122-B

CERTIFICATION REPORT No. CRP255

Citrix XenServer
5.6 Platinum Edition

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 XenServer 5.6 Platinum Edition		
Platform:	n/a		
Description:	Citrix XenServer 5.6 Platinum Edition is a server virtualisation product that runs directly on server hardware and establishes an environment comprising a number of virtual machines (or "domains"), each configured to operate with a set of virtual CPU, memory, storage, and network resources.		
CC Version:	Version 3.1 Revision 3		
CC Part 2:	Conformant	CC Part 3:	Conformant
EAL:	EAL2 augmented by ALC_FLR.2		
PP Conformance:	None		
CLEF:	SiVenture		
CC Certificate:	CRP255	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 XenServer 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 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 4th August 2010:

- **Citrix XenServer 5.6 Platinum Edition**

It is abbreviated to 'XenServer' in this document.

4. The Developer was Citrix Systems Inc.

5. XenServer is a server virtualisation product that runs directly on server hardware and establishes an environment comprising a number of virtual machines (or "domains"), each configured to operate with a set of virtual CPU, memory, storage, and network resources. In this way, a single physical server can present a number of separate logical servers, with each server acting as though its resources were independent and running applications on a typical Windows operating system. XenServer maps and schedules the virtual resources onto the physical resources of the server hardware, and thereby provides a number of potential advantages including increased utilisation of the physical server resources.

6. 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.

7. Only Hardware Virtual Machine (HVM) Guests are included in the evaluated configuration; Paravirtualised (PV) Guests are not included. Furthermore, Windows is the only Guest operating system (OS) supported in the evaluated configuration.

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 Section 1.3.1 of the Security Target [ST].

Protection Profile Conformance

9. The Security Target [ST] does not claim conformance to any protection profile.

Security Claims

10. The Security Target [ST] fully specifies the TOE's Security Objectives, the Threats which these Objectives counter and the Security Functional Requirements (SFRs) that refine the Objectives. All of the SFRs are taken from CC Part 2 [CC2]; use of this standard facilitates comparison with other evaluated products.

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 XenServer 5.6 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' comments and recommendations are 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 the TOE's Delivery Procedures [DP], Evaluated Configuration Guide [CCECG] and Administrator's Guide [CCAG], which are all available for download from the XenServer 5.6 Common Criteria Version web page, which is reached by following the steps in paragraph 23 below..

b) The consumer's attention should be drawn to the procedure in the TOE's Evaluated Configuration Guide [CCECG], section Initial Installation] to prepare the pool master during installation to ensure sufficient entropy is available for generation of the pool secret.

c) It should be noted that XenCenter and XenCenterWeb are different applications:

- the XenCenter application supplied by Citrix may be used to manage the TOE in the evaluated configuration, as detailed in paragraph 32 below;

- XenCenterWeb is deprecated and must not be used in the evaluated configuration.

d) Citrix customers should download the TOE from the Citrix website. On completion of the download, the customer should verify the integrity of the TOE by performing an MD5 hash, as detailed in Chapter II 'Delivery' of this report.

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. The consumer should download the TOE from https://www.citrix.com, as follows:

a) the consumer logs in to their Citrix customer account, then clicks Downloads;

b) from the Search Downloads by Products list, select XenServer;

c) from the Select Product Version list, select XenServer 5.6;

d) from the list under Product Software, select XenServer 5.6 Common Criteria Version.

24. On completion of the download of the TOE, the consumer is recommended to:

a) confirm that the correct version of the TOE has been downloaded; and

b) verify the integrity of the TOE, by performing an MD5 hash of the software package and comparing it to the values in the checksum file linked to the XenServer 5.6 Common Criteria Version webpage.

25. For reference, the MD5 hash values published in that checksum file are:

- fad62ddda35ae897bc1e6e273aaf1121 XenServer-5.6.0-install-cd.iso
- b1cd30c131da1bd7de6617bd33c65954 XenServer-5.6.0-source-1.iso
- a776866e5c923f94e58d8a04ccc33371 XenServer-5.6.0-source-4.iso

26. Details of these download procedures are provided in the TOE's Delivery Procedures [DP], which are linked from the above webpage.

