	None		
CLEF:	SiVenture		
CC Certificate:	P271	Date Certified:	30 November 2012

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 Parts 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 Version 5.6 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 of Citrix XenDesktop Version 5.6 Platinum Edition should understand the specific scope of the certification by reading 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 20th November 2012:

- **Citrix XenDesktop Version 5.6 Platinum Edition**

4. It is abbreviated to 'XenDesktop' in this report.

5. The Developer was Citrix Systems Inc.

6. The TOE is a desktop virtualisation product that centralises and delivers Microsoft Windows 7 virtual desktops as a service to users anywhere. Virtual desktops are dynamically assembled on demand, providing users with pristine[2], yet personalised, desktops each time they log on. This ensures that performance never degrades. 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 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.

8. The TOE excludes some Citrix components which are normally included in the XenDesktop product; those exclusions are listed in Section 1.4.3 of [ST]. In addition, the following features of XenDesktop are not included in the scope of the evaluation:

a) Server-side and client-side application virtualisation is not included in the evaluation; 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 included in the evaluation.

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 in the evaluation, nor is the capability for desktop users to be assigned multiple desktops in a desktop group: i.e. in the evaluated configuration, a Desktop user can only use one virtual desktop from one desktop group.

f) The ability for administrators to automatically create virtual desktops using Machine Creation Services is not included in the evaluation, i.e. only virtual desktops of type 'existing', created explicitly by an administrator, are included in the evaluation.

g) The ability for administrators to deploy Personal vDisks for users is not included in the evaluation.

9. 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 Section 1.2.3 of [ST].

Security Target

10. 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 Section 5 of [ST].

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

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

Evaluation Conduct

13. The TOE’s SFRs and the security environment, together with much of the supporting evaluation deliverables, remained mostly unchanged from that of Citrix XenDesktop Version 4, which had previously been certified [CRP256] by the UK IT Security Evaluation and Certification Scheme to EAL2 augmented by ALC_FLR.2.

14. 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 November 2012, were reported in the Evaluation Technical Report [ETR].

Evaluated Configuration

15. The TOE should be used in accordance with the environmental assumptions specified in the Security Target [ST]. 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.

16. 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 download, installation, configuration and operation of the TOE.

Conclusions

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

Recommendations

18. Chapter II 'TOE Security Guidance' of this report includes a number of recommendations regarding the secure download, installation, configuration and operation of the TOE.

19. In addition, the Evaluators' comments and recommendations are as follows:

- All guidance necessary to determine that the TOE has been securely downloaded and to securely install and operate the TOE is provided in, or referenced from [CCECG], which is available for download from the Common Criteria link from the Citrix Security webpage http://www.citrix.com/support/security-compliance.

20. The TOE relies on Microsoft SQL Server 2008 R2 to provide a database for configuration data, and Citrix XenServer 6.0.2 Platinum Edition to provide the VM Host. System integrators and risk owners using the TOE should therefore make suitable arrangements to satisfy themselves that these components are also in their evaluated configuration as recommended in *'Pre Installation Tasks'* of [CCECG].

21. When installing the operating system on machines in the evaluated configuration, the consumer should ensure that all applicable patches, security updates, and hotfixes are applied, as recommended in [CCECG].

Disclaimers

22. This Certification Report and associated Certificate applies only to the specific version of the produced in its evaluated configuration. This is specified in Chapter III 'Evaluated Configuration' of this report. The ETR on which this Certification Report is based relates only to the specific items tested.

23. 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.

24. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the date of the penetration tests (as detailed in Chapter V) and, if appropriate, should check with the Vendor to see if any patches exist for the product and whether those patches have further assurance.

25. The installation of patches for security vulnerabilities, whether or not those patches have further assurance, should improve the security of the TOE but should only be applied in accordance with a consumer's risk management policy. 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.

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

27. Note that the opinions and interpretations stated in this report under 'Recommendations' and 'TOE Security Guidance' are based on the experience of the CESG Certification Body in performing similar work under the Scheme.

