MetaFrame Presentation Server
Security Standards and Deployment Scenarios

Citrix® MetaFrame® Presentation Server 3.0

Last Updated: July 26, 2004 5:26 pm (AM)

Contents

Introduction

About this Document

Citrix products offer the security specialist a wide range of features for securing a Citrix MetaFrame Presentation Server system.

When deploying Citrix MetaFrame Presentation Server 3.0 for Windows within large organizations and government environments, security standards are an important consideration. This document addresses common issues related to such environments.

This document provides an overview of the process of securing communications across a range of deployment models. Details of the individual security features are explained in the relevant product documentation.

Target Audience

This document is designed to meet the needs of security specialists, systems integrators, and consultants working with government organizations worldwide.

Country-Specific Government Information

Sections of this document are of particular importance and relevance to certain countries as shown in the table below. If your country is not listed, contact your local Citrix representative.

Country	Topic	See
United States	• FIPS 140 • TLS • Smart card support • Smart card: Common Access Card • Kerberos authentication	• page 10 • page 12 • page 13 • page 14 • page 14
Canada	• FIPS 140 • TLS • Smart card support • Kerberos authentication • ITS Pre-qualified Product List (IPPL)	• page 10 • page 12 • page 13 • page 14 • page 6
United Kingdom	• FIPS 140 • TLS • Smart card support • Kerberos authentication	• page 10 • page 12 • page 13 • page 14
Australia	• FIPS 140 • TLS • Smart card support • Kerberos authentication	• page 10 • page 12 • page 13 • page 14

For further information concerning issues specific to your country, contact your local Citrix representative.

Government of Canada ITS Pre-qualified Product List.   The previous release of MetaFrame Presentation Server (MetaFrame XP with Feature Release 3) is pre-qualified by the Canadian Communications Security Establishment (CSE) under the Information Technology Security (ITS) Product Pre-qualification Program (IPPP).

The program is relevant to the Government of Canada procurement process and the Canadian Common Criteria Scheme. The program pre-qualifies ITS products for use within the Government of Canada and facilitates the procurement of ITS products by government departments.

Contact your Citrix representative for further details.

Finding More Information

For assistance with securing a MetaFrame Presentation Server deployment, the following documentation is available.

You can use the *Document Center* to access the complete set of guides. The Document Center can be installed from the MetaFrame Presentation Server CD.

If you prefer to access the guides without using the Document Center, you can navigate to the component PDF files using Windows Explorer. The documentation is also available from the Knowledge Center at http://www.citrix.com/. To find the Knowledge Center, go to the Support and Services area of the Citrix Web site.

• The *Citrix MetaFrame Presentation Server Administrator's Guide* explains how to install and configure MetaFrame Presentation Server on Windows servers. Included in this documentation is information about publishing applications, configuring the Citrix XML Service, and configuring the Citrix SSL Relay to provide TLS/SSL-based communications.

• The *Web Interface Administrator's Guide* explains how to install and configure the Web Interface and provides information about securing Web Interface deployments using TLS/SSL-based communications.

• The *Secure Gateway for Windows Administrator's Guide* explains how to install and configure Secure Gateway Version 2.0 to provide a secure Internet gateway for ICA traffic traveling into and out of servers in a farm running MetaFrame Presentation Server.

• The *Client for 32-bit Windows Administrator's Guide, Version 8.x,* explains how to install, configure, and deploy MetaFrame Presentation Server Clients for 32-bit Windows. The guide includes a chapter about client security measures and features.

What's New

A number of security features and enhancements are implemented in Citrix MetaFrame Presentation Server 3.0 for Windows:

Kerberos authentication.   Version 8.*x* MetaFrame Presentation Server Clients for 32-bit Windows support Kerberos authentication. Clients can be configured for pass-through authentication together with Kerberos authentication. See "Kerberos Authentication" on page 14.

Client security features.   Various Version 8.*x* MetaFrame Presentation Server Clients now support additional security features:

Client	Security feature, new in this release
Clients for (32-bit) Windows Version 8.*x*	• Kerberos authentication
Client for Linux Version 8.*x*	• Smart card support
Client for Solaris SPARC Version 8.*x*	• TLS support • Government ciphersuite • Smart card support
Client for Java Version 8.*x*	• Root certificate source - now dependent on environment

For further details, see "MetaFrame Presentation Server Clients" on page 15.

Web Interface Secure Computing SafeWord Authentication.   The Web Interface now supports Secure Computing SafeWord 2-factor authentication. See "Additional MetaFrame Presentation Server Security Features" on page 19.

Security Considerations in a MetaFrame Presentation Server Deployment

MetaFrame Presentation Server provides server-based computing to local and remote users through the Independent Computing Architecture (ICA) developed by Citrix.

ICA is the communication protocol by which servers and client devices exchange data in a MetaFrame Presentation Server environment. ICA is optimized to enhance the delivery and performance of this exchange, even on low-bandwidth connections.

The ICA protocol transports an application's screens (and audio where relevant) from the server it is running on to the user's client device, and returns the user's input to the application on the server. As an application runs on a server, MetaFrame Presentation Server intercepts the application's display data and uses the ICA protocol to send this data (on standard network protocols) to the client software running on the user's client device.

When the user types on the keyboard or moves and clicks the mouse, the client software sends this data to the application on the server. ICA requires minimal client workstation capabilities and includes error detection and recovery, encryption, and data compression.

A server farm is a grouping of servers running MetaFrame Presentation Server that you can manage as a unit, similar in principle to a network domain. When designing server farms, you should keep in mind the goal of providing users with the fastest possible application access while achieving the degree of centralized administration and network security that you need.

In a MetaFrame Presentation Server deployment including the Web Interface, communication is conducted using both the ICA and HTTP protocols, among three different points: the computer running MetaFrame Presentation Server, a server running the Web Interface, and a client device with a Web browser and client.

In a MetaFrame Presentation Server deployment, you can configure encryption using either:

• Citrix SSL Relay

• Secure Gateway

The Citrix SSL Relay component is integrated into MetaFrame Presentation Sever. The Secure Gateway is provided on the MetaFrame Presentation Server Components CD.

