Windows XP Professional

PKI Enhancements in Windows XP Professional and Windows Server 2003

By DavidCross

Microsoft Corporation

Published: July 2001

Abstract

Microsoft® Windows® XP Professional and Microsoft Windows Server 2003 provide an integrated, public key infrastructure (PKI) that enables you to securely exchange information across the Internet, extranets, intranets, and applications. This white paper introduces Windows XP Professional certificate services and describes enhancements to existing Windows 2000 PKI features.

Acknowledgements

Michael Kessler, Technical Editor, Microsoft Corporation

Introduction

The combination of Microsoft Windows XP Professional and Microsoft Windows Server 2003 provide a range of PKI enhancements that let you securely extend your network to employees, partners, and customers and enhance the management and performance features of the Windows 2000 security infrastructure. Windows XP Professional and Windows Server 2003 offer many PKI-specific business benefits to organizations that require secure business processes and IT infrastructures.

Versatile

Windows Server 2003 lets you securely extend your network to employees, partners, and customers by integrating Virtual Private Network (VPN) services, standards-based authentication, and encryption technologies.

Flexible authentication options include:

- Smart cards
- X.509 certificates
- Kerberos
- Token-based authentication technologies
- Other authentication mechanisms

Strong encryption services include:

- Internet Protocol Security (IPSec)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol with IPSec (L2TP/IPSec)
- Secure Sockets Layer (SSL)
- Transport Layer Security (TLS)
- Encrypting File System (EFS)

Easy-to-Manage

Microsoft Windows XP Professional introduces user certificate auto-enrollment, which allows administrators to easily deploy certificates throughout the enterprise while requiring no user interaction.

Windows XP Professional also provides full support for:

- Full PKI cross-certification
- Name constraints, policy constraints, and policy mapping
- Delta certificate revocation lists (CRLs)
- Bridge certificate authority (CA) configurations
- Delegated policy administration
- Unified user management through Microsoft Active Directory™.

Dependable

Windows XP Professional and Windows Server 2003 expand and enhance the management and performance

features of the Windows 2000 security infrastructure. These improvements include:

- Increased Kerberos performance
- Automatic user enrollment for PKI certificates
- Streamlined access control list (ACL) evaluation
- Simplified authorization framework and ACL editor
- New credential manager for secure multiple identities
- Smart card support for administrators
- Extensible authentication protocol (EAP) for standard 802.11 wireless networking
- Integrated PKI key archival and recovery tools
- Encrypting offline files (client-side cache)

Business Benefits

Windows XP Professional and Windows Server 2003 offer many PKI-specific business benefits to organizations that require secure business processes and IT infrastructures.

Windows Server 2003

Windows Server 2003 includes a full-featured PKI that delivers the business benefits of public key cryptography. These include:

- A secure corporate intranet and extranet
- Confidential and secure e-mail
- Managed trust solutions
- File protection in the event of stolen or lost portable computers and other storage devices
- Access control and single identity authorization across a range of Web and application servers
- Digital signatures that enable tamper-proof, legally-binding transactions
- Trusted, on-demand, access to network resources for remote users
- Trusted, permanent network connectivity for remote offices
- Scalable technology to support millions of users and high-volume transactions

Windows XP Professional

PKI is an integral part of the Windows XP Professional operating system. PKI:

- Requires no per-certificate fees
- Is integrated into normal network management tasks
- Enables single sign-on capabilities to networks and applications
- Offers managed trust capabilities
- Supports all applications through CryptoAPI

This is a definite advantage considering that third-party PKIs must be purchased separately, and require per-certificate license fees and increased management tasks.

Windows XP Professional PKI Components

The Windows XP Professional PKI builds on Microsoft's long-established reputation for shipping robust PKI components. This white paper outlines the new functionality and enhancements that Microsoft has made with respect to these components within the framework of the Windows Server 2003.

The primary PKI components in Windows XP Professional are:

Certificate Services

Certificate Services is the part of the core operating system that allows a business to act as its own certificate authority (CA), and issue and manage digital certificates. Windows XP Professional supports multiple levels of a CA hierarchy and a cross-certified trust network: This includes offline and online certificate authorities.

Active Directory

Active Directory is a core operating system service that provides a single place to find network resources, and serves as both the PKI certificate repository and the management directory. Windows Server 2003 and

Windows XP Professional include an enterprise CA that is integrated with Active Directory to provide low-cost PKI deployments and easily managed policies. The enterprise CA controls operations such as:

- SSL client mapping
- Smart card logon
- Certificate auto-enrollment
- X.509 certificate construction

PKI-enabled Applications

Examples of PKI-enabled applications include: EFS, Microsoft Internet Explorer, Microsoft Money, Internet Information Server, remote access services, Microsoft Outlook®, and Microsoft Outlook Express. Also included are a variety of third-party applications that work with Windows 2000 PKI and Windows XP Professional PKI.

