

**Entrust[®] and
Microsoft[®] Windows[®] 2000:
An Interoperability Overview**

Date: September 1, 2000
Version: 2.0

© Copyright 2000-2003 Entrust. All rights reserved.

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. All other Entrust product names and service names are trademarks or registered trademarks of Entrust, Inc or Entrust Limited. All other company and product names are trademarks or registered trademarks of their respective owners.

© Copyright 2000-2003 Entrust. All rights reserved.

About Entrust

Entrust, Inc. [Nasdaq: ENTU] is a world leader in securing digital identities and information, enabling businesses and governments to transform the way they conduct online transactions and manage relationships with customers, partners and employees. Entrust's solutions promote a proactive approach to security that provides accountability and privacy to online transactions and information. Over 1,200 enterprises and government agencies in more than 50 countries use Entrust's portfolio of security software solutions that integrate into the broad range of applications organizations use today to leverage the Internet and enterprise networks. For more information, please visit www.entrust.com.

Table of Contents

INTRODUCTION	1
ENTRUST SUPPORT FOR WINDOWS 2000.....	2
INTEROPERABILITY GOALS.....	2
INTEROPERABILITY NET RESULTS	2
<i>Entrust Meets Scenario Interoperability Requirements.....</i>	<i>2</i>
<i>Entrust Meets Application Interoperability Requirements</i>	<i>3</i>
CUSTOMER SCENARIOS	3
<i>Scenario 1: Entrust/PKI with Windows 2000 Operating System.....</i>	<i>3</i>
<i>Scenario 2: Entrust/PKI with Windows 2000 PKI.....</i>	<i>4</i>
<i>Directory Requirements For Scenarios</i>	<i>4</i>
WINDOWS 2000 PKI FEATURES	5
DIFFERENCES IN DESIGN ASSUMPTIONS.....	6
DIFFERENCES IN DESIGN ASSUMPTIONS: NET RESULT.....	6
PKI TO PKI INTEROPERABILITY.....	6
PKI TO PKI INTEROPERABILITY: NET RESULT.....	6
THE NETWORK TRUST MODEL.....	7
THE HIERARCHICAL TRUST MODEL	7
THE HYBRID TRUST MODEL.....	8
PKI TO APPLICATION INTEROPERABILITY	8
PKI TO APPLICATION INTEROPERABILITY: NET RESULT.....	9
MICROSOFT CRYPTOAPI.....	9
<i>Entrust/Unity™ Cryptographic Service Provider</i>	<i>9</i>
FILE & FOLDER ENCRYPTION.....	10
SINGLE SIGN-ON	10
SECURE EMAIL	11
VIRTUAL PRIVATE NETWORKING (VPN).....	11
SECURE WEB.....	11
CERTIFICATE HANDLING	12
<i>CRL Distribution Point Extension.....</i>	<i>13</i>
<i>Authority Information Access Extension.....</i>	<i>13</i>
<i>Extended Key Usage Extension</i>	<i>14</i>
<i>Unicode Name Support.....</i>	<i>14</i>
APPLICATION TO APPLICATION INTEROPERABILITY	14
APPLICATION TO APPLICATION INTEROPERABILITY: NET RESULT	15
PKI TO DIRECTORY INTEROPERABILITY.....	15
PKI TO DIRECTORY INTEROPERABILITY: NET RESULT.....	16
ACTIVE DIRECTORY INTEGRATION WITH ENTRUST PRODUCTS	16
ACTIVE DIRECTORY'S DIRECTORY INFORMATION TREE (DIT) & DIRECTORY MIGRATION.....	16
AUTHENTICATION AND SECURITY	17
SUMMARY.....	17
REFERENCE DOCUMENTS.....	18

Table of Figures

Figure 1 - Entrust/PKI with Windows 2000 & Entrust-Ready Applications.....	3
Figure 2 - Entrust/PKI, Windows 2000 PKI, and 3 rd Party PKI with mixed PKI applications.....	4
Figure 3 - Network Trust Model.....	7
Figure 4 - Hierarchical Trust Model.....	7
Figure 5 - Hybrid Trust Model	8
Figure 6 - Generalized Application Security Framework.....	9
Figure 7 - View of a Certificate's Information, including the required Certificate Chain.....	12
Figure 8 - Extended Key Usage Functions found in Internet Explorer 5.5.....	14
Figure 9 - Common Supported Algorithms	15

Introduction

Microsoft[®] Windows[®] 2000 has seen the introduction of new product capabilities with the Microsoft Public Key Infrastructure (PKI) and security framework. The most recent releases of Entrust/PKI[™] have significantly enhanced Entrust's support for both the Microsoft desktop platform, as well as the Microsoft security framework, to enhance the new capabilities found in Windows 2000. This document presents a high level overview of the interoperability between Microsoft Windows 2000 PKI features and Entrust/PKI.

Both companies are committed to PKI standards and have demonstrated interoperability based upon these standards. While Entrust has always ensured that its products will install and run on the latest Windows operating system releases, interoperability can be further considered in the following four areas:

- PKI to PKI – Interoperability of the Microsoft Windows 2000 and Entrust/PKI trust models;
- PKI to Application – Interoperability of Windows CryptoAPI-enabled applications with Entrust/PKI;
- Application to Application – Interoperability of Windows CryptoAPI-enabled applications with Entrust-Ready[™] applications (those designed to take advantage of the advanced key and certificate management capabilities of the Entrust/PKI); and
- PKI to Directory – Interoperability between Entrust/PKI and Microsoft Active Directory[™].

Entrust has successfully demonstrated interoperability with Windows 2000 in all of the above areas.

This document will first outline the goals that were used to guide the development of interoperability in Entrust/PKI. It will then review the customer scenarios expected when Entrust and Windows 2000 are present in a customer environment. With these interoperability goals reviewed, the document will review each of the interoperability areas described above.

Although this white paper is focused on interoperability between Entrust & Microsoft, it is worth noting that Entrust also supports its products on many other platforms, including Sun[™], HP, IBM[®], Novell[®], and Nokia. This strong support for platform diversity, including Microsoft Windows 2000, further strengthens the core value of Entrust as the PKI for any e-Business application.

As a whole, this document provides an overview of the efforts undertaken by both Entrust and Microsoft to ensure that interoperability is provided in a seamless, transparent way to our mutual customers.

Entrust Support for Windows 2000

Before proceeding with a description of the different ways that Entrust supports Windows 2000, some background information is required:

1. The goals that were used to direct the development of interoperability features in Entrust/PKI.
2. Customer scenarios that were used to validate the level of interoperability to be provided.
3. An overview of the Windows 2000 public-key based security features and where emphasis has been placed on ensuring interoperability.
4. An overview of the basic design differences between the products and an explanation of Entrust/PKI features that will bridge these differences.

