UK IT SECURITY EVALUATION AND CERTIFICATION SCHEME

122-B

COMMON CRITERIA CERTIFICATION REPORT No. P201

Citrix MetaFrame XP Presentation Server for Windows

Feature Release 3, with hotfix MPS_FR3_EAL2
running on specified platforms

Issue 1.0

April 2004

UK IT Security Evaluation and Certification Scheme
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. [*]

* Whilst the Arrangement has not yet been extended to address ALC_FLR.2 (flaw remediation procedures), a working agreement exists amongst Parties to the Arrangement to recognise the Common Evaluation Methodology ALC_FLR supplement (Reference [i] in this report) and the resultant inclusion of ALC_FLR.2 elements in certificates issued by a Qualified Certification Body.

CERTIFICATION STATEMENT

Citrix MetaFrame XP 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.

Citrix MetaFrame XP Presentation Server for Windows, Feature Release 3 with hotfix MPS_FR3_EAL2, has been evaluated under the terms of the UK IT Security Evaluation and Certification Scheme and has met the Common Criteria Part 3 conformant requirements of Evaluation Assurance Level EAL2 augmented with ALC_FLR.2 for the specified Common Criteria Part 2 extended functionality in the specified environment when running on the platforms specified in Annex A.

Originator	**CESG** Certifier
Approval and Authorisation	**CESG** Head of the Certification Body UK IT Security Evaluation and Certification Scheme
Date authorized	27 April 2004

(This page is intentionally left blank)

TABLE OF CONTENTS

(This page is intentionally left blank)

ABBREVIATIONS

CC	Common Criteria
CEM	Common Evaluation Methodology
CLEF	Commercial Evaluation Facility
DMZ	(DeMilitarized Zone) A network separated by firewall devices from an internal, private network and a connection to an external, public network.
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
FIPS	Federal Information Processing Standards
HTML	HyperText Markup Language
HTTP	HyperText Transmission Protocol
HTTPS	HTTP, Secure
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
IP	Internet Protocol
IPsec	IP Security, a set of standard extensions to IP providing authenticated encrypted communications
OSP	Organizational Security Policy
SFR	Security Functional Requirement
SoF	Strength of Functions
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
TOE	Target of Evaluation

TSF	TOE Security Function
UDP	User Datagram Protocol
UKSP	United Kingdom Scheme Publication
XML	EXtensible Markup Language

REFERENCES

a. Security Target for Citrix MetaFrame XP Presentation Server for Windows with Feature Release 3,
Citrix Systems Inc.,
ST/T434, Version 1.6, 24 March 2004.

b. Common Criteria Part 1,
Common Criteria Interpretations Management Board,
CCIMB-99-031, Version 2.1, August 1999.

c. Common Criteria Part 2,
Common Criteria Interpretations Management Board,
CCIMB-99-032, Version 2.1, August 1999.

d. Common Criteria Part 3,
Common Criteria Interpretations Management Board,
CCIMB-99-033, Version 2.1, August 1999.

e. Description of the Scheme,
UK IT Security Evaluation and Certification Scheme,
UKSP 01, Issue 5.0, July 2002.

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

g. CLEF Requirements - Conduct of an Evaluation,
UK IT Security Evaluation and Certification Scheme,
UKSP 02: Part II, Issue 1.0, October 2003.

h. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology,
Common Criteria Evaluation Methodology Editorial Board,
CEM-099/045, Version 1.0, August 1999.

i. Common Methodology for Information Technology Security Evaluation,
Part 2: Evaluation Methodology, Supplement: ALC_FLR - Flaw Remediation,
Common Criteria Evaluation Methodology Editorial Board,
CEM-2001/0015R, Version 1.1, February 2002.

j. Evaluation Technical Report: Common Criteria EAL2 Evaluation of Citrix MetaFrame XP Presentation Server for Windows with Feature Release 3,
BT Syntegra CLEF,
LFS/T434/ETR, Issue 1.0, 14 April 2004.

k. Administrator's Guide, Citrix MetaFrame XP Server for Windows with Feature Release 3,
Citrix Systems Inc.,
Document Code: April 30, 2003 12:57 pm (MP).

