

Windows Server® 2008 PKI and Certificate Security

Brian Komar

PREVIEW CONTENT This excerpt contains uncorrected manuscript from an upcoming Microsoft Press title, for early preview, and is subject to change prior to release. This excerpt is from *Windows Server® 2008 PKI and Certificate Security* from Microsoft Press (ISBN 978-0-7356-2516-7, copyright 2008 Brian Komar, all rights reserved), and is provided without any express, statutory, or implied warranties

To learn more about this book, visit Microsoft Learning at
<http://www.microsoft.com/MSPress/books/9549.aspx>

978-0-7356-2516-7

Microsoft®
Press

© 2008 Brian Komar. All rights reserved.

Table of Contents

1 Cryptography Basics

- Encryption Types
- Algorithms and Keys
- Data Encryption
- Digital Signing of Data
- Cryptography Next Generation
- Case Study: Microsoft Applications and their Encryption Algorithms
- Additional Information

2 Primer to Public Key Infrastructure

- Certificates
- Certification Authorities
- Revocation
- Revocation Methods
- Certificate Revocation Lists
- OCSF
- Case Study: Inspecting an X.509 Certificate
- Additional Information

3 Policies and PKI

- How a PKI Affects Policy Design
- Security Policy
- Certificate Policy
- Certification Practice Statement (CPS)
- Case Study: Planning Policy Documents
- Additional Information

4 Preparing an Active Directory Environment

- Analyzing the AD Configuration
- Preparing the Active Directory for PKI
- Preparing non-Active Directory Environments
- Case Study: Preparing Active Directory
- Additional Information

5 Designing a Certification Authority Hierarchy

- Determining the Number of Tiers in a CA Hierarchy
- Organizing Issuing CAs
- Choosing an Architecture
- Gathering Required Information
- Case Study: Identifying Requirements

6 Implementing a CA Hierarchy

- How to Use this Chapter
- Preparing Configuration Scripts for Installation
- Implementing an Enterprise Root CA
- Implementing a Standalone Root CA
- Implementing an Offline Policy CA
- Implementing an Online Issuing CA
- Case Study: Deploying a PKI
- Additional Information

7 Upgrading Your Existing Microsoft PKI

- Supported Scenarios
- Performing the Upgrade
- Additional Information

8 Verifying and Monitoring Your Microsoft PKI

- Verifying the Installation
- Ongoing Monitoring
- Case Study: Monitoring CA Issues
- Additional Information

9 Securing a CA Hierarchy

- Designing Logical Security Measures
- Designing Physical Security Measures
- Securing the CA's Private Key
- Hardware Security Modules
- Case Study: HSM Deployment
- Additional Information

10 Certificate Revocation

- When do you Revoke Certificates
- Methods of Identifying Revoked Certificates
- Problems with CRLs
- Online Certificate Status Protocol (OCSP)
- Case Study: Planning Revocation
- Additional Information

11 Certificate Validation

- Certificate Validation Process
- Building Certificate Chains
- Designing PKI Object Publication
- Troubleshooting Certificate Validation
- Case Study: Choosing Publication Points
- Additional Information

12 Designing Certificate Templates

- Certificate Template Versions
- Modifying Certificate Templates
- Best Practices for Certificate Template Design
- Case Study: Certificate Template Design
- Additional Information

13 Common Criteria Roles

- Common Criteria Levels
- Windows Server 2008 Implementation of Common Criteria
- Assigning Common Criteria roles
- Implementing Certificate Manager Restrictions
- Enforcing Common Criteria Role Separation
- Other PKI Management Roles
- Case Study: Planning PKI Management Roles
- Additional Information

14 Planning and Implementing Disaster Recovery

- Developing Required Documentation
- Choosing a Backup Method
- Availability Options
- Performing System State Backups
- Performing Manual Backups
- Restoration Procedures
- Evaluating Backup Methods
- Case Study: Replacing Server Hardware
- Additional Information

15 Deploying Certificates

- Certificate Enrollment Methods
- Choosing an Enrollment Method
- Publishing Certificate Templates for Enrollment
- Performing Manual Enrollment
- Performing Automatic Enrollment
- Credential Roaming
- Case Study: Selecting a Deployment Method
- Additional Information

16 Creating Trust between Organizations

- Methods of Creating Trust
- Qualified Subordination Conditions
- Implementing Qualified Subordination
- Verifying Qualified Subordination
- Case Study: Trusting Certificates from another Forest
- Additional Information

17 Identity Lifecycle Manager 2007 Certificate Management

- Overview
- Installing ILM 2007
- Configuring Profile Templates
- Additional Information

18 Archiving Encryption Keys

- Roles in Key Archival
- The Key Archival Process
- Requirements for Key Archival
- Performing Key Recovery
- Best Practices
- Case Study: Lucerne Publishing
- Additional Information

19 Implementing SSL Encryption for Web Servers

- How SSL Works
- Certificate Requirements for SSL
- Choosing a Web Server Certificate Provider
- Placement of Web Server Certificates
- Choosing a Certificate Template (update for Server 2k8)
- Issuing Web Server Certificates
- Certificate-Based Authentication
- Performing Certificate-Based Authentication
- Best Practices
- Case Study: The Phone Company
- Additional Information

20 Encrypting File System

- EFS Process
- One Application, Multiple Recovery Methods
- Deploying EFS
- Best Practices
- Case Study: Lucerne Publishing
- Additional Information

21 Deploying Smart Cards

- Deploying Smart Cards with Windows Vista
- Deploying Smart Cards with ILM 2007 CM
- Additional Information

22 Secure E-mail

- Securing E-mail
- Choosing Certification Authorities
- Choosing Certificate Templates
- Choosing Deployment Methods
- Enabling Secure E-mail
- Best Practices
- Case Study: Adventure Works
- Additional Information

23 Virtual Private Networking

- Certificate Deployment for VPN
- Certificate Template Design
- Deploying a VPN Solution
- Best Practices
- Case Study: Lucerne Publishing
- Additional Information

24 Wireless Networking

- Threats Introduced by Wireless Networking
- Protecting Wireless Communications
- 802.1x Authentication Types
- Planning Certificates for 802.1x Authentication
- Deploying Certificates to Users and Computers
- Implementing 802.1x Authentication
- Best Practices
- Case Study: Margie's Travel
- Additional Information

25 Document and Code Signing

- How Code Signing Works
- How Document Signing Works
- Certification of Code and Document Signing Certificates
- Planning Deployment of Signing Certificates
- Performing Code Signing
- Performing Document Signing
- Verifying the Signature
- Case Study: Lucerne Publishing
- Additional Information

26 Network Access Protection with IPSec

- Health Certificates for IPSec Enforcement
- Deploying Health Registration Authorities and CAs
- Additional Information

27 Deploying Certificates to non-Windows Platforms

- General Process
- Example Request
- Additional Information

28 Network Device Enrollment Service (NDES)

- History of NDES and Microsoft PKI
- Simple Certificate Enrollment Protocol Enroll Process
- Implementing NDES
- Configuring NDES
- Best Practices
- Additional Information

29 Remote Desktop Services

- Prerequisites
- Configuring the Terminal Server
- Configuring the TLS Client
- Additional Information

Chapter 2

Primer to PKI

Certificates

Certificates provide the foundation of a public key infrastructure (PKI). These are electronic credentials, issued by a certificate authority (CA), that are associated with a public and private key pair.