Interoperability Goals

Several new security features and capabilities based on public-key technology have been introduced in Windows 2000. These are either first generation features or modified capabilities from Windows NT[®] 4.0. As a result, Entrust/PKI 5.0 required some changes from previous releases to provide support for these new Windows 2000 public-key based security features. Requirements for this support were guided by the following criteria:

- Allow Entrust/PKI customers to leverage their managed Entrust Digital ID by making them accessible to Windows 2000 applications;
- Use Windows 2000 security framework APIs, protocols and certificate formats to provide the best level of support for Windows 2000 applications and features;
- Allow customers to continue to be able to benefit from the Entrust/PKI features including: automated certificate lifecycle management, encryption key backup and recovery, and centralized PKI security policy with distributed administration;
- Provide interoperability between Entrust-Ready applications and Windows 2000 applications using industry standards and protocols; and
- Provide interoperability between the Entrust/PKI and Windows 2000 PKI through using industry standards and protocols.

Both Entrust/PKI and Microsoft Windows 2000 PKI consist of several different architectural components. The infrastructure component includes the Certification Authority (CA) and other supporting services that provide central support for the PKI. The application components are the end software packages that use the public-key capabilities provided by the PKI. The administration component allows customers to administer and control the operation of both the infrastructure and application components.

Interoperability Net Results

Entrust Meets Scenario Interoperability Requirements

The different scenarios described in the following sections and their required interoperability relationships may be organized into four high-level requirements for Entrust/PKI. Entrust/PKI provides support for the following areas of interoperability:

PKI to PKI Interoperability;	✓
PKI to Application Interoperability;	✓
Application to Application Interoperability;	✓
PKI to Directory Interoperability	✓

Entrust Meets Application Interoperability Requirements

The different scenarios may touch on any or all of the five key areas that are required at the application level. Entrust/PKI provides support for interoperability in the following key application areas:

File & Folder encryption	✓
Single Sign-on	✓
Secure Email	✓
Secure Web	✓
Virtual Private Networking (VPN)	✓

Customer Scenarios

Entrust interoperability with Windows 2000 centers on the interactions between these different components and their usage within customer scenarios. The following customer scenarios were used to direct the development and testing required to ensure interoperability and meet customer requirements.

Scenario 1: Entrust/PKI with Windows 2000 Operating System

Scenario 1 represents the case where a customer wishes to exclusively use Entrust/PKI with Windows 2000. The customer has chosen to take advantage of the Entrust-Ready application environment, as well as make use of the Windows 2000 PKI-ready applications. This scenario covers both customers with an existing Entrust/PKI wishing to upgrade their computing environment to Windows 2000 from Windows NT 4.0, and customers wishing to install a new Entrust/PKI in a Windows 2000 environment. Adding Entrust/PKI into a Windows 2000 enterprise environment ensures that companies can scale into the millions with a single infrastructure should they decide to expand into Business-to-Business (B2B) or Business-to-Consumer (B2C) activities.

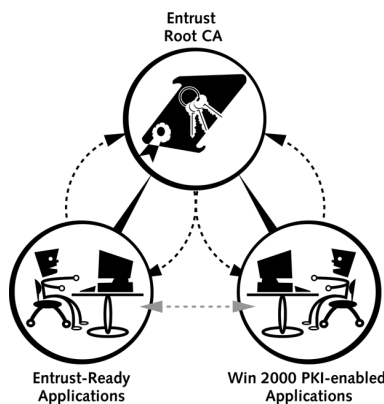


Figure 1 - Entrust/PKI with Windows 2000 & Entrust-Ready Applications

This scenario requires that the following interoperability relationships be verified:

1. Entrust/PKI to Windows 2000 applications
2. Entrust-Ready applications to Windows 2000 applications
3. Entrust/PKI to Microsoft Active Directory (optionally)

Scenario 1 Results: Interoperability tested and verified for relationships one and two. The third relationship (Entrust/PKI to Microsoft Active Directory) is not currently a commercially available in product. While an organization is not required to use only Active Directory, some may wish to do so (rather than using an X.500 directory and Active Directory). Entrust is currently in the process of working with both Microsoft and key customers to release a version of Entrust/PKI that will support the use of Active Directory as the primary certificate repository. This support is expected to be released in the first half of 2001.

Scenario 2: Entrust/PKI with Windows 2000 PKI

Scenario 2 represents the case where a customer wishes to use both the Entrust/PKI and the Windows 2000 PKI, with both Entrust-Ready applications and Windows 2000 PKI-ready applications. One of the many values of using Entrust/PKI in addition to the Windows 2000 PKI in this scenario is the ability to easily secure and use non-Microsoft applications [such as SAP, Peoplesoft, and Netscape], which have proven interoperability with Entrust. This scenario could occur in several different instances, including when:

1. A large customer centralizes PKI management after several divisions have already implemented different PKIs respectively;
 2. A customer acquires another company that has implemented a different PKI; or
 3. A customer wishes to manage both internal and external relationships using PKI capabilities.
- Examples for external relationships include both Business-to-Consumer (B2C) and Business-to-Business (B2B) applications.

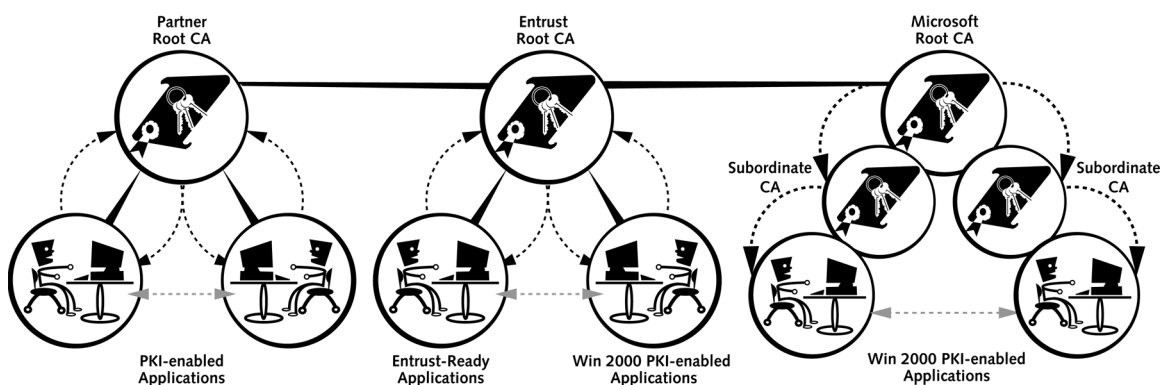


Figure 2 - Entrust/PKI, Windows 2000 PKI, and 3rd Party PKI with mixed PKI applications

This scenario demands that the following interoperability relationships be verified:

- Entrust/PKI to Windows 2000 PKI;
- Entrust/PKI to other 3rd Party PKI;
- Entrust/PKI to Windows 2000 applications;
- Entrust-Ready applications to Windows 2000 infrastructure; and
- Entrust-Ready applications to Windows 2000 applications.