l. Administrator's Guide, Citrix Web Interface for MetaFrame XP, Feature Release 3,
Citrix Systems Inc.,
Document Code: February 25, 2003 5:52 pm (LM).

m. Administrator's Guide, Citrix Secure Gateway for MetaFrame, Version 2.0,
Citrix Systems Inc.,
Document Code: April 29, 2003 4:15 pm (KT).

n. Advanced Concepts Guide for Citrix MetaFrame XP for Windows, with Feature Release 3,
Citrix Systems Inc.,
Document Code: July 30, 2003 11:55 am (MP).

o. Common Criteria Evaluated Configuration Guide: Citrix MetaFrame XP Server for Windows with Feature Release 3,
Citrix Systems, Inc.,
Document Code: March 22, 2004 2:30 pm (AM).

I. EXECUTIVE SUMMARY

Introduction

1. This Certification Report states the outcome of the Common Criteria security evaluation of Citrix MetaFrame XP Presentation Server for Windows, Feature Release 3, 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 [Reference a], which specifies the functional, environmental and assurance evaluation requirements.

Evaluated Product

3. The version of the product evaluated was:

Citrix MetaFrame XP Presentation Server for Windows, Feature Release 3 with hotfix MPS_FR3_EAL2.

This product is also described in this report as the Target of Evaluation (TOE). The Developer was Citrix Systems, Inc.

4. 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.

5. These Editions differ in a number of features which are not security relevant and the evaluation covers all three Editions. For their independent testing, the Evaluators used the Enterprise Edition, which includes all features available in the other Editions. This version is also sometimes known as Citrix MetaFrame Presentation Server (XPe license).

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 uses a web browser and Citrix ICA Client software; and

b. the Server Component consisting of a Citrix Secure Gateway Server, a Secure Web Server, a Web Interface, an ICA server component, a Secure Ticket Authority and the Citrix XML service.

8. This configuration covers five separate platforms, which are briefly described below.

a. *Presentation Servers:*
MetaFrame XP allows multiple users to logon and run applications in separate protected sessions on the same server. MetaFrame is installed on servers with the Windows 2000 Operating System. These servers install and publish the applications for use through the Client component. Server software includes the Independent Management Architecture (IMA) interface. Servers can be grouped together to form a MetaFrame Server Farm, managed as a single entity.

b. *ICA Clients:*
ICA Clients exchange information between a user's client device and the published application resources on the MetaFrame 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) protocol, which supports server authentication, encryption and message integrity checks.

c. *Web Interface:*
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[1]. The Web Interface dynamically creates an HTML page for the MetaFrame Server Farm for each authorized user. After logging on the user sees a web page that includes all the applications and resources in the MetaFrame 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.

d. *Secure Gateway:*
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 MetaFrame resources and provides a link between two encrypted data tunnels (TLS and IPsec protocols, provided by the Operating System) for client-server communication.

e. *Secure Ticket Authority (STA) Server:*
When the Web Interface receives a request for a Secure Gateway ticket it calls the STA to generate and validate tickets for access to MetaFrame published applications. The secure Ticket Authority software is installed as part of the Citrix Secure Gateway software.

9. Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

[1] 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 2000 Operating System, which is out of scope of the TOE.

10. An overview of the TOE's security architecture can be found in Annex B.

TOE Scope

11. The scope of the TOE consists of the following:

- *Presentation Servers:* Citrix MetaFrame XP Server, which includes the Citrix extensible markup language (XML) service.
- *ICA Clients:* Citrix ICA Client version 7.0. (The Web browser, Microsoft Internet Explorer, and the implementations of HTTP, HTTPS and TLS are considered as parts of the TOE environment.)
- *Web Interface:* Citrix Web Interface, version 2.1, for MetaFrame XP. (The Secure Web Server, Microsoft IIS version 5.0 is considered as part of the TOE environment.)
- *Secure Gateway:* Citrix Secure Gateway, version 2.0, for MetaFrame XP.
- *Secure Ticket Authority:* This is installed as part of the Citrix Secure Gateway, version 2.0, for MetaFrame XP software.

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

13. Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

14. The following are explicitly excluded from the TOE configuration, but are included in its environment:

- hardware platforms and Windows 2000 Operating Systems;
- the web browser, Microsoft Internet Explorer;
- the Secure Web Server, Microsoft IIS;
- hardware and software provided by the firewalls; and
- execution of the cryptographic services of the operating system.