Installation and Guidance Documentation

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

a) Common Criteria Delivery Procedures for Citrix XenServer 5.6, Platinum Edition [DP];

b) Citrix XenServer 5.6 Installation Guide [XIG];

c) Citrix XenServer 5.6 Virtual Machine Installation Guide [XVMIG];

d) Common Criteria Evaluated Configuration Guide for Citrix XenServer 5.6, Platinum Edition [CCECG];

e) Common Criteria Administrator's Guide for Citrix XenServer 5.6, Platinum Edition [CCAG].

28. The Administration Guide documentation is as follows:

a) XenServer 5.6 Administrator's Guide [XAG];

b) Citrix XenServer Management API [XAPI];

c) Common Criteria Administrator's Guide for Citrix XenServer 5.6, Platinum Edition [CCAG];

d) Common Criteria Evaluated Configuration Guide for Citrix XenServer 5.6, Platinum Edition [CCECG].

29. Owing to the nature of the TOE, User Guide documentation is not necessary.

III. EVALUATED CONFIGURATION

TOE Identification

30. The TOE is Citrix XenServer 5.6 Platinum Edition, consisting of "Citrix XenServer 5.6" as downloaded from https://www.citrix.com (as detailed in Chapter II 'Delivery' of this report).

TOE Documentation

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

TOE Scope

32. The TOE Scope is defined in the Security Target [ST] Sections 1.3 and 1.4. Functionality that is outside the TOE Scope is defined in [ST] Section 1.3.1. It should be noted that although the XenCenter management console is not included in the TOE (because it does not implement any security functions, and it is not necessary for their operation), it may be used in the evaluated configuration as a method of administering the TOE over the XML-RPC interface[2].

TOE Configuration

33. The evaluated configuration of the TOE is defined in [ST] Section 1.3.1, and in the TOE's Evaluated Configuration Guide [CCECG] and Administrator's Guide [CCAG], as shown in Figure 1 below:

[2] Note the distinction in paragraph 16 between XenCenter and XenCenterWeb.