Exchange Key Management Service

The Exchange Key Management Service (KMS) is a component of Microsoft Exchange that allows for the archiving and retrieval of keys used to encrypt e-mail. In Windows .NET Advanced Server, a tool will be provided to migrate existing users' private keys (located in the KMS database) to a Windows .NET Advanced Server CA. The result: an enterprise-wide key management system with a single repository for enrollment and key archival.

Windows XP Professional Client Enhancements

User Auto-Enrollment

Using Windows 2000

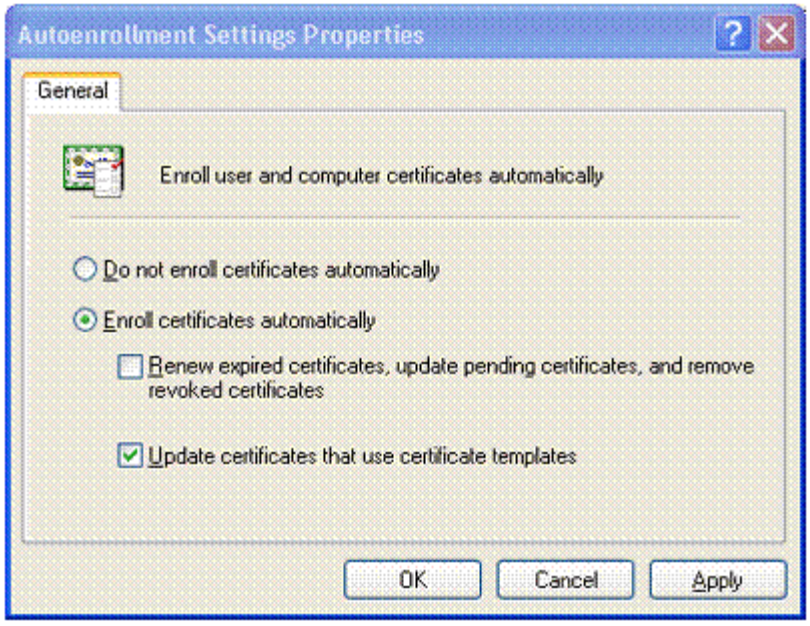
The Windows 2000 implementation of Certificate Services and PKI first introduced the feature of certificate auto-enrollment. Using Windows 2000, computers or domain controllers can automatically enroll for machine-type certificates in an Active Directory environment.

Auto-enrollment for machine or domain controller certificates is enabled through Group Policy and the Active Directory. Auto-enrollment of machine certificates is most useful in facilitating an IPSec or L2TP/IPSec VPN connection with Windows 2000 Routing and Remote Access service (RRAS) servers and other similar devices.

Using Windows XP Professional

Using Group Policy settings combined with Version 2 certificate templates, Windows XP Professional enables users to be automatically enrolled for user-type certificates when they log on. Automatic enrollment of user certificates is quick and simple, and enables PKI applications (smart card logon, EFS, SSL, S/MIME, and others) within an Active Directory environment. User auto-enrollment minimizes the high cost of normal PKI deployments. It reduces total cost of ownership for a PKI implementation when Windows XP Professional clients are configured to use the Active Directory.

Figure 1 shows some of the options available for setting up certificate autoenrollment.



If your browser does not support inline frames, click here to view on a separate page.

Figure 1 Autoenrollment Settings Properties

Pending Certificate Requests and Renewal

User auto-enrollment in Windows XP Professional supports both pending certificate requests and renewal features.

You can manually or automatically request a certificate from a Windows Server 2003 CA. This request is held until administrative approval is received or the verification process is completed. Once the certificate has been approved or issued, the auto-enrollment process will complete and install your certificates automatically.

The process for renewing expired user certificates also takes advantage of the auto-enrollment mechanism. Certificates are automatically renewed on behalf of the user—dependent upon the specifications in the certificate template.

Delta CRL Support

A Windows XP Professional client supports delta CRLs for revocation status checking; in fact, it will use any module that is installed and made available to CryptoAPI for revocation status checking. By default, the Windows XP Professional client will try to use delta CRLs first, and normal CRLs second. Additional modules, such as other Online Certificate Status Protocol (OCSP) clients, in their order of preference, may be installed. For more information, refer to the Platform Software Development Kit (SDK) in MSDN® (Microsoft Subscriber Developer Network).

Smart Cards

Windows 2000 introduced the capability to use smart cards for logging on to workstations and servers. In addition to auto-enrollment support, Windows XP Professional expands the capability of smart cards by adding the following key features:

Smart Card Support for Key Tools and Utilities

Administrators need tools and utilities that allow them to use alternate credentials so they can do their normal business—with normal user privileges—while at the same time carrying out their special administrator functions. Utilities such as Net.exe and Runas.exe meet this need. In Windows XP Professional, these tools have been enabled to support smart card credentials.