15. 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 2000 and its services; and firewall software) will operate correctly and securely.

Protection Profile Conformance

16. The Security Target [a] did not claim conformance to any protection profile.

Assurance

17. The Security Target [a] specified the assurance requirements for the evaluation. The assurance incorporated predefined evaluation assurance level EAL2, augmented by ALC_FLR.2. Common Criteria (CC) Part 3 [d] describes the scale of assurance given by predefined assurance levels EAL1 to EAL7. An overview of CC is given in CC Part 1 [b].

Strength of Function Claims

18. The minimum Strength of Function (SoF) was SoF-Basic. There are no mechanisms in the TOE requiring SoF assessment.

Security Policy

19. The TOE organizational security policy (OSP), detailed in the Security Target [a], states that: ‘Cryptographic functions shall be validated to FIPS-140-1 or FIPS-140-2 Level 1’.

Security Claims

20. The Security Target [a] fully specifies the TOE’s security objectives, threats and OSPs which these objectives counter and security functional requirements (SFRs) and security functions to elaborate the objectives. Most of the SFRs are taken from CC Part 2 [c]; use of this standard facilitates comparison with other evaluated products.

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

Evaluation Conduct

22. 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 [e - g]. The Scheme has established a Certification Body which is managed by CESG on behalf of Her Majesty’s Government. As stated on page ii of this Certification Report, the Certification Body is a member of the Common Criteria Mutual Recognition Arrangement, and the evaluation was conducted in accordance with the terms of this Arrangement.

23. The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its Security Target [a], 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 [d] and the Common Evaluation Methodology (CEM) [h].

24. For the Flaw Remediation assurance Component, ALC_FLR.2, the Evaluators used the Supplement to CEM [i].

25. The Certification Body monitored the evaluation which was carried out by the BT Syntegra Commercial Evaluation Facility (CLEF). The evaluation was completed when the

CLEF submitted the Evaluation Technical Report (ETR) [j] to the Certification Body in April 2004. The Certification Body then produced this Certification Report.

General Points

26. The evaluation addressed the security functionality claimed in the Security Target [a] with reference to the assumed operating environment specified by the Security Target. The evaluated configuration was that specified in Annex A. 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.

27. 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 such patches have been evaluated and certified.

28. The issue of a Certification Report is not an endorsement of a product.

(This page is intentionally left blank)

II. EVALUATION FINDINGS

Introduction

29. The evaluation addressed the requirements specified in the Security Target [a]. The results of this work were reported in the ETR [j] under the CC Part 3 [d] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with the subsequent assurance maintenance and re-evaluation of the TOE.

Delivery

30. The software for the TOE is delivered in a sealed pack, labelled with the reference number 635-0042, marked 'Citrix MetaFrame XP Presentation Server Feature Release 3 Delivery Pack'.

31. Each Delivery Pack contains the following CDs.

a. Marked 'Citrix MetaFrame XP Feature Release 3, Service Pack 3' and identified by the reference number 645-1663. This contains the MetaFrame software for installation on the ***Presentation Servers***.

b. Marked 'Citrix MetaFrame XP Feature Release 3, Components Disk' and identified by the reference number 645-1637. This contains the software for the ***ICA Clients***, the ***Web Interface***, the ***Secure Gateway*** and the ***Secure Ticket Authority***, together with software for other components not covered in the TOE scope. (Note that, as described below, the version of ***Web Interface*** software on the CD is not used in the evaluated configuration.)

c. Other CDs not used in the evaluated configuration.

32. A license pack is provided separately to give a licence number to allow use of the software beyond a limited trial period.

33. In addition to the components provided on CD, the Web Interface software version 2.1 should be downloaded from the Citrix web site www.mycitrix.com, and the hotfix MPS_FR3_EAL2 should be downloaded from www.citrix.com/download.

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

Installation and Guidance Documentation

35. For guidance on the installation of the components of the TOE, see the Administration Guides for MetaFrame XP Server, the Web Interface, and the Secure Gateway [k - m] and the Advanced Concepts Guide [n].

