122-B

COMMON CRITERIA CERTIFICATION REPORT No. CRP241

Citrix Presentation Server™ 4.5,
Platinum Edition For Windows

Issue 1.0

July 2007

UK Certification Body,
CESG, Hubble Road,
Cheltenham, GL51 0EX
United Kingdom

**ARRANGEMENT ON THE
RECOGNITION OF COMMON CRITERIA CERTIFICATES
IN THE FIELD OF INFORMATION TECHNOLOGY SECURITY**

The Certification Body of the UK IT Security Evaluation and Certification Scheme is a member of the above Arrangement 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 contained in the certificate and Certification Report are those of the Qualified Certification Body which issued it and of the Evaluation Facility which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

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 and Developer	**Citrix Systems Inc.**
Product and Version	**Citrix Presentation Server™ 4.5,** **Platinum Edition For Windows**
Description	Citrix Presentation Server™ 4.5, Platinum Edition For Windows, provides users with secure access to information and applications on a Windows server from a range of devices over a network connection.
CC Part 2	**Extended**
CC Part 3	**Conformant**
EAL	**EAL2** augmented by ALC_FLR.2
CLEF	**BT**
Date authorised	25 July 2007

The evaluation was carried out in accordance with the requirements of the UK IT Security Evaluation and Certification Scheme as described in United Kingdom Scheme Publication 01 (UKSP 01) and UKSP 02 ([a] - [c]). The Scheme has established a 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 [d], 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 [e] and CC Part 3 [g], the Common Evaluation Methodology (CEM) [h], and relevant Interpretations.

The issue of a Certification Report is a confirmation that the evaluation process has been carried out properly and that no exploitable vulnerabilities have been found. It is not an endorsement of the product.

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Citrix Presentation Server™ 4.5, Platinum Edition For Windows, to the Sponsor, Citrix Systems, Inc., 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 [d], which specifies the functional, environmental and assurance requirements.

Evaluated Product and TOE Scope

3. The version of the product evaluated was:

Citrix Presentation Server™ 4.5, Platinum Edition For Windows.

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'.

6. The TOE provides users with secure network access to applications and information. This access can be from a range of devices over any network connection including Local Area Networks, Wide Area Networks, dial-up or wireless connections, or the Internet.

7. The TOE configuration consists of:

a. the Client Component, which gives users access to the applications; and

b. the Server Component, on which the applications reside.

8. The TOE is assumed to operate in a secure environment and the TOE scope excludes the platforms and Operating Systems on which the product is installed.

9. An overview of the product and its security architecture can be found in Chapter IV 'Product Security Architecture'.

Security Claims

10. The Security Target [d] fully specifies:

a. The product's security objectives;

b. The threats which those objectives counter;

c. The Organizational Security Policies which those objectives meet;

d. Security Functional Requirements (SFRs) and security functions to elaborate those objectives. Most of the SFRs are taken from CC Part 2 [f]; use of this standard facilitates comparison with other evaluated products.

11. The only SFR not taken from CC Part 2 [f] is the extended component FTP_ITC.2, which has been closely modelled on FTP_ITC.1 (taken from CC Part 2).

12. The TOE Organizational Security Policy, detailed in the Security Target [d], states: "Cryptographic functions shall be validated to FIPS 140-1 Level 1 or FIPS 140-2 Level 1".

13. The TOE has an explicit access control Security Function Policy, details of which are given in the Security Target [d].

Strength of Function Claims

14. **The minimum Strength of Function (SoF) is SoF-Basic**. There are no mechanisms in the TOE requiring SoF probabilistic or permutational assessment.

Evaluation Conduct

15. The TOE Security Functions and security environment, together with much of the supporting evaluation deliverables, remained largely unchanged from that of Citrix Presentation Server 4.0 for Windows, which had previously been certified by the UK Security Evaluation and Certification Scheme to EAL2 augmented by ALC_FLR.2 [i].

16. For this evaluation of Citrix Presentation Server 4.5, Platinum Edition For Windows, the Evaluators addressed every CEM [h] work unit for EAL2 augmented by ALC_FLR.2, but made some use of Citrix Presentation Server 4.0 for Windows evaluation results where these remained valid for Citrix Presentation Server 4.5, Platinum Edition For Windows.

17. The Certification Body monitored the evaluation, which was carried out by the BT Commercial Evaluation Facility (CLEF). The evaluation addressed the requirements specified in the Security Target [d]. The results of this work, completed in July 2007, were reported in the Evaluation Technical Report (ETR) [j].