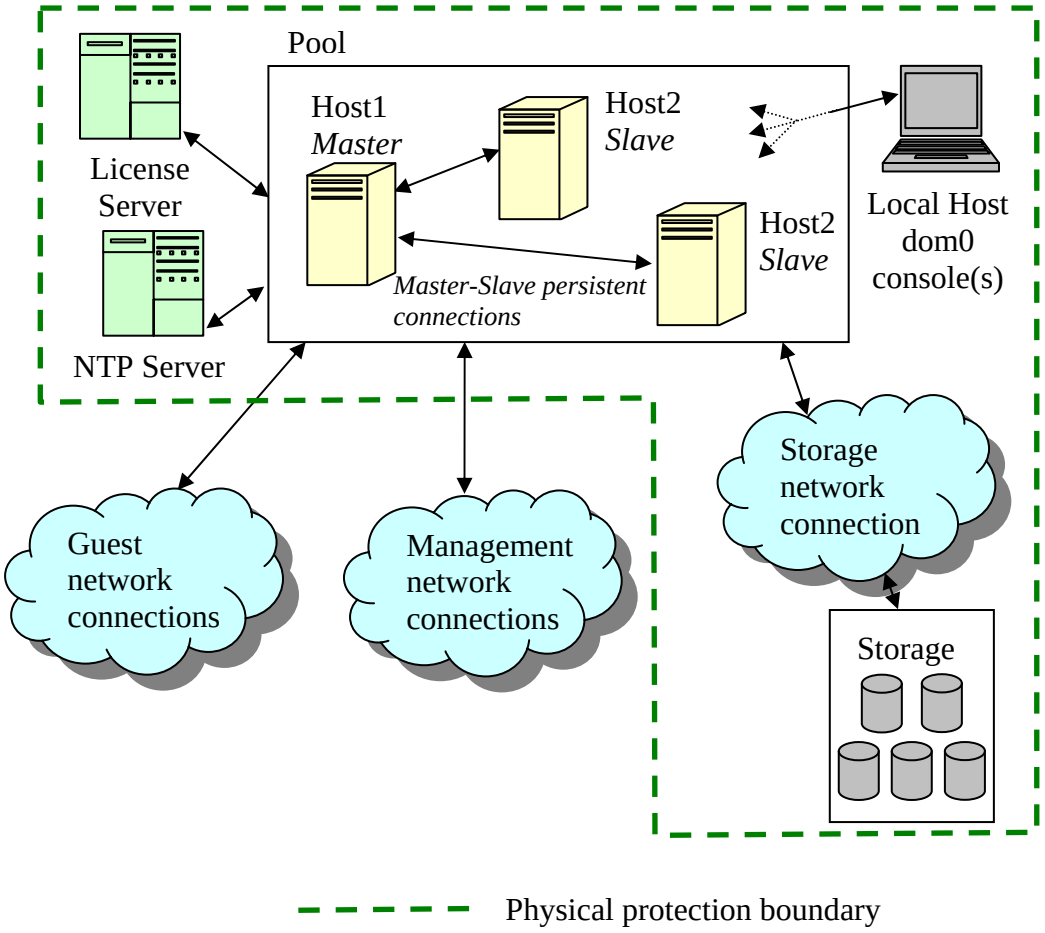

Figure 1 - TOE Evaluated Configuration

34. The TOE should be installed on at least 2 servers (maximum of 16 servers) configured in a pool, containing a Master Host and at least one Slave Host. The servers must satisfy the limitations specified in [ST] Section 1.2.2. The host network interface cards (NICs) should be set up as follows, as specified in [CCECG] section 'Network Configuration'.

a) NIC0 - Management Network;

b) NIC1 - Storage Network;

c) NIC2 ... NICn - One or more further NICs must be added as required to create Guest Networks.

35. The environment should provide network attached storage offering Network File System (NFS) storage, as specified in [ST] Section 1.2.2. The TOE should connect to the storage as detailed in [CCECG] section 'Storage Configuration'.

Environmental Requirements

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

37. The environmental IT configuration is detailed in [ST] Section 1.2.2 and [CCECG].

38. The TOE was evaluated running on Dell Power Edge R710 servers, which met the requirements for the servers specified in [ST] Section 1.2.2.

39. The TOE is required to be connected to the following non-TOE components:

- Storage: Virtual Hard Disk (VHD) on NFS;
- Citrix License Server;
- Network Time Protocol (NTP) server.

40. Only Windows operating systems should be configured as a Guest OS in a Guest Domain, in accordance with the Virtual Machine (VM) Installation Guide [XVMIG]. Windows 2003 Server and Windows 2008 Server were configured as Guest VMs for Developer and Evaluator testing.

Test Configuration

41. The Developers used a configuration consistent with that detailed in 'TOE Configuration' above for their testing. To enable the Developers to run their automated test suite, Secure Shell (SSH) was enabled for their testing. The Evaluators determined that the use of SSH for testing did not adversely affect the results of the TOE security functionality tests.

42. The Evaluators used the same configuration for their testing as that used by the Developer. The only exception was that, for the Evaluators' testing, the [CCECG] 'SSH Configuration' (which disabled SSH) was not applied, as the SSH connection to the host was used to complete the configuration necessary for some test cases. The Evaluators determined that this change had no impact on the TOE or on the functionality being tested.

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, described in [ST] Sections 1.3 and 1.4.2, incorporates Dom0 and XenHypervisor running directly on server hardware.