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

Strength of Function

37. The SoF claim for the TOE was as given above under “Strength of Function Claims”. Based on their examination of all the evaluation deliverables, the Evaluators confirmed that there were no probabilistic or permutational mechanisms in the TOE and that the SoF claim of SoF-Basic was therefore upheld.

Vulnerability Analysis

38. The Evaluators’ vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

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

- Cryptool 1.3.05,
- OpenSSL 0.9.61,
- Ethereal 0.1.10a,
- Microsoft Baseline Security Analyzer v1.2,
- Nikto 1.32,
- Nessus,
- RetinaMSGSVC,
- RetinaRPCDCOM,
- Retina Network Security Scanner, and
- Rp3.

40. The Evaluators vulnerability analysis included an analysis of possible vulnerabilities in the TOE environment, focussed on the Windows 2000 Operating System. They did not find any vulnerabilities that could be exploited in the evaluated configuration

III. EVALUATION OUTCOME

Certification Result

41. After due consideration of the ETR [j], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, the Certification Body has determined that Citrix MetaFrame XP Presentation Server for Windows, Feature Release 3 with hotfix MPS_FR3_EAL2, running on specified platforms meets the specified Common Criteria Part 3 augmented requirements of Evaluation Assurance Level EAL2 with ALC_FLR.2 for the specified Common Criteria Part 2 extended functionality, in the specified environment, when running on the platforms specified in Annex A.

42. The minimum Strength of Function was SoF-basic. The Evaluators confirmed that there were no probabilistic or permutational mechanisms in the TOE and that the SoF claim of SoF-Basic was therefore upheld.

Recommendations

43. Prospective consumers of Citrix MetaFrame XP Presentation Server for Windows, Feature Release 3, should understand the specific scope of the certification by reading this report in conjunction with the Security Target [a]. The TOE should be used in accordance with a number of environmental considerations as specified in the Security Target.

44. Only the evaluated TOE configuration should be installed in the specified environmental configuration. Configurations are specified in Annex A with further relevant information given above under ‘TOE Scope’ and ‘Evaluation Findings’.

45. The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.

46. Users of the TOE should be aware that its operation depends on the operation of the underlying operating systems and hardware platforms as described above under 'TOE Scope'.

47. The above ‘Evaluation Findings’ include a number of recommendations relating to the secure receipt, installation, configuration and operation of the TOE.

(This page is intentionally left blank)

ANNEX A: EVALUATED CONFIGURATION

TOE Identification

1. The TOE consists of:

   a. Citrix MetaFrame XP Presentation Server for Windows with Feature Release 3;

   b. Citrix Web Interface 2.1 for MetaFrame XP;

   c. Citrix Secure Gateway 2.0 for MetaFrame[2] (delivered with Citrix MetaFrame XP Presentation Server for Windows, Feature Release 3); and

   d. Citrix ICA Client Version 7.0. (delivered with Citrix MetaFrame XP Presentation Server for Windows, Feature Release 3).

2. The Citrix MetaFrame XP Presentation Server for Windows software is identified by the reference number 645-1633 on its delivery CD. When installed, this becomes a number of components at version numbers which may not be readily identifiable as Feature Release 3.

3. Citrix Secure Gateway 2.0 for MetaFrame; Citrix ICA Client Version 7.0. (and Citrix Web Interface 2.0 for MetaFrame XP) are identified by the reference number 645-1637 on the delivery CD for the Citrix components.

4. For the delivery and installation of hotfix MPS_FR3_EAL2 (which affects only the Presentation Server software) and Citrix Web Interface 2.1 for MetaFrame XP, see the section above on 'Delivery' and the Citrix MetaFrame XP Server for Windows - Common Criteria Evaluated Configuration Guide [o].

TOE Documentation

5. The supporting guidance documents evaluated were as follows.

   a. Administration Guide for Citrix MetaFrame XP Server for Windows, Feature Release 3 [k].

   b. Administration Guide for Citrix Web Interface for MetaFrame XP, Feature Release 3 [l].

   c. Administration Guide for Citrix Secure Gateway for MetaFrame, Version 2.0 [m].

   d. Advanced Concepts Guide for Citrix MetaFrame XP for Windows, with Feature Release 3 [n].

6. Further discussion of the supporting guidance material is given in Section II under the heading ‘Installation and Guidance Documentation’.