Scenario 2 Results: Interoperability verified

Directory Requirements For Scenarios

Both scenarios may also require PKI interoperability with one or more directory systems. In a new Windows 2000 environment there may be only one logical directory based on Microsoft Active Directory (a required component if using Windows 2000 PKI). In an upgrade scenario, there is most likely an

existing directory system not based on Active Directory (i.e. X.500). In this case the customer may either migrate fully to Active Directory or opt to run multiple directory systems. In either case, the interoperability relationship is:

- Entrust/PKI to Active Directory.

Directory Scenario Requirements Results: Although not commercially available, Entrust is fully committed to providing support for Active Directory in a mid-2001 release of Entrust/PKI. Initial testing has shown that interoperability is definitely attainable, and final results will be published with the commercial release of Entrust/PKI in 2001.

Windows 2000 PKI Features

To aid in understanding the various potential areas for interoperability, the following provides a brief summary of new security-related features in Windows 2000:

Kerberos V5.0 Protocol

Support for the Kerberos version 5.0 security protocol provides single logon to Windows 2000 Server-based enterprise resources. As well as supporting the usual identity and password method for logon, Windows 2000 supports the ability to use PKI credentials for authenticating to the Kerberos server for logon. This is commonly referred to by Microsoft as “PKI Login” to Windows 2000. This feature has a built-in automatic enrollment method that is currently limited to being used only by a Microsoft CA. However, the PKI Login capability is able to use other PKI vendor’s certificates (such as Entrust) through alternate certificate population methods.

NT File System (NTFS) Encrypted Files

The Encrypting File System (EFS) provides transparent file-encryption protection on disk for sensitive data stored on Windows 2000 NTFS file systems (this capability does not extend to NT 4 NTFS file systems). NTFS encrypted files use public-key based technology to encrypt files for a user. There currently is no ability to secure files for multiple users or to move files off the original Windows 2000 drive without them becoming unprotected, removing the ability to share secure files with other Windows versions. In this release of Windows 2000, EFS is currently closed to alternative cryptographic providers. This translates into requiring end users to use the included Microsoft Cryptographic Service Provider (CSP), causing EFS to not support the use of smart cards (through smart card CSPs) or the Entrust CSP (which delivers managed Entrust certificates to Microsoft’s cryptographic framework).

Internet Protocol Security

Microsoft Internet Protocol Security (IPSEC) governs end-to-end enterprise secure communication. After an administrator has implemented IPSEC for an enterprise, communications are secured transparently. Public-key based technology is used by IPSEC for both confidentiality and authentication. This has been introduced at both the PKI level (server) and the desktop level (integrated IPSEC client) for Windows 2000. At both these levels, the automatic methodology introduced for certificate enrollment is specific to the Windows 2000 environment. This security addition can only be enforced in a pure Windows 2000 environment; it is not available to previous versions of Windows.

PC/SC Support

Windows 2000 provides plug and play smart card support through the PC/SC standard (the original and most widely implemented industry standard is PKCS 11). Smart cards may be used for secure portable storage and authentication within a public-key based security system. As mentioned, there is no support for the use of smart cards in conjunction with EFS.

Improved CA Services

An X.509-based public-key certificate server and integration with Active Directory allow the use of public-key certificates for authentication.

Central Security Policy Management

Windows 2000 provides central security policy administration that allows administrators to centrally define trust relationships and distribute CA certificates to enterprise users in a homogeneous Windows 2000 environment.

Active Directory

Active Directory provides LDAP directory services to Windows 2000, centralizing user administration for all operating system features.

Differences in Design Assumptions

Both the Entrust/PKI and the Windows 2000 PKI are based on industry standards such as X.509 v3 and the IETF PKIX RFCs. However, these standards are flexible and allow vendors to implement the standards to varying levels of completeness, as well as different levels of interpretation. This flexibility in the standards allows different products to be standards-compliant while also not being compatible or interoperable. There are several differences between Windows 2000 PKI and the Entrust/PKI.

Differences in Design Assumptions: Net Result

The differences found between the Entrust/PKI and Windows 2000 PKI may be attributed to the design assumptions incorporated in the development of the two PKI products. While the differences exist, Entrust/PKI provides the appropriate bridges between the products so that interoperability may be achieved. In addition, the design considerations used to bring Entrust/PKI to its current 5th generation status allow it to be a multipurpose, multi-platform trust infrastructure, able to be leveraged across the enterprise, and easily scale into high volume B2B, and B2C environments (including wireless applications). Microsoft's 1st generation PKI is primarily focused on providing integrated security services in the enterprise through its suite of applications and core PKI features.

PKI to PKI Interoperability

Interoperability between PKIs, regardless of vendor, requires a consistent model for establishing trust. There exist two trust models for ensuring that end entities can determine whether or not to trust other parties with whom secure transactions are being conducted. Referred to as the "Network Trust" model and the "Hierarchical Trust" model, a PKI must support at least one common scheme to ensure interoperability between PKIs. In addition, these two models can be combined to form a third "Hybrid Trust" model.

PKI to PKI Interoperability: Net Result

While Microsoft supports only the hierarchical trust model, Entrust/PKI supports all three trust models. As support for hierarchical trust has been incorporated into both Entrust/PKI and the Entrust application engines used by Entrust-Ready applications, customers are able to manage their users as part of a trust hierarchy or interact with members of another trust domain that is a hierarchy. This allows Entrust customers to operate in any one of three trust models: the network trust model, the hierarchical trust model and the hybrid trust model. This flexibility allows for maximum interoperability between Entrust,

Microsoft, and other PKI vendors, and gives customers confidence that they will be able to interoperate with other organizations in the future. The following sections review these models with additional detail.

The Network Trust Model

In a network trust model, end users trust the CA closest to them while trust between domains is created by establishing cross-certificates between domains. The level of trust between domains is set through the use of business controls placed in the cross-certificates. These business controls allow CA administrators to limit the scope of trust between their CA and other CAs.