A certificate is a digitally signed collection of information roughly two to four KB in size. A certificate typically includes the following information:

- Information about the user, computer, or network device that holds the private key corresponding to the issued certificate. The user, computer, or network device is referred to as the subject of the certificate.
- Information about the issuing CA.
- The public key of the certificate's associated public and private key pair.
- The names of the encryption and/or digital signing algorithms supported by the certificate.
- A list of X.509 version 3 extensions included in the issued certificate.
- Information for determining the revocation status and validity of the certificate.

The CA must ensure the identity of the requestor before issuing a certificate. Identity validation can be based on the user's security credentials or might include a face-to-face or in-person interview to validate requestor identity. Once identity is confirmed, the CA issues the certificate and digitally signs the certificate with its private key to prevent content modification.

It is nearly impossible for another user, computer, network device, or service to impersonate the subject of a certificate because impersonation requires access to the certificate holder's private key. Impersonation is not possible if an attacker has access to the certificate only.

Three versions of digital certificates can be used in a PKI:

- X.509 version 1 certificates
- X.509 version 2 certificates
- X.509 version 3 certificates

X.509 Version 1

The X.509 version 1 certificate definition was defined in 1988. Its advanced age means you rarely see version 1 certificates in networking. The exceptions are some of the older root certificates and older Exchange Key Management Service (KMS) deployments. The X.509 version 1 format defines the certificate fields, as shown in Figure 2-1.

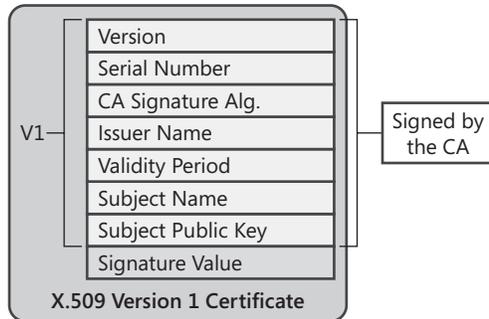


Figure 2-1 The X.509 version 1 certificate fields

An X.509 version 1 certificate contains the following fields:

Version.

- Contains a value indicating that the certificate is an X.509 version 1 certificate.

Serial Number.

- Provides a numeric identifier that is unique for each CA-issued certificate.

CA Signature Algorithm.

- The name of the algorithm the CA uses to sign the contents of a digital certificate. Figure 2-1 shows the fields included when creating the digital signature.

Issuer Name.

- The distinguished name of the certificate's issuing CA. Typically, the distinguished name is represented in an X.500 or distinguished name format specified in the X.509 specification and Request for Comment (RFC) 3280, "Internet X 509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile."

Validity Period.

- The range of time for which the certificate is considered valid. In some offerings, the validity period is split into two fields: Valid From and Valid To.

Subject Name.

- The name of the computer, user, network device, or service represented by the certificate. Typically, the subject name is represented in an X.500 or distinguished name format specified in the X.509 specification, but it can include other name formats, such as an RFC 822, "Standard for the Format of ARPA Internet Text Messages," e-mail name format.

Subject Public Key Info.

- The public key of the certificate holder. The public key is provided to the CA in a certificate request and is included in the issued certificate. This field also contains the public key algorithm identifier, which indicates which public key algorithm is used to generate the key pair associated with the certificate.

Signature Value.

- Contains the signature value that results from the CA signature algorithm used to sign the digital certificate.

In a version 1 certificate, the Issuer Name and Subject Name fields allow certificates to be organized into a chain of certificates that starts at the certificate issued to a user, computer, network device, or service and terminates with a root CA certificate.

Certificate chaining is fully discussed in Chapter 10, "Certificate Validation."

X.509 Version 2

While the X.509 version 1 certificate format provides basic information about the certificate holder, the format offers little information about the certificate issuer. By including only the issuer, issuer name, CA signature algorithm, and signature value, the version 1 format does not provide any provisions for CA renewal.

When a CA's certificate is renewed, two certificates possess the same Issuer Name field value. Likewise, it is possible for another organization to create a CA with the same issuer name. To address this, the X.509 version 2 certificate format was introduced in 1993. The version 2 format introduced two new fields to the certificate, as shown in Figure 2-2.

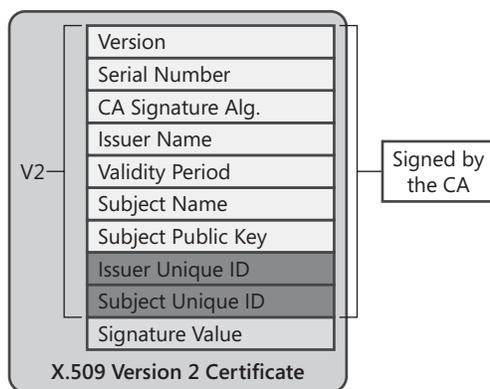


Figure 2-2 The X.509 version 2 certificate fields

The X.509 version 2 certificate format introduced the following fields:

Issuer Unique ID.

- An optional field that contains a unique identifier, typically a hexadecimal string, for the issuing CA as defined by the issuing CA. When a CA renews its certificate, a new Issuer Unique ID is generated for that certificate version.

Subject Unique ID.

- An optional field that contains a unique identifier, typically a hexadecimal string, for the certificate's subject as defined by the issuing CA. If the subject is also a CA, this unique identifier is placed in the Issuer Unique ID.

In addition to introducing the Issuer Unique ID and Subject Unique ID fields, the X.509 version 2 certificate's Version field changed to a value of 2 to indicate the version number.

The Issuer Unique ID and Subject Unique ID fields improved the certificate chaining process. The process now finds the CA certificate by matching the issuer name in the issued certificate to the subject name in the CA certificate and performs a second check by matching the Issuer Unique ID in the issued certificate with the Subject Unique ID of the CA certificate.

This additional level of matching allows a distinction between CA certificates when the CA renews a certificate. This method also allows for a distinction between CAs with the same subject name. (The likelihood of CA certificates with the same name increases when simple names are used—for example, *CN=Root CA* rather than *CN=Fabrikam Industries Inc. Corporate Root CA,O=Fabrikam,C=NL.*)

Although the addition of the Issuer Unique ID and Subject Unique ID aids in chain building, it's still possible for collisions to occur. A collision occurs when two certificates share the same Subject Name and Subject Unique Identifier fields.

Although the X.509 version 2 format improved on the version 1 format, the standard was not widely supported. In fact, RFC 3280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," recommends the omission of these X.509 version 2 fields.

