UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P219

Citrix Presentation Server 4.0 for Windows
running on specified platforms

Issue 1.0

August 2005

UK Certification Body,
CESG, Hubble Road,
Cheltenham, Glos 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	**Citrix Systems, Inc.**
Product and Version	**Citrix Presentation Server 4.0 for Windows.**
Description	Citrix Presentation Server 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	**EAL 2** augmented by ALC_FLR.2
CLEF	**BT CLEF**
Certifier	**CESG**
Approval and Authorisation	**CESG**, Technical Manager of the Certification Body UK IT Security Evaluation and Certification Scheme.
Date authorised	17 August 2005

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 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 4.0 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 4.0 for Windows.

4. The Developer was Citrix Systems, Inc.

5. 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.

6. The TOE configuration consists of:

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

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

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

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 TOE’s security architecture can be found in Chapter IV 'Product Security Architecture'.

Security Claims

10. The Security Target [d] fully specifies:

- The product's security objectives

- The threats and organizational security policies which these objectives counter and meet respectively
- Security functional requirements (SFRs) and security functions to elaborate the 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 that: 'Cryptographic functions shall be validated to FIPS-140-1 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) was SoF-Basic. There are no mechanisms in the TOE requiring SoF 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 MetaFrame XP Presentation Server for Windows, Feature Release 3[1], which had previously been certified by the UK Security Evaluation and Certification Scheme to EAL2 augmented by ALC_FLR.2 [i]. For the evaluation of Citrix Presentation Server 4.0 for Windows, the Evaluators addressed every CEM [h] work unit for EAL2 augmented by ALC_FLR.2, but made some use of Citrix MetaFrame XP Presentation Server for Windows, Feature Release 3 evaluation results where these were valid for Citrix Presentation Server 4.0 for Windows.

16. 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 2005, were reported in the ETR [j].

Conclusions and Recommendations

17. The conclusions of the Certification Body are summarized in the Certification Statement on page 2.

18. **Prospective consumers of Citrix Presentation Server 4.0 for Windows should understand the specific scope of the certification by reading this report in conjunction with the Security Target [d].** The product should be used in accordance with the environmental assumptions specified in the Security Target. Prospective

[1] Version 4 contains two additional features which were evaluated - using cut-and-paste facilities and accessing local drives.

consumers are advised to check that this matches their identified requirements and to give due consideration to the recommendations and caveats of this report.

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

20. **The product 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.

21. Users of Citrix Presentation Server 4.0 for Windows should make sure that its IT environment is securely configured, including the installation of appropriate security patches and hotfixes.

22. **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 products 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

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

Delivery

24. 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.

25. 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 4.0 - Media Kit - English'.

26. Each Delivery Pack contains the following CDs.

a. Marked 'Citrix Presentation Server for Microsoft Windows Server 2003 - English Version 4.0' and identified by the reference number 645-1852. This contains the Citrix software for the ***Presentation Servers***, including the ***Secure Ticket Authority***.

b. Marked 'Citrix Presentation Server Components Disk - English Version 4.0' and identified by the reference number 645-1865. This contains the software for the ***ICA Clients***, the ***Web Interface***, and the ***Secure Gateway***.

c. Other CDs not used in the evaluated configuration.

27. The CDs are placed in a plastic wallet in a cardboard sleeve. A Web Key, unique to every order, is generated and maintained on the 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.

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

Installation and Guidance Documentation

29. The supporting guidance documents evaluated were as follows.

a. MetaFrame Presentation Server Administrator's Guide, Citrix MetaFrame Presentation Server 4.0 for Windows [k].

b. Web Interface Administrator's Guide, Citrix MetaFrame Presentation Server 4.0 [l].

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

30. For secure installation and configuration of the evaluated TOE, see also the Common Criteria Evaluated Configuration Guide [n].

31. There is no specific document providing user documentation. Information which the user needs to know comes from the administrator (as advised in administrator guidance).

32. 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

33. The TOE consists of:

a. Citrix Presentation Server 4.0 for Windows, including the STA software;

b. Citrix Web Interface 4.0;

c. Citrix Secure Gateway 3.0 ; and

d. Citrix ICA Client Version 9.0.

TOE Documentation

34. The relevant guidance documentation for the evaluated configuration is identified above under 'Installation and Guidance Documentation'.

TOE Scope

35. The TOE consists of the parts listed above under 'TOE Identification'.

36. All parts of the Windows Operating Systems 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

37. The TOE configuration is described in detail in the Common Criteria Evaluated Configuration Guide [n].

38. 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 9.0.

b. The ***Web Interface*** server, running Citrix Web Interface, Version 4.0.

c. The ***Secure Gateway*** server, running Citrix Secure Gateway, Version 3.0.

d. One or more ***Presentation Servers***, running Citrix Presentation Server 4.0 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

39. 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 excluded software (e.g. Microsoft Windows Operating Systems and their services; and firewall software) will be securely configured and will operate correctly.