II. TOE SECURITY GUIDANCE

Introduction

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

Delivery and Installation

29. Before installation of the TOE, the consumer is recommended to check that the evaluated version has been downloaded, and to check that the security of the TOE has not been compromised. Specific advice on download and installation is provided in the following documents of the TOE:

a) *'Before You Begin'* section of [CCECG];

b) *'To Update the Virtual Desktop Agent'* section of [CCECG];

c) *'Secure Delivery of Common Criteria Documentation'* section of [CCECG].

30. The TOE is available for download from the Downloads section of My Citrix (http://www.citrix.com/mycitrix). An MD5 checksum accompanies each download package and is available from the download page, which is secured using Secure Sockets Layer (SSL). The customer is instructed to verify the checksum in [CCECG], Chapter 4, *'Before You Begin'*. The following file name and checksum comprise the TOE:

File Name:	XenDesktop56.iso
Checksum (MD5):	64a9146af44a6085a727f9427f57d01d

31. The above iso file includes the following components:

- Desktop Delivery Controller (DDC) v5.6
- Desktop Studio (DS) v5.6
- Web Interface (WI) (including Web Interface Management Console (WIMC)) v5.4
- Virtual Desktop Agent (VDA) v5.5.100
- Citrix Receiver (CR) v3.1
- Online Plug-in v13.1

32. The TOE also includes the following patch files for the VDA (downloaded separately): XdsAgent_x64.msi and XdsAgent_x86.msi, as described in [CCECG], Chapter 4, *'To Update the Virtual Desktop Agent'*.

33. It should be noted that the VDA, when installed in its unpatched state, is visible to users as v5.5.100, but in the installed evaluated configuration (with patch applied) it is visible to users as v5.5.107. Thus the versions are consistent with those in Section 1.4.2 of [ST].

34. The customer is directed to [CCECG] Chapter 1, *'Secure Delivery of Common Criteria Documentation'*, to download the TOE related documentation from the Citrix website over HTTPS.

Guidance Documentation

35. The [CCECG] includes guidance on installing and configuring the TOE as required for the evaluated configuration.

36. Specific configuration advice is provided in the Secure Configuration documentation:

a) [CCECG] Common Criteria Evaluated Configuration Guide for Citrix XenDesktop 5.6 Platinum Edition;

b) [LS] Citrix Licensing 11.10;

c) [OP] Online Plug-in for Windows 12.1[3].

d) [REC] Receiver for Windows 3.1;

e) [WI] Web Interface 5.4;

f) [XD_5.6] XenDesktop 5.6;

g) [XD_ADMIN] Manage (Managing XenDesktop 5).

37. 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'*.

[3] In the TOE, the Online Plug-in is v13.1, but the document reference title states v12.1 since there were no changes that were necessary for v13.1.

III. EVALUATED CONFIGURATION

TOE Identification

38. The TOE is Citrix XenDesktop Version 5.6, which consists of:

a) Desktop Delivery Controller (DDC) v5.6;

b) Desktop Studio (DS) v5.6;

c) Web Interface (WI) (including Web Interface Management Console (WIMC)) v5.4;

d) Virtual Desktop Agent (VDA) v5.5.107;

e) Citrix Receiver (CR) v3.1 with Online Plug-in v13.1.

TOE Documentation

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

TOE Scope

40. 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 in the evaluation, nor is the capability for desktop users to be assigned multiple desktops in a desktop group: i.e. in the evaluated configuration, a Desktop user can only use one virtual desktop from one desktop group.

TOE Configuration

41. The evaluated configuration of the TOE is defined in [ST] Section 1.4 and specific configuration advice is provided in [CCECG].

42. The physical boundary of the TOE encompasses the TOE Server components and the TOE Client component (as illustrated in Figure 1):

a) the TOE Server components comprise the Desktop Delivery Controller (including Desktop Studio), the Web Interface, the Database, the Virtual Machine (VM) Host and the Virtual Desktop Agents;

b) the TOE Client component is the Citrix Receiver running on a User Device.