X.509 Version 3

Released in 1996, the X.509 version 3 format introduced **extensions** to address the problems associated with matching the Issuer Unique ID with Subject Unique ID, as well as other certificate-validation issues. An X.509 version 3 certificate can contain one or more certificate extensions. (See Figure 2-3.)

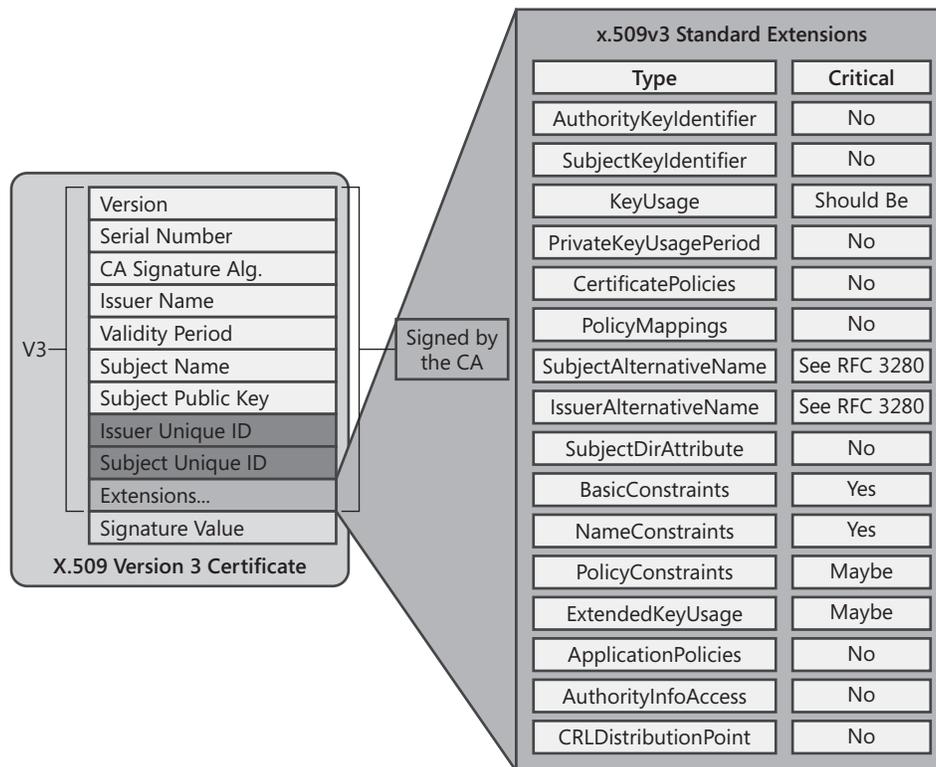


Figure 2-3 The X.509 version 3 certificate fields

Each extension in an X.509 version 3 certificate is composed of three parts:

Extension Identifier.

- An object identifier (OID) that indicates the format and definitions of the extension.

Criticality Flag.

- An indicator that identifies whether the information in an extension is important. If an application cannot recognize the critical extension, the certificate cannot be accepted or used. If the criticality flag is not set, an application can use the certificate even when the application does not recognize the extension.

Extension Value.

- The value assigned to the extension. The value varies depending on the specific extension.

In an X.509 version 3 certificate, the following certificate extensions can exist:

Authority Key Identifier.

- This extension can contain one of two values. The value can be either
- The subject of the CA and serial number of the CA certificate that issued the current certificate.
- A hash of the public key of the CA certificate that issued the current certificate.

Subject Key Identifier.

- This extension contains a hash of the current certificate's public key.

The use of the Authority Key Identifier and Subject Key Identifier in certificate chaining and validation is described in Chapter 9, "Certificate Validation."

Key Usage.

- A CA, user, computer, network device, or service can have more than one certificate. The Key Usage extension defines the security services for which a certificate can be used. The options can be used in any combination and can include the following:

Digital Signature.

- The public key can be used to verify signatures. This key is also used for client authentication and data-origin validation.

Non-Repudiation.

- The public key can be used to validate the signer's identity, preventing a signer from denying that he/she signed a package.

Key Encipherment.

- The public key can be used for key transport for processes, such as symmetric key exchange. This Key Usage value is used when an RSA key is used for key management.

Data Encipherment.

- The public key can be used to directly encrypt data, rather than exchanging a symmetric key for data encryption.

Key Agreement.

- The public key can be used for key transport for processes such as symmetric key exchange. This value is used when a Diffie-Hellman key is used for key management.

Key Cert Sign.

- The public key can be used to verify a certificate's signature.

CRL Sign.

- The public key can be used to verify a CRL's signature.

Encipher Only.

- This value is used in conjunction with the Key Agreement Key Usage extensions. The resulting symmetric key can only be used for data encryption.

Decipher Only.

- This value is used in conjunction with the Key Agreement Key Usage extensions. The resulting symmetric key can only be used for data decryption.

Private Key Usage Period.

- This extension allows a different validity period to be defined for the private key of a key pair. The Private Key Usage Period can be set to a period shorter than the certificate's validity period. This gives the private key the ability to sign documents for a shorter period (say, one year), while the public key can be used to validate the signature for the certificate's entire five-year validity period.

Certificate Policies.

- This extension describes the policies and procedures used to validate a certificate's subject before the certificate is issued. Certificate policies are represented by OIDs. Optionally, a certificate policy can include a policy qualifier, which is typically a URL that describes, in text, the policies and procedures.

Policy Mappings.

- This extension allows for policy-information translation between two organizations. For example, imagine that one organization defines a certificate policy named Management Signing, which is in certificates used for signing for large purchase orders. Another organization can have a certificate policy named Large Orders, which also is used to sign large purchase orders. Policy mapping allows the two certificate policies to be deemed equivalent.

Policy mapping typically requires that the participating organizations' legal departments inspect each certificate policy. The policies can be deemed equivalent only after the legal departments are satisfied.

Subject Alternative Name.

- This extension provides a list of alternate names for the certificate's subject. While the subject can include the subject name in an X.500 distinguished name format, the Subject Alternative Name allows for other representations, such as a User Principal Name (UPN), e-mail address, IP address, or DNS name.

Issuer Alternative Name.

- This extension provides a list of alternate names for the issuing CA. Though it is not typically implemented, the Issuer Alternative Name extension can contain the e-mail name associated with a CA.

The Subject Alternative Name and Issuer Alternative Name extensions can be either critical or noncritical. RFC 3280 defines that if the Subject field is not empty, these extensions can be marked noncritical. If the Subject field is empty, these extensions must be marked critical to allow applications to inspect the names formats.

Subject Dir Attribute.

- This extension can include any attributes from an organization's X.500 or Lightweight Directory Access Protocol (LDAP) directory. For example, the country attribute from a directory can be included in the Subject Dir Attribute extension. This extension can contain multiple attributes from the organization's directory. For each attribute, the OID and its corresponding value must be included.

Basic Constraints.