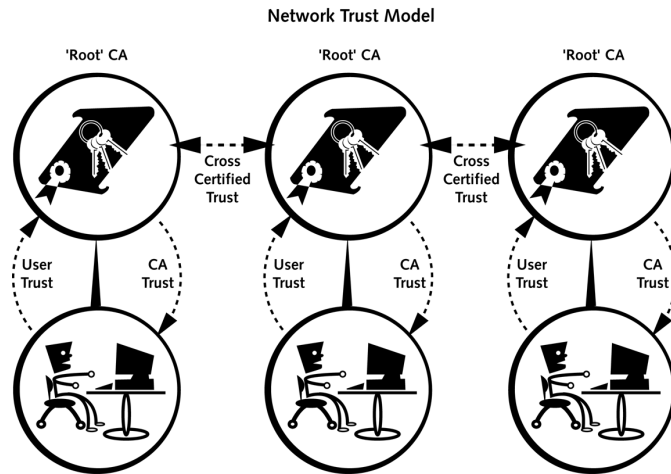


Figure 3 - Network Trust Model

The Hierarchical Trust Model

In a hierarchical trust model, end users trust the root CA at the root of their hierarchy. Trust between CAs flows down from the root. Users will only directly trust users with CAs that are members of the same hierarchy. Trust between hierarchies cannot be established at the root or any other level but users may individually trust other roots.

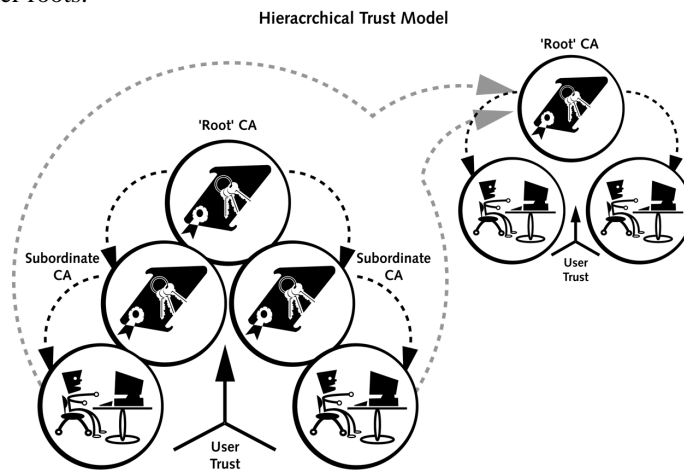


Figure 4 - Hierarchical Trust Model

By securely obtaining multiple root CA certificates, a user may trust other users in other trust hierarchies. This is the model used by Web browsers, as illustrated by the number of embedded root CAs that are installed with a browser (including the Entrust root, Entrust.net). In a hierarchy, the level of trust for a CA is dependent on the level of trust associated with the CA at the root of the hierarchy.

The Hybrid Trust Model

The hybrid trust model is a combination of the network and the hierarchical trust models. The two models may be combined by allowing network CAs to cross-certify with hierarchy root CAs and by adding the network CAs to hierarchical users' trusted CA lists. This is the model that would be used to join an existing Entrust/PKI network of CAs to an existing hierarchy of CAs.

Entrust/PKI supports PKI to PKI interoperability with Windows 2000 PKI through the support of either the hierarchical or hybrid trust model.

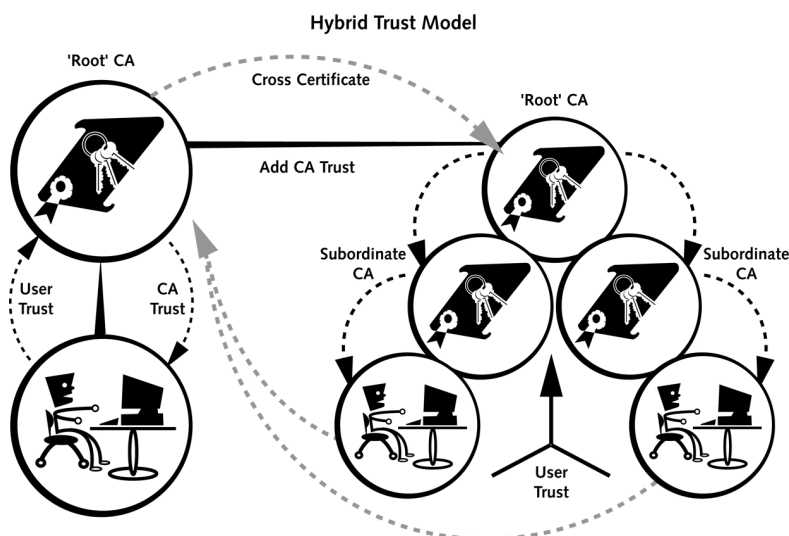


Figure 5 - Hybrid Trust Model

In a hybrid trust environment, an existing Entrust network PKI may join an existing Windows 2000 hierarchical PKI. The Entrust CA creates a cross-certificate for the Windows 2000 root CA so that members of the Entrust CA may trust members of the Windows 2000 hierarchy.

Within the Windows 2000 hierarchy, the administrator can use the Group Policy manager to push out the Entrust CA certificate to client systems as a trusted root. Alternatively, the Entrust CA certificate can be published to the Certification Authority Container in Active Directory. By doing so, CA trust is automatically achieved for all clients. This allows the Windows 2000 hierarchy users to trust users in the Entrust CA.

PKI to Application Interoperability

The primary type of interoperability that is of concern here is the ability for Entrust/PKI to support Windows 2000 PKI-enabled applications. It is unlikely that Entrust-Ready applications will have to directly interact with the Windows 2000 PKI.

Several areas affect the level of interoperability that may be supported between applications and a PKI. These areas include: cryptographic capabilities of the applications, certificate content and validation capabilities, trust model capabilities, and application to PKI protocol capabilities.

PKI to Application Interoperability: Net Result

Entrust has ensured that Entrust/PKI can support Windows 2000 PKI-enabled applications, and that Entrust certificates are understood by Microsoft applications (such as email programs) that may encounter them.

Microsoft CryptoAPI

Within the Windows 2000 security framework, applications use Microsoft CryptoAPI to gain access to cryptographic and certificate capabilities. Microsoft CryptoAPI provides Windows applications access to cryptographic functions, public key credential management, and certificate validation functions.

CryptoAPI supports a service provider environment that allows Microsoft, as well as other vendors, to plug-in alternate cryptographic service providers (CSPs). These CSPs are used to provide different algorithms as well as access to different types of cryptographic hardware. For example, smart card support provided in Windows 2000 is accessed through smart card CSPs provided by the respective vendors.