FIPS 140 and Citrix MetaFrame Presentation Server

Federal Information Processing Standard 140 (FIPS 140) is a U.S. federal government standard that details a benchmark for implementing cryptographic software. It provides best practices for using cryptographic algorithms, managing key elements and data buffers, and interacting with the operating system. An evaluation process that is administered by the National Institute of Standards and Technology's (NIST) National Voluntary Laboratory Accreditation Program (NVLAP) allows encryption product vendors to demonstrate the extent to which they comply with the standard, and thus, the trustworthiness of their implementation.

Some U.S. government organizations restrict purchases of products that contain cryptography to those that have FIPS 140 validated modules.

In the UK, according to CESG published guidance http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=5&displayPage=5 where the required use is for information below RESTRICTED, but still sensitive; that is, PRIVATE, CESG recommends the use of FIPS-140-approved products.

The security community at large values products that follow the guidelines detailed in FIPS 140 and the use of FIPS 140-validated cryptographic modules.

To facilitate implementing secure application server access and to meet the FIPS 140 requirements, Citrix products can use cryptographic modules that are FIPS 140-validated in Windows 32-bit implementation of secure SSL/TLS connections.

The following MetaFrame Presentation Server components can use cryptographic modules that are FIPS 140-validated:

- MetaFrame Presentation Server Clients for 32-bit Windows (including Program Neighborhood, Program Neighborhood Agent, and the Web Client)

- Secure Gateway for Windows

- MetaFrame Presentation Server

- Citrix SSL Relay

- Web Interface for MetaFrame Presentation Server

When using the client and server components listed above with the SSL/TLS connection enabled, the cryptographic modules that are used are FIPS 140-validated. The cryptographic modules used are those provided by the Microsoft Windows operating system.

The government ciphersuite is RSA_WITH_3DES_EDE_CBC_SHA. As defined in Internet RFC 2246 http://www.ietf.org/rfc/rfc2246.txt, this ciphersuite uses RSA key exchange and TripleDES encryption.

This is achieved as follows:

- According to the Microsoft information concerning the cryptographic provider types in the document http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/cryptographic_provider_types.asp, the only cryptographic provider type supporting RSA key exchange and TripleDES encryption is the PROV_RSA_SCHANNEL (Type 012) cryptographic provider type.

- By inspection of a particular configuration, the only cryptographic provider of this type is the "Microsoft RSA Schannel Cryptographic Provider" that is hosted in rsaenh.dll.

- According to the Microsoft document "FIPS 140 Evaluation" http://www.microsoft.com/technet/Security/topics/issues/fipseval.mspx, the protocols whose cryptographic processing takes advantage of the components that completed FIPS-140-1 evaluation includes the SSL protocol that is used between a Web browser (Internet Explorer) and a Web server (Internet Information Server);

- The Microsoft document lists the following supported and FIPS-validated cryptographic algorithm implementations of Microsoft Windows operating system platforms:

FIPS-46-3 DES (ECB, CBC)	Windows NT4, 2000, XP, Server 2003 rsaenh.dll and dssenh.dll, Windows 2000, XP, Server 2003 fips.sys
FIPS-46-3 3DES (ECB, CBC)	Windows NT4, 2000, XP, Server 2003 rsaenh.dll and dssenh.dll, Windows 2000, XP, Server 2003 fips.sys
FIPS-197 AES-128, -192, -256 (ECB, CBC)	Windows XP SP1, Windows Server 2003 rsaenh.dll
FIPS-186-2 DSA	Windows NT4, 2000, XP, Server 2003 dssenh.dll
FIPS-186-2 RSA	Windows NT4, 2000, XP, Server 2003 rsaenh.dll
FIPS-180-2 SHA-1	Windows NT4, 2000, XP, Server 2003 rsaenh.dll and dssenh.dll, Windows 2000, XP, Server 2003 fips.sys
FIPS-198 HMAC-SHA-1	Windows XP, Server 2003 rsaenh.dll, Windows XP, Server 2003 fips.sys

Given the accuracy of the above statements and assuming the system is configured as described above, the resulting Citrix configuration would use FIPS 140-validated cryptomodules.

For a list of currently validated FIPS 140 modules, see the NIST Web site at: http://csrc.nist.gov/cryptval/140-1/1401val.htm.

For additional details regarding FIPS 140 and NIST, visit the NIST site at: http://csrc.nist.gov/cryptval/.

TLS/SSL

Secure Socket Layer (SSL) is an open, nonproprietary protocol that provides data encryption, server authentication, message integrity, and optional client authentication for a TCP/IP connection. Where SSL is used to secure communications between clients and servers within the server farm, the Citrix SSL Relay is required at each server within each farm, or you can use the Secure Gateway. Both solutions are discussed in this document.

Transport Layer Security (TLS) is the latest, standardized version of the SSL protocol. TLS is an open standard and like SSL, TLS provides server authentication, encryption of the data stream, and message integrity checks. The Citrix SSL Relay, described above, supports TLS and you can configure the SSL Relay, the Secure Gateway, and the Web Interface to use TLS. Support for TLS Version 1.0 is included in MetaFrame Presentation Server 3.0 for Windows.

Because there are only minor differences between SSL and TLS, the server certificates in your MetaFrame Presentation Server installation can be used for both SSL and TLS purposes.

Government Ciphersuites

You can configure MetaFrame Presentation Server, the Web Interface, and the Secure Gateway to use government-approved cryptography to protect "sensitive but unclassified" data. The government ciphersuite is RSA_WITH_3DES_EDE_CBC_SHA.

IPSec

IP Security (IPSec) is a set of standard extensions to the Internet Protocol (IP) that provides authenticated and encrypted communications with data integrity and replay protection. IPSec is a network-layer protocol set, so higher level protocols such as Citrix ICA can use it without modification.

Although such deployment scenarios are not within the scope of this document, you can use IPSec to secure a MetaFrame Presentation Server deployment within a Virtual Private Network (VPN) environment.

IPSec is described in Internet RFC 2401.

Microsoft Windows 2000 (and later releases) has built-in support for IPSec.

Smart Cards

You can use smart cards with MetaFrame Presentation Server, supported MetaFrame Presentation Server Clients, and the Web Interface to provide secure access to applications and data. Using smart cards with MetaFrame Presentation Server and Clients simplifies the authentication process while enhancing logon security. MetaFrame Presentation Server supports smart card authentication to published applications, including "smart card enabled" applications such as Microsoft Outlook.

In a business network, smart cards are an effective implementation of public-key technology and can be used to:

• Authenticate users to networks and computers

• Secure channel communications over a network

• Use digital signatures for securing content

If you are using smart cards for secure network authentication, your users can authenticate to applications and content published on your server farms. In addition, smart card functionality within these published applications is also supported.