- This extension allows a certificate to designate whether the certificate is issued to a CA or to a user, computer, network device, or service. Also, the Basic Constraints extension includes a path length constraint, which limits how many subordinate CAs can exist below a specific CA's issued certificate.

Name Constraints.

- This extension allows an organization to designate which name spaces are allowed or disallowed in a CA-issued certificate. A separate name constraint must be defined for each name-space format used in certificates. For example, separate constraints are required for LDAP names versus e-mail names.

PolicyConstraints.

- This extension can be included in CA certificates. The extension can prohibit policy mapping between CAs or require that each certificate in a certificate chain includes an explicit certificate policy OID.

Enhanced Key Usage.

- This extension indicates how a certificate's public key can be used. These are beyond the general purposes defined in the Key Usage extension. For example, OIDs exist for Client Authentication (1.3.6.1.5.5.7.3.2), Server Authentication (1.3.6.1.5.5.7.3.1), and Secure E-mail (1.3.6.1.5.5.7.3.4). When a certificate is presented to an application, an application can require the presence of an EnhancedKeyUsage OID specific to that application.

Enhanced Key Usage OIDs are also used when defining qualified subordination constraints. These constraints are discussed in Chapter 13, "Creating Trust Between Organizations."

CRL Distribution Points.

- This extension contains one or more URLs where the issuing CA's base CRL is published. If revocation checking is enabled, an application will use the URL to retrieve an updated version of the CRL. URLs can use Hypertext Transfer Protocol (HTTP), File Transfer Protocol (FTP), or LDAP.

Authority Information Access.

- This extension contains one or more URLs where the issuing CA's certificate is published. An application uses the URL when building a certificate chain to retrieve the CA certificate if it does not exist in the application's certificate cache.

Inhibit Any Policy.

- This extension is included in a CA certificate to inhibit the use of the All Issuance Policies OID (2.5.29.32.0) in subordinate CA certificates. This extension prevents the All Issuance Policies OID from being considered a match to a specific certificate policy OID in a subordinate CA certificate. The value of this extension defines the number of certificates that can appear below the CA certificate before the All Issuance Policies OID is not recognized.

Freshest CRL.

- This extension contains one or more URLs where the issuing CA's delta CRL is published. The delta CRL contains only the certificates revoked since the last base CRL was published. If revocation checking is enabled, an application will use the URL to retrieve an updated version of the delta CRL. URLs can use the HTTP, LDAP, or FTP protocols.

The use of base CRLs and delta CRLs is discussed in [Chapter 9](#), "Certificate Validation."

Subject Information Access.

- This extension contains information on how to access additional details about the certificate's subject. If the certificate is a CA certificate, the information can include particulars about the certificate validation services or the CA policy. If the certificate is issued to a user, computer, network device, or service, the extension can contain information about the services offered by the certificate subject and how to access those services.

In addition to introducing the extensions listed here, the X.509 version 3 certificate's Version field changed to a value of 3 to indicate the version number.

Certification Authorities

A CA is an essential component of the Microsoft PKI solution. In a Windows Server 2003 network, a CA is a Windows Server 2003 computer with Certificate Services installed. It performs the following tasks:

Verifies the identity of a certificate requestor.

- The CA must validate the requestor's identity before it can issue a certificate. Validation can range from ensuring that the requestor has the necessary permissions

to ask for a specific type of certificate to having a certificate manager perform a face-to-face interview with the certificate requestor.

Issues certificates to requestors.

- After the requestor's identity is validated, the CA issues the requested type of certificate to the user, computer, network device, or service. The type of certificate requested determines the content of the issued certificate. For example, a Web server certificate request results in a certificate that can only be used by the Web server to setup Secure Sockets Layer (SSL) connections.

Manages certificate revocation.

- The CA publishes a CRL at regularly scheduled intervals. The CRL contains a list of serial numbers of certificates that are revoked and the reason codes for each revocation.

In an enterprise PKI, more than one CA is typically implemented. The CAs are organized into a CA hierarchy consisting of a single root CA and several other subordinate CAs, as shown in Figure 2-4.

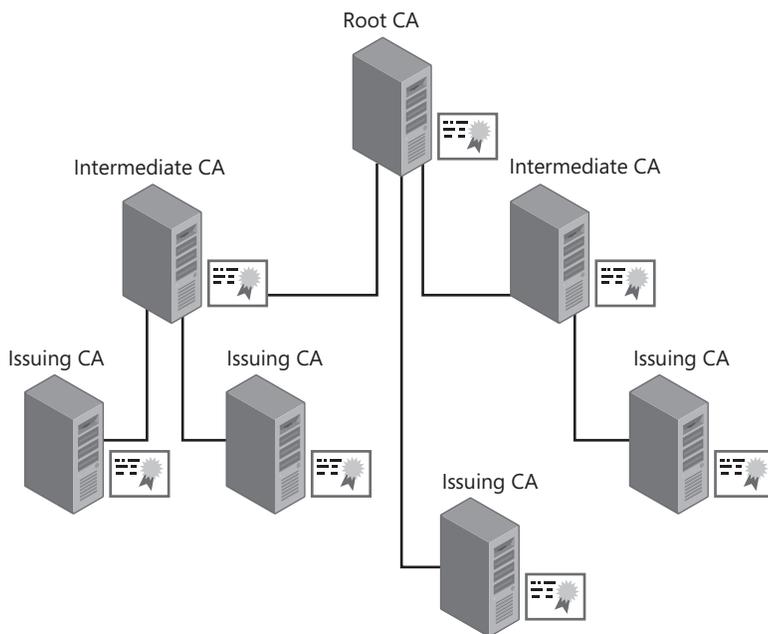


Figure 2-4 CA hierarchy roles

In Figure 2-4, the CAs are organized in a root CA hierarchy, which increases security and scalability of a CA hierarchy by allowing nonissuing CAs to be removed from the network. If the root CA and second-tier CAs in a root CA hierarchy are removed from the network, the offline CAs are protected from network-sourced attacks.

Do not assume that a root CA hierarchy always implements offline CAs. It is possible to deploy a root CA hierarchy without offline CAs, but it is not recommended because of security issues.

A root CA hierarchy allows the delegation of administration to different business units or divisions within an organization. Common-criteria role separation allows the designation of CA management roles at each CA in the hierarchy, giving different administration groups the ability to manage one CA in the CA hierarchy but not others.

The root CA hierarchy is supported by all leading commercial CA vendors, including RSA, Thawte, and VeriSign. The root CA hierarchy is also supported by most applications and network devices, allowing for interoperability with a variety of applications and network devices.

Root CA

A root CA is the topmost CA in a CA hierarchy. In a PKI, the root CA acts as the trust point for certificates issued by CAs in the hierarchy. This means that if a certificate can be traced up through the CA hierarchy to a root CA that is trusted by a user, computer, network device, or service, the certificate is considered trusted.

A root CA is special in that its certificate is self-issued. This means that the certificate's Issuer Name and Subject Name fields contain the same distinguished name. The only way to validate whether a root certificate is valid is to include the root CA certificate in a trusted root store. The trusted root store contains the actual root CA certificate to designate that the certificate is trusted.