The CryptoAPI credential management functions help to match CSPs with certificates stored in the different CryptoAPI certificate stores. The certificate stores maintain information about trusted CA certificates (and possibly subordinate CAs), and certificate revocation lists. CryptoAPI uses the stores to perform certificate validation, and can retrieve subordinate CA certificates and CRLs as required. The current version of CryptoAPI supports X.509v3 certificates and the hierarchical trust model. Network trust model cross-certificates are supported by pushing a trusted Entrust CA root certificate into the user certificate store using the Windows 2000 Group Policy mechanism. Alternatively, the Entrust CA certificate can be published to the Certification Authority Container in Active Directory.

The Microsoft PKI-ready applications access public-key credentials and perform certificate validation through CryptoAPI. CryptoAPI does not directly provide certificate lifecycle management. Applications wishing to acquire certificates from a CA may either use CryptoAPI to generate a PKCS#10 request that can be submitted to a CA, or it may use the Microsoft X.509 Certificate Enrollment Control (X-enroll). The Windows 2000 PKI provides enrollment web pages using X-enroll that allow the user to request a certificate through Internet Explorer. Windows applications that make use of CryptoAPI to implement public-key based security include: Microsoft[®] Internet Explorer 5, Microsoft Office[®] 2000 applications (including Microsoft Outlook[®] 2000), Microsoft Outlook[®] Express, NTFS File Encryption, IPSEC, Public Key Logon, Authenticode and Internet Information Server 5.0. Most of these applications and features may be integrated with Entrust through the use of an Entrust CSP that is delivered as part of the Entrust/Unity product.

Entrust/Unity™ Cryptographic Service Provider

Entrust/Unity is part of Entrust's desktop security framework integration strategy, providing access to managed Entrust credentials through a full-featured CSP.

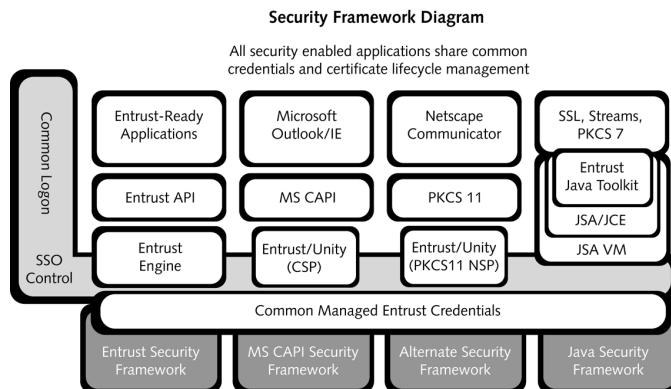


Figure 6 - Generalized Application Security Framework

This strategy allows applications that comply with multiple security frameworks to have access to a common set of managed PKI credentials as shown in the figure above.

As mentioned previously, most Microsoft PKI-enabled applications may leverage the advanced capabilities of an Entrust/PKI through CryptoAPI. Unfortunately, NTFS File Encryption and Windows 2000 Public-key logon cannot use the Entrust CSP, as they both require specific CSPs to operate. NTFS file encryption only uses the Microsoft CSP, while public-key logon requires a smart card and its associated CSP.

Bottom line: Almost all Microsoft CryptoAPI applications can access managed Entrust certificates transparently through Entrust/Unity. The two exceptions include Windows 2000 NTFS file encryption & Microsoft PKI login, which are currently undocumented & closed to non-Microsoft vendors.

File & Folder Encryption

Although NTFS File Encryption (Encrypting File System -- EFS) may not be able to use Entrust/Unity to access a user's enterprise PKI credentials, it can receive a separate set of credentials. An Entrust/PKI CA may be set up to specifically handle the issuing of certificates to NTFS File Encryption. This CA may be either a subordinate or a peer to the enterprise CA. NTFS file encryption requires user certificates that contain a special extended key usage value. Entrust/PKI supports the issuance of these special certificates through its flexible certificate specification capability that allows for the customization of certificate contents. Once a flexible certificate specification containing the NTFS file encryption extend key usage is configured for the secondary CA, credentials may be issued using the same distinguished name as used in the enterprise credentials. The placing of Entrust credentials in the Microsoft certificate store is currently only achievable through a manual process (either user or programmatically initiated), as the automatic enrollment method used by the Windows 2000 PKI is not open to other vendors for use.

Bottom line: Entrust supports NTFS Encryption through manual enrollment for unmanaged credentials, and will expand its support as Microsoft opens interfaces for alternate PKI vendors.

Single Sign-On

Public-key logon on Windows 2000 requires that users have a smart card for storing their PKI credentials. Entrust currently supports the PKCS 11 interface for accessing smart card and other cryptographic hardware. Windows 2000 uses a combination of PC/SC and smart card vendor CSPs for smart card support. In order to achieve Entrust's goal of maintaining a single set of managed enterprise PKI credentials across all applications, credentials on a smart card must be accessible through both PKCS 11 and PC/SC. Through Entrust working with industry-leading smart card vendors, there are CSPs being designed that will interface with both PC/SC and PKCS 11. With this approach, a smart card can be used for both smart card logon and Entrust-Ready applications to access and use the managed enterprise PKI credentials.

Alternatively, given Windows 2000's continued support of the GINA login capability, users can benefit from single sign-on using Entrust/SignOn™, which fully supports using smart cards. As well, with the ability to mandate the use of Entrust/SignOn as the primary authentication method for the workstation, administrators have the ability to enforce login using a user's digital identity.

Bottom line: Entrust supports integrated login to Windows and the Entrust security platform through Entrust/SignOn. By eliminating the need for multiple logins to Windows and secure applications, Entrust/SignOn reduces the number passwords users need to remember, translating into fewer helpdesk calls and easy to use desktop security.

Secure Email

Secure email in Windows 2000 requires an application that is able to use both certificates and keys to send S/MIME secured messages. Microsoft Outlook 2000 and Microsoft Outlook Express 5.0 are both S/MIME enabled email clients that Entrust has the ability to provide certificates to through Microsoft CryptoAPI. Newly released Microsoft Outlook 2000 SR1 provides new support for a subset of the S/MIMEv3 standard, which allows Entrust/PKI customers to use Entrust certificates with an S/MIMEv3 enabled client for secure messaging.

Entrust/Express, an Entrust-Ready application plug-in for Microsoft Outlook, provides additional levels of functionality over the core email application, including advanced trust management. Entrust/Express properly handles certificates that have been issued by a Microsoft CA or an Entrust CA.