Conclusions and Recommendations

18. The conclusions of the Certification Body are summarised in the Certification Statement on Page 2.

19. **Prospective consumers of Citrix Presentation Server 4.5, Platinum Edition For Windows, should understand the specific scope of the certification by reading this report in conjunction with the Security Target [d]**. The TOE should be used in accordance with the environmental assumptions specified in the Security Target. Prospective consumers are advised to check that this matches their identified requirements, and to give due consideration to the recommendations and caveats of this report.

20. **This Certification Report is only valid for the evaluated TOE**. This is specified in Chapter III 'Evaluated Configuration'.

21. **The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration**. Chapter II 'Product Security Guidance' below includes a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

22. Users of Citrix Presentation Server 4.5, Platinum Edition For Windows, should make sure that its IT environment is securely configured, including the installation of appropriate security patches and hotfixes.

23. If any changes are proposed to the TOE's functionality, or to components that were examined during the evaluation, such changes should be handled under the Assurance Continuity Scheme. If the change falls outside the scope of Assurance Continuity, a partial or complete re-evaluation of the product should be performed.

24. **Certification is not a guarantee of freedom from security vulnerabilities:** there remains a small probability (smaller with greater assurance) that exploitable vulnerabilities may be discovered after a certificate has been awarded. This Certification Report reflects the Certification Body's view at the time of certification. Consumers (both prospective and existing) should check regularly for themselves whether any security vulnerabilities have been discovered since this report was issued, and, if appropriate, should check with the Vendor to see if any patches exist for the product, and whether these patches have further assurance. The installation of patches for security vulnerabilities, whether or not they have further assurance, should improve the security of the product.

II. PRODUCT SECURITY GUIDANCE

Introduction

25. The following sections note considerations that are of particular relevance to purchasers of the product.

Delivery

26. The software for the product is delivered by courier to the customer site in a sealed pack, labelled with the reference number 635-1502, marked 'Citrix Presentation Server Platinum Edition'.

27. On receipt of the TOE, the consumer is recommended to check that the evaluated versions of its constituent components have been supplied, and to check that the security of the TOE has not been compromised in delivery.

28. Each Delivery Pack contains the following CDs:

a. Marked 'Citrix Presentation Server for Microsoft Windows Server 2003 64-bit – English Version 4.5' and identified by the reference number 645-2031. This contains the Citrix software for the **Presentation Servers**, including the **Secure Ticket Authority** to be installed on the 64-bit edition of Microsoft Windows 2003.

b. Marked 'Citrix Presentation Server for Microsoft Windows Server 2003 32-bit – English Version 4.5' and identified by the reference number 645-2024. This contains the Citrix software for the **Presentation Servers**, including the **Secure Ticket Authority** to be installed on the 32-bit edition of Microsoft Windows 2003.

c. Marked 'Citrix Presentation Server Components Disk – English Version 4.5' and identified by the reference number 645-2038. This contains the software for the **ICA Clients, the Web Interface**, and the **Secure Gateway**.

d. Other CDs not used in the evaluated configuration.

29. The CDs are contained in a plastic wallet in a cardboard sleeve. A Web Key, unique to every order, is generated by Citrix and maintained on its order management system. This Web Key is packaged with the CDs and shrink-wrapped. The customer then logs on to the Citrix secure web site, using their user account details provided by email, and enters the Web Key. This enables the downloading of the licence file which activates the product.

30. Installation and guidance documentation is delivered with the software.

Installation and Guidance Documentation

31. The supporting guidance documents evaluated were as follows:

a. Evaluated Configuration Guide [n];

b. Administrator's Guide, Citrix Presentation Server 4.5 for Windows [k];

c. Administrator's Guide, Citrix Web Interface 4.5 [l];

d. Administrator's Guide, Secure Gateway for Windows [m].

32. The Evaluated Configuration Guide [n] describes the procedures that must be followed to install and configure the product in its evaluated configuration, and to operate it securely. It also describes the procedures that must be followed to configure the environment. Hence it is recommended that those procedures are read first.

33. The intended audience of the installation and guidance documents is the administrator.

34. Users should note that "Citrix Presentation Server" was previously referred to as "Citrix MetaFrame Presentation Server" and this is still reflected in some guidance documentation.