For example, a published Microsoft Outlook application can be configured to require that users insert a smart card into a smart card reader attached to the client device to log on to a computer running MetaFrame Presentation Server. After users are authenticated to the application, they can digitally sign email using certificates stored on their smart cards.

Citrix supports the use of Personal Computer Smart Card (PC/SC) based cryptographic smart cards. These cards include support for cryptographic operations such as digital signatures and encryption. Cryptographic cards are designed to allow secure storage of private keys such as those used in Public Key Infrastructure (PKI) security systems. These cards perform the actual cryptographic functions on the smart card itself, meaning the private key and digital certificates never leave the card. In addition, you can use two-factor authentication for increased security. Instead of merely presenting the smart card (one factor) to conduct a transaction, a user-defined PIN (a second factor), known only to the user, is used to prove that the cardholder is the rightful owner of the smart card.

Smart Card Support

Citrix continues testing various smart cards to address smart card usage and compatibility issues with MetaFrame Presentation Server. Currently, Citrix is developing hotfixes to address specific smart card issues.

Citrix is working with suppliers of Common Access Card (CAC) products to ensure compatibility with MetaFrame Presentation Server. Contact your Common Access Card vendor or Citrix representative about supported versions of Common Access Card hardware and software. In some cases, specific hotfixes for MetaFrame Presentation Server may be required.

Citrix tests smart cards using certificates from common certificate authorities such as those supported by Microsoft. If you have any concerns regarding your certificate authority and compatibility with MetaFrame Presentation Server, contact your local Citrix representative.

Kerberos Authentication

Kerberos is an authentication protocol. Version 5 of this protocol is standardized as Internet RFC 1510. Many operating systems, including Microsoft Windows 2000 and later, support Kerberos as a standard feature.

MetaFrame Presentation Server extends the use of Kerberos. After users log on to a client device, they can connect to MetaFrame Presentation Server without needing to authenticate again. The user's password is not transmitted to Presentation Server - instead, authentication tokens are exchanged using the Generic Security Services API (GSSAPI) standardized in Internet RFC 1509.

This authentication exchange is performed within a Citrix ICA virtual channel and does not require any additional protocols or ports. The authentication exchange is independent of the logon method, so it can be used with passwords, smart cards, or biometrics.

To use Kerberos authentication with Presentation Server, client and server must be appropriately configured. Microsoft Active Directory Group Policy can also be used selectively to disable Kerberos authentication for specific users and servers.

MetaFrame Presentation Server Clients

Users access applications running on server farms using MetaFrame Presentation Server Client software installed on their client devices. ICA lets virtually any type of client device access applications over any type of network connection, including LAN, WAN, dial-up, and direct asynchronous connections. Because ICA does not download applications to client devices (as in the Network Computing architecture), application performance is not limited by bandwidth or device performance.

MetaFrame Presentation Server Clients are available for Windows, Macintosh operating system, UNIX, Linux, EPOC, Windows CE, DOS, and Java operating systems. Additionally, the Web Client (Win32) can be used with Web browsers that support ActiveX controls or Netscape plug-ins.

As described earlier, MetaFrame Presentation Server Clients for 32-bit Windows use cryptographic modules provided by the Microsoft Windows operating system. Other clients, including the MetaFrame Presentation Server Client for Java, contain their own cryptographic modules. The Client for Java can, therefore, be used on older Microsoft Windows operating systems that are not upgraded to support strong encryption.

The following table lists the available clients and details whether or not the client is FIPS 140 compliant, supports TLS, includes smart card support, uses government ciphersuites, and supports certificate revocation checking. Note that certificate revocation checking is applicable to clients running on Windows 2000 and Windows XP only.

Note   Clients not listed in the table do not support any of the security features listed below.

	FIPS 140	TLS Support	Government Ciphersuite	Certificate Revocation Checking	Smart Card Support	Kerberos Authentication Support
Program Neighborhood (Win32) Version 8.*x*	▶	▶	▶	▶	▶	▶
Program Neighborhood Agent (Win32) Version 8.*x*	▶	▶	▶	▶	▶	
Web Client (Win32) Version 8.*x*	▶	▶	▶	▶	▶	▶
Client for Windows CE WBT Version 8.*x*		▶	▶		▶	
Client for Pocket PC Version 8.*x*		▶	▶			
Client for Java Version 8.*x*		▶	▶			
Client for Mac OS X Version 7.0		▶	▶		▶	
Client for Win16 Version 6.20						
Client for Linux Version 8.*x*		▶	▶		▶	
Client for UNIX (Sun Solaris SPARC) Version 8.*x*		▶	▶		▶	
Client for UNIX (IBM AIX) Version 6.30		▶			▶	
Client for UNIX (SGI IRIX) Version 6.0						
Client for UNIX (HP-UX) Version 6.30		▶				
Client for OS/2 Version 6.012						
Client for EPOC Versions 1 and 2						

Certificates

The table below details the maximum certificate key lengths and the certificate source for the FIPS 140-compliant clients.

	Max Certificate Key Length (OS or bits)	Root Certificate Source (OS or Client)
Program Neighborhood (Win32) Version 8.*x*	OS	OS
Program Neighborhood Agent (Win32) Version 8.*x*	OS	OS
Web Client (Win32) Version 8.*x*	OS	OS
Client for Windows CE WBT Client Version 8.*x*	2048	Client
Client for Pocket PC Version 8.*x*	2048	Client
Client for Java Version 8.*x*	2048	Client (or JRE)
Client for Mac OS X Version 7.0	2048	Client
Client for Linux Version 8.*x*	2048	Client
Client for UNIX (Sun Solaris SPARC) Version 8.*x*	2048	Client
Client for UNIX (IBM AIX) Version 6.30	2048	Client
Client for UNIX (HP-UX) Version 6.30	2048	Client

Maximum Certificate Key Length (bits). The table shows the maximum certificate key length for clients. For clients marked with OS, the maximum certificate key length is determined by the cryptographic module service provider and the operating system.

Certificate Source. The table details the certificate source for each client. Clients marked with OS use certificates stored in the operating system certificate store. Clients marked with Client use certificates bundled with the client. Clients include native support for the following certificate authorities:

- VeriSign, Inc., http://www.verisign.com

- Baltimore Technologies, http://www.baltimore.com

Government organizations may use a different certificate authority. If so, you must install the root certificate for the certificate authority on each client device.