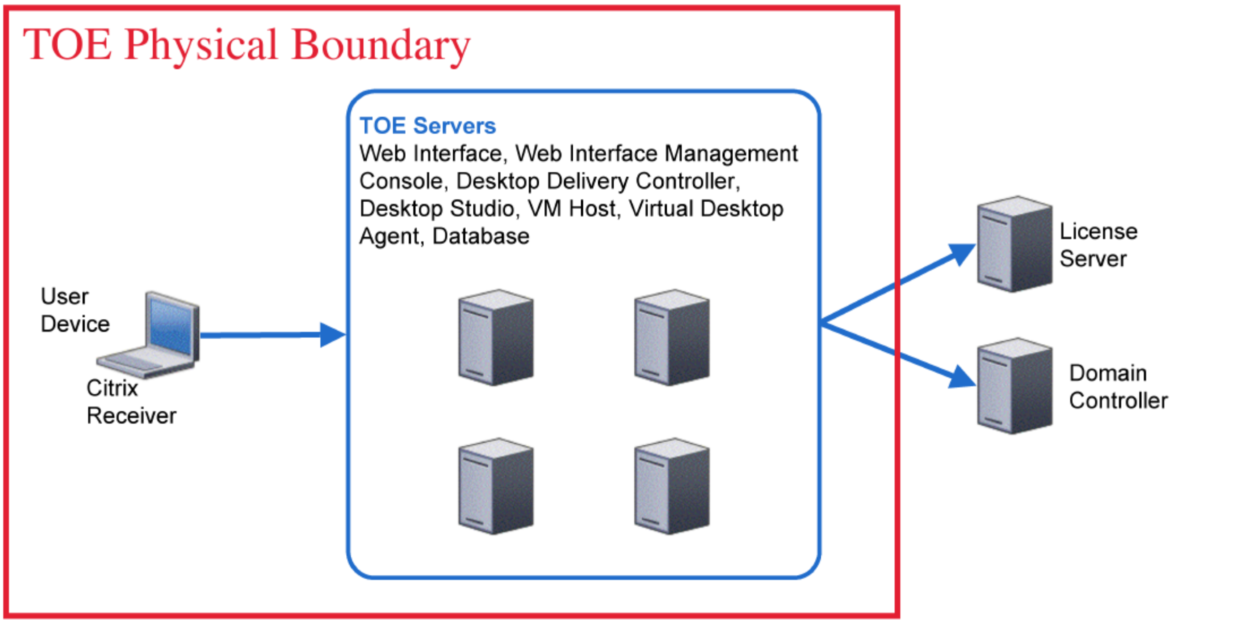
TOE Physical Boundary
TOE Servers
Web Interface, Web Interface Management Console, Desktop Delivery Controller, Desktop Studio, VM Host, Virtual Desktop Agent, Database
User Device
Citrix Receiver
License Server
Domain Controller

