CERTIFICATION REPORT No. CRP281

Citrix XenDesktop
7.6 Platinum Edition
running on Microsoft Windows Server 2012 Datacenter Edition
and Microsoft Windows 7 Ultimate

Issue 1.0

March 2015

CESG Certification Body
Industry Enabling Services, CESG
Hubble Road, Cheltenham
Gloucestershire, GL51 0EX
United Kingdom

CERTIFICATION STATEMENT

The products detailed below have been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme ('the Scheme') and have met the specified Common Criteria (CC) [CC] requirements. The scope of the evaluation and the assumed usage environment are specified in the body of this Certification Report.			
Sponsor	Citrix Systems Inc.	Developer	Citrix Systems Inc.
Product(s), Version(s)	Citrix XenDesktop 7.6 Platinum Edition		
Platform(s)	*Server Components*: Microsoft Windows Server 2012 Datacenter Edition. *Client Devices and VMs*: Microsoft Windows 7 Ultimate.		
Description	Citrix XenDesktop Platinum Edition (hereinafter referred to as "XenDesktop") is a product that centralises and delivers Microsoft Windows virtual desktops and published applications as a service to users.		
CC Version	Version 3.1 Revision 4		
CC Part 2	Extended	CC Part 3	Conformant
PP(S) Conformance	None		
EAL or [c]PP	EAL2 Augmented by ALC_FLR.2		
CLEF	SiVenture		
CC Certificate	P281	Date Certified	19 March 2015

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 Target of Evaluation (TOE) in meeting its Security Target (ST) [ST], which prospective consumers are advised to read. To ensure that the ST gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against that baseline. Both parts of the evaluation were performed in accordance with CC Parts 1, 2 and 3 [CC], the Common Evaluation Methodology [CEM] and relevant Interpretations.

The issuing 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 (CCRA)

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 Certification 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.

SENIOR OFFICIALS GROUP – INFORMATION SYSTEMS SECURITY (SOGIS) MUTUAL RECOGNITION AGREEMENT OF INFORMATION TECHNOLOGY SECURITY EVALUATION CERTIFICATES (MRA)

The SOGIS MRA logo which appears below confirms that the conformant certificate has been authorised by a Participant to the above 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 performed 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 SOGIS 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 7.6 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 7.6 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 assurance level augmented by ALC_FLR.2 in March 2015:

- **Citrix XenDesktop 7.6 Platinum Edition running on Microsoft Windows Server 2012 Datacenter Edition and Microsoft Windows 7 Ultimate**

4. The Developer was Citrix Systems Inc.

5. Citrix XenDesktop 7.6 Platinum Edition (hereinafter referred to as "XenDesktop") is a virtualisation product that centralises and delivers Microsoft Windows virtual desktops as a service to users anywhere. Personalised virtual desktops hosted on Microsoft Windows 7 can be run on-demand each time the user logs on. This ensures that performance never degrades, while the high speed delivery protocol provides unparalleled responsiveness over any network.

6. The TOE gives access to both virtual desktops and published applications. 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.

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 the Microsoft platform components with which XenDesktop integrates. The TOE also excludes some Citrix components which are normally included in the XenDesktop product, as listed in Section 1.4.3 of [ST]. In addition, the following features of XenDesktop are not included in the scope of the evaluation:

- Only one desktop delivery method is included in the evaluation: VDI desktops. These are virtual applications each running a Windows desktop operating system, rather than running in a shared, server-based environment. These virtual desktops are delivered to physical Windows desktop machines. All other desktop delivery methods are excluded from the evaluation.

- All desktop delivery groups in the evaluation deliver desktops of the static type, meaning each user connects to the same desktop each time. Desktops of the random type are not included in the evaluation. Furthermore, administrators must pre-assign a user to each desktop, rather than allowing the desktop to be assigned to a user on first use.

