122-B

CERTIFICATION REPORT No. CRP257

Citrix XenApp 6.0 for Windows Server 2008 R2 - Platinum Edition
Version 6.0

running on Windows Server 2008 R2

Issue 1.0

February 2011

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 (CC) 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 XenApp 6.0 for Windows Server 2008 R2 - Platinum Edition		
Platform:	Running on Windows Server 2008 R2		
Description:	XenApp provides users (endpoint device users) with secure access to applications and information, allowing multiple users to log on and run applications in separate, protected sessions.		
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:	P257	Date Certified:	28th February 2011

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 in 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 XenApp 6.0 for Windows Server 2008 R2 - 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 10th February 2011:

- **XenApp 6.0 for Windows Server 2008 R2 - Platinum Edition**

4. The Developer was Citrix Systems Inc.

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

6. Control over use of endpoint device resources is managed through global control policies; not on a per user basis.

7. The use of smartcards for user authentication is supported in the evaluated configuration, but smartcards are outside the scope of the TOE. The role of the TOE, when smartcard authentication is configured, is limited to conveying requests and responses between the smartcard and the operating system (including user authentication credentials collected and sent to the smartcard), and reacting appropriately to the authentication result from the operating system.

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 of [ST].

Protection Profile Conformance

9. The Security Target [ST] does not claim conformance to any Protection Profile (PP).

Security Claims

10. The Security Target [ST] fully specifies the TOE's Security Objectives, the Threats / Organisational Security Policies (OSPs) which those Objectives counter / meet and the Security

Functional Requirements (SFRs) that elaborate the Objectives. Most of the SFRs are taken from CC Part 2 [CC2]; use of that standard facilitates comparison with other evaluated products.

11. Extended security (functional) requirements are detailed in Section 5 of [ST], and are completed in Section 6.2.3 of [ST].

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

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

Evaluation Conduct

14. The TOE's SFRs and the security environment, together with much of the supporting evaluation deliverables, remained mostly unchanged from that of Citrix Presentation Server 4.5 Platinum Edition for Windows, which had previously been certified [CR] by the UK IT Security Evaluation and Certification Scheme to the CC EAL2 assurance level (augmented by ALC_FLR.2). For the evaluation of Citrix XenApp 6.0 for Windows Server 2008 R2 - Platinum Edition, the Evaluators made some re-use of those previous evaluation results where appropriate.

15. 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 that work, completed in February 2011, were reported in the Evaluation Technical Report ([ETR] and [ETRS]).

Conclusions and Recommendations

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

17. Prospective consumers of Citrix XenApp 6.0 for Windows Server 2008 R2 - 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.

18. 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.

19. The TOE relies on the underlying platform (Windows Server 2008 R2) for authentication. At the time of the TOE's evaluation, the evaluation of Windows Server 2008 R2 by the US Common Criteria Evaluation and Validation Scheme (CCEVS) was scheduled to complete on 31st December 2010 (i.e. before completion of the TOE's evaluation). However, at the time of writing this report, the CCEVS had re-scheduled the Windows Server 2008 R2 evaluation

completion date to 31st December 2011. System integrators and risk owners using the TOE should therefore make suitable arrangements to satisfy themselves that they have appropriate confidence in the authentication mechanism(s) of the underlying platform.

Disclaimers

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

21. 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.

22. Existing and prospective consumers should check regularly for themselves whether any security vulnerabilities have been discovered since the Evaluation Technical Report ([ETR] and [ETRS]) 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.

23. 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.

24. 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

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

Delivery

26. On receipt of the TOE, the consumer should check that the evaluated versions of its constituent components have been supplied, and should check that the security of the TOE has not been compromised during delivery.

27. The media kit containing most of the TOE components is shipped to the consumer directly from Citrix Systems Inc. using reputable carriers. The Common Criteria Evaluated Configuration Guide [CCECG] Chapter 3 ("Before Installing XenApp") directs the consumer to check specified delivery documents, to verify the authenticity of the received media kit.

28. [CCECG] Chapter 3 directs the consumer to download the Web Interface (detailed in sub-section "Installing Web Interface") and Online Plug-in[2] (detailed in sub-section "To download and install the web plug-in"). The consumer should verify that the MD5 hashes of those downloaded TOE components are as below (also posted on the secure area of the Citrix website):

a) Citrix Online Plug-in 12.1 (Citrix Online Plug-in – web) MD5 checksum:
A783CD22DD4786B8F89FB36FC432955C

b) Citrix Web Interface 5.4 MD5 checksum:
D4B606BC06DB3803844D0D5B63057776

29. [CCECG] Chapter 5 ("To apply the Citrix hotfixes") directs the consumer to download two Citrix hotfixes (XA600W2K8R2X64002 and XA600W2K8R2X64021), as part of the TOE.