The root certificates used by the Client for Java depend on the environment. When running in the Microsoft JVM environment, the client uses root certificates bundled with the client or root certificates provided by the archive file on the Web server.

When running in the Java 2 environment, the client uses root certificates in the Java Runtime Environment (JRE) Java keystore.

Virtual Channels

The following table illustrates which ICA virtual channels or combination of virtual channels can be used for authentication and application signing/encryption methods.

	Smart card virtual channel	Kerberos virtual channel	Core ICA protocol (no virtual channel)
Authentication method			
Smart card	►	►	
Biometric		► *	
Password		►	►
Application signing/encryption	►		

* Third party equipment is required for biometric authentication.

Additional MetaFrame Presentation Server Security Features

The following MetaFrame Presentation Server security features are supported. However, they are not discussed in this document and are not included in any of the example deployment scenarios. For details concerning these features, see the relevant product documentation.

Web Interface RSA SecurID Authentication

RSA SecurID can be used as an authentication method for the Web Interface running on Windows servers. If enabled, users must log on using their credentials (user name, password, and domain) plus their PASSCODE. The PASSCODE comprises a PIN (Personal Identification Number) followed by the RSA SecurID tokencode (the number displayed on the RSA SecurID token).

Web Interface Secure Computing SafeWord Authentication

Secure Computing SafeWord can be used as an authentication method for the Web Interface running on Windows servers. If enabled, users must log on using their credentials (user name, password, and domain) plus their SafeWord passcode. The passcode comprises the code displayed on their SafeWord token plus (optionally) a PIN (Personal Identification Number).

ICA Encryption (SecureICA)

ICA encryption (SecureICA) is integrated into MetaFrame Presentation Server. You can use SecureICA (128-bit encryption) to protect the information sent between a MetaFrame Presentation Server and clients.

SecureICA does not use FIPS 140-compliant algorithms. You can configure clients and computers running MetaFrame Presentation Server to avoid using SecureICA.

Sample Deployments

Both Citrix SSL Relay and Secure Gateway are capable of supporting TLS-based and SSL-based encryption. Selection is largely a matter of deciding which topology best meets the needs of the organization's security policies. Each approach has its own advantages and the relative merits of the two are best illustrated by considering the following sample deployment models:

Sample Deployment A.   Using Citrix SSL Relay to provide end-to-end TLS/SSL encryption between a computer running MetaFrame Presentation Server and a client device.

Sample Deployment B.   Using Secure Gateway in the single-hop deployment to provide TLS/SSL encryption between a secure Internet gateway server and an SSL-enabled client, combined with encryption of the HTTP communication between the Web browser and the Web server. Additionally, you can secure ICA traffic within the internal network using IPSec.

Sample Deployment C.   Using Secure Gateway in the double-hop deployment to provide TLS/SSL encryption between a secure Internet gateway server and an SSL-enabled client, combined with encryption of the HTTP communication between the Web browser, Web Interface, and Secure Gateway proxy. Additionally, you can secure ICA traffic within the internal network using IPSec.

Sample Deployment D.   Using SSL Relay with the Web Interface to encrypt the ICA and HTTP communication between the computer running MetaFrame Presentation Server and the server running the Web Interface, combined with encryption of the HTTP communication between the Web browser and the Web server.

Note   The sample deployment scenarios show MetaFrame Presentation Server components installed on computers running Microsoft Windows Server 2003. Microsoft Windows 2000 can be used and offers the same security features.
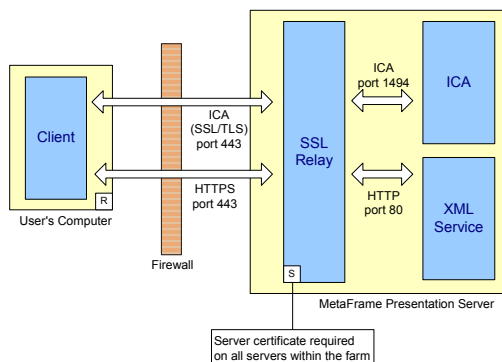
Sample Deployment A - Using SSL Relay

The computers running MetaFrame Presentation Server in sample deployment A comprise MetaFrame Presentation Server 3.0 for Windows on Microsoft Windows Server 2003 with Terminal Services. Users in deployment A are running the Program Neighborhood Client (32-bit Windows, Version 8.x).
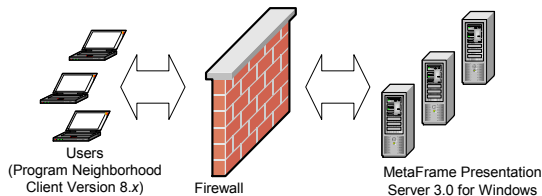
Sample Deployment A - SSL Relay

How the Components Interact

You use TLS/SSL to secure the connection between a client and the computer running MetaFrame Presentation Server. To do this, you deploy TLS/SSL-enabled clients and configure SSL Relay on the computer running MetaFrame Presentation Server.

Sample Deployment A - Detailed View

This deployment provides end-to-end encryption of the communication between the client and the server. Both SSL Relay and the appropriate server certificate must be installed and configured on each server within the server farm.

The SSL Relay operates as an intermediary in the communications between the client and the XML Service at each server. Each client authenticates the SSL Relay by checking the SSL Relay's server certificate against a list of trusted certificate authorities. After this authentication, the client and SSL Relay negotiate requests in encrypted form. The SSL Relay decrypts the requests and passes them to the server. When returning the information to the client, the server sends all information through the SSL Relay, which encrypts the data and forwards it to the client to be decrypted. Message integrity checks verify each communication was not tampered with.

FIPS 140 Validation

In sample deployment A, the SSL Relay uses the Microsoft Cryptographic Service Providers (CSPs) and associated cryptographic algorithms available in the Microsoft Windows CryptoAPI to encrypt/decrypt communication between client and server. Direct questions regarding the FIPS 140 validation of the CSPs to Microsoft Corporation.

For Microsoft Windows XP and Windows Server 2003, the TLS/SSL support and supported ciphersuites can also be controlled by the Microsoft security option:

- System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing. Refer to Microsoft product documentation for details.