If a self-signed certificate is not included in the trusted root store, it is considered a nontrusted root CA. If revocation checking is enabled in an application, a certificate that is chained to a nontrusted root CA is considered nontrusted.

The root CA can issue certificates to other CAs or to users, computers, network devices, or services on the network. When the root CA issues a certificate to another network entity, the root CA certificate signs the certificate with its private key to prevent content modification and to indicate that the certificate was issued by the root CA.

Typically, the root CA only issues certificates to other CAs, not to users, computers, network devices, or services on the network.

Intermediate CA

An *intermediate CA* is a CA that is subordinate to another CA and issues certificates to other CAs in the CA hierarchy. The intermediate CA can exist at any level in the CA hierarchy, except at the root CA level.

The CA that issues a certificate to another CA is often referred to as a *parent CA*. For example, a root CA that issues a certificate to an intermediate CA is referenced as the parent CA to the intermediate CA. The intermediate CA is also referred to as a *subordinate CA*, as it is directly subordinate to the parent CA in the hierarchy.

Policy CA

A special category of intermediate CA is a policy CA. A *policy CA* describes the policies and procedures an organization implements to validate certificate-holder identity and secure the CAs in the CA hierarchy. A policy CA only issues certificates to other CAs in the hierarchy. It is assumed that all CAs that are subordinate to a policy CA, whether directly subordinate or two or more levels below the policy CA, enforce the policies and procedures defined at the policy CA.

If an organization must implement multiple policies and procedures when issuing certificates, multiple policy CAs must exist in the CA hierarchy. (See Figure 2-5.)

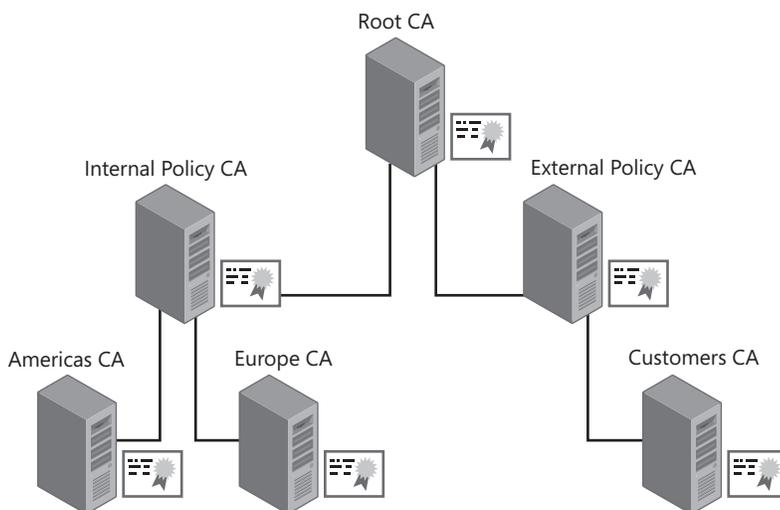


Figure 2-5 Policy CA example

In this example, two policy CAs exist in the CA hierarchy. The Internal Policy CA defines the policies and procedures used to validate the identity of certificates issued to employees. The two issuing CAs (Americas CA and Europe CA), which are directly subordinate to the Internal Policy CA, must enforce the policies and procedures defined by the Internal Policy CA.

The External Policy CA defines the policies and procedures used to validate identity and secure the process of issuing certificates to nonemployees. The Customers CA, as a subordinate CA to the External Policy CA, must enforce the policies and procedures defined by the External Policy CA.

More than one policy or procedure can be defined at a policy CA, but it is also valid to implement one policy CA for each policy or procedure applied by the organization.

Issuing CA

An issuing CA issues certificates to users, computers, network devices, or services on the network. An issuing CA is typically located on the third tier of a CA hierarchy, but it can exist on the second level, as shown in Figure 2-4.

As mentioned, an issuing CA must enforce any policies and procedures defined by a policy CA that exists between the issuing CA and the root CA in the CA hierarchy.

Certificate Revocation Lists

In some cases, a CA must revoke a certificate before the certificate's validity period expires. When a certificate is revoked, the CA includes the serial number of the certificate and the reason for the revocation in the CRL.

Types of CRLs

Windows Server 2003 supports the issuance of two types of CRLs: base CRLs and delta CRLs.

Windows Server 2003 does not support the issuance of indirect (or partitioned) CRLs.

A *base CRL* contains the serial numbers of all certificates revoked on a CA, as well as the reason for each revocation specific to a given private key used by the CA. The base CRL contains all certificates signed by a CA's specific private key. If a CA's certificate is renewed with a new key pair, a new CRL is generated that includes only revoked certificates signed with the CA's new private key.

A *delta CRL* contains only the serial numbers and revocation reasons for certificates revoked since the last base CRL was published. A delta CRL is implemented to provide more timely revocation information from a CA and to decrease the amount of data downloaded when retrieving a CRL. When a new base CRL is published, the revoked certificates in the delta CRL are rolled into the base CRL. The next delta CRL will only contain certificates revoked since the new base CRL was published.

The delta CRL is much smaller than a base CRL because only the most recent revocations are included. The base CRL, which contains all revoked certificates, can be downloaded less frequently.

If you implement delta CRLs, you must still download the base CRL. It is the combination of the base CRL and the delta CRL that provides the complete information on all revoked certificates.

Revocation Reasons

When a certificate is revoked, the CRL entry can contain further information about the revocation. The reason codes can include:

Key Compromise.

- The private key associated with the certificate has been stolen or otherwise acquired by an unauthorized person, such as when a computer is stolen or a smart card is lost.

CA Compromise.

- The private key of a CA has been compromised. This can occur when the computer running Certificate Services or the physical device that stores the CA's private key is stolen. If a CA's certificate is revoked, every certificate issued by the CA is also considered revoked because the CA that issued the certificates is no longer considered trustworthy.

Affiliation Changed.

- The subject of the certificate, typically a user, is no longer affiliated with an organization.

Superseded.

- The revoked certificate has been replaced by a new certificate. This can occur because of changes in the extensions in a certificate or the certificate's subject name changes.

Cessation Of Operation.

- The certificate's subject has been decommissioned. This can take place when a Web server is replaced by a new Web server with a new name. Likewise, this can occur when a merger takes place and the previous DNS name is decommissioned, requiring replacement of all Web server certificates.

Certificate Hold.

- A revocation where a certificate is determined to be temporarily revoked. This can occur when an employee takes a leave of absence. The Certificate Hold reason is the only revocation reason that allows a certificate to be unrevoked.

Although Certificate Hold allows a certificate to be unrevoked, use of the Certificate Hold reason code is not recommended, as it can be difficult to determine if a certificate was valid at a specific time.

Remove From CRL.

- This reason is used when a certificate is unrevoked after being revoked with the Certificate Hold reason. This revocation reason is only used in delta CRLs to indicate that a certificate revoked in the base CRL is unrevoked in the delta CRL.