Figure 1 TOE Physical Boundary

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

44. The Citrix Receiver 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 shaded elements are components of the TOE.

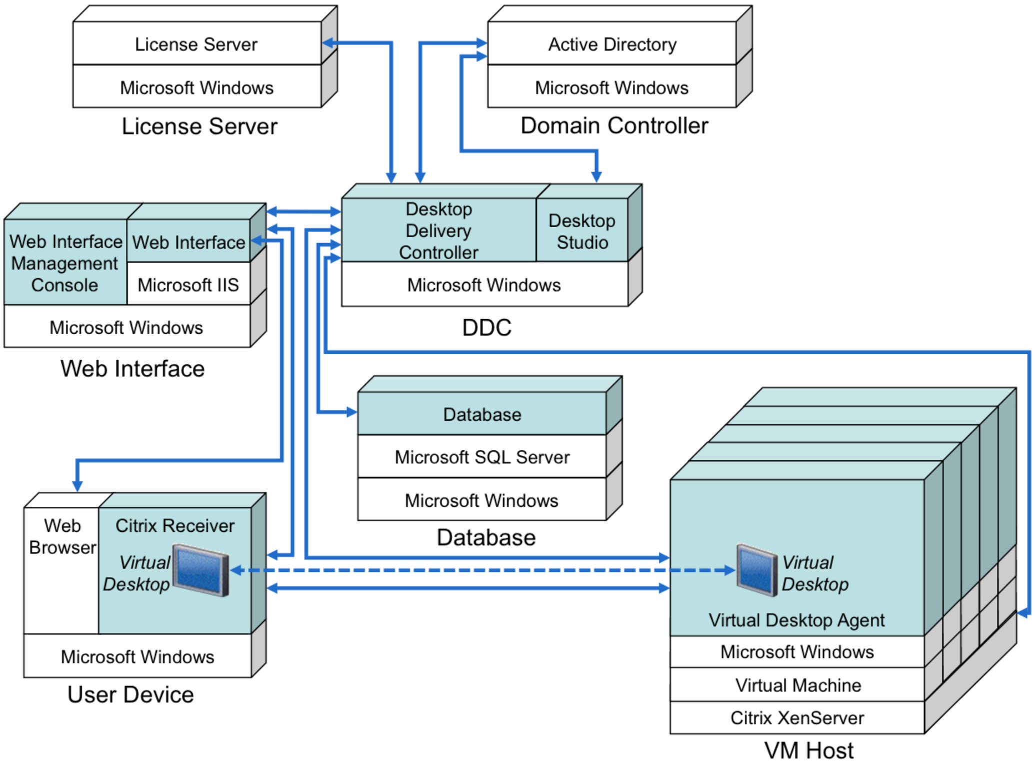

Figure 2 Logical Boundaries

Environmental Requirements

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

46. The TOE was evaluated running Microsoft Windows Server 2008 R2 SP1 (64-bit) on the server components and Microsoft Windows 7 Ultimate SP1 (32-bit or 64-bit) on the User Devices and Virtual Machines.

47. The environmental IT configuration, detailed in [ST] section 1.2.3 and [CCECG], 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 2008 R2 SP1, Enterprise Edition, 64-bit;
- Microsoft .NET Framework 3.5, SP1;
- Microsoft Internet Information Server (IIS) 7.5;

- Microsoft ASP.NET 2.0;
- Microsoft Visual J# 2.0 Second Edition Redistributable Package.

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

- Microsoft Windows Server 2008 R2 SP1, Enterprise Edition, 64-bit.

c) For the Desktop Delivery Controller (DDC) including Desktop Studio (DS), a server is required with the following software:

- Microsoft Windows Server 2008 R2 SP1, Enterprise Edition, 64-bit;
- Microsoft .NET Framework 3.5, SP1;
- Microsoft Internet Information Server (IIS) 7.5;
- Microsoft ASP.NET 2.0.

d) The DDC requires a Database with the following software:

- Microsoft Windows Server 2008 R2 SP1, Enterprise Edition, 64-bit;
- Microsoft SQL Server 2008 R2.

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

- Microsoft Windows 7 Ultimate SP1, 32-bit; or
- Microsoft Windows 7 Ultimate SP1, 64-bit.

f) Each Virtual Desktop will require the following software:

- Microsoft Windows 7 Ultimate SP1 32-bit; or
- Microsoft Windows 7 Ultimate SP1 64-bit.

g) The virtual desktops will be provided on the hosting infrastructure, which requires at least one server running Citrix XenServer 6.0.2 Platinum Edition.

h) 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 Configurations

48. The Developers used the following configuration for their testing:

a) The XenDesktop hardware and software used for testing was consistent with that specified in [CCECG] and in [ST] Sections 1.4 and 1.2.3.

49. The Evaluators used the following configuration for their testing:

a) They used the same configuration for their testing as that used by the Developers.

b) The only exception to that was identified during the on-site repeat of developer testing, where an Internet Explorer setting to ‘Check for Publisher’s Certification Revocation’ (Internet Explorer > Internet Options > Advanced > Security) was prohibiting the developer testing from being repeated within a timely manner, as it resulted in Desktop Studio taking a long time to launch (approximately 10 minutes). That was because this setting was trying to look for a revocation list using the internet, and the test environment was not connected to the internet. The ‘Check for Publisher’s Certification Revocation’ setting was therefore disabled for the purposes of evaluator on-site testing. The evaluators determined that this change had no impact, for the purposes of the evaluation, on the TOE or on the server functionality that was being tested.

c) The following server components were provided for evaluator testing:

- DDC running Desktop Studio;
- Web Interface (and Web Interface Management Console);
- License Server;
- VM Hosting Infrastructure, comprising 2 XenServer 6.0.2 hosts;
- Smartcard enrolment station;
- XenServer Management Console Server;
- Database running Microsoft SQL Server 2008 R2;
- Domain Controller, running Microsoft Active Directory Server; and
- Storage Server used to house the virtual machines.

d) The following 4 virtual desktops were made available:

- Microsoft Windows 7 Ultimate SP1 (2 x 32-bit and 2 x 64-bit).

e) The following 4 User Device PCs were made available:

- 2 domain-joined and 2 non-domain-joined PCs running Microsoft Windows 7 Ultimate SP1 (2 x 64-bit and 2 x 32-bit respectively).

IV. PRODUCT ARCHITECTURE

Introduction

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

Product Description and Architecture

51. 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.

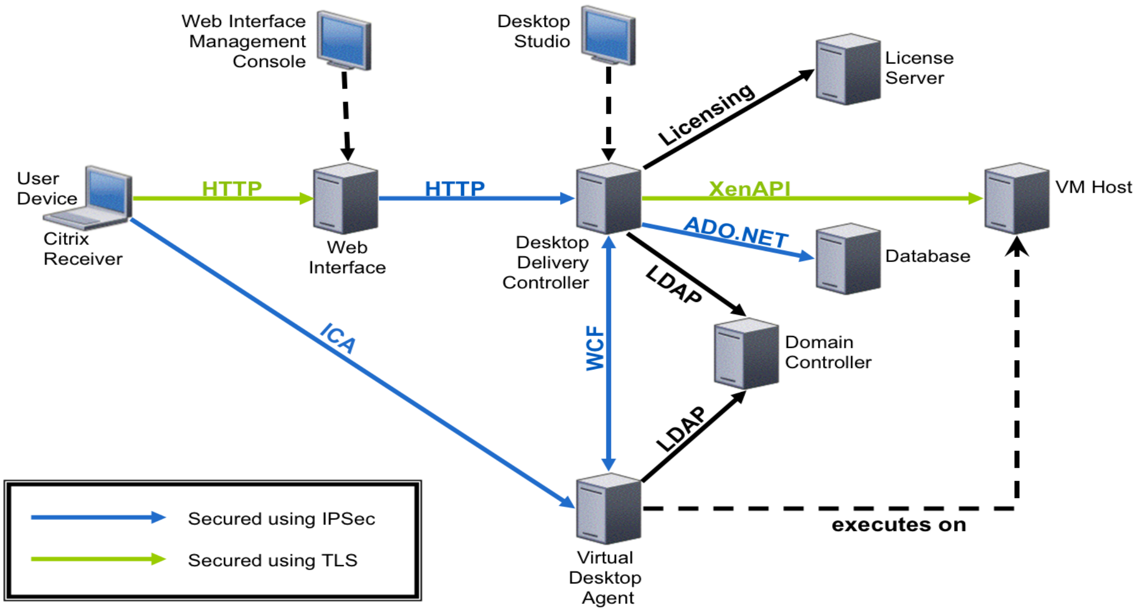

Figure 3 XenDesktop Components

TOE Design Subsystems

52. The high-level TOE subsystems, and their security features/functionality, are as follows:

a) **Desktop Delivery Controller (DDC)**. Installed on servers in the data centre, the DDC requires that desktop users are authenticated, manages the assembly of desktop users' virtual desktop environments and access permissions for administrators, 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.