For earlier Microsoft operating systems, see the following Microsoft Knowledge Base articles on the Microsoft support Web site (http://support.microsoft.com/):

- Microsoft Knowledge Base article Q238268
  "FIPS-Compliant Browser and Web Server for Windows NT 4.0"

- Microsoft Knowledge Base article Q245030
  "How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll"

TLS/SSL Support

You can configure MetaFrame Presentation Server to use either the Transport Layer Security (TLS) protocol 1.0 or the Secure Sockets Layer (SSL) protocol 3.0. In sample deployment A, the components are configured for TLS.

For details about configuring TLS, see the:

- *Citrix MetaFrame Presentation Server Administrator's Guide* and the online application help for the SSL Relay Configuration tool. When using the SSL Relay Configuration tool, ensure that **TLS** is selected at the **Connection** tab.

- *Client for 32-bit Windows Administrator's Guide, Version 8.x.*

Supported Ciphersuites

In sample deployment A, you configure MetaFrame Presentation Server to use government-approved cryptography to protect "sensitive but unclassified" data. The government ciphersuite is:

RSA_WITH_3DES_EDE_CBC_SHA

For details about configuring government ciphersuites, see the:

- *Citrix MetaFrame Presentation Server Administrator's Guide* and the online application help for the SSL Relay Configuration tool. When using the SSL Relay Configuration Tool, ensure that only **GOV** is selected at the **Ciphersuite** tab.

- *Client for 32-bit Windows Administrator's Guide, Version 8.x.*

Certificates and Certificate Authorities

Citrix products use standard Public Key Infrastructure (PKI) as a framework and trust infrastructure. In sample deployment A, you configure a separate server certificate for each server on which you use SSL Relay. A root certificate is required for each client. For further details, see the *Citrix MetaFrame Presentation Server Administrator's Guide.*

Smart Card Support

In sample deployment A, you can configure MetaFrame Presentation Server to provide a smart card logon. To do this, you must configure authentication using the Microsoft Active Directory and use the Microsoft Certificate Authority.

For more information, see the latest version of the *Advanced Concepts Guide for MetaFrame Presentation Server*, available from the Citrix Web site.

Clients

The Program Neighborhood Client is used in sample deployment A. For details concerning the security features and capabilities of MetaFrame Presentation Server Clients, see "MetaFrame Presentation Server Clients" on page 15.

# Sample Deployment B - Using Secure Gateway (Single-Hop)

The computers running MetaFrame Presentation Server in sample deployment B comprise MetaFrame Presentation Server 3.0 for Windows on Microsoft Windows Server 2003 with Terminal Services. Citrix SSL Relay is enabled.

The server running the Web Interface in sample deployment B comprises the Web Interface for MetaFrame Presentation Server 3.0, on Microsoft Windows Server 2003, with Microsoft Internet Information Services Version 6.0 or later.

The Secure Gateway in sample deployment B is running on Microsoft Windows Server 2003.

The Secure Ticket Authority in sample deployment B is running on Microsoft Windows Server 2003.

Users in deployment B are running a TLS-enabled Web browser and the Citrix Program Neighborhood Client (32-bit Windows, Version 8.x).
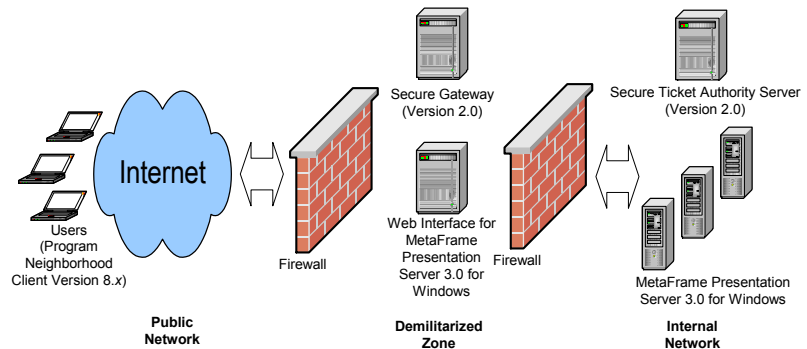
Deployment B - Secure Gateway

How the Components Interact

You use TLS to secure the connection between a client and the Secure Gateway. To do this, you deploy TLS/SSL-enabled clients and deploy the Secure Gateway at the network perimeter, typically in a demilitarized zone (DMZ). You secure the connection between the Web browser and the Web Interface using HTTPS. Additionally, you secure communication between the Web Interface and the Secure Ticket Authority using HTTPS and the Web Interface using TLS.
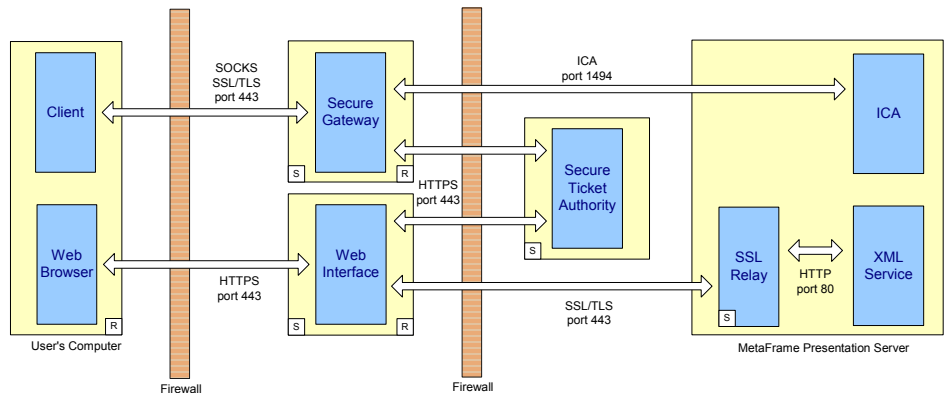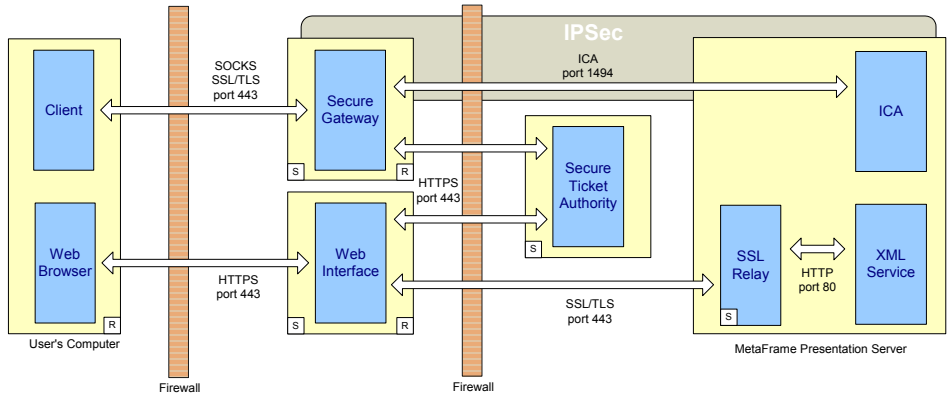

Sample Deployment B.1 - Detailed View

In sample deployment B, the Secure Gateway removes the need to publish the addresses of every MetaFrame Presentation Server, and allows a single point of encryption and access to the Citrix servers. It does this by providing a gateway that is separate from the computers running MetaFrame Presentation Server and reduces the issues for firewall traversal to a widely accepted port for ICA traffic in and out of firewalls.