- Each user in the evaluated configuration can only use one virtual desktop from one desktop delivery group. The capability for users to belong to multiple desktop delivery groups is not included in the evaluation; nor is the capability for Desktop Users to be assigned multiple desktops in a desktop delivery group.

- Only one application delivery method is included in the evaluation: XenApp published apps, also known as server-based hosted applications. These are published applications hosted from a Windows server to a Windows desktop. All other application delivery methods are excluded from the evaluation.

- In the evaluated configuration each user is given access to only a single application delivery group. The capability for users to belong to multiple application delivery groups is not included in the evaluation.

- Only Full Administrators are included in the evaluation; other delegated administrator roles are excluded.

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

- Desktop appliances and client devices other than Windows PCs are not included as User Devices in the evaluation;

- The ability for administrators to automatically create virtual desktops and servers using Machine Creation Services is not included; only virtual desktops of type ‘existing’ created explicitly by an administrator, will be included in the evaluation

- Because only virtual machines of the existing type are included, power management of virtual machines via the Delivery Controller is not included in the evaluation.

- Connection leasing is not included in the evaluation.

- Streaming applications using AppV is not included in the evaluation.

- The ability for administrators to deploy Personal vDisks for users and stream applications using AppV is not included.

- The ability for users to access their personal office PC remotely from Citrix Receiver using the Remote PC Access feature is not included.

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

10. It should be noted that the capability for Desktop Users to belong to multiple desktop Delivery Groups is not included in the evaluation. However, multiple virtual desktops may be included in a single desktop Delivery Group.

11. Furthermore, it should be noted that the capability for Application Users to belong to multiple application Delivery Groups is also not included in the evaluation. Each user is given access to only a single application delivery group.

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

Security Target

13. The Security Target [ST] fully specifies the TOE's Security Objectives, the Threats which these Objectives counter, 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.

14. The extended components are defined in [ST] Section 5.

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

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

Evaluation Conduct

17. The methodology described in [CEM] was used to conduct the evaluation. The TOE's SFRs and the security environment, together with much of the supporting evaluation deliverables, were based on those of Citrix XenDesktop Version 5.6 Platinum Edition which had previously been certified [CRP271] by the UK IT Security Evaluation and Certification Scheme to the CC EAL2 assurance level, augmented with ALC_FLR.2. For the evaluation of Citrix XenDesktop 7.6 Platinum Edition, the Evaluators performed all evaluation activities as specified in [CEM], using the previous evaluation results for guidance where appropriate.

18. The CESG Certification Body monitored the evaluation, which was performed by the SiVenture Commercial Evaluation Facility (CLEF), and witnessed a sample of Evaluator tests. The evaluation addressed the requirements specified in the Security Target [ST]. The results of this work, completed in March 2015, were reported in the Evaluation Technical Report [ETR].

Evaluated Configuration

19. 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.

20. The TOE should be used in accordance with its 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

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

Recommendations

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

23. 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 https://www.citrix.com/support/security-compliance.

24. The TOE relies on Microsoft Windows Server 2012 to provide platforms for server components and SQL Server 2012 to provide a database for configuration data. 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 the Security Target is that the selected hypervisor should meet A.VM_Host (see [ST] Section 3.5) and OE.Config_VM_Host (see [ST] Section 4.2.1). The list of supported hypervisors is regularly updated and can be found at http://support.citrix.com.

25. 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].

Disclaimers

26. This Certification Report and associated Certificate applies only to the specific version of the product in its evaluated configuration (i.e. the TOE). 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.

27. Certification is *not* a guarantee of freedom from security vulnerabilities. There remains a small probability that exploitable vulnerabilities may be discovered after the Evaluators' penetration tests were completed. This report reflects the CESG Certification Body's view on that date (see paragraph 68).

28. 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.

29. 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.