Unspecified.

- If a certificate is revoked without providing a revocation reason, the unspecified reason is automatically included in the CRL.

For more information about certificate revocation reason codes, see RFC 3280.

Online Certificate Status Protocol (OCSP)

Windows Server 2008 introduces an alternative to certificate revocation lists to determine whether a certificate is revoked. Rather than a client download a base CRL or delta CRL, the client (OCSP client) sends an HTTP-based certificate status request to a server (referred to as an OCSP responder). The client determines the OCSP responder's URL by inspecting the certificate's Authority Information Access URL. If the URL contains an OCSP responder

URL and the client support OCSP, the client can proceed with sending an OCSP request to the OCSP responder.

The responder communicates with the certification authority that issued the queried certificate to determine the revocation status and returns a digitally signed response indicating the certificate's status. The OCSP responder can communicate directly with the certification authority or inspect the CRLs issued by the CA to determine the revocation status of the requested certificate.

The advantage of OCSP is that the amount of data in the request and response is a fixed size. The number of certificates actually revoked by the certification authority does not affect the size of the OCSP responder's response. Additionally, the OCSP responder typically provides more up-to-date revocation information to the OCSP client.

The biggest issue faced when deploying OCSP is scalability of the OCSP responder. High availability is a must, requiring multiple servers in a Windows Load Balancing Services (WLBS) cluster. The nodes in the cluster are often dispersed to major network hubs to allow timely responses to the OCSP clients.

OCSP Client

Windows Vista and Windows Server 2008 support the use of OCSP for certificate revocation status determination. The OCSP client meets RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP but also implements the recommendations in standards track RFC 5019 - The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments for optimization of OCSP for high-volume scenarios.

What does RFC 5019 Support Add to OCSP?

The big reason for drafting RFC 5019 was to add functionality and performance to OCSP. Some of the major differences between the full profile (RFC 2560) and RFC 5019 include:

- The Lightweight OCSP Profile supports both the Hypertext Transfer Protocol (HTTP) and Secure Hypertext Transfer Protocol (HTTPS).
- Lightweight OCSP Profile responses must specify `notBefore` and `notAfter` dates, which are not required in the full profile.
- Signed requests are not supported in the Lightweight OCSP Profile. The client cannot create a signed request; if a signed request, which can be created by third-party OCSP clients, is sent to the Online Responder an "Unauthorized" response is returned.
- With the Lightweight OCSP Profile, `nonce` is not supported in the request and ignored in the response. However, the Online Responder supports the `nonce` extension and will return a response that includes the `nonce` extension if configured to do so.

Ryan Hurst

Co-Author of RFC 5019

Online Responder Service

The Online Responder is a Microsoft Windows service (ocspvc.exe) that runs on the OCSP server with Network Service privileges. The following operations are performed by the Online Responder service:

- Manages OCSP configuration. The Online Responder service attributes that can be configured include public interfaces, access control settings, audit settings, and Web proxy cache settings. The settings are stored in the registry of the OCSP server under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\OCSPSvc\Responder.
- Retrieves and caches revocation information. The Online Responder can retrieve and cache revocation information (such as base CRLs and delta CRLs) for future responses.
- Signs OCSP responses. When the OCSP server responds to an OCSP request, the Online Responder service signs the response with a pre-defined signing key.
- Audits configuration changes. You can audit any changes to the configuration of the Online Responder. The auditing configuration meets Common Criteria requirements for auditing.

Case Study: Inspecting an X.509 Certificate

In this case study, you will examine a sample certificate and answer questions related to the fields and extensions included in the certificate.

Opening the Certificate File

Use the following procedure to open the sample certificate file on the compact disc that accompanies this book.

1. Insert the companion media in your CD-ROM drive.
2. Open Windows Explorer.
3. Open the folder CD:\Case Studies\Chapter2\
4. In the CD:\Case Studies\Chapter2 folder, double-click Samplecertificate.cer.
5. In the Certificate dialog box, click the Details tab.
6. From the resource materials for this chapter, open the Samplecertificate.cer file.

Case Study Questions

1. What version is the certificate?

The certificate is an X.509 version 3 certificate. You can verify this by viewing the Version field on the Details tab.

2. What is the name of the issuing CA?

The name of the issuing CA is CN=adatumCA,DC=adatum,DC=msft. You can verify this by viewing the Issuer field on the Details tab.

3. What is the subject name of the certificate?
The subject name of the certificate is CN = SCUser1, OU = Module09. OU = Labs, DC = adatum, DC = msft. You can verify this by viewing the Issuer field on the Details tab.
4. Are any other names included in the certificate for the subject?
The Subject Alternative Name extension contains an additional name for the subject. The name is a user principal name, SCUser1@ADATUM.msft.
5. What is the length of the public key associated with the certificate?
The public key length is 1024 bits. You can verify this by viewing the Public Key field on the Details tab.
6. What other X.509 extensions are included in the sample certificate?
On the Details tab, the following X.509 version 3 extensions are included: Key Usage, Application Policies, Certificate Policies, Enhanced Key Usage, Subject Key Identifier, Authority Key Identifier, CRL Distribution Points, Authority Information Access, and Subject Alternative Name.
7. What extensions must you inspect to determine what forms of revocation checking are supported by the CA that issued the X.509 certificate?
You must inspect both the Authority Information Access and CRL Distribution Point extensions to determine what forms of revocation checking are supported by the CA that issued the X.509 certificate. If the CA supports OCSP, the URL of the OCSP Responder is included in the Authority Information Access extension. If the CA supports CRLs, the URLs for CRL Distribution Points are included in the CRL Distribution Point extension.
8. What forms of revocation checking are supported by the CA that issued the X.509 certificate?
The CA only supports CRLs. The Authority Information Access extension does not contain any URLs referencing an OCSP responder.
9. Where is the CRL published when revocation checking is performed against the certificate?
**On the Details tab, two URLs are included in the CRL Distribution Points extension indicating where the CRL is published:
ldap://CN=adatumCA,CN=VANCOUVER,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=adatum,DC=msft?certificateRevocationList?base?objectClass=cRLDistributionPoint and
*http://vancouver.adatum.msft/CertEnroll/adatumCA.crl.***

Additional Information

- Microsoft Official Curriculum, course 2821: “Designing and Managing a Windows® Public Key Infrastructure” (www.microsoft.com/traincert/syllabi/2821afinal.asp)
- RFC 3280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (<http://www.faqs.org/rfcs/rfc3280.html>)
- RFC 2560 - X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP (<http://www.faqs.org/rfcs/rfc2560.html>)
- RFC 5019 - The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments (<http://tools.ietf.org/html/rfc5019>)

Chapter 3

Policies and Public Key Infrastructure (PKI)

How a PKI Affects Policy Design

A PKI is only as secure as the policies and procedures that are implemented by an organization in conjunction with its PKI. Three policy documents directly affect the design of an organization's PKI:

Security policy.