[2] This consists of the Secure Gateway Service and the Secure Ticket Authority software.

TOE Configuration

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

8. The TOE configuration consists of Citrix MetaFrame Presentation Server software distributed over the following platforms.

a. One or more ***ICA Client*** platforms, running Citrix ICA Client version 7.0 on Microsoft Windows 2000 Professional - with Microsoft Internet Explorer 6, Service Pack 1 (with hotfixes Q828750 and Q824145), configured for TLS, considered part of the TOE environment.

b. The ***Web Interface*** server, running Citrix Web Interface for MetaFrame XP, Version 2.1 with security update on Microsoft Windows 2000 Server - with the Secure Web Server, Microsoft IIS, version 5.0, and Microsoft Java Virtual Machine, considered part of the TOE environment.

c. The ***Secure Gateway*** server, running Citrix Secure Gateway for MetaFrame on Microsoft Windows 2000 Server.

d. The ***Secure Ticket Authority*** server, running Citrix Secure Gateway for MetaFrame software on Microsoft Windows 2000 Server - with Microsoft IIS version 5.0 considered part of the TOE environment.

e. One or more ***MetaFrame Presentation Servers***, running Citrix MetaFrame XP Server for Windows (which includes the ICA Server, the IMA server and Citrix XML service) on Microsoft Windows 2000 Server with Terminal Services. Software for Microsoft SQL Server 2000 Desktop Engine with Service Pack 3 (which is available on the Citrix MetaFrame XP Presentation Server for Windows installation CD) is required for these platforms. MetaFrame Presentation Servers can be grouped together by Citrix as Server Farms.

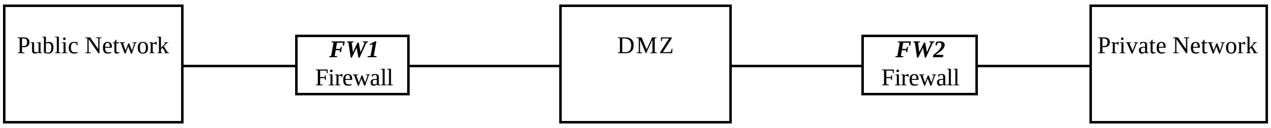
9. Each of these platforms should be a 166 MHz or faster Pentium-compatible processor with 256 Mbytes RAM and a 2 Gbyte hard disk with at least 1 Gbyte free. All versions of Microsoft Windows 2000 should include Service Pack 4 and a number of hotfixes[3].

10. The configuration used for testing is described below under ‘Environmental Configuration’.

[3] The required hotfixes are detailed in [o].

Environmental Configuration

11. The TOE environment is assumed to be configured as three networks separated by two firewalls as shown in the following diagram.



12. The platforms listed above under 'TOE Configuration' are located as follows:

- ***ICA Clients*** are in the public network.
- ***Web Interface*** and ***Secure Gateway*** servers are in the DMZ.
- The ***STA*** and ***MetaFrame Presentation Servers*** are in the private network.

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

14. ***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.

15. ***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 ***STA*** and the ***MetaFrame Presentation Servers***).

16. Fuller details of the firewall configurations are given in the Citrix MetaFrame XP Server for Windows - Common Criteria Evaluated Configuration Guide [o].