III. EVALUATED CONFIGURATION

TOE Identification

35. The TOE consists of:

a. Citrix Presentation Server 4.5, Platinum Edition For Windows, including the Secure Ticket Authority (STA) software, Independent Client Architecture (ICA) Server, Independent Management Architecture (IMA), Access Management Console (AMC) and XML Service;

b. Citrix Web Interface, 4.5, including the AMC;

c. Citrix Secure Gateway 3.0 with Hotfix SGE300W003;

d. Citrix ICA Client Version 10.0.

36. The figure below shows the components and scope of the TOE:

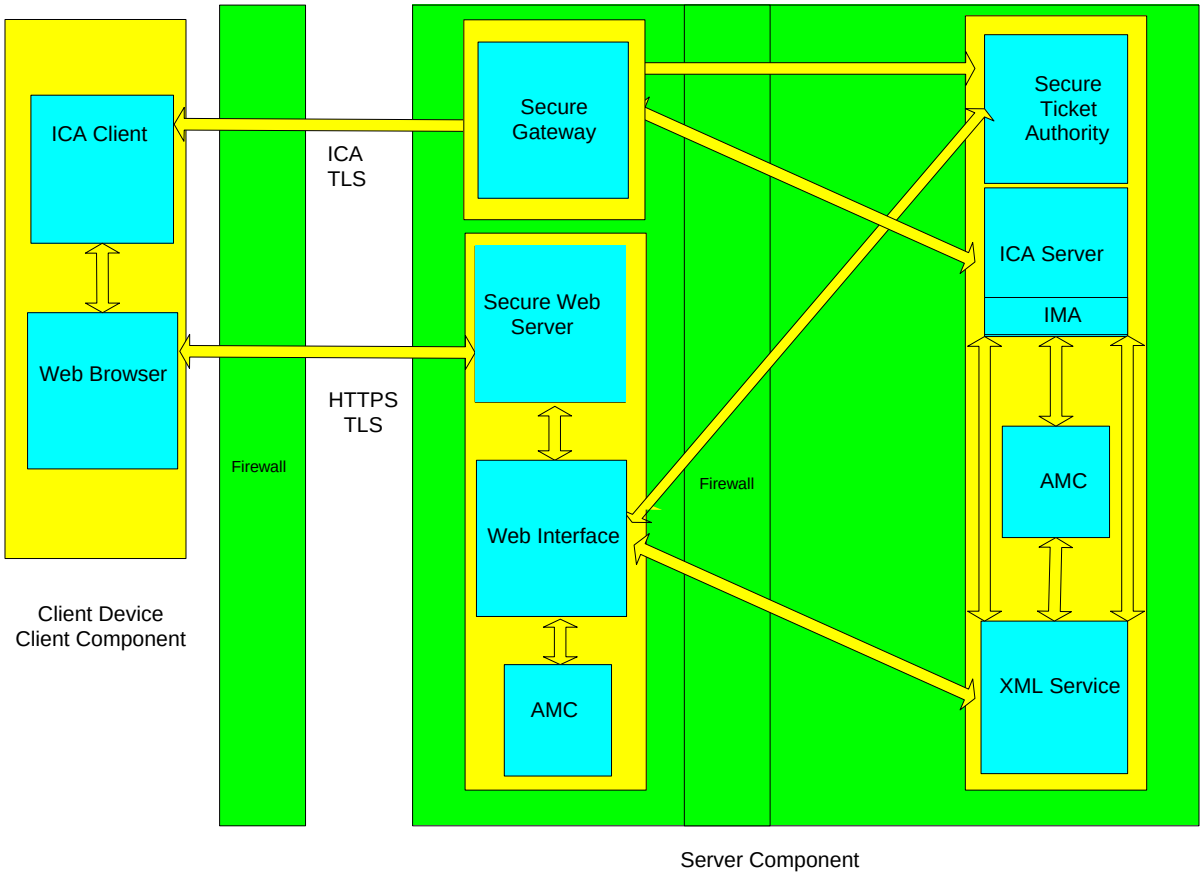


Figure 1: Components and Scope of the TOE

TOE Documentation

37. The relevant guidance documentation for the evaluated configuration is identified in Chapter II 'Product Security Guidance'.

TOE Scope

38. The TOE is identified above under 'TOE Identification'.

39. All parts of the Microsoft Windows Operating Systems (Windows 2003 Server 32-bit edition, Windows 2003 Server 64-bit edition and Windows XP) are considered as part of the environment, including the web browser, Microsoft Internet Explorer, implementations of HTTP, HTTPS and TLS and the Secure Web Server, Microsoft IIS version 6.0.