Bottom line: Entrust/Express provides powerful and easy-to-use S/MIME capabilities with Microsoft's Outlook and Exchange e-mail clients. Entrust managed certificates are also available to native Outlook and Outlook Express through Entrust/Unity.

Virtual Private Networking (VPN)

Virtual Private Networks (VPNs) provide secure network services over a public network at a reduced cost. Windows 2000 provides multiple types of VPN connections, including:

- Point-to-Point Tunneling Protocol (PPTP);
- Layer Two Tunneling Protocol (L2TP); and
- Internet Protocol Security (IPSEC).

Windows 2000 has introduced support for IPSEC on the desktop through a built-in IPSEC client. IPSEC, when implemented in conjunction with certificates, provides enhanced security between two computers, so that no section of the connection is insecure. Windows 2000 does provide support for use of certificates (machine) with their built-in client, but does not require that certificates be present to initiate a secure connection. User authentication is based on existing protocols, coupled with machine certificates to initiate the IPSEC tunnel. The Windows 2000 IPSEC client is available only on Windows 2000; the capability does not extend to other versions of the Windows operating system.

Entrust can provide certificates for use by the Windows 2000 IPSEC client through Entrust/WebConnector. This process today entails the user taking the steps to enroll the machine, either through a Web browser interface, or via a Microsoft utility. The automatic enrollment capability provided by Windows 2000 is currently not available for use by non-Microsoft applications.

Entrust also has many large industry partners who provide VPN client software which is both Entrust-Ready [tested to work against an Entrust environment] and runs on Windows 2000. These client software packages provide value-add over and above the native Windows client, including enforcement of algorithm type and size.

Bottom line: Entrust provides support for Microsoft's built-in VPN client through manual enrollment for unmanaged certificates. Entrust's industry partners deliver value-add VPN technology for the Microsoft platform.

Secure Web

Secure Web sessions in a Windows 2000 environment are enabled through Internet Explorer and its integration with CryptoAPI. Internet Explorer provides enhanced site security through the ability to use

digital certificates for authenticating users. These digital certificates are used to set up a secure session with the Web server (Secure Socket Layer – SSL), thereby protecting the session transmissions between the end user and the server. Entrust/PKI provides both managed or unmanaged certificates for use by Internet Explorer in a secure Web browsing session. Managed certificates are provided through Entrust/Unity and unmanaged certificates are provided through Entrust/WebConnector.

When accessing each secured site, users are prompted to choose which certificate they wish to use for authenticating. Once chosen, the certificate is validated at the Web server as trusted (or not), and the session is then established.

Bottom line: Entrust managed certificates are available to Internet Explorer through Entrust/Unity.

Certificate Handling

Trust within a PKI is based on the application's ability to properly process and validate the certificates issued within the PKI. All Entrust-Ready applications perform certificate validation automatically, and in a consistent fashion. CryptoAPI is called to perform these types of functions by a Microsoft PKI-enabled application; it is, however, up to the application what functions are called to perform certificate handling. The primary function performed by both products is to create chains of trust from the certificate being validated to a CA trusted by the user. First a chain of certificates must be formed and then each certificate in the chain must be validated. As each certificate is validated, it must be checked for revocation by looking for the certificate on a certificate revocation list (CRL) maintained by the issuer of the certificate. Depending on the application that is using the certificate (or the private key associated with the certificate's public key), the key usage or enhanced key usage values may also be checked.

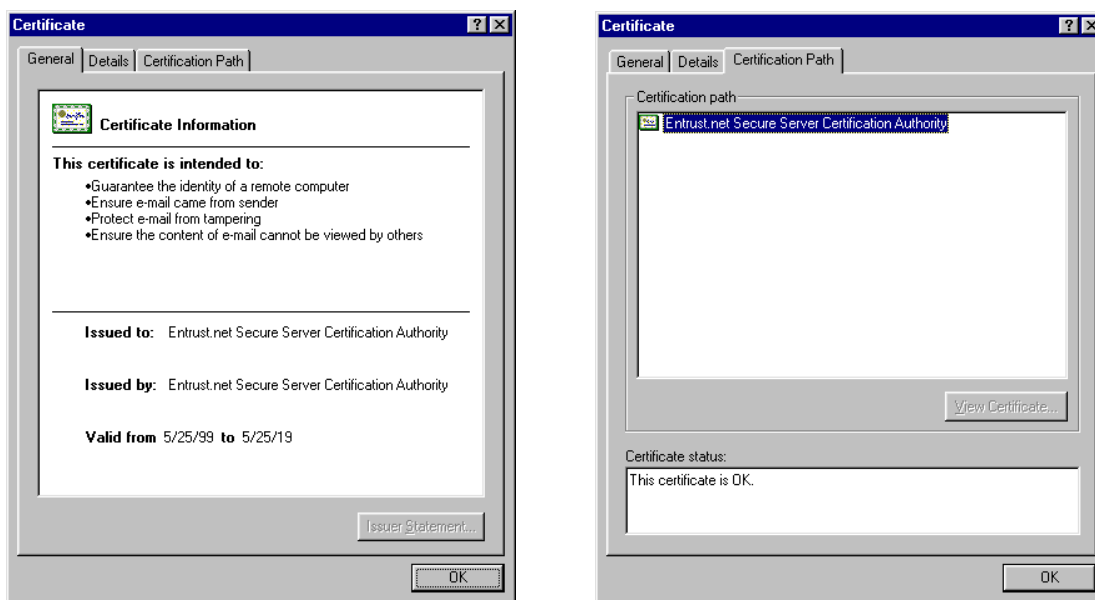


Figure 7 - View of a Certificate's Information, including the required Certificate Chain

Two certificate handling scenarios must be considered. An Entrust-Ready application processing a Windows 2000 generated certificate and a Microsoft PKI-enabled application processing an Entrust generated certificate. Part of the certificate processing is based on fields or extensions contained within the certificates that the PKIs use. The fields or extensions listed in this section contain explanatory notes on functionality that Entrust/PKI delivers to ensure interoperability or relevant information needed by

administrators. Fields or extensions not listed are either not used by either PKI product or have no known interoperability impact.

Bottom line: Entrust CRL information is available to Entrust and Microsoft clients alike; Entrust clients understand Microsoft-issued CRLs and Microsoft clients understand Entrust-issued CRLs. In addition, Entrust support for the Flexible Certificate Specification allows customers to define Entrust certificates that will be understood by Microsoft CryptoAPI, enhancing the support for PKI-enabled Microsoft applications (including IPSEC and NTFS encryption).