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

31. 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

32. The following sections provide guidance that is of particular relevance to consumers of the TOE.

Delivery and Installation

33. The TOE is only delivered via download from the Citrix website (https://www.citrix.com), ensuring "https" is specified in the address to provide a protected channel over which to perform the download). When downloading the TOE, the consumer is recommended to check that the evaluated versions of its constituent components have been downloaded, and to check that the security of the TOE has not been compromised during delivery. Specific advice on delivery and installation is provided in the TOE documents detailed below:

- Section 4 of [CCECG] "Before you begin"
- Section 4 of [CCECG] Task 1 to Task 4

34. In particular, Administrators should verify the MD5 checksum values against those published on the Citrix download page, as detailed in Section 4 of [CCECG] "Download and Verify the Installation Media". Furthermore, Administrators should note the methods of verifying the version of the installed TOE components as detailed in Section 4 of [CCECG] Task 1 to Task 4.

Guidance Documents

35. Specific configuration advice is in the Secure Configuration documents below:

- [CCECG]

36. The administration guidance documentation is as follows:

- Appendix A of [CCECG]
- [XAXD]
- [SF]
- [REC]
- [LIC]
- [GPO]

37. To maintain secure operation, the consumer is recommended to apply all installation and preparative configuration steps detailed in [CCECG] to ensure the deployment adheres to the evaluated configuration. This is particularly relevant because the protection of some TOE components and mechanisms rely upon the specific configuration and protection afforded by the environment. To aid the configuration of the server environment, [GPO_ZIP] provides the group policy templates described in [GPO] so that the group policy objects can be imported directly into the domain controller.

38. Administrators should note that guidance to be provided to their Desktop Users is defined in Appendix B of [CCECG].

III. EVALUATED CONFIGURATION

TOE Identification

39. The TOE is Citrix XenDesktop 7.6 Platinum Edition, which consists of:

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

40. It should be noted that Delivery Controller, Citrix Studio, StoreFront and Virtual Delivery Agent are delivered as part of the .iso file (downloaded from the Citrix website). Citrix Receiver v4.2.0.10 with Online Plug-in v14.2.0.10 is to be downloaded separately and used to replace the version of Citrix Receiver and Online Plug-in that is included in the .iso (instructions are provided in Section 4 of [CCECG] Task 4). Desktop Lock is also downloaded as a separate component.

TOE Documentation

41. The relevant guidance documents for the evaluated configuration are identified in Chapter II (in 'Guidance Documents') of this report.

42. The guidance document bundle is to be downloaded from https://www.citrix.com/security, then selecting the "Common Criteria" option and navigating to the page for Citrix XenDesktop 7.6 Platinum Edition.

TOE Scope

43. 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.

TOE Configuration

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

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

- The TOE Server components comprise the Delivery Controller (including Citrix Studio), the StoreFront (including the StoreFront Management Console), the Virtual Delivery Agents and the Database;

- The TOE Client component is the Citrix Receiver and (optionally) Desktop Lock running on a User Device.