- A security policy is a document that defines an organization's standards in regard to security. The policy usually includes the assets an organization considers valuable, potential threats to those assets, and, in general terms, measures that must be taken to protect these resources.

Certificate policy.

- A certificate policy is a document that describes the measures an organization will use to validate the identity of a certificate's subject. Validation might require a requestor-provided account and password combination submitted to the organization's directory or photo identification and submission to a background check through a registration authority (RA) process.

Certificate practice statement (CPS).

- A CPS is a public document that describes how a certification authority (CA) is managed by an organization to uphold its security and certificate policies. A CPS is published at a CA and describes the operation of the CA.

Security policies, certificate policies, and CPSs are typically created by members of an organization's legal, human resources, and information technology (IT) departments. The PKI design must enforce these policies.

Certificate policies and CPSs are used by other organizations to determine how well they trust certificates issued by an organization's CA hierarchy. You trust a certificate from another organization when you allow that certificate to be used on your network for signing or encryption purposes. Deploying a PKI without implementing certificate policies and CPSs can result in a PKI that causes your organization to be deemed untrustworthy by other organizations.

A dependency exists between the security policy, certificate policy, and CPS in a PKI, as shown in Figure 3-1.

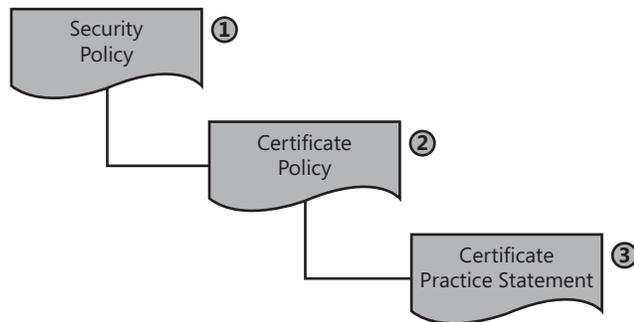


Figure 3-1 The dependency between the security policy, certificate policy, and certificate practice statement (CPS)

An organization must first develop a security policy, which defines the organization's security standards. Next, a certificate policy is drafted to enforce and reflect the organization's security policy. Finally, the CPS defines the CA's management procedures that enforce the certificate policy.

Security policies, certificate policies, and CPSs are typically legal documents that must be reviewed by an organization's legal department or legal representatives before publication to ensure that the documents are enforceable and do not misrepresent the organization's intent.

Security Policy

The design of a PKI starts with an inspection of the organization's security policy. A PKI designer uses a security policy to answer the following questions:

What data should be secured with certificates?

- Not all applications support certificate-based security. Typically, a security policy defines classes of data within the organization and measures that must be taken to protect that data when stored and when transmitted across a network. With a PKI in place, these measures can include the use of protocols such as Secure Sockets Layer (SSL) or Internet Protocol Security (IPSec) to protect transmitted data and Encrypting File System (EFS) to protect stored data.

What measures must be taken to protect the private keys associated with a certificate?

- Measures can include storing the certificate on a smart card, protecting a CA's private key by implementing hardware security modules (HSMs), or preventing the export of a certificate's private key.

What measures must be taken to validate the identity of a certificate requestor?

- Whoever has access to a certificate's private key is considered to be the person identified in the certificate's subject. An organization might want to use certificates for applications that require higher trust. For example, background checks can be required prior to issuance of a certificate used to digitally sign for high-value purchases.

Defining Effective Security Policies

A security policy defines an organization's security standards. An organization typically has several security policy documents that provide comprehensive definitions of security issues, the risks and threats faced by the organization, and the measures that must be taken to protect the organization's data and assets.

An organization must do more than just define security policies. It must ensure that it deploys security solutions to enforce the security policies and it must ensure that employees are aware of those security policies and their roles and responsibilities in maintaining security.

Once an organization defines its security policies, an initial assessment must be performed to identify measures that enforce those policies. Once these measures are identified, a *gap analysis* determines whether additional measures should be implemented to meet the defined security policies. After proper planning, the security policy implementation process can begin.

An organization should periodically review its security policies and the measures taken to enforce them to determine if modifications are necessary. Modifications might involve updating security policies or revising the processes and procedures that enforce them.

Resources for Developing Security Policies

Two of the most commonly used resources for defining a security policy are ISO 17799/BS 7799, "Code of Practice for Information Security Management," and RFC 2196, "The Site Security Handbook."

ISO 17799 is an International Organization for Standardization document that is based on the British Standards 7799 document.

ISO 17779, available for purchase at <https://www.bspsl.com/secure/iso17799software/cvm.cfm>, provides detailed information and recommendations for developing enforceable security policies. Several Web sites provide security policy samples based on the intent and recommendations of ISO 17799.

RFC 2196, "Site Security Handbook," available at www.ietf.org/rfc/rfc2196.txt, is another guide for developing security policies. Although directed more toward computer security policies, the RFC describes several types of resources that should be covered in an overall security policy, as well as recommendations for securing those resources.

Affects of External Policies on your PKI

As more and more organizations consider using certificates to authenticate, sign, or encrypt communications between their organization and other organizations, external policies are starting to influence your PKI design. To allow exchange and trust of certificates between your organization and a partner organization, you may need to meet the security policies defined in these common standards:

Qualified Certificates

- A **Qualified Certificate** (see RFC 3739 - Internet X.509 Public Key Infrastructure Qualified Certificates Profile) refers to a certificate issued in Europe that is defined to meet the requirements for the European Directive on Electronic Signature, The primary purpose of a qualified certificate is to identify a person with a high level of assurance.

A qualified certificate can optionally include biometric information, such as the digital image of the subject's written signature or a digital picture of the subject, to further validate the identity of the certificate subject.

Sarbanes Oxley

- The Sarbanes-Oxley Act of 2002 , often referred to SOX, is a United States federal law that establishes reporting and operations standards for all US public companies or public companies that do business in the US. The Act also covers issues such as auditor independence, corporate governance, internal control assessment, and enhanced financial disclosure. The act affects PKI deployments and policies regarding change control and auditing requirements and log maintenance. Likewise, PKI can assist an organization with SOX compliance by supporting initiatives for strong authentication, data encryption, and digital signing.

FIPS 201 - Personal Identity Verification (PIV) of Federal Employees and Contractors

- FIPS 201 is a standard developed by NIST to meet the deadlines set by US president George W. Bush in Homeland Security Presidential Directive 12 (HSPD-12). The standard defines a standard for electronic identification for federal employees and contractors for both physical and logical access control.

The standard is made up of two major sections.

- Part one describes the minimum requirements for a Federal personal identity verification system. The requirements include recommendations for personal identity proofing, registration, and issuance.
- Part two provides detailed specifications on storing, processing, and retrieving identity credentials from a two-factor device to allow interoperability between different devices.

Federal Bridge CA

- The US government has established a bridge CA to allow organizations participating in the Federal Bridge to accept certificate issued to other participating organizations in the Federal Bridge. The bridge CA acts as a hub between the relying parties allowing them to trust certificates issued to all participants in the bridge.