Installation and Guidance Documentation

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

- Common Criteria Evaluated Configuration Guide [CCECG].

31. The Administration Guide documentation is as follows:

- Common Criteria Evaluated Configuration Guide [CCECG];
- Administration [AG];
- Online Plug-in 12.1 for Windows Guide [OLP];

[2] The Security Target [ST] refers to the client portion of the TOE as "online plug-in", whereas [CCECG] refers to it as "web plug-in". That nomenclature is clarified in the Note section of [CCECG], Chapter 1, Page 7.

- Secure Gateway Administration guide [SG_Admin];
- Web Interface 5.4 guide [WI_Guide].

III. EVALUATED CONFIGURATION

TOE Identification

32. The TOE is Citrix XenApp 6.0 for Windows Server 2008 R2 - Platinum Edition, which consists of:

a) a physical deployment of all of the XenApp Server version 6.0 components (i.e. the Independent Computing Architecture (ICA) Server, the Extensible Markup Language (XML) Service and the Secure Ticket Authority[3], as provided on the DVD labelled *"Citrix XenApp™ for Microsoft® Windows Server™ 2008 R2, Version 6.0, part number 745-0108"*, with the two Hotfixes XA600W2K8R2X64002 and XA600W2K8R2X64021, as detailed in [CCECG] Chapter 3), including at least two physical instances of the ICA Server component operating as a Server Farm;

b) Secure Gateway version 3.2;

c) Web Interface version 5.4;

d) Online Plug-in version 12.1.

TOE Documentation

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

34. Generally, Citrix documents are provided as on-line e-document libraries. For this TOE, PDF versions of necessary guidance documents ([CCECG], [AG], [SG_Admin], [OLP], [WI_Guide]) are provided for download from the "Common Criteria" area of the "Security & Compliance" Citrix support website (**https://www.citrix.com/lang/English/support.asp**).

TOE Scope

35. The TOE Scope is defined in the Security Target [ST] Section 1.4. Functionality that is outside the TOE Scope is defined in [ST] Section 1.4.3

TOE Configuration

36. The evaluated configuration of the TOE is defined in [ST] Section 1.3 and in [CCECG]. The following diagram shows the evaluated configuration.

[3] The ICA Server, the XML Service and the Secure Ticket Authority are described in Chapter IV (in 'Product Description and Architecture') of this report.

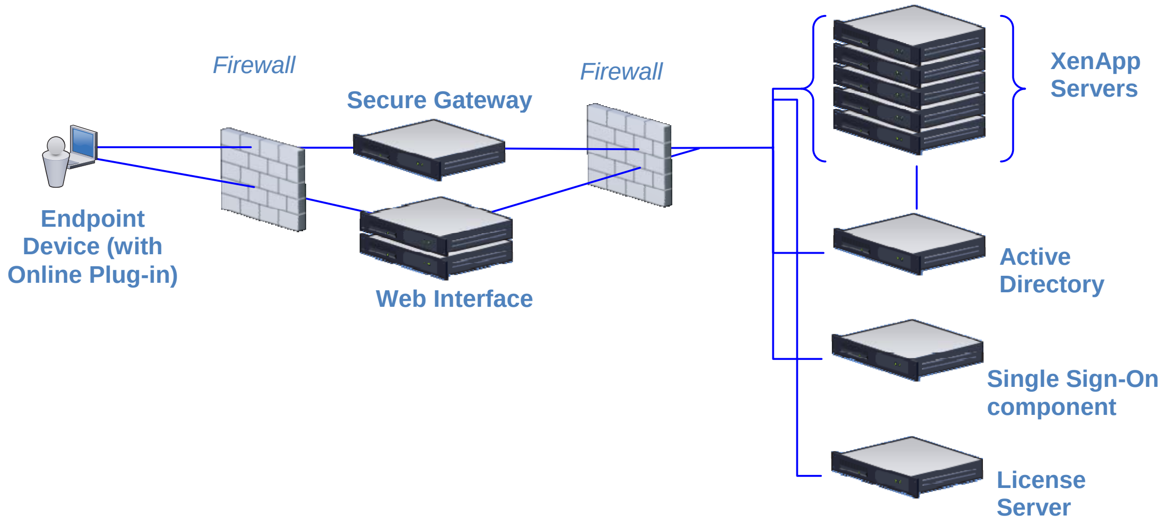

Figure 1 - TOE Configuration

Environmental Requirements

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

38. The TOE was evaluated running on Windows Server 2008 R2, with online plug-in installed on the following client platforms.

a) Windows 7 x86 64-bit;

b) Windows 7 x86 32-bit;

c) Vista x86 64-bit;

d) Vista x86 32-bit.