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

c) **Citrix Receiver (CR) (and online plug-in).** Installed on user devices, the CR enables direct ICA connections from user devices to virtual desktops.

d) **Web Interface (WI).** Installed on a server in the data centre, WI 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 WI using an Internet browser and are given the ICA file that the CR needs to connect to the VDA for access to an authorised virtual desktop.

e) **Desktop Studio (DS).** This provides an administration interface to the DDC, making use of Windows authentication for administrators. The DS provides administrators with a number of functions, to manage the configuration of virtual desktops and manage desktop users' access permissions for virtual desktops, and provides administrators with a function to manage the Endpoint data access control policy. The DS is installed on the DDC.

f) **Web Interface Management Console (WIMC).** This provides an administration interface to WI, making use of Windows authentication for administrators. The WIMC provides administrators with functions to manage the configuration of WI, including setting the desktop user authentication method. The WIMC is installed on the WI server.

g) **Database.** This stores the configuration data managed by the administrators with the Desktop Studio, including the Endpoint data access control policy, configuration of virtual desktops, desktop users' access permissions for virtual desktops and access permissions for administrators, as well as data used by the Desktop Delivery Controller to manage virtual desktops, users and sessions.

TOE Dependencies

53. The TOE dependencies on the IT environment are identified in Chapter III 'Environmental Requirements' of this report:

TOE Interfaces

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

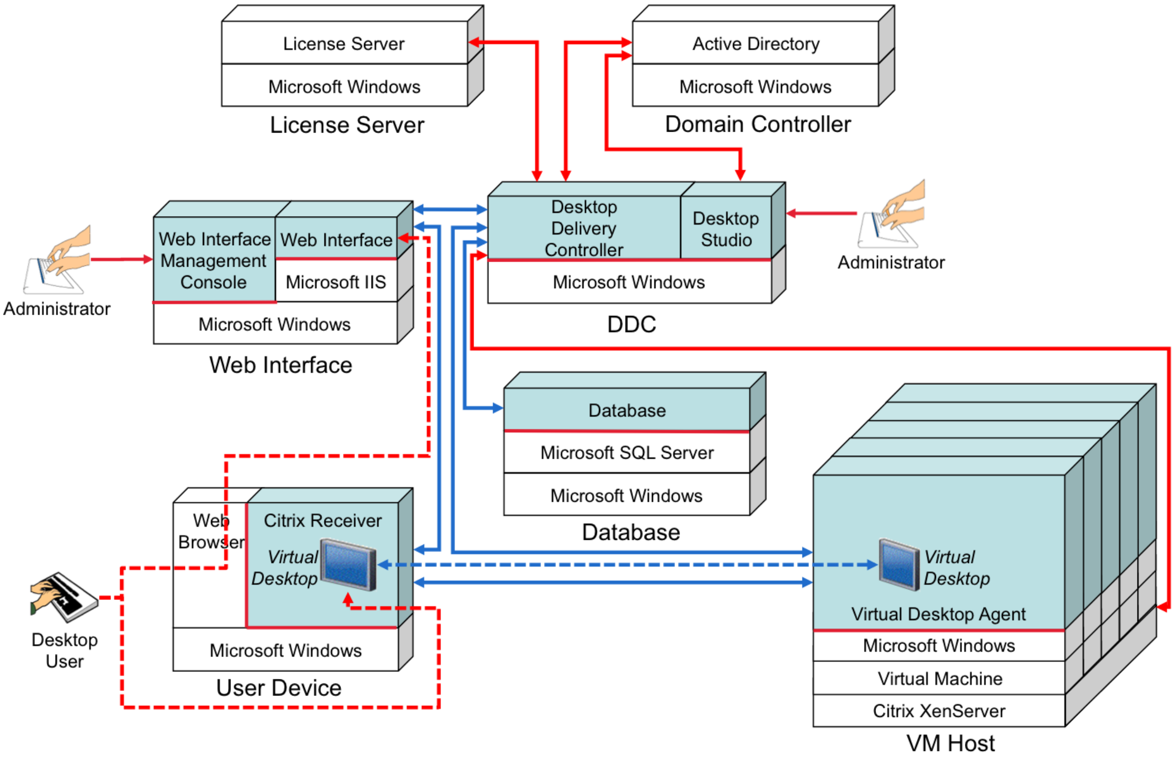

Figure 4 Interfaces to XenDesktop and between components

55. In Figure 4 above, 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.

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

V. TOE TESTING

Developer Testing

57. The Developer's security tests covered:

- all SFRs;
- all TOE high-level subsystems, as identified in Chapter IV (in 'TOE Design Subsystems') of this report;
- all Security Functions (SFs);
- the TSFI, as identified in Chapter IV (in 'TOE Interfaces') of this report.