Smart Card for Terminal Server

Windows XP Professional lets you connect a smart card and a smart card reader to a Terminal Server client computer and perform smart card operations on the Terminal Server computer. To have this capability you must have Windows Server 2003 and Windows XP Professional running on the Windows .NET Terminal Server, and Windows XP Professional on the Windows .NET Terminal Server client computer. The Windows .Net

Terminal Server client software can also run on Windows 2000 computers.

Encrypting File System

The increased functionality of the EFS has significantly enhanced the power of the Windows XP Professional client.

Windows XP Professional now provides additional flexibility for corporate users when they deploy security solutions based on encrypted data files and folders. These new features include:

- Full support for revocation checking on certificates used by the system
- Alternate color support (green) for encrypted files
- Support for encrypted offline folders (client-side cache)
- Multi-user support on encrypted files in the shell user interface (UI)
- Folders in the shell UI.
- All of the new EFS features are available only in the Windows XP Professional client.

Multi-User Support on Encrypted Files

Windows XP Professional now supports file sharing between multiple users of an individual encrypted file. Although support for groups is not provided, EFS file sharing provides another opportunity for data recovery and business collaboration by adding users to an encrypted file. Encrypted file sharing is a useful and easy way to enable collaboration using encrypted files without having to share private keys among users.

File sharing is enabled through the new **Details** button on the advanced file attributes UI. This button is available once a file has been encrypted. A file must be encrypted and saved, before additional users can be added.

To add users, select the Advanced Properties of an encrypted file and click the **Details** button. Individual users may add other users (but not groups) from the local machine or from the Active Directory, provided the added users have a valid certificate for the EFS.

See Figure 2 for an illustration of encryption attributes.

Figure 2 Encryption Attibutes

EFS over WebDAV

Web-based Distributed Authoring and Versioning (WebDAV) is a file access protocol described in Extensible Markup Language (XML). It uses the Hypertext Transfer Protocol (HTTP) and runs over existing Internet infrastructure—for example, firewalls and routers.

EFS, combined with WebDAV folders, provides simple and secure ways to share sensitive data across networks. EFS with WebDAV eliminates the need to purchase specialized software to securely share encrypted files. The strong encryption capabilities of EFS, combined with the file-sharing functionality in Windows XP Professional, simplifies the process of sharing sensitive data. You can store files on common file servers—or on Internet

communities, such as Microsoft Network (http://www.msn.com/) — for easy access while maintaining strong security through EFS.

EFS with WebDAV folders facilitate numerous collaboration scenarios for organizations that want to achieve simple security solutions without deploying complex infrastructure or expensive technologies.

Encrypted Offline Files (Client-side Caching)

Windows 2000 introduced client-side caching, also known as Offline Files. This is a Microsoft IntelliMirror™ management technology that allows network users to access files on network shares — even when the client computer is disconnected from the network.

When a mobile user views a share while disconnected from the network, he or she can still browse, read, and edit files, because these files have been cached on the client computer. When the user connects to the server at a later time, the system reconciles the changes with the older versions of the documents on the server.

The Windows XP Professional client now allows offline files and folders to be encrypted using EFS. This feature is especially attractive for traveling professionals who need to work offline and maintain the security of their data.

See Figure 3 for an illustration showing options for encrypting the Offline Files database.