40. The environment platforms are configured as follows.

a. The ***ICA Client*** platforms have Microsoft Windows XP Professional, Service Pack 2, with Microsoft Internet Explorer 6, Service Pack 2, configured for TLS. Internet Explorer has a number of hotfixes as listed in the Evaluation Configuration Guide [n].

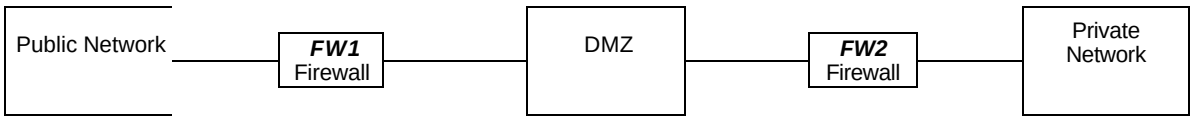
b. The ***Web Interface*** server has Microsoft Windows 2003 Server - with the Secure Web Server, Microsoft IIS, version 6.0, and Microsoft Visual J# .NET 1.1.

c. The ***Secure Gateway*** server has Microsoft Windows 2003 Server.

d. The ***Presentation Servers*** have Microsoft Windows 2003 Server with Terminal Services. Software for Microsoft SQL Server 2000 Desktop Engine with Service Pack 3 (which is available on the Citrix Presentation Server 4.0 for Windows installation CD) is required for these platforms.

41. Each of these platforms should be a 166 MHz or faster Pentium-compatible processor with 256 Mbytes RAM and a 2 Gbyte hard disk with at least 1 Gbyte free. All versions of Microsoft Windows 2003 should include Service Pack 1.

42. In addition to the servers described above, the Environmental Configuration is assumed to include two firewall devices connecting a private network to a public network. The Presentation Servers lie on the private network, and the ICA Clients are on the public network. The Web Interface and Secure Gateway are located in the DMZ between the two firewalls. The network configuration is illustrated in the following diagram.



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

44. ***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.

45. ***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***).

46. The environmental configuration also includes two further devices, in the private network, as follows.

- A Domain Controller.
- A terminal used for Operating System administration and user enrolment.

47. The ***Web Interface***, the ***Presentation Servers*** and the user enrolment platform all need to be in the same Windows domain as the Domain Controller.

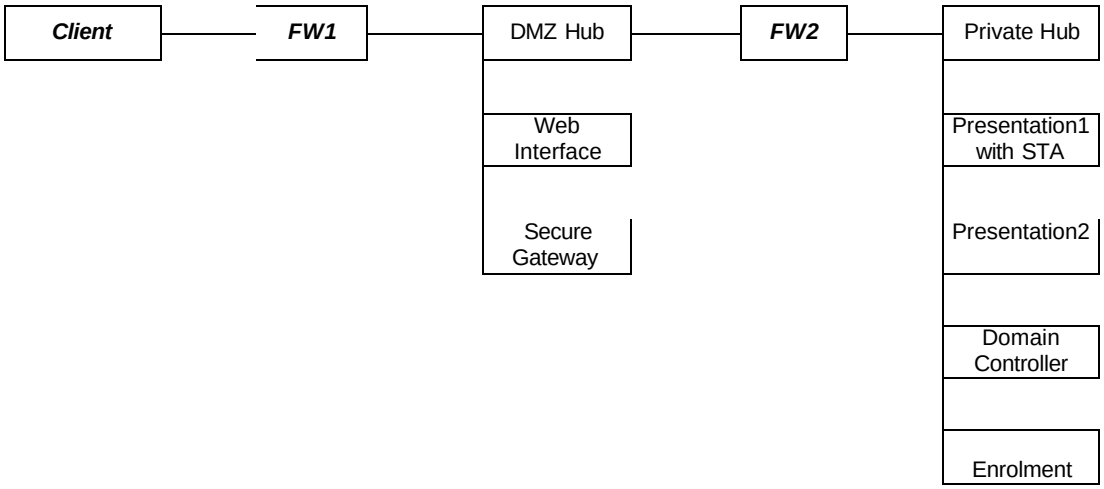
48. For full details of the environmental configuration see the Common Criteria Evaluated Configuration Guide [n].

Test Configuration

49. For the test configuration, there were two ***Presentation Servers*** and just one ***ICA Client*** platform. Each of the nine platforms (i.e. five platforms supporting Citrix, two firewalls, and two additional environment servers) was a Dell OptiPlex GX260, a 32-bit 2GHz Intel Pentium 4 based PC with 512 MB RAM and 40 GB hard disk. The firewalls, configured with Red Hat Linux (version 9), use the Operating System for firewall software.