39. The environmental IT configuration is detailed in [ST] Section 1.4.4.

Test Configuration

40. The Developer's testing used a configuration consistent with Figure 1 above, which shows the single configuration of the server components supported in the evaluated configuration. Four client platforms (listed above in 'Environmental Requirements') are supported in the evaluated configuration. The Developer performed all tests using the Windows 7 x86 64-bit client platform, then repeated subsets of tests on the other three client platforms (i.e. Windows 7 x86 32-bit, Vista x86 64-bit and Vista x86 32-bit) based on the relevance of the tests to the client portion of the TOE and the differences between the client platforms.

41. The Evaluators performed an analysis of the client platform variations, from which they determined that it was sufficient to perform the complete set of independent tests on a single client platform and to repeat limited subsets of tests on the other three client platforms.

The evaluators therefore chose the Windows 7 x86 64-bit client platform to perform the complete set of independent tests. The platform rationale was agreed in advance with the CESG Certification Body. The Evaluators' test configuration was consistent with Figure 1 above.

IV. PRODUCT ARCHITECTURE

Introduction

42. 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

43. The architecture of the TOE incorporates the following software components that work together to provide to TOE users their permitted published applications (and associated data) via an Online Plug-in that resides on their local endpoint device:

a) The Online Plug-in allows the user access to published applications on an Independent Computing Architecture (ICA) Server, as if they were running locally (note that this is the 'Online Plug-in – web' version of the Online Plug-in). The Online Plug-in intercepts and sends key strokes, mouse clicks, etc. from the local operating system and communicates them to the ICA Server. It receives screen updates in return, which it passes to the local operating system for display.

b) The ICA Server is the XenApp component that runs published applications and may exist as one or more instances on one or more physical servers. XenApp Administrators install and publish the applications that are to be deployed by an ICA Server.

c) The Web Interface gives users access to published applications. A user logs on to Web Interface using a web browser, and is presented with a dynamically created web page containing a list of links to the applications that he/she is authorised to launch (i.e. the user's permitted published applications).

d) The Secure Gateway permits users authenticated by Web Interface to access resources on an internal network and provides a link between two encrypted data tunnels (using Transport Layer Security (TLS) and Internet Protocol Security (IPsec) protocols that invoke FIPS 140-2 validated cryptographic functions provided by the operating system) for client-server communications.

e) The Secure Ticket Authority generates and validates tickets that allow an Online Plug-in to gain access through the Secure Gateway to an ICA Server to run a published application for a particular authenticated user.

f) The XML Service is used by the Web Interface to retrieve the list of permitted published applications for a user, and the identity of the least loaded server (on which to run a selected application for a user).

g) Independent Management Architecture (IMA) acts as an intelligent interface between the XenApp Server components of the TOE, and between the XenApp Server components and components of the Windows operating system. It is involved with authentication, session management and connections across the network.

h) The Delivery Services Console (DSC) provides the administration interface to a XenApp Server farm (via IMA), presenting administrators with various management functions.

i) Web Interface Management is a console interface that allows administration activities at the Web Interface. This component can be used by administrators to configure the type of authentication required for users to the Web Interface (username/password or smartcard/Personal Identification Number (PIN)).

44. The above software components run on Microsoft Windows Server/Client platforms as identified in [ST] Sections 1.3 and 1.4.4, and detailed in [CCECG] Chapter 2.

TOE Design Subsystems

45. The TOE subsystems equate to the above software components, shown in Figure 2 below. Their security functionality is described in the component interaction in [ST] Section 1.3.4.

46. The security features provided by the subsystems can be summarised as:

a) **Authentication of users**: endpoint device users are authenticated before access is granted to published applications. Authentication can be by username/password or by smartcard/PIN.

b) **User Access Control**: XenApp administrators can assign user access to published applications. This is achieved by associating a user’s Active Directory account with published applications.

c) **Control over use of endpoint device resources**: centralised control policies, set by a XenApp administrator, determine whether an endpoint device user can access local endpoint device resources such as clipboard transfer and local storage devices (through client drive mapping).

d) **Secure communications**: high performance, standards-based encrypted transmissions are used for communications between server components (IPsec) and between the endpoint device and server components (TLS).