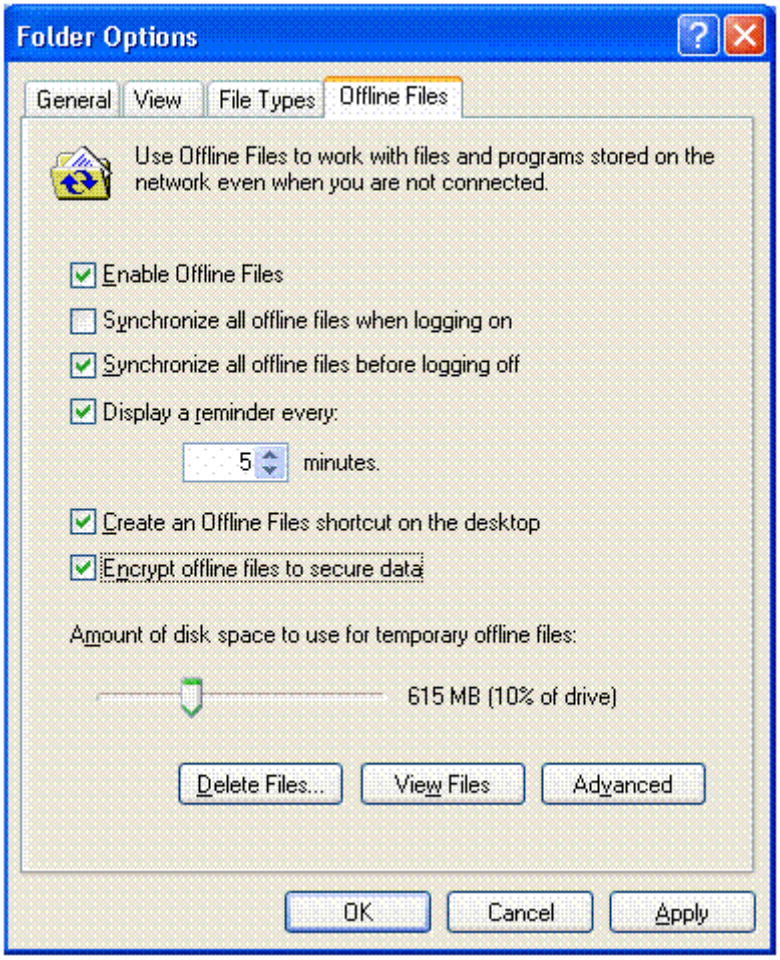


Figure 3 Encrypting the Offline Files Database

Additional Algorithm Support

The Windows XP Professional client now supports stronger optional encryption for EFS than the default Data Encryption Standard (DESX) algorithm. The client may now be used with a Federal Information Processing Standards (FIPS) 140-1 compliant algorithm, such as the 3DES algorithm, which is included in Windows XP Professional.

The 3DES algorithm may be chosen by changing the "Default algorithm policy for FIPS compliant applications" option in Local or Group Policy in the Active Directory. To do this, follow this path: Security Settings > Local Policies > Security Options.

Disabling Data Recovery

The functionality in Windows XP Professional client, combined with the enhancements in Active Directory for Windows Server 2003, enables organizations to have a more flexible data recovery policy.

Data Recovery Agents (DRAs) are no longer mandatory for EFS in Windows XP Professional. Data recovery can now be disabled in Group Policy for Windows XP Professional clients in those organizations that are deploying a key archival and recovery strategy and do not require DRAs.

CAPICOM

CAPICOM is a Component Object Model (COM) client that supports automation. It performs cryptographic functions using Microsoft ActiveX® and COM objects.

CAPICOM can be used to perform fundamental cryptographic tasks in applications created using many different programming languages, such as Microsoft Visual Basic®, Microsoft Visual Basic Scripting Edition, and Microsoft Visual C++®.

For example, a Visual Basic application can use CAPICOM objects to digitally sign data, verify digital data signatures, envelop data for privacy, and encrypt and decrypt arbitrary data. CAPICOM-based applications use the most common parameters as default property settings, but can set properties for sophisticated signing or encryption.

CAPICOM and CryptoAPI

CAPICOM uses a PKI and is built on CryptoAPI—an application programming interface. It provides services that let application developers use cryptography to add security to applications.

CryptoAPI includes capabilities for encrypting and decrypting data for simple and complex message handling, for creating and verifying digital signatures, and for authentication using digital certificates. Since CAPICOM uses CryptoAPI, digital signing applications can take advantage of smart cards and other hardware devices that support CryptoAPI through the CSP interface.

Root CA AutoUpdate

Before a CA can use a new root certificate (root), it must wait for its client base to install it. Historically, roots were shipped along with major product releases—for example, Microsoft Internet Explorer and Windows 2000 contained root certificates when they were released.

Because there was no automatic way to deliver new root certificates to those customers, CAs had to wait until they upgraded to new software products containing the new root before they were able to offer certificate services based on the new root certificate.

Windows Update

Windows XP Professional keeps you up-to-date with the latest CA root certificates. They're available for download on the Windows Update Web site, at http://windowsupdate.microsoft.com/.

When users visit a secure Web site (using Hypertext Transfer Protocol [HTTPS]), read a secure e-mail message that uses Secure/Multipurpose Internet Mail Extensions (S/MIME), or download an ActiveX control that uses a new root certificate, the Windows XP Professional Certificate Chain Verification software will check Windows Update and download the root certificate you need. This experience is seamless, and the download happens automatically in the background.

Trusted Root Certificates

Windows XP Professional gives administrators greater control over the root certificates trusted by their clients. All third party root certificates are moved into a separate logical certificate store which is periodically updated by the AutoUpdate of Root Certificates feature. An administrator in a Windows Server 2003 domain has the ability to disable this store through group policy.