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

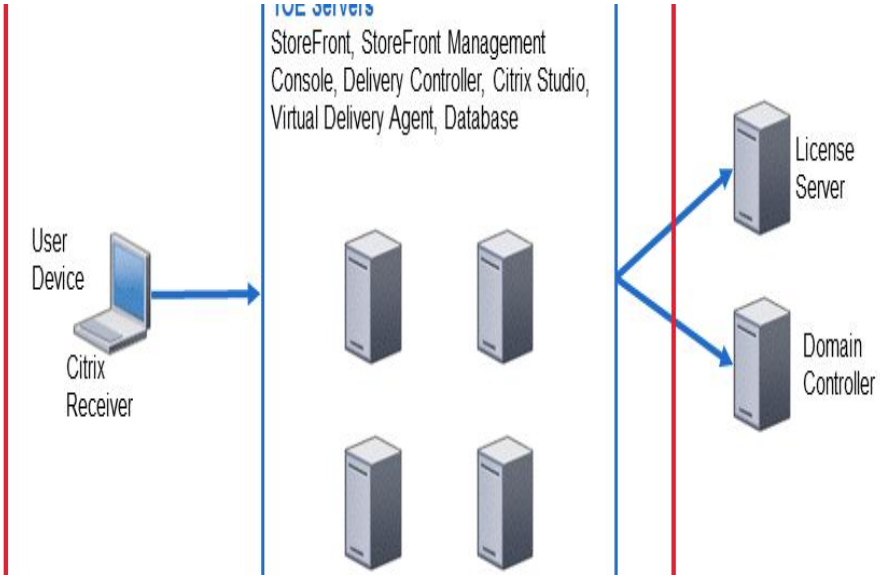

Figure 1: TOE Physical Boundary

47. 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.

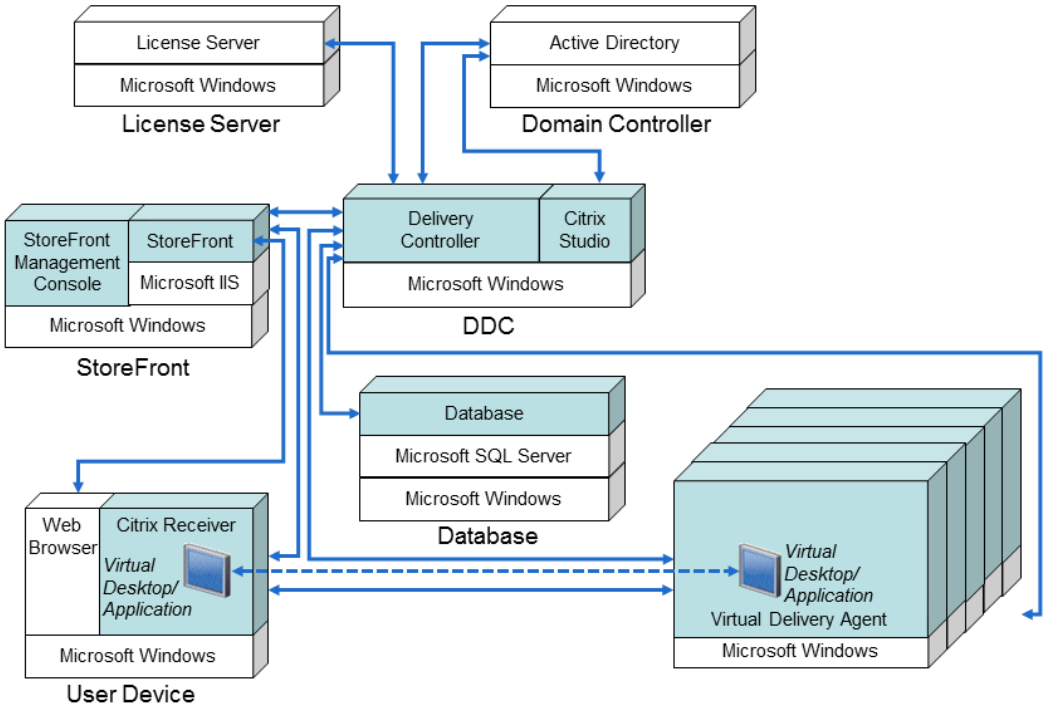

Figure 2: TOE Logical Boundary

Environmental Requirements

48. The environmental objectives for the TOE are stated in [ST] Section 4.2. The environmental assumptions are stated in [ST] Section 3.5.

49. The TOE was evaluated running on Server Components: Microsoft Windows Server 2012, Datacenter Edition; and Client Devices and VMs: Microsoft Windows 7 Ultimate SP1.

50. The environmental IT configuration is detailed in [ST] section 1.2.3 and [CCECG].

Test Configurations

51. The Developers used this configuration for their testing:

- 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 and was configured as depicted in Figure 3 below.