TOE Configuration

40. The TOE configuration is detailed in the Evaluated Configuration Guide [n].

41. The TOE configuration consists of Citrix Presentation Server software, distributed over the following platforms:

a. One or more **ICA Client** platforms, running Citrix ICA Client version 10.0.

b. The **Web Interface** server, running Citrix Web Interface, Version 4.5.

c. The **Secure Gateway** server, running Citrix Secure Gateway, version 3.0 with Hotfix SGE300W003.

d. One or more **Presentation Servers**, running Citrix Presentation Server 4.5, Platinum Edition For Windows. (Presentation Servers can be grouped together by Citrix as Server Farms. One of the Presentation Servers also acts as a **Secure Ticket Authority**.)

Environmental Requirements

42. It is assumed that the environment will counter the threats of unauthorized access to the physical components of the TOE – server and client platforms. It is also assumed that software outside the scope of the TOE (e.g. Microsoft Windows Operating Systems and their services; and firewall software) will be securely configured and operate correctly.

43. The environment platforms are configured as follows.

a. The **ICA Client** platforms have Microsoft Windows XP, Service Pack 2, with Internet Explorer 7.0, configured for TLS. Hotfixes are installed as listed in the Evaluated Configuration Guide [n]. The hardware platform should be a 233MHz, or faster, Pentium-compatible processor with 256MB of RAM and a 8GB hard disk.

b. The **Web Interface** server has Microsoft Windows 2003 Server, Service Pack 2, with Microsoft IIS version 6.0 (with ASP.NET) and the Microsoft .NET 2.0 and Visual J#.NET 2.0. The hardware platform should be a 550MHz, or faster, Pentium-compatible processor with 256MB of RAM and a 8GB Hard disk.

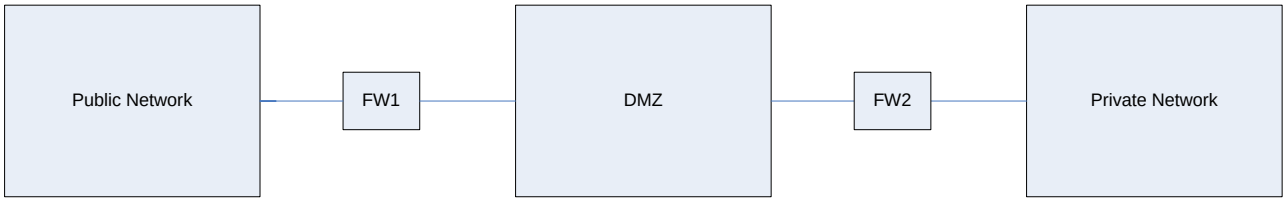
c. The **Secure Gateway** server has Microsoft Windows 2003 Server, Service Pack 2. The hardware platform should be a 550MHz, or faster, Pentium-compatible processor with 512MB of RAM and a 6GB hard disk.

d. The **Presentation Servers** have Microsoft Windows 2003 Server (32-bit or 64-bit editions) with Terminal Services (Service Pack 2) and Microsoft IIS 6.0. On the primary Presentation Server, Microsoft SQL Express 2005 Service Pack 1 and Citrix Access Suite License Server must also be installed. Note that:

i. for the 32-bit edition, the hardware platforms should be a 600MHz or faster Pentium-compatible processor, 256MB RAM and a 8GB hard disk;

ii. for the 64-bit edition, the hardware platforms should be a 600MHz x64 architecture-based computer with Intel Pentium or Xeon family with Intel Extended Memory 64 Technology, or AMD Opteron family, AMD Athlon 64 family, or compatible processor, 512MB RAM and a 8GB hard disk.

44. In addition to the above servers, the Environmental Configuration is assumed to include two firewall devices connecting a private network to a public network. The Presentation Servers are on the private network. The ICA Clients are on the public network. The Web Interface, AMC, Secure Gateway and Secure Web Server are in the Demilitarized Zone (DMZ) between the two firewalls. The configuration is illustrated below:



45. The two platforms shown in the diagram as **FW1** and **FW2** are firewall devices, running any suitable firewall software.

46. **FW1** should be configured to allow traffic between the **ICA Clients** and the servers in the DMZ (the **Web Interface** and **Secure Gateway**) on port 443 (the TLS port) using Network Address Translation. Only new connections from the public network to the DMZ are allowed.