CRL Distribution Point Extension

The CRL Distribution Point (CDP) extension is a certificate extension that identifies how revocation information for that certificate may be obtained. The value that previous releases of Entrust/PKI have placed in this extension is the distinguished name of the distribution point location within the LDAP directory. To improve revocation information retrieval performance, the Entrust/PKI uses high performance partitioned CRLs to manage the size of CRLs. When using partitioned CRLs, the CRL must contain a critical extension called the Issuing Distribution Point (IDP). The IDP is required to prevent a security attack involving the transposition of the partitioned CRLs.

Windows applications use CryptoAPI to process the relevant CRLs. A CDP entry is required in the Certificate before CRL processing will be attempted. The CDP entry must be in the form of a Uniform Resource Identifier (URI). This allows Windows applications to support CRL retrieval using any one of HTTP://, LDAP://, FTP:// or FILE:// protocols. Unfortunately Microsoft PKI-enabled applications do not support partitioned CRLs (these are an option within the standard). Although the CDP attribute may be used to point to partitioned CRLs, Windows 2000 does not support the IDP extension in the CRLs. Proper validation software must fail certificate and CRL validation when encountering a critical extension that it does not support.

Entrust/PKI also publishes an Authority Revocation List (ARL) used to indicate revocations for CA cross-certificates and subordinate certificates. CryptoAPI assumes a single CRL per CA for both end entity revocation and CA revocation. This is evident in CryptoAPI's CRL caching mechanism that supports only one CRL cache per CA. This caching mechanism also inhibits the use of partitioned CRLs. Entrust resolves these interoperability issues while also maintaining compliance with x.509, IETF RFC 2459, CRADA MISPC and FPKI. Entrust/PKI supports the creation of CDP entries in both the distinguished name format and the URI format. This allows both Entrust and Windows applications to process the CDP. Entrust/PKI may also be configured to issue a single, combined CRL in addition to the high performance partitioned CRLs. This combined CRL contains all certificate revocations for the CA as required by Windows.

Entrust engines used by Entrust-Ready applications also support CDP entries with a URI format of LDAP://. The Windows 2000 PKI can be readily configured to place this LDAP:// value in certificates and publish the CRL to the Active Directory. This allows Entrust-Ready applications to properly process Windows 2000 PKI issued certificates. Further support for other URI protocols in the Entrust Engine will be introduced over time in order to further enhance interoperability.

Authority Information Access Extension

The Authority Information Access (AIA) extension indicates how to access information and services about the CA that issued the certificate in which the attribute appears. CryptoAPI uses this extension to assist in building trust chains while validating certificates. By placing a URI value in the AIA that points to the location of a CA certificate, Windows applications may retrieve CA certificates while building chains. Entrust does not populate or make use of this extension, as it relies on the directory for chain building. Entrust support for the Flexible Certificate Specification (FCS) allows customers to define certificates that contain this extension. As part of the Entrust/PKI, a utility is provided to more easily generate this extension for inclusion in an Entrust FCS.

Extended Key Usage Extension

The Extended Key Usage (EKU) extension indicates the purposes for which the public-key contained in the certificate may be used. Windows 2000 uses EKU extensively to indicate certificates that support special functions. These functions include things like IPSEC, NTFS File Encryption backup, as well as others. Entrust, through the FCS mechanism, can support the creation of many different certificate types containing different EKUs.

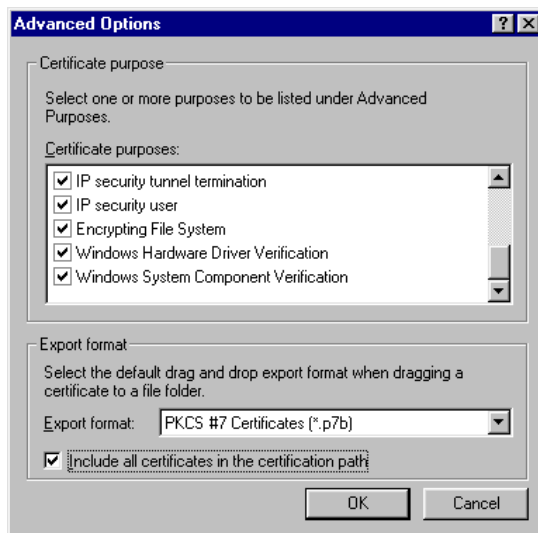


Figure 8 - Extended Key Usage Functions found in Internet Explorer 5.5

Unicode Name Support

Within the X.509v1 fields, there is the Issuer X.500 Name and the Subject X.500 Name. The Issuer X.500 Name field specifies the X.500 distinguished name (DN) of the CA that issued the certificate. The Subject X.500 Name field specifies the X.500 DN of the entity holding the private key corresponding to the public-key identified in the certificate. The DNs may contain international characters. To support international characters in certificates, both Entrust/PKI and Windows 2000 PKI support Unicode.

Application to Application Interoperability

Application to application interoperability is affected by the following: application protocol support, application certificate processing support and cryptographic algorithm support.

Both Entrust and Microsoft participate in ongoing protocol interoperability testing so that their products, as well as those of other vendors, interoperate properly. The current protocols that are supported through these trials include S/MIME for secure e-mail, and IPSEC for network transport security.

Certificate handling interoperability was discussed in the previous section on Application to PKI interoperability. Entrust/PKI and Entrust-Ready applications using the Release 5.0 Entrust engines are able to properly handle certificates generated by a Windows 2000 PKI. Windows 2000 certificates are required to be published in a directory supporting LDAPv3 and the CDP will need to contain an LDAP:// based

URI. This is the default configuration for the Windows 2000 PKI when an Active Directory is present. Trust between the Entrust/PKI and Windows 2000 PKI also needs to be established as outlined in the section on PKI to PKI interoperability.

Lastly the applications will need to support a common set of cryptographic algorithms. Entrust engines provide cryptographic capability to Entrust-Ready applications. Microsoft CryptoAPI provides cryptographic capability to Windows applications. The following table lists the common algorithms supported by both the Entrust engine and the Microsoft Base and Enhanced CSPs (there are others supported by both vendors).