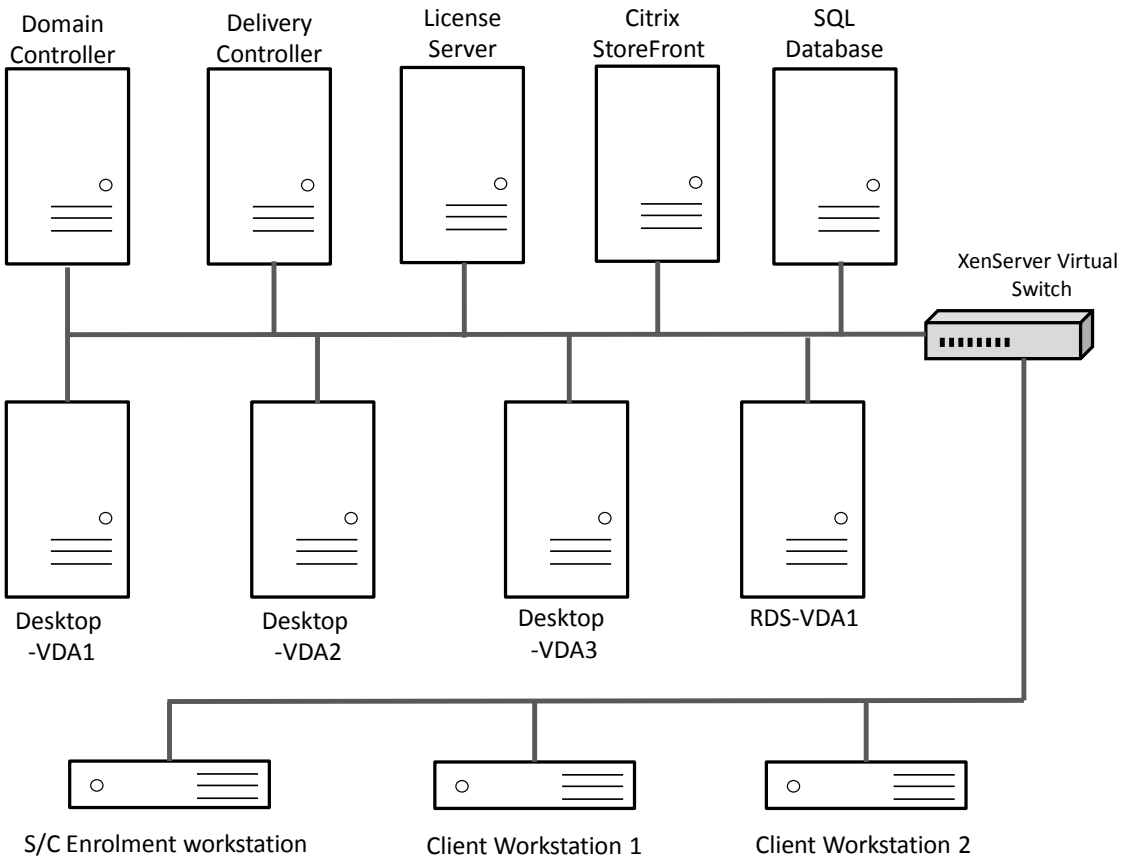

Figure 3: Test configuration

52. The Evaluators used the same configuration as that used by the Developers.

    a. Server components:

    - Delivery Controller (Microsoft Windows Server 2012, Datacenter Edition, with Microsoft .NET Framework 4.5), running Citrix Studio version 7.6.0.5026;

    - StoreFront server (Microsoft Windows Server 2012, Datacenter Edition, Microsoft .NET Framework 4.5.1, Microsoft Internet Information Server (IIS) 8.0, Microsoft ASP.NET 4.5), running Citrix StoreFront (and StoreFront Management Console) version 2.6.0.5031;

    - License Server (Microsoft Windows Server 2012, Datacenter Edition), running Citrix License Manager version 11.12.1 build 14008;