47. **FW2** should be configured to allow IPsec and UDP traffic between the DMZ Servers (the **Web Interface** and **Secure Gateway**) and the private network servers (the **Presentation Servers**).

48. The environmental configuration also includes four further devices, in the private network, as follows:

a. a Domain Controller;

b. a terminal used for Operating System administration and user enrolment;

c. a Citrix Password Manager (CPM) Service Machine;

d. a CPM Console Machine.

49. The CPM machines were included in order to demonstrate the correct operation of CPM 4.5 with the TOE.

50. The Web Interface, the **Presentation Servers**, the user enrolment platform, the CPM Service Machine and the CPM Console Machine all need to be in the same Microsoft Windows domain as the Domain Controller.

51. For full details of the environmental configuration, see the Evaluated Configuration Guide [n].

Test Configuration

52. For the test configuration, there were four **Presentation Servers** (two running Microsoft Windows 2003 32-bit edition and two running Microsoft Windows 2003 64-bit edition) and one **ICA Client** platform.

53. The environmental configuration used by the developer and the evaluators to test the TOE is summarised in the table below and in Figure 2.

Quantity	Hardware Type
11 (all machines except Firewalls)	HP xw4300 (32bit 2.8GHz Intel Pentium4 based PC; 1024MB RAM; 150GB Hard Disk Drive; CD-ROM; Broadcom NetXtreme Network Interface Card)
2 (FW1 and FW2)	Dell 1400 Workstations (32bit, 800MHz Intel Pentium3 based PC; 512MB RAM; 8GB Hard Disk Drive; CD-ROM; 2* Intel Pro 1000 Network Interface Cards
2	Monitors (various specifications, all 1024 x 768 > 70Hz capable)
2	Generic 2 button mice (Microsoft compatible)
2	Generic 105 key UK keyboards
2	8 port 10baseT Ethernet hubs
1	4 port 10baseT Ethernet hub
15	RJ45 Ethernet cables (CAT5)
3	GemPC410-SL GemPlus smartcard readers
3	GemSafe (GEM-159) smartcard
1	Test Racks
3	10 way power extension cables
1	Toshiba M1 Laptop with Microsoft Windows XP Professional

