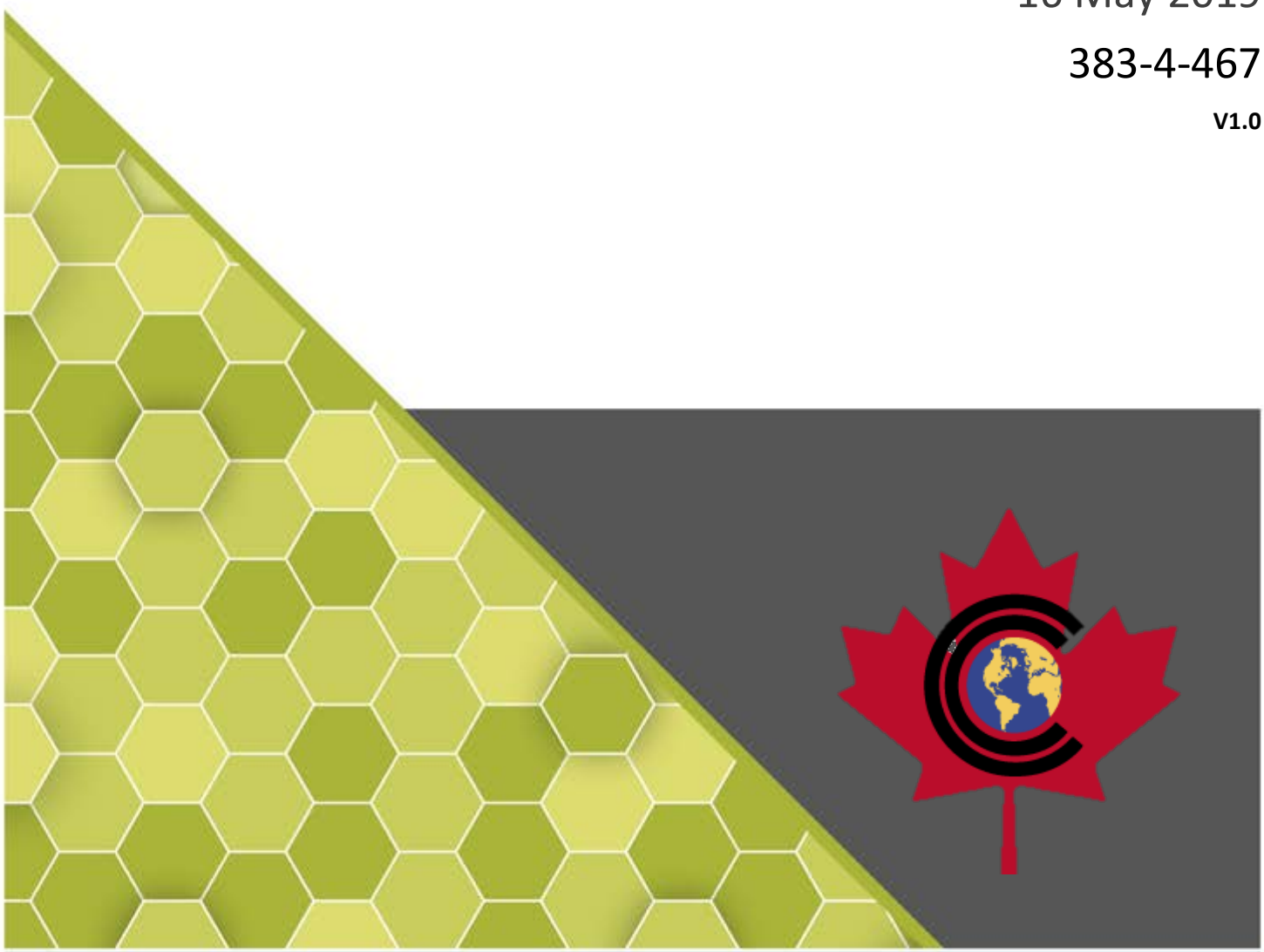
COMMON CRITERIA CERTIFICATION REPORT

Citrix XenServer ® 7.1 LTSR Enterprise Edition (CU2)

16 May 2019

383-4-467

V1.0



Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Scheme – using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian CC Scheme, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

OVERVIEW

The Canadian Common Criteria Scheme provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

The certification report, certificate of product evaluation and security target are posted to the Certified Products list (CPL) for the Canadian CC Scheme and to the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Citrix XenServer ® 7.1 LTSR Enterprise Edition (CU2) (hereafter referred to as the Target of Evaluation, or TOE), from Citrix Systems Inc., was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

DXC Security Testing/Certification Laboratories is the CCEF that conducted the evaluation. This evaluation was completed 16 May 2019 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

Communications Security Establishment, as the Certification Body, declares that the TOE evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the Canadian Certified Products list (CPL) and the Common Criteria portal (the official website of the International Common Criteria Project).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1 TOE Identification

TOE Name and Version	Citrix XenServer ® 7.1 LTSR Enterprise Edition (CU2)
Developer	Citrix Systems Inc.
Conformance Claim	EAL 2+ (ALC_FLR.2)

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

1.2 TOE DESCRIPTION

The TOE is a server virtualisation product that runs directly on server hardware. It establishes execution environments that create the appearance of physical computers into which guest operating systems may be installed and run. Each running virtual machine, referred to as a domain, is configured to operate with a set of virtual CPU, memory, storage, and network resources.