    - VM Hosting Infrastructure, comprising three XenServer 6.2 hosts (three Microsoft Windows 7 SP1 Ultimate Edition VDAs for virtual desktops and one Microsoft Windows Server 2012, Datacenter edition VDA for the virtual applications);

- Smartcard enrolment station;
- XenServer Management Console Server;
- Database (Microsoft Windows Server 2012, Datacenter Edition), running Microsoft SQL Server 2012, SP1 Enterprise Edition;
- Domain Controller (Microsoft Windows Server 2012, Datacenter Edition), running Microsoft Active Directory Server.

b. User Device PC components:

- Microsoft Windows 7 Ultimate SP1, running Citrix Receiver version 4.2.0.10 with On-line Plug-in version 14.2.0.10;
- Microsoft Windows 7 Ultimate SP1, running Citrix Receiver version 4.2.0.10 with On-line Plug-in version 14.2.0.10 and Desktop Lock version 14.2.0.10.

IV. PRODUCT ARCHITECTURE

Introduction

53. 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

54. 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 4 below.

TOE Design Subsystems

55. The high-level TOE subsystems, and their security features/functionality, 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 any published applications, and brokers connections between users and their virtual desktops and any published 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 published 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 published application. When configured with XenApp, StoreFront is also accessed from an Internet browser running within the virtual desktop to launch published 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 published applications, manage users' access permissions for virtual desktops and published 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.

TOE Dependencies

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

TOE Security Functionality Interfaces

57. The external TOE Security Functionality Interfaces (TSFI) are shown in Figure 4 below:

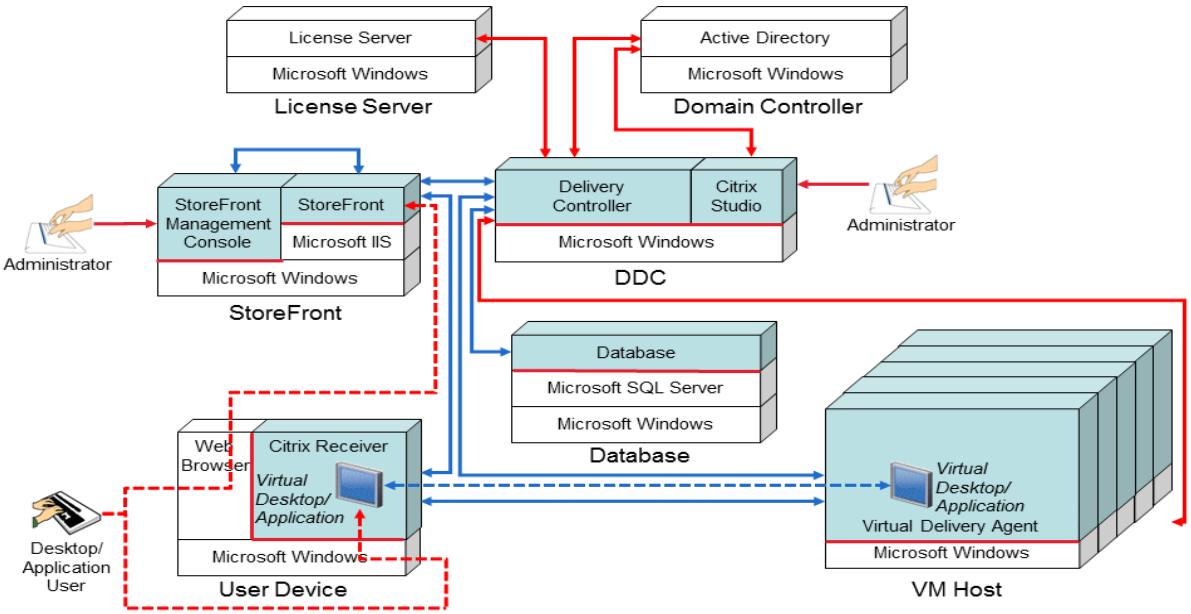

Figure 4: XenDesktop TSFI

58. 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). The dashed red line shows where the Desktop User interacts with a TOE component (Citrix Receiver / StoreFront) via an environment component (Web Browser). This is still considered to be a TSFI between the user and the TOE component.