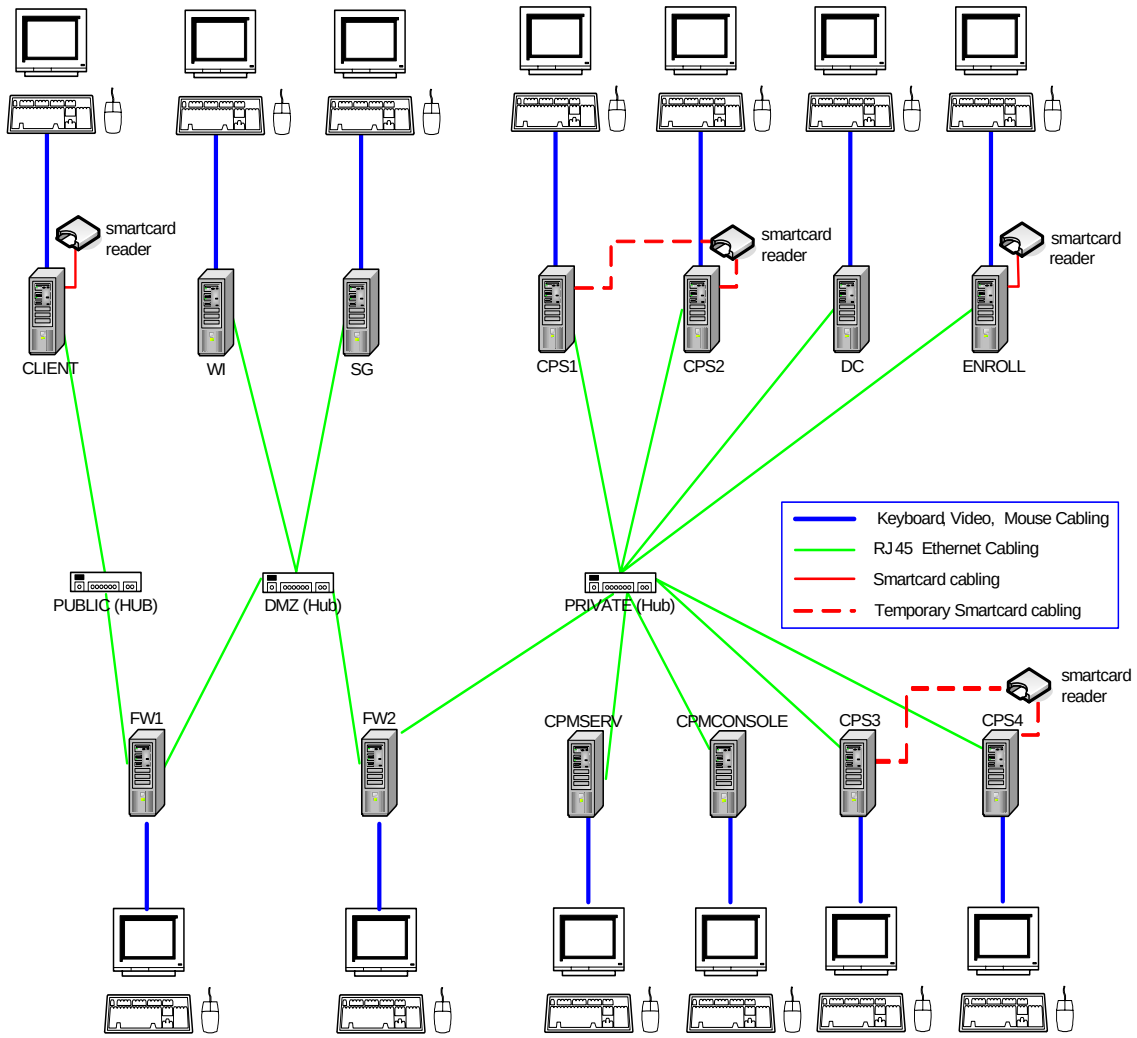


Figure 2 - Test Configuration

54. Note that, although Figure 2 shows individual workstations, the test network used two Keyboard, Video, Mouse (KVM) switches to reduce the number of keyboards and monitors required.

IV. PRODUCT SECURITY ARCHITECTURE

Introduction

55. This Chapter gives an overview of the main product architectural features. Other details of the scope of evaluation are given in Chapter III 'Evaluated Configuration'.

Product Description and Architecture

56. A description of the product is provided in Chapter 2 of the Security Target [d].

57. The product architecture is illustrated in Figure 1.

58. The product consists of a Client Component and a Server Component.

59. The Client Component consists of Citrix ICA Client software and a Web Browser[1]

60. The Server Component consists of a Citrix Secure Gateway Server, a Secure Web Server[2], a Web Interface, and a Presentation Server. The Presentation Server is further composed of an ICA Server component, a Secure Ticket Authority, the Citrix XML service, and the Independent Management Architecture (IMA) interface.

61. The Presentation Server[3] allows multiple users to logon and run applications in separate protected sessions on the same server. These servers install and publish the applications for use through the Client component. Servers can be grouped together to form a Presentation Server Farm, managed as a single entity.

62. One of the Presentation Servers is configured as a Secure Ticket Authority (STA). The Web Interface calls the STA to generate and validate tickets for access to Presentation Server published applications.

63. ICA Clients exchange information between a user's client device and the published application resources on the Presentation Server. ICA Client software is available for a range of different devices and platforms. Keystrokes, mouse clicks and screen updates are sent between the server and the client – encrypted to provide confidentiality and integrity. Published applications run entirely on the server, but to the user of the client device it appears as if the software is running locally. Security is provided via the Transport Layer Security (TLS) and IPsec protocols, which support server authentication, encryption and message integrity checks.

---

[1] The Web Browser is part of the Operating System software and is excluded from the TOE scope.

[2] The Secure Web Server is also part of the Operating System software and excluded from the TOE scope.

[3] Readers should note carefully the following terms which may sometimes appear ambiguous:
- "Citrix Presentation Server 4.5, Platinum Edition For Windows" is the overall name for the product;
- the "Presentation Server" is one of the platforms which make up the configured product;
- "Citrix Presentation Server 4.5, Platinum Edition For Windows" - or "Presentation Server" - is also used for the part of the product software on the Presentation Server platform.

64. The Web Interface gives authorized users access to published applications and information, via the network connection. Users log on to the Web Interface using an internet browser and see links to the applications that they are authorized to run[4]. The Web Interface dynamically creates an HTML page for the Presentation Server Farm for each authorized user. After logging on, the user sees a web page that includes all the applications and resources in the Presentation Server Farm configured for that user. When the user selects an application from that web page, Web Interface generates the ICA file for the client to connect to the Presentation Server via the Secure Gateway.