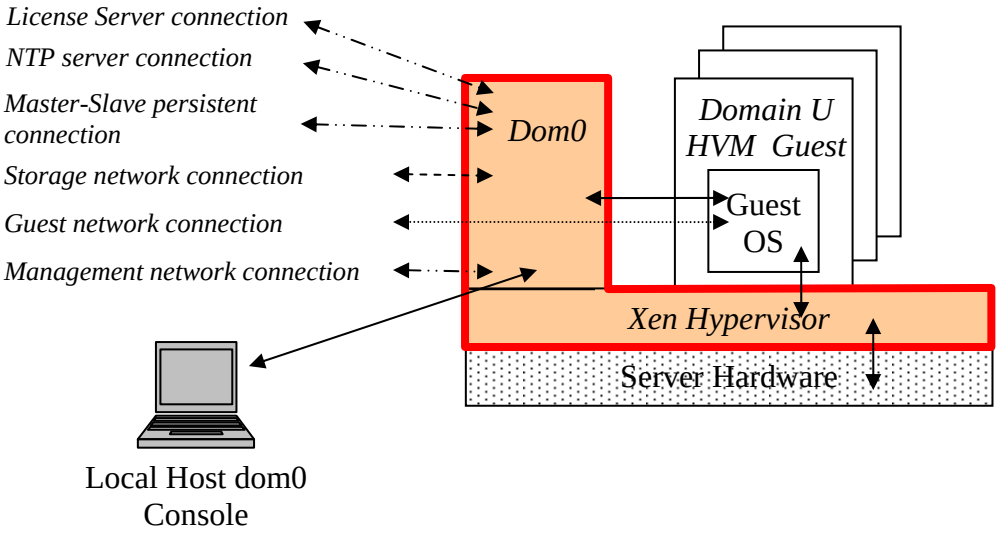

Figure 2 - TOE Architecture

45. These provide other domains (referred to collectively as "Domain U") in which an OS such as Windows is installed, and the domain will then behave as a separate server.

TOE Design Subsystems

46. The TOE subsystems, and their security functionality, are as follows[3]:

a) The Xen Hypervisor: A virtual machine monitor that provides the virtual environment that supports and separates domains, schedules execution on the Host CPU(s), and maintains memory page mappings for all domains (including dom0) in its own memory (this Hypervisor memory is not accessible to any domain, including dom0). The Hypervisor implements a number of interfaces (hypercalls) used by domains or

[3] Terminology used within the description of the TOE subsystems is defined in Chapter VII ('Abbreviations') of this report and in [ST] Section 0.6.

processes running within them: dom0 is able to make privileged hypercalls; other domains are only able to make unprivileged hypercalls.

b) Dom0: A privileged domain which is also a PV domain – meaning that it knows that it operates in a virtual environment. Dom0 is the only privileged domain, and indeed the only PV domain, in the evaluated configuration; it has a special status because it is responsible for creating the Guest Domains (using hypercalls) and provides access to all physical devices. Dom0 runs the xapi process that (amongst other tasks) maintains a database (XML file) containing information about the Pool structure and status[4], and handles XenAPI requests. Dom0 also contains the XenStore database which stores information about domains and provides a means of communicating between Domain U and dom0[5].

47. The security properties identified in [ST] Section 5.2 and Chapter 6 concern the ability of XenServer to provide the following:

a) Authentication of Administrators (FIA_UID.2 & FIA UAU.2):

- This is concerned with connections from the Local Host dom0 Console, submission of xapi commands (as described in XenServer Management API [XAPI] as XML-RPC calls over the Management Network, and use of the HTTP Handlers over the Management Network. Administrators authenticate to dom0.

b) Maintaining separation of data between Guest VMs (FDP_IFC.1/VMData & FDP_IFF.1/VMData):

- Separation of VMs is established primarily by the setting up of the domain in which the (Guest) VM runs: this is responsible for the allocation of memory and other resource connections (notably network and storage) for the VM.

- From the point of view of an Administrator, the main task involved in setting up an instance of a Guest VM is to use the XenAPI interface (as described in [XAPI]) to request the creation of a virtual machine into which the Guest OS is then installed (as described in [XVMIG] and, for setting up networking for the Guest (as described in [CCECG]). The installation of the Guest OS in the Guest VM is essentially the same as installation onto a non-virtualised host, followed by the installation of the PV drivers. Administrators operate directly only on VMs, not domains, but creation of a VM will also entail dom0 creating a Guest Domain to contain the VM.

- From the point of view of XenServer, a XenAPI command requesting creation of a new VM is sent to the Pool Master, which identifies a suitable Slave Host on

[4] The Master-Slave database is in fact a part of the xapi database. All changes to the Master-Slave database (in particular updates from Slaves) are carried out by modifying the database on the Master (Slaves perform these updates over the Master-Slave Persistent Connection). The database on the Master is then regularly synchronised with the databases on the Slaves, so that (after synchronisation) all Hosts in the Pool have the same xapi database

[5] In the evaluated configuration, Guest domains cannot use XenStore to share memory with each other.

which to create the VM and executes a VM.start (or VM.start_on) operation on the selected Host, referring to a VM that has previously been created (as above, which creates a VM in the Halted state, without a domain). This will cause the Host to create a new domain (using the domain builder process), then to locate the referenced VM inside the domain and start it running.