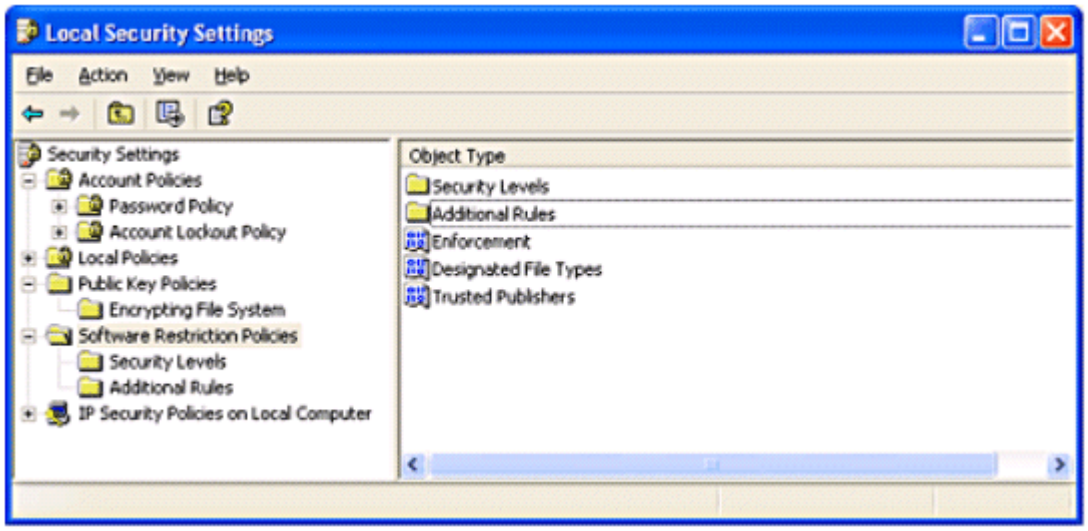
Other root certificate authorities that want to make their root CA certificates available through AutoUpdate should submit a request to: casubmit@microsoft.com.

Software Restriction Policies

Software restriction policies in Windows XP Professional provide a policy-driven method to identify software and control its ability to run. Administrators define rules that control when software is allowed to run. These rules are contained in group policy, which enables them to be set on a site, domain, or organizational unit (OU).

A software restriction policy consists of a default rule that determines whether or not software should be allowed to run—along with exceptions to that rule. This allows administrators to define a policy that specifies where all software runs. For example: One default option could be that all software runs, except for a specified set of programs. Another default option could be that no software runs, except for a specified set of programs.

See Figure 4 for an illustration of software restriction policy settings.



If your browser does not support inline frames, click here to view on a separate page.

Figure 4 Software Restriction Policies—Local Security Settings

Software Identification Rules

An administrator identifies software through one of the following rules:

Hash Rule

A software restriction policy's Microsoft Management Console (MMC) snap-in allows an administrator to browse to a file and identify that program by calculating its hash. A hash is a digital fingerprint that uniquely identifies a program or file. A file can be renamed or moved to another folder or computer and it will still have the same hash.

Path Rule

A path rule can identify software by a full path name, such as C:\Program Files\Microsoft Office\Office\excel.exe; or by the path name leading to the containing folder, such as C:\Windows\System32. (This would refer to all programs in that directory and its subdirectories.)

Path rules can also use environment variables, such as %userprofile%\Local Settings\Temp.

Certificate Rule

A certificate rule identifies software by the publisher certificate used to digitally sign the software. For example, an administrator can configure a certificate rule that only allows software signed by Microsoft or its IT organization to be installed.

Zone Rule

A zone rule identifies software that comes from the Internet, local intranet, trusted sites, or restricted sites zones.

Controlling Digitally Signed Software

Software restriction policies improve an administrator's ability to control digitally signed software in the following ways:

Limiting Active X Controls

An administrator can specify the ActiveX® controls that will run in Internet Explorer for a particular domain by using a software restriction policy that lists trusted software publisher certificates. If the publisher of an ActiveX control is on the trusted publisher list, its software automatically runs when downloaded. A software restriction policy can also list disallowed publishers. This automatically prevents ActiveX controls signed by those publishers from running.

Using a software restriction policy, it's also possible to control who can make a trust decision about an unknown publisher—a publisher that's not explicitly trusted or distrusted. Software restriction policies can be set up to allow only local administrators, or domain administrators, to decide which publishers to trust, and to

prevent users from making those decisions.

Using Windows Installer

Programs installed using the Windows Installer can be digitally signed. Using a software restriction policy, an administrator can require that only software digitally signed by certain software publishers can be installed. Windows Installer will then check to verify that an approved signature is present before installing software on the computer.

Digitally-signing Visual Basic Script

Visual Basic Script files can be digitally signed. An administrator can configure a software restriction policy so that Visual Basic Script files (.vbs) have to be digitally signed by approved software publishers before they can run.

What's New in Windows Server 2003

Version 2 Certificate Templates

Windows 2000 and Windows XP Professional PKI use certificate templates that are stored in Active Directory. These templates provide the default contents of a certificate request to an enterprise CA—as opposed to using a standalone CA. Policy management in an Active Directory environment is provided through the use of certificate templates.

Enterprise CAs use certificate templates to determine authentication, certificate format, cryptographic service provider (CSP), key size, and X.509 extension requirements. To allow for a registration authority, CA officer, and other approvals, Windows XP Professional templates have been extended to merge the signing and authentication requirements necessary to issue a certificate.

Version 1 and Version 2 Certificate Templates

Version 1 Templates

Windows 2000 Server and Windows 2000 Professional clients support a default set of certificate templates in the Active Directory that cannot be customized or added to. These are Version 1 templates. Version 1 templates can only be used as defined or copied.