65. The Secure Gateway is used in combination with the Web Interface to securely transport data using standard security technology. It permits users authenticated by the Web Interface to access Presentation Server resources and provides a link between two encrypted data tunnels (TLS and IPsec protocols), for the client-server communication.

66. The product relies on the following, in its environment, for its successful operation:

a. Operating Systems software to run the product components and for communication between the components;

b. the Web Browser and Secure Web Server;

c. additional platforms acting as firewalls.

Design Subsystems

67. The design subsystems are described below:

a. the ICA Client subsystem is the user component that provides a representation of the application running on the ICA Server;

b. the Web Interface subsystem provides the user interface used to authenticate the user and provide the user with the applications they can use;

c. the XML Service subsystem provides an interface for the Web Interface to talk to the ICA Server and the IMA;

d. the Secure Ticket Authority subsystem provides a mechanism to authenticate users after the application has been selected for running;

e. the Secure Gateway subsystem provides a secure conduit to the ICA Server. It works with the Secure Ticket Authority subsystem to validate the user;

f. the ICA Server subsystem runs the applications selected by the user;

g. the IMA subsystem provides authentication of users; lists of applications for authenticated users; and other management functions outside the scope of the evaluation.

[4] Note that, while the Citrix administrator defines which applications are published for individual users, the creation and management of users remains part of the Windows 2003 Operating Systems.

Hardware and Firmware Dependencies

68. All hardware is considered to be part of the environment. The product interfaces with hardware via the Operating Systems in its environment. There is no firmware within the product.

Product Interfaces

69. The user interfaces into the product are identified as:

a. a User Interface to the Web Interface, via the web browser and web server;

b. the User Interface to the ICA Client;

c. the Administrator's Interface to the IMA;

d. the Administrator's Interface to the Web Interface.

70. In addition, the following Operating System and programmatic product interfaces (i.e. Application Programming Interfaces (APIs)) were identified:

a. ICA Client;

b. Web Interface;

c. XML Service;

d. Secure Ticket Authority;

e. Secure Gateway;

f. ICA Server;

g. IMA.

V. PRODUCT TESTING

IT Product Testing

71. For their independent testing, the evaluators used the TOE installed on the 64-bit Enterprise Edition of the Microsoft Windows 2003 operating system. The developers performed all their tests on both the 32-bit Standard Edition of Microsoft Windows 2003 Server and the 64-bit Enterprise Edition of Microsoft Windows 2003 Server.

72. The environmental configuration used by the evaluators to test the TOE was the same as that used by the developers to test the TOE, as summarised in Figure 2 above.

73. The TOE was tested against the set of external interfaces that comprise the TSFI, as listed above under Chapter IV 'Product Interfaces'.

74. The developer performed tests against all aspects of the TSFI. Those tests also exercised:

a. all related security functions specified in the Security Target [d];

b. all high-level design subsystems identified above under Chapter IV 'Design Subsystems'.

75. All developer tests were manual tests.

76. The evaluators performed the following independent testing:

a. A sample of the developer's tests was repeated to validate the developer's testing. The sample included 20% of the developer tests.

b. For each functional area, the evaluators devised a test that was different from the test(s) performed by the developer, wherever possible.

77. In addition, the evaluators repeated the following two procedures (detailed in the Evaluated Configuration Guide [n]) which demonstrate that CPM 4.5 installed in a configuration similar to its evaluated configuration (see CPM Certification Report [o]) worked correctly with the TOE:

a. verify that the single sign-on is functioning correctly;

b. verify that the Key Management feature is working properly.

78. The evaluators also devised and performed penetration tests to confirm the non-exploitability of potential vulnerabilities that had been noted during the evaluation, and to confirm the developer's vulnerability analysis and strength of function claim.

79. The evaluators used the following tools for their functional and penetration tests:

- Ethereal 0.99.0;
- Openssl 0.9.61;
- Microsoft Baseline Security Analyzer v2.0.1 (Catalog File dated 2007/06/05);
- Nikto 1.36;
- Nessus 3.0.5;
- RetinaMSGSVC 1.0.0;
- RPC3;
- RetinaRPCDCOM v1.0.3;
- Ike-scan v1.9;
- Ike-probe v0.1 Beta;
- Ipsecscan v1.1;
- Screaming Cobra v1.04.

80. The evaluators on-site functional and penetration tests were performed at Citrix Systems Inc, Fort Lauderdale, Florida, USA from 5th to 12th June 2007.