- Sharing of memory by any domain other than dom0 is disabled in the evaluated configuration (as described in [CCECG], section Dynamic Memory Control).

c) Maintaining separation of data between guest VDisks (FDP_IFC.1/VDisk & FDP_IFF.1/VDisk):

- Separation of virtual disks is established by the allocation of separate Virtual Block Devices (VBDs) and Virtual Disk Images (VDIs) to VMs, and the linking of front-end drivers (used by the Guest OS in its Guest Domain) to back-end drivers (which connect the front-end drivers to dom0 in order to implement the communications with a physical storage device).

d) Protection of memory de-allocated from a VM (FDP_RIP.1):

- Memory is de-allocated from a VM when its domain is destroyed, at which point the Hypervisor will overwrite the memory with zeroes.

e) Provision of secure channels (FTP_ITC.1):

- Secure channels are implemented by enforcing the use of HTTP over TLS/SSLv3 for connections to XenConsole, communications over the Management Network[6], and communications on the Master-Slave Persistent Connection.

TOE Dependencies

48. The TOE dependencies on the IT environment are identified in Chapter III 'Environmental Requirements'.

TOE Interfaces

49. The external TOE Security Functions Interface (TSFI) is described in [ST] Section 1.3 and shown in Figure 2 above.

[6] It should be noted that the License Server and NTP connections take place over the Management Network but do not use (or require) a secure channel.

V. TOE TESTING

TOE Testing

50. The Developer's tests covered:

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

51. The Developer used the test configuration described in Chapter III (in 'Test Configuration') of this report. As also stated there, the Evaluators used the same test configuration as that used by the Developer.

52. The Evaluators repeated 8 of the Developer's automated test cases and 9 additional tests from the Developer's automated regression test suite. The Evaluators confirmed the results were consistent with those reported by the Developer.

53. The Evaluators devised and ran a total of 7 independent functional tests, different from those performed by the Developer. No anomalies were found.

54. The Evaluators also devised and ran a total of 6 penetration tests to address potential vulnerabilities considered during the evaluation and 4 additional tests to identify whether further penetration tests were necessary. No exploitable vulnerabilities or errors were detected.

55. The Evaluators finished running their penetration tests on 16th July 2010.

Vulnerability Analysis

56. 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, in particular the Developer's Security Architectural Design.

Platform Issues

57. The platform on which the TOE is installed should meet the requirements specified in [ST] Section 1.2.2, namely:

a) Servers each contain more than one CPU core[7];

b) Processor type: 64-bit Intel-VT with Extended Page Tables (EPT);

c) At least 3 NICs per host, configured to support the separate networks identified in paragraph 34 above.

[7] Where only one CPU core is available then different code paths are used in the TOE, and these were not tested in the evaluated configuration.

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.

[CCAG] Common Criteria Administrator's Guide for Citrix XenServer 5.6, Platinum Edition, Citrix Systems Inc, 1.0 Edition, August 2010.

[CCECG] Common Criteria Evaluated Configuration Guide for Citrix XenServer 5.6, Platinum Edition, Citrix Systems Inc, 1.0 Edition, August 2010.

[DP] Common Criteria Delivery Procedures for Citrix XenServer 5.6, Platinum Edition, Citrix Systems Inc, 1.0 Edition, August 2010.

[ETR] Citrix XenServer 5.6 Platinum Edition Evaluation Technical Report, SiVenture CLEF, LFV/T006, CIN3-TR-0001, Issue 1.0, 3 August 2010.

[ETRSup1] Review Form, containing Certifier Comments and Evaluator Responses,
CESG Certification Body,
CB/100806/LFV/T006, 6 August 2010, updated 18 August 2010.

[ETRSup2] Review Form, containing Certifier Comments and Evaluator Responses,
CESG Certification Body,
CB/100817(NW-A)/LFV/T006, 17 August 2010, updated 18 August 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).

[ST] Common Criteria Security Target For Citrix XenServer 5.6 Platinum Edition,
Citrix Systems Inc,
CIN3-ST-0001, Version 1-0, 30 July 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.

[XAG] XenServer 5.6 Administrator's Guide,
Citrix Systems Inc,
1.1 Edition, June 2010.

[XAPI] Citrix XenServer Management API,
Citrix Systems Inc,
Revision 1.7, 21 May 2010.