50. In this test configuration a separate laptop platform was attached to each of the networks in order to test traffic over the networks. For some tests this laptop acted as a second ***ICA Client*** platform.

51. This configuration used in testing is illustrated below.

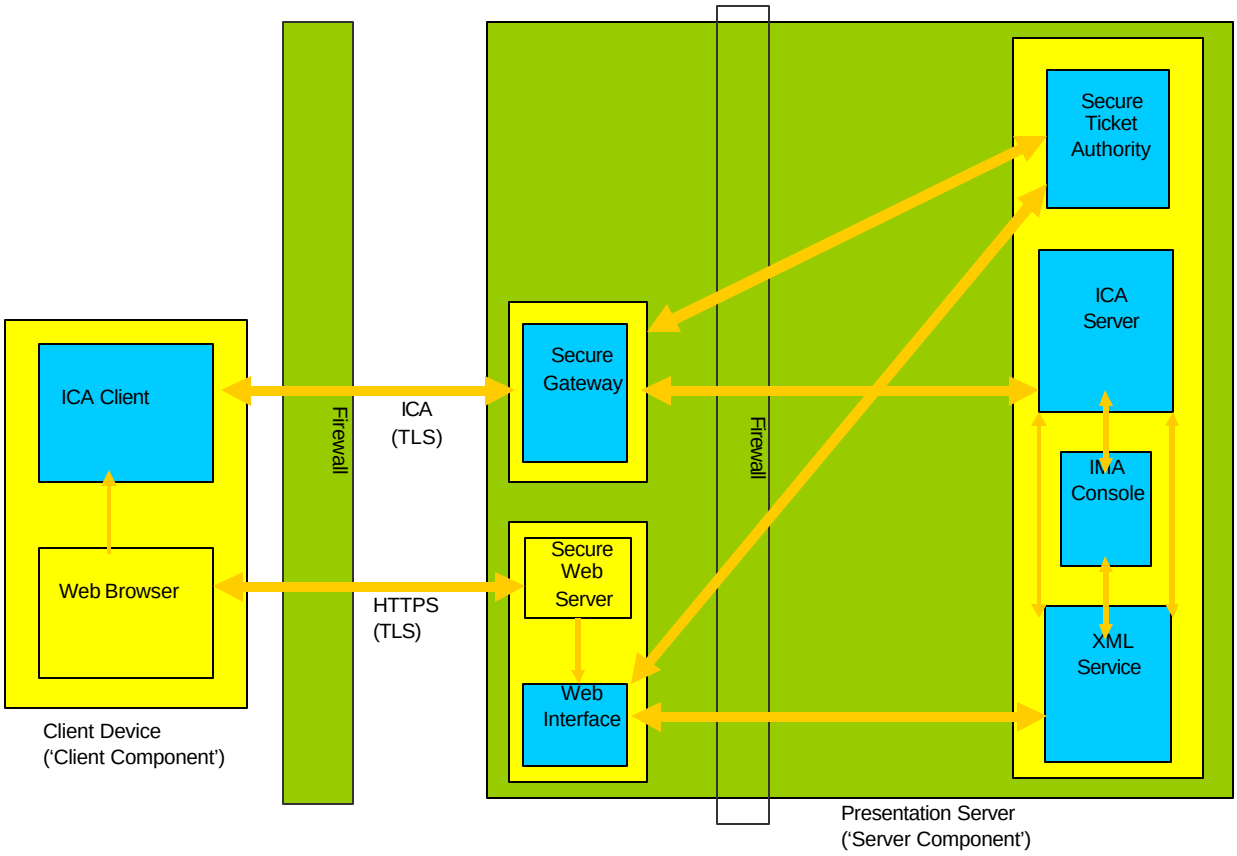


IV. PRODUCT SECURITY ARCHITECTURE

52. 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

53. The Product architecture is illustrated in the following diagram.



54. The product consists of a Client Component and a Server Component,

55. The Client Component consists of Citrix ICA Client software and a Web Browser[2].

56. The Server Component consists of a Citrix Secure Gateway Server, a Secure Web Server[3], 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.

[2] The Web Browser is part of the configured Citrix system but is actually part of the Operating System software and is excluded from the TOE scope.

[3] The Secure Web Server is also part of the Operating System software but excluded from the TOE scope

57. *Presentation Server*[4], 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.

58. 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.

59. *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.

60. The *Web Interface* gives authorized users access to published applications and information through the network connection. Users logon to the Web Interface using an internet browser and see links to the applications that they are authorized to run[5]. 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 that the client needs to connect to the Presentation Server via the Secure Gateway.