The resources allocated to each domain are isolated from any other domain (other than the control domain, Domain 0); this isolation is enforced by the TOE itself and does not rely on the behaviour of guest operating systems running within the domains.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

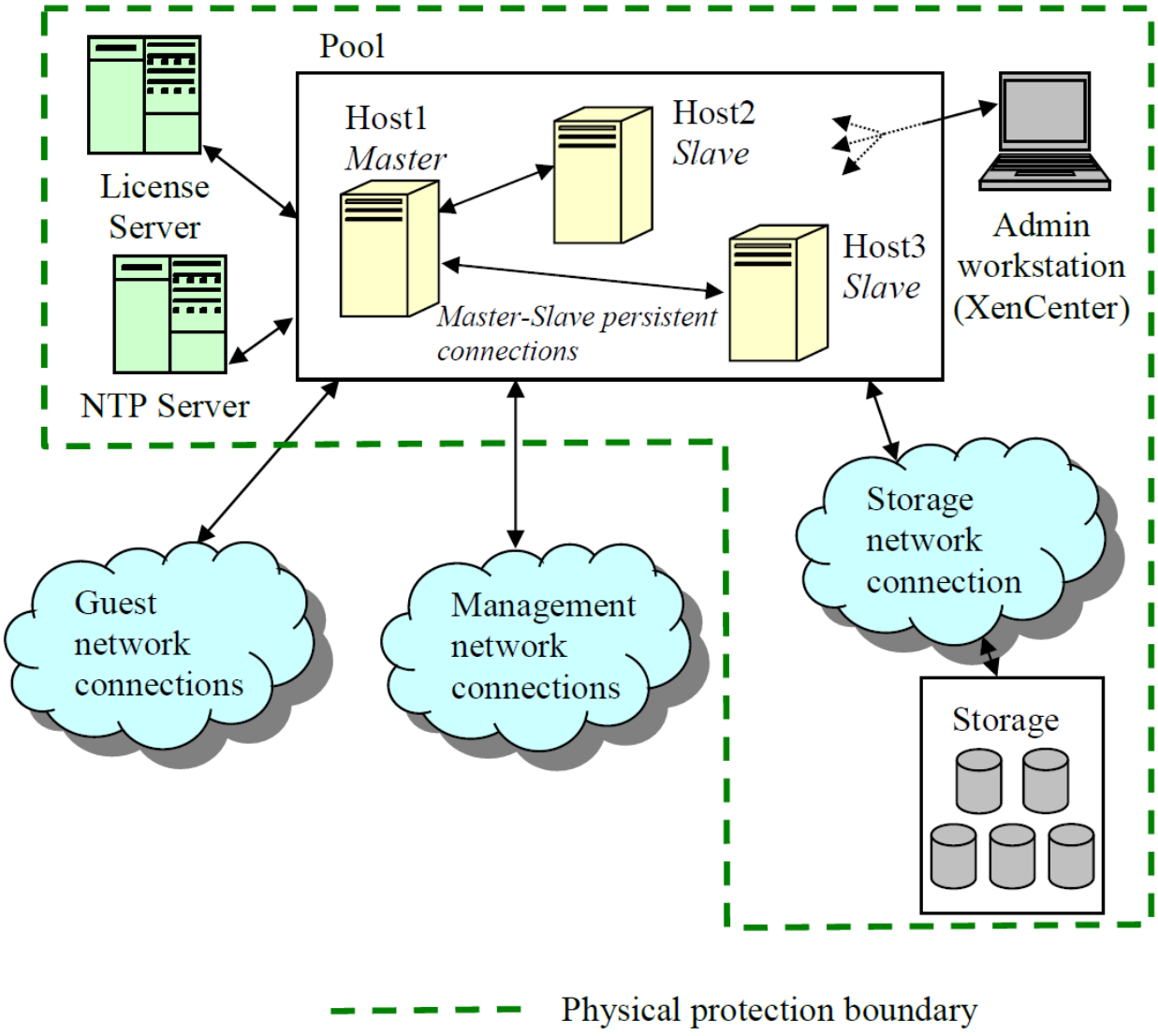


Figure 1 TOE Architecture

2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

- Memory Separation
- Virtual Disk Separation
- Administrator Authentication
- Channel Protection