Version 2 Templates

Windows Server 2003 extends the range of properties that can be configured in a Version 1 template. These extensions include the ability to:

- Create new certificate templates
- Copy existing templates
- Supersede templates already in use

Using Windows Server 2003, Version 2 templates can be edited to meet the needs of an application or the enterprise. When a Version 1 template is copied, it is automatically updated and becomes a Version 2 template.

Enrollment and Certificate Issuance in Version 2

The following new features have been added to Version 2 templates. They provide additional functionality during the enrollment and certificate issuance process, such as:

- Customization of enrollment policies
- Certificate authorization
- Domain authentication
- Certificate administrator
- Enrollment agent signed
- Key creation
- Key type and CSP type
- Certificate contents
- Validity, issuance, and application policies—and key usages
- Key archiving

Creating and Customizing Certificate Templates

Certificate templates can be created and customized to meet specific business requirements and operational needs. The ability to have one template supersede another makes creating or customizing templates easy. Users or computers can be renewed automatically by providing an updated certificate; all you have to do is apply user auto-enrollment and supersede one template with another. Certificate deployments can be rapidly and easily modified by merely superceding an existing certificate template (or templates). This functionality removes the worry in deploying certificates that may need to be modified or updated at a time prior to the natural expiration of the certificates.

Key Archival and Recovery

Comparing Windows 2000 Server and Windows Server 2003

Windows 2000 Server

For data recovery, Windows 2000 Server uses a data recovery agent to decrypt files that have been encrypted using the EFS.

Exchange Server's Key Management Server uses a key recovery method for S/MIME-encrypted e-mail (Secure/Multipurpose Internet Mail Extensions).

Windows Server 2003

With Windows Server 2003, the CA may be used to archive and recover the private key associated with an individual certificate request. Private key recovery does not recover any data or messages. It only enables a user to retrieve lost or damaged keys, or allows an administrator to assume the role of a user for data access or data recovery purposes. Often data recovery cannot occur without key recovery occurring first.

The Key Archival and Recovery Process

The steps in the key archival and recovery process include:

1. An enterprise CA uses a certificate template definition to determine if a client certificate request should also include private key archival.
2. The client generates a public-private key pair, and sends a certificate request to the CA. The client uses the Certificate Management protocol, with Cryptographic Message Syntax (CMS), for the certificate request. (This protocol is also known as CMC).
3. The payload of the Certificate Management protocol (using CMS) request contains the encrypted private key of the user. The private key of the user is encrypted with the public key of the CA.
4. The CA first decrypts the private key in the request, then cryptographically validates that the private key of the user corresponds to the public key in the certificate request. An enterprise CA will also validate the certificate template in the Active Directory to ensure that the private key is eligible to be archived.
5. A random 3DES (Data Encryption Standard) symmetric key will be generated by the CA to encrypt the user's private key.

Key Recovery Agents

Based on the policy settings, the symmetric key protecting the user's private key will be encrypted with one or more public keys from key recovery agents (KRA). The result of this process will be stored as a recovery blob within the certificate request, located in the CA database.

The key archival process allows the CA administrator to configure the minimum number of KRAs that will have the ability to decrypt the private key of a user. A KRA must hold a special certificate type that may—or may not—be issued by the same CA on which it is used. A CA administrator may also decide to allow a sequential and cyclical selection of the KRAs.

An important aspect of the CA's archival and recovery attributes is that no private key material exists on the CA to decrypt private keys protected by the key recovery agent. Only public key certificates are used to encrypt end-entity private keys, and recovery may occur on an administrative console. This ensures that no person can compromise the security of the archived keys.

The capability exists to use multiple key recovery agents. Multiple key recovery agents ensure that no single KRA can recover all of the private keys from the certificates issued by a particular CA. Split key pairs are available through the use of 3rd party CSPs.

Delta Certificate Revocation Lists

In Windows 2000, certificate authorities are responsible for providing certificate status information by publishing a complete CRL, as defined in RFC 2459. The CRL may be published manually or automatically at predefined intervals. In Windows Server 2003—as specified in RFC 2459—a CA may also publish a delta CRL.

Delta CRL vs. Full CRL

A delta CRL is a list that contains only certificates whose status has changed since the last full (base) CRL was compiled. Delta CRLs have several key advantages over standard CRL publishing:

- Much smaller objects than in a full CRL
- Can be published very frequently with little or no impact on client machines or network infrastructure
- Low latency of revocation status
- Minimal infrastructure or network impact

Qualified Subordination

When a subordinate CA is created in a hierarchy of certificate authorities, the parent CA has the opportunity to restrict its capabilities. Qualified subordination also permits a robust cross-certification capability to the Windows Server 2003 CA.