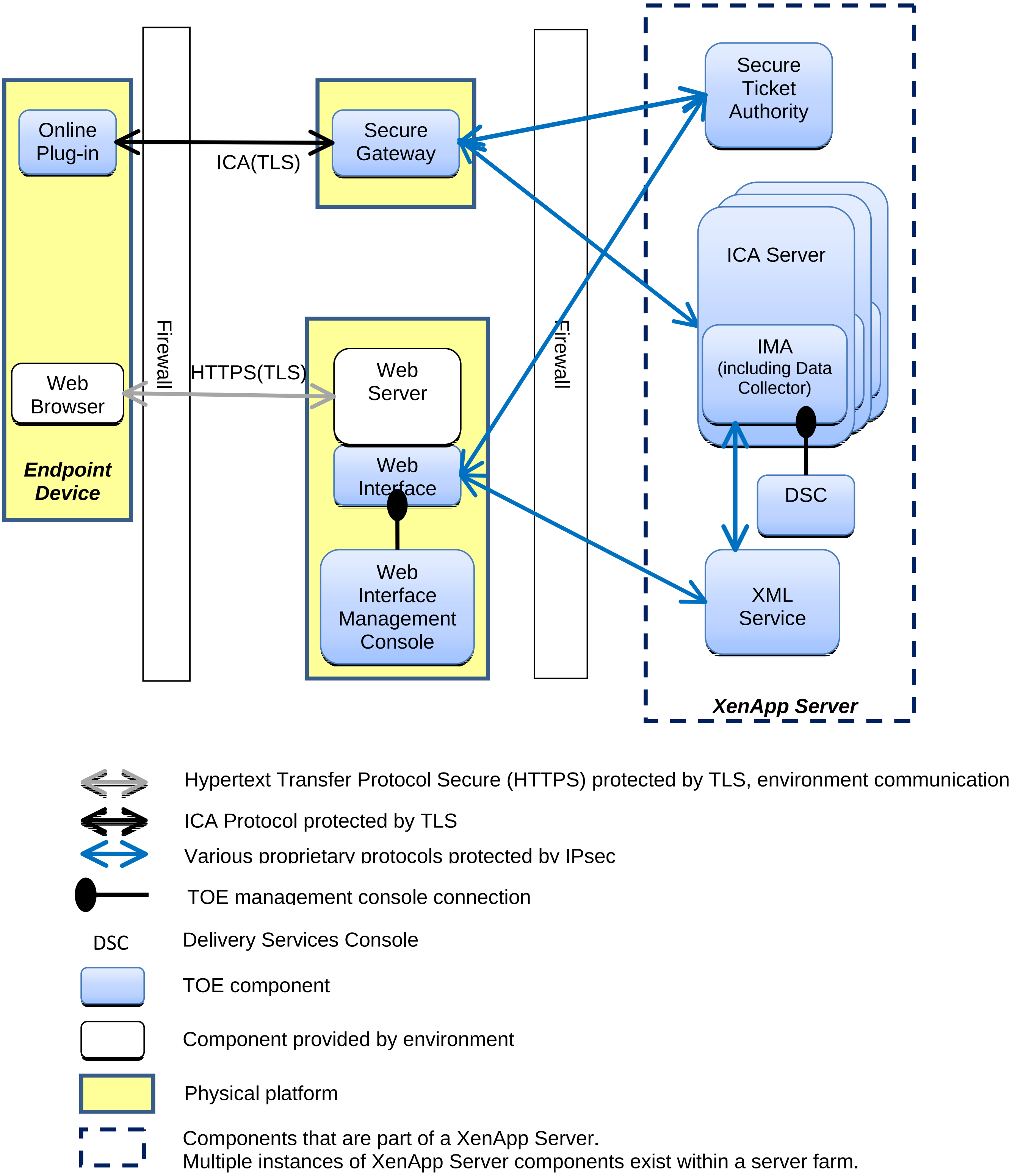
Online Plug-in
ICA(TLS)
Secure Gateway
Secure Ticket Authority
Firewall
Firewall
ICA Server
IMA (including Data Collector)
Web Browser
HTTPS(TLS)
Web Server
Web Interface
Web Interface Management Console
DSC
XML Service
Endpoint Device
XenApp Server
Hypertext Transfer Protocol Secure (HTTPS) protected by TLS, environment communication
ICA Protocol protected by TLS
Various proprietary protocols protected by IPsec
TOE management console connection
DSC
Delivery Services Console
TOE component
Component provided by environment
Physical platform
Components that are part of a XenApp Server.
Multiple instances of XenApp Server components exist within a server farm.