[XIG] Citrix XenServer 5.6 Installation Guide,
Citrix Systems Inc,
1.1 Edition, June 2010.

[XVMIG] Citrix XenServer 5.6 Virtual Machine Installation Guide,
Citrix Systems Inc,
1.0 Edition, May 2010.

VII. ABBREVIATIONS & GLOSSARY

This glossary and 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].

API	Application Programming Interface.
Dom0	see Domain 0
DomU	see Domain U
Domain	A running instance of a VM.
Domain 0	A special-purpose domain (based on a Linux kernel) that exists in a single instance on each XenServer host. Domain 0 is the only privileged domain (meaning that it can use privileged hypervisor calls, for example to map physical memory into and out of domains) on a XenServer host, and is thus the only domain that can control access to physical input/output resources directly and access the content of other domains (i.e. Domain U).
Domain U	The collection of domains other than dom0. Each of these domains is either an HVM Guest or PV Guest, and is a domain in which a guest operating system has been (or will be) installed.
Domain U Guest	An HVM Guest or a PV Guest. (Only HVM Guests are included in the evaluated configuration of the TOE.)
Guest OS	An operating system that has been installed in a Guest Domain. (Windows is the only Guest OS included in the evaluated configuration.)
Host	An installation of XenServer on a dedicated server.
HTTP	Hypertext Transfer Protocol.
HTTPS	Hypertext Transfer Protocol Secure. A combination of HTTP and SSL/TLS to provide encryption and secure identification of the server.
HVM	Hardware Virtual Machine.
HVM Guest	A member of Domain U in which an unmodified Guest OS can be installed and run. (Only HVM Guests are included in the evaluated configuration)
Hypercall	Synchronous calls made from a domain to the hypervisor. Any domain may make calls to the hypervisor, but only dom0 can make privileged calls, such as those that cause memory (including memory representing physical resources) to be mapped into or out of domains.

Hypervisor	An abstraction layer implementing a set of software calls (hypercalls) that can be made by domains, and providing an asynchronous event-based interface for communication from the hypervisor to domains. The hypervisor controls the scheduling of the CPU and the partitioning of memory between virtual machines, but has no knowledge of the actual physical devices on the host (when the devices are used, this knowledge is provided by device drivers running in dom0).
NFS	Network File System. A protocol developed by Sun Microsystems, and defined in RFC 1094, which allows a computer to access files over a network as if they were on its local disks.
NIC	Network Interface Card.
NTP	Network Time Protocol.
OS	Operating System.
Pool	A group of hosts in which one host takes the role of master and the others are slaves. Storage and configuration metadata are shared across the pool. The master can decide which hosts to start VMs on.
PV	Paravirtualised. A virtualization technique that presents a software interface to VMs that is similar but not identical to that of the underlying hardware.
PV Drivers	Drivers that replace default drivers in an HVM Guest, in order to accelerate storage and network data paths. These are treated as part of the Guest OS, use unprivileged XenServer interfaces, and are not involved in implementing XenServer security functions.
PV Guest	A member of Domain U in which a modified Guest OS can be installed and run. (PV Guests are not included in the evaluated configuration.)
SFR	Security Functional Requirement.
SSL	Secure Sockets Layer. An open, non-proprietary protocol that provides data encryption, server authentication, message integrity and optional client authentication for a TCP/IP connection.
TLS	Transport Layer Security. The latest, standardised, version of SSL, providing server authentication, data stream encryption and message integrity checks
VHD	Virtual Hard Disk. A file format containing the complete contents and structure representing a virtual Hard Disk Drive.
VM	Virtual Machine. An abstraction of a real hardware machine that creates an environment in which software (typically an operating system) that would otherwise run directly on hardware as the only software to be executing can

	be run with the illusion of exclusive access to a set of physical resources. In XenServer a virtual machine is characterised by a defined set of resources (e.g. memory and storage capacities and available network connections). A virtual machine that has been allocated real resources and in which processes are running is a Domain.
xapi	A process running in dom0 which implements and presents the XenAPI interface in [XAPI], used to manage XenServer hosts and the pool.
XenAPI	The API for managing XenServer installations, i.e. for remotely configuring and controlling domains running on hosts in a XenServer pool.
XML-RPC	A protocol for sending Remote Procedure Calls (RPC) formatted as XML. (See www.xmlrpc.com).