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following Government of Canada approved cryptographic algorithms were evaluated by the CAVP and used by the TOE:

Table 2 Cryptographic Algorithm(s)

Cryptographic Algorithm	Standard	Certificate Number
Advanced Encryption Standard (AES)	FIPS 197	#4397
Rivest Shamir Adleman (RSA)	FIPS 186-4	#2379
Secure Hash Algorithm (SHS)	FIPS 180-3	#3626
Deterministic Random Bit Generation (DRBG)	SP 800-90A	#1417
Component Validation List	SP 800-56A	#1106

3 ASSUMPTIONS AND CLARIFICATIONS OF SCOPE

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- The following components of the TOE and IT environment are kept physically secure so that no unauthorised persons have access to the components, either physically or for connection (e.g. via console ports):
    - Hardware on which the TSF is running, and any connections between the hardware items (e.g. between hosts in a pool).
    - The License Server
    - NTP server.
    - Any local host dom0 console.
    - Any remote administration console.
    - Storage devices used by the TOE, and their connections to the TOE.
- The controls in the environment allow only authorised, trusted administrators access to the management network. (The use of TLS for remote administration provides a second layer of security that complements this separation at the network layer.)
- Workstations used by remote administrators are assumed to be physically secured, as well as protected against operational security threats such as shoulder surfing. Since remote administration is conducted over an encrypted XAPI connection, these workstations do not need to be in the same physical location as the TOE.
- The storage connection and storage devices used by the TOE are physically isolated from the other networks used by the TOE, and that the management, storage, and guest networks each use separate NICs (more than one NIC may be used for the guest network).

3.2 CLARIFICATION OF SCOPE

The TOE incorporates CAVP validated cryptography and was not subject to a CMVP validation.

The TOE must be connected via the Management Network to a physical License Server with a XenServer license (the use of a License Server deployed as a virtual appliance is not included in the evaluated configuration).

DomU virtual machines are configured not to use local devices (printers, CD-ROM drive, etc.) beyond a disk image stored on local EXT3-based storage.

IntelliCache (i.e. use of local storage on a host as a cache for NFS storage) is not used in the evaluated configuration

No virtual machines are directly assigned to PCI devices, including SR-IOV devices

GPU Pass-Thru and vGPU are not enabled

The storage connection is physically isolated and protected from other networks (management network and guest network)

Servers are configured to use a separate, dedicated NIC (or NICs) for management traffic (i.e. for XenServer administrative operations, such as use of XenAPI), storage traffic, and guest network traffic.

Only HVM guests are created.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

- The TOE installed on a dedicated x86 Server with the following characteristics;
  - Multiple CPU cores
  - 64-bit Intel-VT with EPT processor
  - At least 3 NICs per host
- Storage repositories supporting VHD on NFS, local EXT3-based storage, and read only ISO on NFS
- Citrix License server version 11 (Deployed as a separate server)
- NTP server that supports NTP version 4

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a. Release Notes, February 2017, 1.0 Edition

b. Quick Start Guide, February 2017, 1.0 Edition

c. Installation Guide, February 2017, 1.0 Edition

d. Administrator's Guide, July 2018, 1.0 Edition

e. Virtual Machine User's Guide, July 2018, 1.1 Edition

f. Citrix XenServer Management API, API Revision 2.6

g. Common Criteria Evaluated Configuration Guide for Citrix XenServer ® 7.1 LTSR Enterprise Edition, Version 1.0, January 2019

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements (SFRs). The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

6.1 ASSESSMENT OF DEVELOPER TESTS

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT FUNCTIONAL TESTING

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. Repeat of Developer's Tests: The evaluator repeated a subset of the developers tests;

b. Host to Host communications: This test verifies secure communication between hosts;

c. User to Host communications: This test verifies secure communication between users and hosts; and

d. Host Master-Slave operations: This test verifies that master-slave operations are preserved when an master is taken out of service.

6.3.1 FUNCTIONAL TEST RESULTS

The developer's tests and the independent functional tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 INDEPENDENT PENETRATION TESTING

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST; and

b. SSH Access Denial : This test attempts to access the TOE via SSH when it is disabled in the evaluated configuration.

6.4.1 PENETRATION TEST RESULTS

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for this evaluation is **PASS**. These results are supported by evidence in the ETR.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 5, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 5. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Security Target for Citrix XenServer ® 7.1 LTSR Enterprise Edition v1.3, May 2019
Evaluation Technical Report for Citrix XenServer ® 7.1 LTSR Enterprise Edition v1.1, 16/05/2019