Figure 2 - TOE Subsystems

TOE Dependencies

47. The TOE dependencies are identified in Chapter III ‘Environmental Requirements’ of this report.

TOE Interfaces

48. The external TOE Security Functions Interface (TSFI) are split into two categories:

a) User interfaces into the TOE – these include:

i. User interface to the Web Interface;

ii. User interface to the Online Plug-in;

iii. Administrator’s interface to the DSC;

iv. Administrator’s interface to the Web Interface.

b) Non-user external interfaces – these deal with interfaces between the TOE and the underlying platforms, and where two TOE components interact with each other through underlying platform interfaces.

V. TOE TESTING

TOE Testing

49. The Developer’s tests covered:

a) all SFRs;

b) all TOE high-level subsystems, as identified in Chapter IV (in ‘TOE Design Subsystems’) of this report;

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

50. The Developer’s tests were performed on the single server platform and one of the client platforms, and a subset of the remaining client platforms as described in Chapter III (in ‘Test Configuration’) of this report.

51. The Evaluators devised and ran a total of 20 independent tests, different from those performed by the Developer. Those tests included penetration tests to address potential vulnerabilities considered during the evaluation. No anomalies, exploitable vulnerabilities or errors were detected.

52. All of the Evaluators’ tests were performed on the Windows Server 2008 R2 server platform using the Windows 7 x86 64-bit client platform, with subsets of tests performed using the three other client platforms (i.e. Windows 7 x86 32-bit, Windows Vista x86 64-bit and Windows Vista x86 32-bit) as detailed in Chapter III (in ‘Test Configuration’) of this report.

53. The Evaluators finished running their penetration tests on 21st January 2011.

Vulnerability Analysis

54. The Evaluators’ vulnerability analysis, which preceded penetration testing and was reported in the Evaluation Technical Report ([ETR] and [ETRS]), was based on public domain sources and the visibility of the TOE provided by the evaluation deliverables, in particular the Developer’s security architecture design evidence.

Platform Issues

55. The platforms which are included within the scope of the TOE are listed in Chapter III ‘TOE Identification’ of this report. No platform issues were identified.

VI. REFERENCES

[AG] Administration,
Citrix Systems Inc.,
Document Code: November 04 2010 10:00:07, 4th November 2010.

[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 XenApp 6.0 for Windows Server 2008 R2,
Citrix Systems Inc,
Document code: February 9 2011 16:28:33, 9th February 2011.

[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.

[CR] Common Criteria Certification Report No. CRP241,
UK IT Security Evaluation and Certification Scheme,
CRP241, Issue 1.0, July 2007.

[ETR] Citrix XenApp 6.0 for Windows Server 2008 R2 - Platinum Edition Evaluation Technical Report,
SiVenture CLEF,
LFV/T007/ETR, Issue 1.1, 22nd February 2011.

[ETRS] Review Form (supplement to [ETR]), CESG Certification Body,
CB/110217/LFV/T007, 17th February 2011 (resolved 25th February 2011).

[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).

[OLP] Online Plug-in 12.1 for Windows,
Citrix Systems Inc.,
Document code: January 14 2011 10:56:20, 14th January 2011.

[SG_Admin] Secure Gateway Administration,
Citrix Systems Inc.,
Document Code: September 22 2010 15:03:40, 22nd September 2011.

[ST] Common Criteria Security Target For Citrix XenApp v6.0, for Windows Server 2008 R2 - Platinum Edition,
Citrix Systems Inc.,
CIN4-ST-0001, version 1-0, 7th February 2011.

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

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

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

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

[WI_Guide] Web Interface 5.4,
Citrix Systems Inc.,
Document code: December 14 2010 09:06:29, 14th December 2010.

VII. ABBREVIATIONS

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

CCEVS	US Common Criteria Evaluation & Validation Scheme
DSC	Delivery Services Console
FIPS	Federal Information Processing Standard
HTTPS	Hypertext Transfer Protocol Secure
ICA	Independent Computing Architecture
IMA	Independent Management Architecture
IPsec	Internet Protocol Security
PDF	Portable Document Format (developed by Adobe Systems)
PIN	Personal Identification Number
TLS	Transport Layer Security
XML	Extensible Markup Language

This page is intentionally blank.