Vulnerability Analysis

81. The Developer's vulnerability analysis documented the search for all vulnerabilities in the TOE. It considered all relevant information and provided, for each vulnerability, a suitable rationale as to why it was not exploitable in the TOE's intended environment.

82. The Evaluators' vulnerability analysis, which preceded penetration testing, was based on both public domain sources and the visibility of the TOE given by the evaluation deliverables.

83. The Evaluators vulnerability analysis included an analysis of possible vulnerabilities in the TOE environment. They did not find any vulnerabilities that could be exploited in the evaluated configuration.

Platform Issues

84. Section 2.3 of the ST [d] details the minimum hardware requirements for the platforms running the components of the TOE.

85. The Citrix Presentation Server can be installed on a Microsoft Windows 2003 platform in either 32-bit or 64-bit architecture. The 32- and 64-bit architecture differences are minimal, with 64-bit architecture providing the ability to double the size of the fundamental unit of data handled by processors while preserving compatibility with the 32-bit x86 architecture. There are a few features that are not included in 64-bit Windows, however the databases, business applications, Terminal Server, Active Directory, Internet Information Services (IIS), and technical computing services used by Citrix Presentation Server are all unaffected.

86. Also, the platforms supporting the firewalls in the TOE environment can be any platforms supporting firewall software that provides the facilities described in Chapter III under 'Environmental Requirements'.

87. Consumers should note that the hardware platforms, the underlying Microsoft Windows operating systems and the firewalls were outside the scope of the evaluation of the TOE.

VI. REFERENCES

[a] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 6.1, March 2006.

[b] CLEF Requirements - Startup and Operation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part I, Issue 4, April 2003.

[c] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 2.1, March 2006.

[d] Security Target for Citrix Presentation Server 4.5, Platinum Edition For Windows,
Citrix Systems Inc.,
Version 2.0, July 2007.

[e] Common Criteria for Information Technology Security Evaluation,
Part 1, Introduction and General Model,
Common Criteria Maintenance Board,
CCMB-2005-08-001, Version 2.3, August 2005.

[f] Common Criteria for Information Technology Security Evaluation,
Part 2, Security Functional Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-002, Version 2.3, August 2005.

[g] Common Criteria for Information Technology Security Evaluation,
Part 3, Security Assurance Requirements,
Common Criteria Maintenance Board,
CCMB-2005-08-003, Version 2.3, August 2005.

[h] Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Maintenance Board,
CCMB-2005-08-004, Version 2.3, August 2005.

[i] Common Criteria Certification Report No. P219:
Citrix Presentation Server 4.0 for Windows,
UK IT Security Evaluation and Certification Scheme,
Issue 1.0, August 2005.

[j] Evaluation Technical Report: Common Criteria EAL2 Evaluation of Citrix Presentation Server 4.5, Platinum Edition For Windows, BT CLEF, LFS/T528/ETR, Issue 1.0, July 2007.

[k] Citrix Presentation Server Administrator's Guide, Citrix Presentation Server 4.5 for Windows, Citrix Systems Inc., Document Code: 2/21/07 (LW).

[l] Web Interface Administrator's Guide, Citrix Web Interface 4.5, Citrix Systems Inc., Document Code: August 8, 2006 11:12 am (ER).

[m] Secure Gateway for Windows Administrator's Guide, Citrix Systems Inc., January 17, 2007 6:27 pm (SV).

[n] Common Criteria Evaluated Configuration Guide, Citrix Presentation Server 4.5 for Windows, Citrix Systems Inc., Document Code: May 18, 2007 6:08 pm (SV).

[o] Common Criteria Certification Report No. P235: Citrix Password Manager, Enterprise Edition, Version 4.5, UK IT Security Evaluation and Certification Scheme, Issue 1.0, June 2007.

VII. ABBREVIATIONS

This list does not include well known IT terms such as LAN, GUI, HTML, ... and standard Common Criteria abbreviations such as TOE, TSF, ... (see Common Criteria Part 1 [e]):

AMC	Access Management Console
CPM	Citrix Password Manager
CPS	Citrix Presentation Server
ICA	Independent Computing Architecture (a presentation services protocol for Microsoft Windows)
IIS	Internet Information Services (part of Microsoft Windows)
IMA	Independent Management Architecture (a Citrix server-side interface)
SSL	Secure Sockets Layer
STA	Secure Ticket Authority
TLS	Transport Layer Security