Algorithm	Entrust Engine	Microsoft CSP (Base + Enhanced)
MD5	✓	✓
SHA-1	✓	✓
MD2	✓	✓
Other Hash Algorithms	MAC (ANSI X9.9), HMAC	MAC (RFC 1423, PKCS#5), HMAC
RSA Signing	Up to 2048 bits	Up to 16384 bits
RSA Key Exchange	Up to 2048 bits	Up to 1024 or 16384 bits
DSS Signing	Up to 1024 bits	Up to 1024 bits
Diffie-Hellman Store & Forward	Up to 1024 bits	Up to 1024 / 2048 bits
Diffie-Hellman Ephemeral	Up to 1024 bits	Up to 1024 / 2048 bits
RC2	40 or 128 bits	56 or 128 bits
DES	✓	✓
Triple DES	✓	✓

Figure 9 - Common Supported Algorithms

The Microsoft Base CSP is available internationally while the Enhanced provider is currently restricted by US export laws and is available only to some international customers. All of these listed algorithms are available for distribution in North America while Entrust engines are also available in Europe. Like Entrust, the Microsoft DSS and DH CSPs also support the Digital Signature Standard and Diffie-Hellman algorithms.

Note: Current export restrictions are in the process of being changed for retail software vendors like Entrust and Microsoft. These changes will likely translate into the ability to more freely distribute software to international customers. More information on export restrictions can be found at <http://www.cdt.org/crypto/admin/000110cryptoregs.shtml>.

Application to Application Interoperability: Net Result

Both Entrust and Microsoft participate in ongoing interoperability testing so that their products, as well as those of other vendors, interoperate properly. Through this testing and cooperation, Entrust and Microsoft application interoperability has been successfully verified. In addition, Entrust recently further strengthened their commitment to the Windows platform by committing to moving Entrust desktop applications to a state where they will be able to be Windows Logo Certified.

PKI to Directory Interoperability

Windows 2000 makes extensive use of the newly released Active Directory. Active Directory supports the lightweight directory access protocol (LDAP) to provide a single point of administration for all published resources.

PKI to Directory Interoperability: Net Result

Entrust has demonstrated interoperability with a wide range of directories that support the LDAP protocol and is committed to ensuring future interoperability with members of the LDAP community, including Microsoft. Due to that fact that there are some differences between Active Directory and other standard LDAP directories, Entrust does not currently support the use of Microsoft Active Directory with Entrust/PKI. Entrust is currently working with Microsoft and key customers to provide a solution that will allow use of Active Directory with Entrust/PKI in the first half of 2001.

Active Directory Integration with Entrust Products

Entrust products support any directory that conforms to the LDAP and X.500 standards. Entrust products can use both LDAPv2 and LDAPv3 to communicate with such directories. In general, Entrust products will support interaction with Active Directory through the use of the LDAPv3 protocol. However, because Active Directory behaves differently from standard X.500 directories, certain interoperability issues exist.

Specifically, Active Directory does not support the use of auxiliary object classes for dynamic extension of the directory schema. Changes were made to Entrust/PKI (Entrust/Authority and Entrust/RA) to remove reliance on auxiliary object classes. Some Entrust applications, however, still rely on the use of auxiliary object classes (e.g., Entrust/ProfileServer and Entrust/VPNConnector). These applications will be updated so that they do not require directory support for auxiliary object classes.

Active Directory's Directory Information Tree (DIT) & Directory Migration

Entrust products impose no restrictions on how information is organized within directories. For example, each Entrust CA entry has traditionally been represented by a Distinguished Name (DN) containing the organization's name and country; e.g.:

o=Company,c=US.

More recently, the domainComponent (dc) attribute has been used in DITs to specify the domain under which a CA operates. For example, the DN of a CA configured under this scheme may look like:

dc=company,dc=com

Entrust products support both of these DIT structures, and any other standard X.500 naming schemes.

While Active Directory can support different DIT structures, it employs a specific DIT structure to achieve tight integration with the Windows 2000 operating system and various Microsoft applications. This structure consists of several specific locations in the DIT called containers. There is, for example, an *AIA* container where Microsoft PKIs publish their CA certificates. In addition, the *Certificate Authorities* container is used to store CA certificates to be trusted by all applications. Entrust/Authority supports publishing of CA certificates to both the AIA and Certification Authorities containers. This allows Entrust CAs to establish themselves as trusted root CAs for all Microsoft applications.

Entrust is currently investigating migration options from X.500 directories to Active Directory for customers with existing PKIs. When planning such a migration, customers should consider the following:

- To take advantage of the tight integration between Active Directory, the Windows 2000 operating system and Microsoft applications, the customer's CA entry should be located in the AIA container. This will require the customer's CA DN to be changed to reflect the location of the AIA container. In addition, all of the CA's end users would likely need to be relocated to appropriate user containers in Active Directory.

- Active Directory does not support attribute aliases (e.g., commonName as an alias for cn). This isn't a problem for core Entrust applications, but may be a problem for custom applications built using the Entrust/Toolkits if the standard LDAP v3 names have not been used for attributes.
- Active Directory does not support the use of multiple attribute value assertions (AVAs) in a relative distinguished name (RDN). For example, the DN

cn=Bob Jones+serialNumber=1234,cn=users,dc=company,dc=com

is not permissible in Active Directory. This is not an issue for Entrust applications, as they do not place any restrictions or requirements on DNs. However, it does present an interoperability problem for customers who want to cross-certify a PKI setup using Active Directory with a PKI using an X.500 directory configured to use multi-AVA RDNs.

Authentication and Security

Entrust/PKI will support the use of Windows NT Challenge/Response (NTLM - Authentication methodology for Windows2000.) authentication as an LDAP authentication mechanism. This will allow Entrust applications installed on Windows platforms to authenticate to Active Directory before performing updates or before reading data. Entrust is currently investigating adding support for Kerberos as another Windows 2000 LDAP authentication mechanism.

Summary

This document has presented a high level overview of interoperability between Windows 2000 and Entrust. In a collaborative effort, Microsoft and Entrust are continually working to ensure seamless interoperability with their respective PKI offerings through support of multiple trust models, cryptographic algorithms, certificate handling, and application behavior. Going forward, Entrust and Microsoft are committed to working together on standards in the PKI area (such as being among the five co-founders of the PKI Forum. www.pkiforum.org), as well as further definition of interoperability between their products. This will ensure that at all times mutual customers of Entrust and Microsoft can be confident that these products will work together seamlessly, without additional complexity or costs.

Reference Documents

The following documents or references provide for further information on areas discussed in this white paper:

1. Entrust 5.0 Directory Requirements
<http://www.entrust.com/resourcecenter/pdf/entrust5directory.pdf>
2. Cross-Certification and PKI Policy Networking
http://www.entrust.com/resourcecenter/pdf/cross_certification.pdf
3. Key Update and the Complete Story on the Need for Two Key Pairs
<http://www.entrust.com/resourcecenter/pdf/2keypairs11.pdf>
4. X.509 (2000): 4th edition: Overview of PKI & PMI Frameworks
http://www.entrust.com/resourcecenter/pdf/509_overview.pdf