61. 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 client-server communication.

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

- Operating Systems software to run the product components and for communication between the components.
- The Web Browser and Secure Web Server.
- Additional platforms acting as firewalls.

[4] Readers should note carefully the following terms which may sometimes appear ambiguous:
Citrix Presentation Server 4.0 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 4.0 for Windows or ***Presentation Server*** is also used for the part of the product software on the Presentation Server platform.

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

63. The product is available in three separate Editions as follows, designed for organisations of varying size.

- The *Standard Edition* is for small sized organisations.
- The *Advanced Edition* is for small to medium sized organisations.
- The *Enterprise Edition* is for large organisations.

64. These Editions differ in a number of features which are not security relevant and the evaluation covers all three Editions.

Design Subsystems

65. 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.

Hardware and Firmware Dependencies

66. All hardware and firmware is considered to be part of the environment. The product interfaces with hardware via the Operating Systems in its environment.

Product Interfaces

67. The User Interfaces into the product are identified as:

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

b. the User Interface to the ICA Client;

c. the Administrator's Interface to the IMA; and

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

68. In addition the following Operating System and programmatic product interfaces 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

69. For their independent testing, the Evaluators used the Enterprise Edition, which includes all features available in the other Editions.

70. The Evaluators used the following tools in their Penetration Testing of the TOE:

- OpenSSL 0.9.61,
- Ethereal 0.1.11a,
- Microsoft Baseline Security Analyzer v1.2.1,
- Nikto 1.35,
- Nessus 2.2.2,
- RetinaMSGSVC v1.0.0,
- RetinaRPCDCOM v1.0.3,
- ISS Security Scanner v7.0, SP2, and
- RPC3.

71. The Developers' tests and the Evaluators' functional tests covered all of the TOE subsystems and covered all Security Functions claimed in the Security Target [d].

72. All User Interfaces were tested.

Vulnerability Analysis

73. 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 process.

74. 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

75. Each of the client and server platforms supporting the TOE can be any 166 MHz or faster Pentium-compatible processor with 256 Mbytes RAM and a 2 Gbyte hard disk (with at least 1 Gbyte free.)

76. In addition, the platforms supporting the firewalls in the TOE environment can be any platforms supporting firewall software able to provide the facilities described in Chapter III under 'Environmental Requirements.'

77. Consumers should note that the hardware platforms, the underlying Windows Operating Systems and the firewalls are excluded from the TOE.

VI. REFERENCES

[a] Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 5.0, July 2002

[b] CLEF Requirements - Startup and Operations,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part 1, Issue 4, April 2003

[c] CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part 2, Issue 1.0, April 2003

[d] Security Target for Citrix Presentation Server 4.0 for Windows,
Citrix Systems Inc.,
ST/T488, Version 1.0 , July 2005.

[e] Common Criteria Part 1,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-001, Version 2.2, January 2004.

[f] Common Criteria Part 2,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-002, Version 2.2, January 2004.

[g] Common Criteria Part 3,
Common Criteria Interpretations Management Board,
CCIMB-2004-01-003, Version 2.2, January 2004.

[h] Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Interpretations Management Board ,
CCIMB-2004-01-004, Version 2.2, January 2004.

[i] Common Criteria Certification Report No. P201:
Citrix MetaFrame XP Presentation Server for Windows,
Feature Release 3 with hotfix MPS_FR3_EAL2,
UK IT Security Evaluation and Certification Scheme,
P201, Issue 1.0, April 2004.

[j] Evaluation Technical Report: Common Criteria EAL2 Evaluation of Citrix Presentation Server 4.0 for Windows,
BT CLEF,
LFS/T488/ETR, Issue 1.0, 8 July 2005.

[k] MetaFrame Presentation Server Administrator's Guide, Citrix MetaFrame Presentation Server 4.0 for Windows,
Citrix Systems Inc.,
Document Code: February 21, 2005 (MM).

[l] Web Interface Administrator's Guide, Citrix MetaFrame Presentation Server 4.0,
Citrix Systems Inc.,
Document Code: January 28, 2005 4:51 pm (LD).

[m] Secure Gateway for Windows Administrator's Guide,
Citrix Systems Inc.,
Document Code: March 3, 2005 (CG).

[n] Common Criteria Evaluated Configuration Guide: Citrix MetaFrame Server 4.0 for Windows,
Citrix Systems, Inc.,
Document Code: June 29, 2005 2:07 pm (RW).

VIII. ABBREVIATIONS

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
STA	Secure Ticket Authority
SSL	Secure Sockets Layer, a protocol which provides server authentication and encryption
TLS	Transport Layer Security, a standardized version of the SSL protocol
XML	EXtensible Markup Language

[This page is intentionally blank]