Set against the increased scalability of sample deployment B is the fact that ICA communication is encrypted only between the client and the gateway. ICA communication between the gateway and MetaFrame Presentation Server is not encrypted.

Note that the SSL Relay in sample deployment B.1 is used to encrypt communication between the Web Interface and the XML Service running on MetaFrame Presentation Server. The Secure Gateway communicates with MetaFrame Presentation Server directly (the SSL Relay is not used for Secure Gateway to MetaFrame Presentation Server communication).

To achieve FIPS 140, you can secure the communication between the Secure Gateway and MetaFrame Presentation Server using IPSec. This is illustrated in the next diagram.

Sample Deployment B.2 - Detailed View (IPSec)

IPSec

To enable IPSec to secure communication between the Secure Gateway and the computers running MetaFrame Presentation Server, you must configure IPSec for the following servers:

- Secure Gateway
- All the computers running MetaFrame Presentation Server

IPSec is configured using the Local Security Settings (IP Security Policies) for each server. IPSec can be configured on Windows 2000 (or later) Servers. In deployment B.2, IPSec is enabled on the required servers and the security method is configured for 3DES encryption and SHA-1 integrity to meet FIPS 140 requirements.

FIPS 140 Validation

In sample deployment B, the Citrix SSL Relay uses the Microsoft Cryptographic Service Providers (CSPs) and associated cryptographic algorithms available in the Microsoft Windows CryptoAPI to encrypt/decrypt communication between client and server. Direct questions regarding the FIPS 140 validation of the CSPs to Microsoft Corporation.

For Microsoft Windows XP and Windows Server 2003, the TLS/SSL support and supported ciphersuites can also be controlled by the Microsoft security option:

• System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing. Refer to Microsoft product documentation for details.

For earlier Microsoft operating systems, see the following Microsoft Knowledge Base articles on the Microsoft support Web site (http://support.microsoft.com/):

• Microsoft Knowledge Base article Q238268
  "FIPS-Compliant Browser and Web Server for Windows NT 4.0"

• Microsoft Knowledge Base article Q245030
  "How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll"

TLS/SSL Support

In sample deployment B, you can configure Secure Gateway and the Web Interface to use either the Transport Layer Security (TLS) protocol 1.0 or the Secure Sockets Layer (SSL) protocol 3.0. In sample deployment B, the components are configured for TLS.

For details about configuring TLS, see the:

• *Web Interface for MetaFrame Presentation Server Administrator's Guide*

• *Secure Gateway for Windows Administrator's Guide*

• *Client for 32-bit Windows Administrator's Guide, Version 8.x*

Supported Ciphersuites

In sample deployment B, you configure Secure Gateway Version 2.0 and the Web Interface to use government-approved cryptography to protect "sensitive but unclassified" data. The government ciphersuite is:

RSA_WITH_3DES_EDE_CBC_SHA

For details about configuring government ciphersuites, see the:

• *Secure Gateway for Windows Administrator's Guide*

• *Client for 32-bit Windows Administrator's Guide, Version 8.x*

Certificate Authorities

Citrix products use standard Public Key Infrastructure (PKI) as a framework and trust infrastructure. In sample deployment B, you configure one server certificate on the Secure Gateway, and the Web Interface. You also configure a certificate on each computer running MetaFrame Presentation Server. For further details, see the relevant Administrator's Guides.

Smart Card Logon

In sample deployment B, you can configure MetaFrame Presentation Server to provide a smart card logon. To do this, you must configure authentication using the Microsoft Active Directory and use the Microsoft Certificate Authority.

For more information, see the latest version of the *Advanced Concepts Guide for MetaFrame Presentation Server* available from the Citrix Web site.

Clients

The Citrix Program Neighborhood Client is used in sample deployment B.

For details about the security features and capabilities of MetaFrame Presentation Server Clients, see "MetaFrame Presentation Server Clients" on page 15.

Sample Deployment C - Using Secure Gateway (Double-Hop)

The computers running MetaFrame Presentation Server in sample deployment C comprise MetaFrame Presentation Server 3.0 for Windows on Microsoft Windows Server 2003 with Terminal Services. Citrix SSL Relay is enabled.

The server running the Web Interface in sample deployment C comprises the Web Interface for MetaFrame Presentation Server, on Microsoft Windows Server 2003, with Microsoft Internet Information Services Version 6.0 or later.

The Secure Gateway Service in sample deployment C is running on Microsoft Windows Server 2003.

The Secure Gateway Proxy in sample deployment C is running on Microsoft Windows Server 2003.

The Secure Ticket Authority in sample deployment C is running on Microsoft Windows Server 2003.

Users in deployment C are running a TLS-enabled Web browser and the Citrix Program Neighborhood Client (32-bit Windows, Version 8.x).
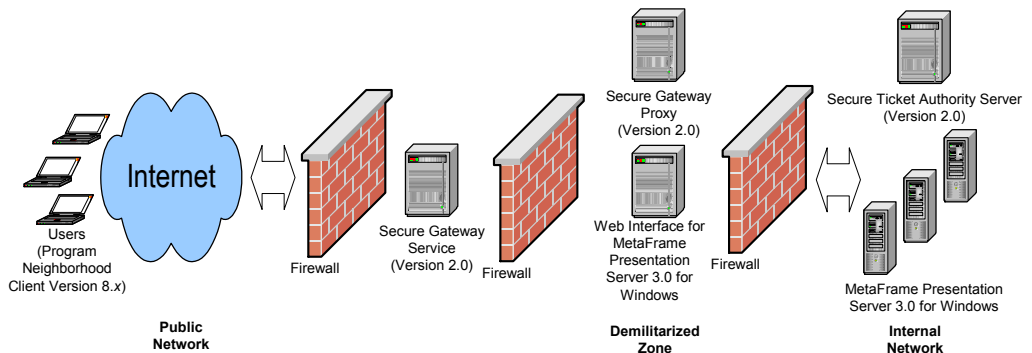

Deployment C - Secure Gateway (double-hop) and IPSEC

How the Components Interact

In sample deployment C, the demilitarized zone (DMZ) is divided into two segments. The Secure Gateway Service is located in the first hop of the DMZ. The Web Interface and Secure Gateway proxy are located in the second hop of the DMZ. Users connect to the Secure Gateway server in the first hop DMZ.