59. 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).

60. 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.

61. 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

62. The Developer's security tests covered:

- all SFRs;
- all Security Functionality;
- the TSFI, as identified in Chapter IV (in 'TOE Security Functionality Interfaces') of this report.

63. 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 at the Developer's premises. The Evaluators confirmed the results were consistent with those reported by the Developer.

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

Evaluator Testing

65. The Evaluators devised and ran a total of 15 independent security functional tests, different from those performed by the Developer. No anomalies were found.

66. The Evaluators also devised and ran a total of 6 penetration tests to address potential vulnerabilities considered during the evaluation. No exploitable vulnerabilities or errors were detected.

67. The Evaluators carried out testing on the hardware described in Chapter III (in 'Test Configurations') of this report. All Evaluator testing was conducted at the Developer's premises.

68. The Evaluators completed their penetration tests on 30 January 2015.

Vulnerability Analysis

69. 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.

Platform Issues

70. 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.

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-2012-09-001, Version 3.1 R4, September 2012.

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2, Security Functional Components, Common Criteria Maintenance Board, CCMB-2012-09-002, Version 3.1 R4, September 2012.

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3, Security Assurance Components, Common Criteria Maintenance Board, CCMB-2012-09-003, Version 3.1 R4, September 2012.

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

[CCRA] Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security, Participants in the Arrangement Group, 2nd July, 2014.

[CEM] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Common Criteria Maintenance Board, CCMB-2012-09-004, Version 3.1 R4, September 2012.

[CRP271] Common Criteria Certification Report No. CRP271, UK IT Security Evaluation and Certification Scheme, Issue 1.0, November 2012.

[CRP282] Common Criteria Certification Report No. CRP282, UK IT Security Evaluation and Certification Scheme, Issue 1.0, March 2015.

[ETR] Citrix XenDesktop 7.6 Platinum Edition and Citrix XenApp 7.6 Platinum Edition: Evaluation Technical Report, SiVenture CLEF, CN11-TR-0001, Issue 1-0, March 2015.

[GPO] Citrix-specific Group Policy Security Templates,
8th January 2015.

[GPO_ZIP] Group Policy Objects files,
"Ref_CC_GPOs - 51353.zip" provided in documentation bundle.

[LIC] Citrix Licensing 11.12.1,
Document code: 2015-02-01 18:49:39 UTC.

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

[REC] Receiver for Windows 4.2,
Document code: 2015-02-03 18:25:19 UTC.

[SF] StoreFront 2.6,
Document code: 2015-02-01 22:00:25 UTC.

[ST] Common Criteria Security Target for
Citrix XenDesktop 7.6 Platinum Edition and Citrix XenApp 7.6 Platinum Edition,
CN11-ST-0001, Version 1-0, 2nd March 2015.

[UKSP00] Abbreviations and References,
UK IT Security Evaluation and Certification Scheme,
UKSP 00, Issue 1.8, August 2013.

[UKSP01] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.6, August 2014.

[UKSP02P1] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4.5, August 2013.

[UKSP02P2] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 3.1, August 2013.

[XAXD] XenApp 7.6 and XenDesktop 7.6[2],
Document code: 2015-02-02 23:06:02 UTC.

[2] This is the Product Guide, although it is not labelled as such in its title.

VII. ABBREVIATIONS

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

DDC	Delivery Controller (the leading 'D' is present for historical reasons)
GPO	Group Policy Objects
ICA	Independent Computing Architecture
SP	Service Pack
VDA	Virtual Delivery Agent
VDI	Virtual Desktop Infrastructure
VM	Virtual Machine

This page is intentionally blank.

VII. CERTIFICATE

The final two pages of this document contain the Certificate (front and back) for the TOE.