58. The Developer's security tests also included those TOE interfaces which are internal to the product and thus had to be exercised indirectly. The Evaluators witnessed a sample of 8 of the Developer's security tests. The Evaluators confirmed the results were consistent with those reported by the Developer.

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

Evaluator Testing

60. The Evaluators devised and ran a total of 12 independent security functional tests, different from those performed by the Developer. No anomalies were found.

61. The Evaluators also devised and ran a total of 9 security penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

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

63. The Evaluators completed their penetration tests on 12th October 2012.

Vulnerability Analysis

64. 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.

65. A new security bulletin (CTX134681) was released during the evaluation (but prior to on-site evaluator testing) which affected the version of Citrix Receiver (with Online Plug-in for Windows) used in the evaluation. This vulnerability could allow arbitrary code execution on the client device in the context of the currently logged on user. This vulnerability is present in all versions of the Citrix Receiver from Windows up to and including version 3.2 and all versions of

the Online Plug-in for Windows up to and including version 12.1. A patch is available for this vulnerability in later versions. However, it was determined that **this vulnerability is not exploitable in the evaluated configuration** as it only applies to a Citrix Receiver running within a VDA – which is not implemented in the evaluated configuration. The vulnerability is further mitigated by the installation of Microsoft Hotfix KB2264104 as part of the evaluated configuration; see the *Operating System Updates* section in [CCECG].

Platform Issues

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

67. There is only one OS that can be used for the User Devices and the VMs: Microsoft Windows 7 Ultimate SP1 (32-bit or 64-bit). There are no variations in the server components. Therefore, no multi-platform rationale is deemed required.

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.

[CCECG] Common Criteria Evaluated Configuration Guide for Citrix XenDesktop 5.6 Platinum Edition,
Citrix Systems Inc.,
Document Code: November 7 2012 11:00:41, 7th November 2012.

[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.

[CRP256] Certification Report No. 256, Citrix XenDesktop 4 Platinum Edition running on Microsoft Windows Server 2003 SP2,
Issue 1.0, August 2010.

[ETR] Evaluation Technical Report,
SiVenture CLEF,
LFV/T017/ETR, CIN9-TR-0001, Issue 1-1, 20th November 2012.

[LS] Citrix Licensing 11.10,
Citrix Systems Inc.,
Version 11.10, licensing-11.10_20120418.pdf, 2011.

[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 for Windows 12.1,
Citrix Systems Inc.,
Version 1.0, online-plugin-12.1-windows_20120415.pdf, 2011.

[REC] Receiver for Windows 3.1,
Citrix Systems Inc.,
receiver_v3.1_20120415.pdf, 2011.

[ST] Common Criteria Security Target for Citrix XenDesktop 5.6 Platinum Edition,
Citrix Systems Inc.,
Issue 1-1, 16th November 2012.

[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 4.3, October 2010.

[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 5.4,
Citrix Systems Inc.,
Version 1.0, web_interface_v5.4_20120415.pdf, 2011.

[XD_5.6] XenDesktop 5.6,
Citrix Systems Inc.,
xendesktop-56_20120420.pdf, 2011.

[XD_ADMIN] Manage (Managing XenDesktop 5),
Citrix Systems Inc.,
xendesktop_managing_20120415.pdf, 2011.

Note that the references [LS], [OP], [REC], [WI], [XD_5.6] & [XD_ADMIN] are snapshots of online documents that were 'frozen' at a point in time for the purposes of the evaluation. The date in the filename is the date they were 'frozen'. The copyright notice within the document itself has a date of 2011, which is why the document date is 2011, but the filename contains 2012.

VII. ABBREVIATIONS

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

CR	Citrix Receiver
DDC	Desktop Delivery Controller
DS	Desktop Studio
HTTPS	Hypertext Transfer Protocol Secure
ICA	Independent Computing Architecture
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
SSL	Secure Sockets Layer
VDA	Virtual Desktop Agent
VM	Virtual Machine
WCF	Windows Communication Foundation
WI	Web Interface
WIMC	Web Interface Management Console