In Windows 2000, subordination is qualified based on implicit policy, which gives any subordinate CA unrestricted powers in this type of delegation model. Windows XP CAs provide the capability to offer qualified subordination.

Qualified subordination allows an administrator to add restrictions to the CA certificate. These restrictions are translated into certificate extensions within the issued certificate, and are added after the initial certificate is made. They are then bound to the original request by a Certificate Management protocol using CMS data structure, and then the new Certificate Management protocol using CMS request is signed by an administrator. The signing certificate can also carry similar restrictions. These restrictions form the basis of this delegation model.

Qualification Extensions

Extensions that can qualify a subordination are listed in the table below, along with a reference to where they can be found within RFC 2459.

Table of Qualification Extensions

Extension Name	RFC 2459	Qualification
Name constraints	4.2.1.11	DNS names only (for example: DNS, e-mail, UPN)
Policy	4.2.1.5	Specifies what issuance policy the CA may use
Policy constraints	4.2.1.12	Inhibit policy mapping only
Policy mapping	4.2.1.6	Maps the issuer’s issuance policy to the subject issuance policy
Basic constraints	4.2.1.10	Limits path length only
Application Policy	None at this time	Specifies which application policies the CA may issue

Name Constraints

Name constraints restrict the valid range of names permitted or excluded by the CA and its subordinates. Windows .NET PKI supplies a variety of names for constraint. These include: Domain Name System (DNS); DNS names, Internet Protocol (IP) addresses, and e-mail names; and universal principal name (UPN).

Policy

Policy defines the list of acceptable issuance policies, identified by object identifier (also known as OID). The object identifiers used are implementation-dependent and may differ based on application or implementation.

Policy Constraints

Policy constraints define whether or not a policy can be mapped in a chain, and if so, where. They also allow the issuance policy to be mandated in the certificate chain.

Policy Mapping

Policy Mapping allows a policy from one domain to be mapped onto a policy of another domain—this is a fundamental part of cross-certification. Policy mapping may also be used for inter-forest subordination.

Basic Constraints

A basic constraint limits the length of a path in a CA hierarchy. This prevents a subordinate CA from signing another subordinate CA.

Application Policies

An application policy defines what a certificate may be used or accepted for. It's similar to the Extended Key Usage extension. However, application policies allow for policy qualifiers that may be mapped against other policy constraints.

Common Criteria Role Separation

Windows .NET Certificate Server requires role separation in the CA that supports common criteria requirements. The purpose of role separation is to ensure that no individual can compromise the services or operation of a CA. Role separation also supports task delegation.

Table of CA Roles

Action	Enrollee	CA admin.	Officer	Auditor	Backup operator	Local server admin.
Install CA						X
Configure CA		X				X
Configure policy and exit module		X				
Stop/start service		X				X
Change configuration		X				
Assign roles		X				
Establish user accounts		X				X
Maintain user accounts		X				X
Configure profiles		X				X
Renew CA keys						X
Define key recovery agent (s)		X				
Define officer roles		X				
Enable role separation		X				
Issue/approve certificates			X			
Deny certificates			X			
Revoke certificates			X			
Unrevoke certificates			X			
Renew certificates			X			
Enable, publish, or configure CRL schedule		X				
Recover archived key			X[1]			
Set extension (request)			X			
Set attribute (request)			X			
Configure audit parameters				X[5]		X
Audit logs				X[5]		X
Back up system					X[2]	X
Restore system					X[2]	X

Read CA properties, CRL	X[4]					
Request certificate	X[3]					
Read CA database		X	X	X	X	
Read CA configuration information		X	X	X	X	
Read issued, revoked, and pending certificates		X	X	X	X	

Explanatory Notes:

1. A CA officer must also hold the private key of a key recovery agent.
2. A backup operator must be a local administrator of the server, or must hold the system backup privilege and be a member of the server operators' group (local machine).
3. A user must have the enrolled ACL on the certificate template to request a certificate.
4. The Everyone group has permission to read the general properties of a CA and fetch a CRL.
5. An auditor must be a local administrator of the server, or must hold the system audit privilege.

Auditing

In both Windows 2000 and Windows Server 2003, the CA database is used to audit all CA events. This database provides the details and history of significant events and actions.

Auditing Enhancements

The Windows Server 2003 CA provides additional auditing enhancements in the NT Event log. The audit log generates two types of events:

- Access check
- System events

System Events

System events are generated in seven key categories:

- CA service
- Backup and restore
- Certificate requests
- Certificate revocation
- CA security
- Key archival and recovery
- CA configuration

Secure Sockets Layer (SSL)

Several significant enhancements to SSL and Transport Layer Security (TLS) services have been made that improve performance and functionality.

PKI-based Authentication over SSL/TLS

The combination of Version 2 certificate templates, name constraints, and auto-enrollment offers highly functional, management-free, PKI-based authentication over SSL/TLS.