CESG CERTIFICATION BODY

CERTIFICATE No.
P281

This Certificate confirms that

Citrix XenDesktop Version 7.6 Platinum Edition

running on Microsoft Windows Server 2012 Datacenter Edition
and Microsoft Windows 7 Ultimate

has been evaluated under the terms of the

UK IT Security Evaluation and Certification Scheme

and complies with the requirements for

EAL2 augmented by ALC_FLR.2

COMMON CRITERIA (ISO 15408) ASSURANCE LEVEL.

The scope of the evaluated functionality was as claimed by the Security Target
and as confirmed by the associated Certification Report **CRP281**.

Certification is not a guarantee of freedom from security vulnerabilities. This certificate reflects the CESG Certification Body's view at the time of certification.
It is the responsibility of users (existing and prospective) to check whether any security vulnerabilities have been discovered since the date of the Evaluators' final penetration tests.

AUTHORISATION
Director for Information Assurance

DATE
19 March 2015

122

122

The CESG Certification Body of the UK IT Security Evaluation and Certification Scheme is accredited by the United Kingdom Accreditation Service (UKAS) to ***ISO/IEC 17065:2012*** to provide product conformity certification as follows:

Category: Type Testing Product Certification of IT Products and Systems.

Standards:

- Common Criteria for Information Technology Security Evaluation (CC) EAL1 - EAL7.

Details are provided on the UKAS website (www.ukas.org).

Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (CCRA), July 2014

The CESG Certification Body is a Participant to the above Arrangement. The current Participants to the above Arrangement are detailed on the Common Criteria Portal (www.commoncriteriaportal.org). The mark (left) confirms that this Common Criteria certificate has been authorised by a Participant to the above Arrangement and it is the Participant's statement that this certificate has been issued in accordance with the terms of the above Arrangement. Upon receipt of this Common Criteria certificate, the vendor(s) may use the mark in conjunction with advertising, marketing and sales of the IT product for which this certificate is issued. *All judgements contained in this certificate, and in the associated Certification Report, are covered by the Arrangement (EAL2, including the augmentation of ALC_FLR.2).*

Senior Officials Group – Information Systems Security (SOGIS)
Mutual Recognition Agreement of Information Technology Security Evaluation Certificates (SOGIS MRA), Version 3.0

The CESG Certification Body is a Participant to the above Agreement. The current Participants to the above Agreement are detailed on the SOGIS Portal (www.sogisportal.eu). The mark (left) confirms that this conformant certificate has been authorised by a Participant to the above Agreement and it is the Participant's statement that this certificate has been issued in accordance with the terms of the above Agreement. The judgments contained in this certificate and in the associated Certification Report are those of the compliant Certification Body which issued them and of the Evaluation Facility which performed the evaluation. Use of the mark 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. *All judgements contained in this certificate, and in the associated Certification Report, are covered by the Agreement.*

The IT product identified in this certificate has been evaluated by the SiVenture Commercial Evaluation Facility (an accredited and approved Evaluation Facility of the UK) using the ***Common Methodology for Information Technology Security Evaluation***, ***Version 3.1 Revision 4*** for conformance to the ***Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4***. This certificate applies only to the specific version and release of the IT product listed in this certificate in its evaluated configuration and in conjunction with the complete, associated Certification Report. The evaluation has been conducted in accordance with the provisions of the UK IT Security Evaluation and Certification Scheme, and the conclusions of the Evaluation Facility in the Evaluation Technical Report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by CESG or by any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CESG or by any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

In conformance with the requirements of ***ISO/IEC 17065:2012***, the ***CCRA*** and the ***SOGIS MRA***, the CESG Certification Body's website (www.cesg.gov.uk) provides additional information, as follows:

- type of product (i.e. product category); and
- details of product manufacturer (i.e. as appropriate: vendor/developer name, postal address, website, point of contact, telephone number, fax number, email address).