You use TLS to secure the connection between a client and the Secure Gateway. To do this, you deploy TLS/SSL-enabled clients and deploy the Secure Gateway at the network perimeter, typically in a DMZ.
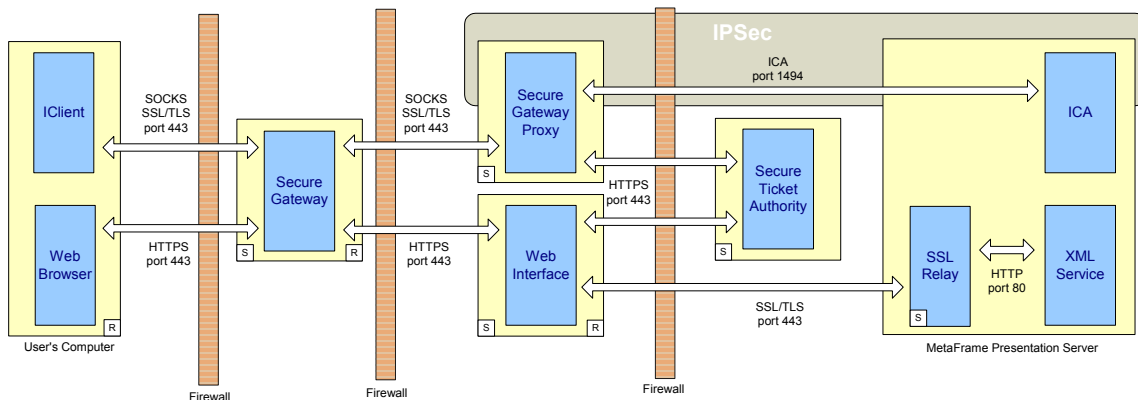
Sample Deployment C - Detailed View

In sample deployment C, the Secure Gateway removes the need to publish the addresses of every computer running MetaFrame Presentation Server and allows a single point of encryption and access to the Citrix servers. It does this by providing a gateway that is separate from the computers running MetaFrame Presentation Server and reduces the issues for firewall traversal to a widely accepted port for ICA traffic in and out of firewalls.

To achieve FIPS 140, you can secure communication between the Secure Gateway proxy and computers running MetaFrame Presentation Server using IPSec.

IPSec

To enable IPSec to secure communication between the Secure Gateway proxy and computers running MetaFrame Presentation Server, you must configure IPSec for the following servers:

• Secure Gateway proxy

• All computers running MetaFrame Presentation Server

IPSec is configured using the Local Security Settings (IP Security Policies) for each server. IPSec can be configured on Windows 2000 (or later) Servers. In deployment C, IPSec is enabled on the required servers and the security method is configured for 3DES encryption and SHA-1 integrity to meet FIPS 140 requirements.

FIPS 140 Validation

In sample deployment C, the Citrix SSL Relay uses the Microsoft Cryptographic Service Providers (CSPs) and associated cryptographic algorithms available in the Microsoft Windows CryptoAPI to encrypt/decrypt communication between client and server. Direct questions regarding the FIPS 140 validation of the CSPs to Microsoft Corporation.

For Microsoft Windows XP and Windows Server 2003, the TLS/SSL support and supported ciphersuites can also be controlled by the Microsoft security option:

• System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing. Refer to Microsoft product documentation for details.

For earlier Microsoft operating systems, see the following Microsoft Knowledge Base articles on the Microsoft support Web site (http://support.microsoft.com/):

• Microsoft Knowledge Base article Q238268
"FIPS-Compliant Browser and Web Server for Windows NT 4.0"

• Microsoft Knowledge Base article Q245030
"How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll"

TLS/SSL Support

In sample deployment C, you can configure Secure Gateway and the Web Interface to use either the Transport Layer Security (TLS) protocol 1.0 or the Secure Sockets Layer (SSL) protocol 3.0. The components are configured for TLS.

For details about configuring TLS, see the:

• *Web Interface for MetaFrame Presentation Server Administrator's Guide*

• *Secure Gateway for Windows Administrator's Guid*e

• *Client for 32-bit Windows Administrator's Guide, Version 8.x*

Supported Ciphersuites

In sample deployment C, you configure Secure Gateway, Secure Gateway proxy, and the Web Interface to use government-approved cryptography to protect "sensitive but unclassified" data. The government ciphersuite is:

RSA_WITH_3DES_EDE_CBC_SHA

For details about configuring government ciphersuites, see the:

• *Web Interface for MetaFrame Presentation Server Administrator's Guide*

• *Secure Gateway for Windows Administrator's Guid*e

• *Client for 32-bit Windows Administrator's Guide, Version 8.x*

Certificate Authorities

Citrix products use standard Public Key Infrastructure (PKI) as a framework and trust infrastructure. In sample deployment C, you configure one server certificate on the Secure Gateway, Secure Gateway Proxy, and the Web Interface. You also configure a certificate on each computer running MetaFrame Presentation Server. For further details, see the relevant Administrator's Guides.

Smart Card Logon

Smart card authentication is not supported in deployment C. It is not possible to configure smart card support where the Secure Gateway is positioned between the clients and the Web Interface.

For more information, see the *Secure Gateway for Windows Administrator's Guid*e.

Clients

The Citrix Program Neighborhood Client is used in sample deployment C. For details about the security features and capabilities of MetaFrame Presentation Server Clients, see "MetaFrame Presentation Server Clients" on page 15.

Sample Deployment D - Using SSL Relay and the Web Interface

The computers running MetaFrame Presentation Server in sample deployment D comprise MetaFrame Presentation Server 3.0 for Windows on Microsoft Windows Server 2003 with Terminal Services. Citrix SSL Relay is enabled.