Using any CA, the Windows Server 2003 Active Directory will allow a user's X.509 certificate to map directly to the user's account in the Active Directory. This is accomplished without having to export or import individual certificates, or provide user names and passwords. Certificate mapping through the s-channel Security System Provider Interface (SSPI) may be used by applications such as Internet Information Server, Commerce Server, remote access services and many others.

Unparalleled Performance with More SSL Handshakes

Together, Windows XP Professional and Windows Server 2003 provide an SSL/TLS-enabled, e-commerce Web site with unparalleled performance capabilities. S-channel improvements expand on the solid performance of Windows 2000 and enable Windows Server 2003 to provide unprecedented software-based

encryption performance.

Windows Server 2003 supports approximately 75 SSL handshakes per second on a single 750-megahertz (MHz) CPU. For sites demanding even higher performance, Microsoft has worked closely with partner independent software vendors (ISVs) to provide optimal performance for hardware-based encryption. With cryptographic-offload hardware, a Windows Server 2003 running Internet Information Server can process over 550 new SSL connections per second, and do so on a very affordable dual-processor, 800-MHz computer.

Shared SSL Sessions

SSL sessions are now shared across processes to improve user experience and to support Microsoft .NET applications. You'll experience the efficiency that comes from reducing the load on your Web server, while gaining an unexpected economic benefit: expensive SSL handshakes only have to be done once for each client—even if the server makes requests from multiple applications.

Dependencies

To take advantage of the new PKI functionality in Microsoft Windows, you'll need to upgrade to a Windows XP Professional client and Windows Server 2003 configuration. Some server-based CA features will only be available on Windows .NET Advanced Server. Specific requirements are detailed in the sections that follow:

Version 2 Templates

To use Version 2 templates, the Active Directory schema must be extended to the Windows Server 2003 schema in the forest.

Windows .NET Advanced Server

To issue a Version 2 template, you'll need Windows .NET Advanced Server running Certificate Services.

Windows .NET Standard Server

A Windows .NET Standard Server running Certificate Services cannot issue a certificate for a Version 2 template.

Windows XP Professional Client

A Windows 2000 client cannot use the MMC to enroll for a Version 2 template. However, Windows 2000, Windows 98, and Windows Millennium Edition (Windows Me) clients can enroll for a Version 2 template using Web enrollment pages.

Key Archival and Recovery

Key archival and recovery depends on Version 2 templates being available—this includes a Windows Server 2003/ Windows XP Professional schema, and a Windows .NET Advanced Server running as an enterprise CA.

Windows .NET Advanced Server

Key archival and recovery may only be performed on a Windows .NET Advanced Server running Certificate Services.

Windows XP Professional Client

A client must support the Certificate Management (using CMS) enrollment protocol. Windows 2000 and Windows Me clients may use the Certificate Management (using CMS) protocol through the Web enrollment pages on a Windows Server 2003 enterprise CA. Through the Web enrollment pages, Windows 2000 and Windows Me clients may make a certificate request for private key archival.

User Auto-Enrollment

User Auto-Enrollment is only available on Windows XP Professional clients and requires a Windows Server 2003 schema domain controller to authenticate the client. This feature also requires a Windows .NET Advanced Server, running as an enterprise CA, to support the Version 2 template.

Delta CRLs

Delta CRLs require a Windows XP Professional client and a Windows Server 2003 CA.

Qualified Subordination

Qualified subordination—with name constraints—requires a Windows XP Professional client and a Windows Server 2003 schema. Windows Server 2003 Internet Information Services (IIS), and PKI-enabled application

servers are designed to take maximum advantage of qualified subordination.

Common Criteria

Common criteria features are specific to the Windows Server 2003 (CA), and are only available on Windows .NET Advanced Server.

Client Dependencies

To use the features described in this white paper you'll need a Windows XP Professional client. The exception to this requirement is Web enrollment of Version 2 templates.

Any Microsoft Web client may download the latest version of the Xenroll.dll ActiveX control and enroll for a Version 2 template.

Summary

Windows XP Professional client and Windows Server 2003 have enhanced features that meet the requirements of almost any customer who wants to deploy a PKI infrastructure, or PKI-enabled applications. The flexibility of user certificate auto-enrollment, Version 2 certificate templates, and key archival lets you deploy a PKI with ease—and at a very low cost compared with other industry solutions.

Windows XP Professional client and Windows Server 2003 support new industry standards that let you interoperate in a heterogeneous environment using PKI on a Windows platform. This includes deploying public key technology components as part of your business-to-business and business-to-consumer solutions.

For More Information

For more information about how PKI works with Windows XP Professional and Windows Server 2003, visit the following Web pages:

What's New in Security for Windows XP

Public Key Infrastructure

Microsoft Windows 2000 Public Key Infrastructure

Windows 2000 Server and Key Management Server Interoperability

Windows 2000 Server and PKI: Using the nCipher Hardware Security Module

For the latest information on Windows XP, check out the Web site.