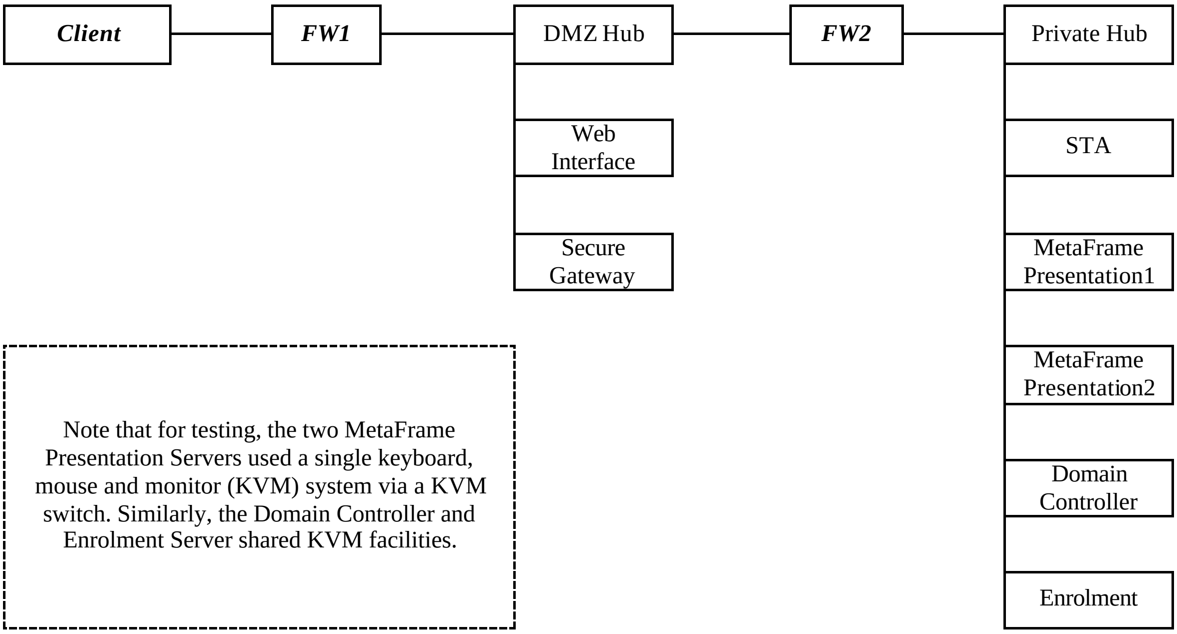
17. The environmental configuration also includes two further devices, in the private network, as follows.

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

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

19. For the test configuration, there were two ***MetaFrame Presentation Servers*** and just one ***ICA Client*** platform. Each of the ten platforms (i.e. six 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. All platforms apart from the firewalls have Windows 2000, Service Pack 4, with a number of hotfixes. The firewalls use the Red Hat Linux (version 9) Operating System.

20. This configuration used in testing is illustrated below.


Client
FW1
DMZ Hub
FW2
Private Hub
Web Interface
Secure Gateway
STA
MetaFrame Presentation1
MetaFrame Presentation2
Domain Controller
Enrolment
Note that for testing, the two MetaFrame Presentation Servers used a single keyboard, mouse and monitor (KVM) system via a KVM switch. Similarly, the Domain Controller and Enrolment Server shared KVM facilities.

21. In this test configuration a separate laptop platform was attached to each of the networks in order to test traffic over the networks.

22. For full details of both the TOE configuration and its environmental configuration see the Common Criteria Evaluated Configuration Guide [o].

ANNEX B: PRODUCT SECURITY ARCHITECTURE

1. This annex gives an overview of the main product architectural features that are relevant to the security of the TOE. Other details of the scope of evaluation are given in the main body of this Report and in Annex A.

Architectural Features

2. The TOE configuration consists of a Client Component (using Citrix ICA Client software) and a Server Component, which consists of a Citrix Secure Gateway Server, a Secure Web Server, a Web Interface, an ICA server component, a Secure Ticket Authority and the Citrix XML service. These are described in this Report under 'Evaluated Product' and 'TOE Scope.'

Design Subsystems

3. The design subsystems identified in this Report under 'Evaluated Product' are further 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. It provides authentication of users; lists of applications for authenticated users; and details of which ICA Server to use (when an application is selected).

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 on first connection.

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 function (outside the scope of the TOE).

TSF Interfaces

4. The User Interfaces into the TOE 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.

5. In addition the following Operating System and programmatic TOE interfaces were identified.

a. ICA Client.

b. Web Interface.

c. XML Service.

d. Secure Ticket Authority.

e. Secure Gateway.

f. ICA Server.

g. IMA.

ANNEX C: PRODUCT TESTING

IT Product Testing

1. The Developers' tests and the Evaluators' functional tests covered all of the subsystems defined in Annex B and covered all Security Functions claimed in the Security Target [a].

2. All User Interfaces listed in Annex B were tested.

Platform Issues

3. 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.)

4. 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 Annex A under 'Environmental Configuration.'

5. Consumers should note that both the hardware platforms and the underlying Windows 2000 Operating System are excluded from the evaluation. Further details are given under the 'TOE Scope' section of this report.

(This page is intentionally left blank)