The server running the Web Interface in sample deployment D comprises the Web Interface for MetaFrame Presentation Server on Microsoft Windows Server 2003, with Microsoft Internet Information Services Version 6.0 or later.

Users in deployment D are running a TLS-enabled Web browser and the Citrix Program Neighborhood Client (32-bit Windows, Version 8.*x*).
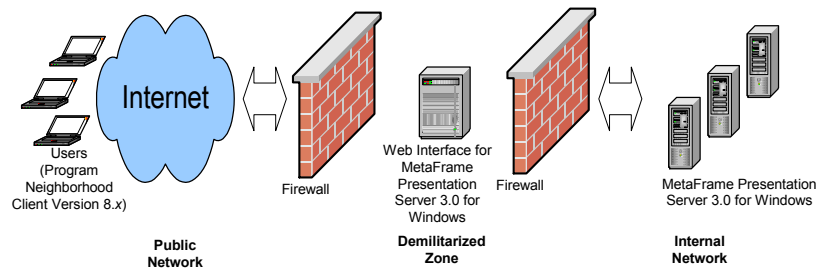
**Sample Deployment D - SSL Relay and the Web Interface**

How the Components Interact

In sample deployment D, you secure the connection between the user's Web browser and the Web Interface using HTTPS. You secure the connection between the Web Interface and the Citrix SSL Relay using TLS.

The connection between the client device and the Citrix SSL Relay is secured using TLS.

The SSL Relay operates as an intermediary in the communications between the clients, the Web Interface, and the XML Service at each computer running MetaFrame Presentation Server. Each client authenticates the SSL Relay by checking the SSL Relay's server certificate against a list of trusted certificate authorities. After this authentication, the client and SSL Relay negotiate requests in encrypted form. The SSL Relay decrypts the requests and passes them to the computer running MetaFrame Presentation Server. When returning the information to the client, the server sends all information through the SSL Relay, which encrypts the data and forwards it to the client to be decrypted. Message integrity checks verify each communication was not tampered with.

The following diagram shows the interaction of these components:
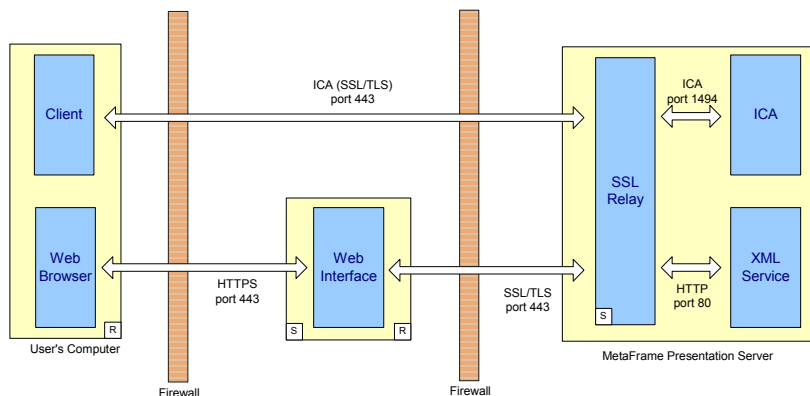
Sample Deployment D - Detailed View

FIPS 140 Validation

In sample deployment D, the Citrix SSL Relay uses the Microsoft Cryptographic Service Providers (CSPs) and associated cryptographic algorithms available in the Microsoft Windows CryptoAPI to encrypt/decrypt communication between client and server. Direct questions regarding the FIPS 140 validation of the CSPs to Microsoft Corporation.

For Microsoft Windows XP and Windows Server 2003, the TLS/SSL support and supported ciphersuites can also be controlled by the Microsoft security option:

- System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing. Refer to Microsoft product documentation for details.

For earlier Microsoft operating systems, see the following Microsoft Knowledge Base articles on the Microsoft support Web site (http://support.microsoft.com/):

- Microsoft Knowledge Base article Q238268
  "FIPS-Compliant Browser and Web Server for Windows NT 4.0"

- Microsoft Knowledge Base article Q245030
  "How to Restrict the Use of Certain Cryptographic Algorithms and Protocols in Schannel.dll"

TLS/SSL Support

In sample deployment D, you can configure the Citrix SSL Relay and the Web Interface to use either the Transport Layer Security (TLS) protocol 1.0 or the Secure Sockets Layer (SSL) protocol 3.0. In sample deployment D, the components are configured for TLS.

For details about configuring TLS, see the:

- *Citrix MetaFrame Presentation Server Administrator's Guide* and the online application help for the SSL Relay Configuration tool. When using the SSL Relay Configuration tool, ensure that **TLS** is selected at the **Connection** tab.

- *Web Interface for MetaFrame Presentation Server Administrator's Guide*

- *Client for 32-bit Windows Administrator's Guide, Version 8.x*

Supported Ciphersuites

In sample deployment D, you configure the Citrix SSL Relay and the Web Interface to use government-approved cryptography to protect "sensitive but unclassified" data. The government ciphersuite is:

RSA_WITH_3DES_EDE_CBC_SHA

For details about configuring government ciphersuites, see the:

- *Citrix MetaFrame Presentation Server Administrator's Guide* and the online application help for the SSL Relay Configuration tool. When you use the SSL Relay Configuration tool, ensure that only **GOV** is selected at the **Ciphersuite** tab.

- *Web Interface for MetaFrame Presentation Server Administrator's Guide*

- *Client for 32-bit Windows Administrator's Guide, Version 8.x*

Certificate Authorities

Citrix products use standard Public Key Infrastructure (PKI) as a framework and trust infrastructure. In sample deployment D, you configure a separate server certificate for each computer running MetaFrame Presentation Server on which you use SSL Relay. For further details, see the *Citrix MetaFrame Presentation Server Administrator's Guide*.

Smart Card Logon

In sample deployment D, you can configure MetaFrame Presentation Server to provide a smart card logon. To do this, you must configure authentication using the Microsoft Active Directory and use the Microsoft Certificate Authority.

For more information, see the latest version of the *Advanced Concepts Guide for MetaFrame Presentation Server* available from the Citrix Web site.

Clients

The Citrix Program Neighborhood Client is used in sample deployment D. For details about the security features and capabilities of MetaFrame Presentation Server Clients, see "MetaFrame Presentation Server Clients" on page 15.