To participate in the bridge, an organization must meet the Federal Bridge CA's certificate policy. To allow flexibility, the original FBCA has evolved to the Federal Public Key INfrastrucutre Architecture (FBKIA) that supports multiple policies and functions. The policies supported by the FPKIA include the FBCA, the Federal PKI Common Policy Framework (FCFP) CA, and the Citizen and Commerce Class Common (C4) CA.

Details on the Federal Bridge CA can be found at <http://www.cio.gov/fbca/>.

Certipath

- Certipath is another implementation of a bridge CA in the United State. The difference between Certipath and FBCA is the scope of the bridge. Participants in the Certipath bridge are aerospace and defense industry companies such as Lockheed Martin, Northrop Grumman, and Boeing. In addition to providing trust between other Certipath bridge members, Certipath is also cross-certified with FBCA. This cross-certification allows all Certipath members to interoperate with all FBCA participants in certificate-based applications.

Bridge CAs for Business to Business (B2B) Trust

As the co-author of the Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003whitepaper for Microsoft (<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.mspx>), it is exciting to see theory come to life.

When David Cross and I drafted the white paper, we were putting on our visionary hats, discussing a future method of providing certificate trust between organizations. In the ensuing years, Certipath and FBCA are now in operation and allowing bridge trust between organizations.

The biggest impact that I am seeing at customers is the certificate policy requirements for the bridge CAs. In some cases, organizations have been forced to establish dedicated CA hierarchies to cross-certify with a bridge CA. Unfortunately, the main reason is that their current CA hierarchy would not pass compliance requirements for the bridge they wish to participate in.

The best advice I can give is that if you see the possibility of participating in the Federal Bridge or another industry bridge, be sure to review the Federal Bridge certificate policy (available at http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf) and ensure that your PKI design meets these certificate policy requirements.

Brian Komar

Co-Author of the cross-certification white paper

Defining PKI-Related Security Policies

Using ISO 17799 as a guide for developing security policies, you should consider updating or creating security policies for the following areas:

Organizational security.

- Establish enforceable security policies for an organization. ISO 17799 is especially helpful when an organization does not have security policies in place prior to starting a PKI design.

Organizational security infrastructure.

- Ensure the existence of security policies that recommend the implementation of a single organization-wide PKI. An organizational PKI is easier to manage than several project-based CAs. For example, an organization should not deploy separate CA implementations for a virtual private network (VPN), Secure/Multipurpose Internet

Mail Extensions (S/MIME), and wireless projects. An enterprise PKI that provides certificates for all applications and services is preferred.

Asset classification and control.

- Identify classes of assets that require public key encryption, digital signing, or other PKI-related technologies to ensure security. PKI-related security can be applied to both data storage and transmission.

Personnel security.

- Include job descriptions and requirements for members of the PKI administration team in security policies. Requirements can include mandatory background checks for all administrators, tasks and procedures that must be followed, and any agreements or policies that administrators must sign when accepting their positions.

Physical and environmental security.

- Ensure that the security policy includes requirements for physical security measures to protect CAs and their deployment in a PKI. Different security measures can be required for offline versus online CAs.

Communications and operations management.

- Define managerial and operational roles for your PKI. These can include CA administrators, certificate managers, backup operators, auditors, certificate template designers, and key recovery agents.

Access control.

- Define what measures will be taken to secure access to a CA. These measures might include manually approving Web-based enrollment requests or placing the physical CA in a server room with keycard access. Access control can dictate what forms of authentication are required to access data. For example, some asset classifications can require two-factor authentication (something you have and something you know) before access is permitted.

Change control process.

- Establish what measures will be taken to maintain and modify a PKI after deployment.

Business continuity management.

- Define measures that will ensure recovery of the PKI in the event of a disaster. These measures should include actions to be taken in advance of a catastrophe so that a CA can be recovered, what information must be documented about the CA configuration, and who will perform the recovery.

Compliance.

- Provide recommendations to ensure that the implemented PKI enforces security policies that affect it. Nonconformance with security policies can devalue a PKI-issued certificate to the point that all certificates must be revoked and reissued to ensure compliance and trust of other organizations.

Certificate Policy

A certificate policy describes the measures taken to validate a certificate's subject prior to certificate issuance. For many organizations, it is the certificate-issuance policy that determines whether the presented certificate will be trusted.

For example, an organization is more likely to trust a certificate issued after a requestor presents photo identification than a certificate issued based on a user knowing an account and password combination.

Contents of a Certificate Policy

A certificate policy should include the following information:

How the user's identity is validated during certificate enrollment.

- Is identity provided by an account and password combination or must requestors present themselves for face-to-face interviews? If interviews are required, what forms of identification must requestors present for validation?

The certificate's intended purpose.

- Is the certificate used for authentication on the network or for signing purchase orders? If the certificate is used for signing purchase orders, is there a maximum value allowed? These questions should be addressed in the certificate policy.

The type of device upon which the certificate's private key is stored.

- Is the private key stored on the computer's local disk in the user's profile or is the private key stored on a hardware device such as a smart card? Other measures such as implementing strong private key protection or requiring a password to access the private key can be described in this information.

The subject's responsibility for the private key associated with the certificate in the event that the private key is compromised or lost.

- Is the user responsible for any actions performed using the acquired private key if the private key is compromised or a backup of the private key is lost? This decision can lead to preventing the archival or export of the private key associated with the certificate.

Revocation policies, procedures, and responsibilities.

- Under what circumstances will your organization revoke an issued certificate before its validity period expires? This decision will determine what actions or events will lead to the revocation of a certificate, how the revocation process is initiated, and who performs the actual revocation procedure.

Certificate Policy Example

An excellent example of certificate policy is the X.509 Certificate Policy for the United States Department of Defense (DoD), available at <http://iase.disa.mil/pki/dod-cp-v90-final-9-feb-05-signed.pdf>

The DoD defines five classes of certificates in its certificate policy document. The distinction between the various classes is based on the following variables:

- The measures taken to validate the subject's identity
- The value of transactions allowed for a certificate class
- The type of storage required for the private key material

A combination of these three variables leads to the following certificate classes:

DoD Class 2.

- Users prove identity by providing a user name and password for an account in the organization's authoritative directory. Once a valid user name and password are provided, a certificate is issued. The certificate is typically stored on the hard drive of the computer where the certificate request is generated. A DoD Class 2 certificate can be used for:
 - Digital signatures for administrative data or day-to-day work on any network.
 - Key exchange for high-value data on an encrypted network or confidentiality of low-value information on nonencrypted networks.

DoD Class 3.

- Users prove identity by providing at least one piece of official federal government photo identification or two credentials issued by other entities, with one of the documents being photo ID (such as a driver's license). The private key associated with the certificate is still stored on the user's hard disk, but the increased subject validation allows the private key to be used for medium-value transactions on a public network.

DoD Class 3 Hardware.

- A DoD Class 3 Hardware certificate uses the same subject validation process as a DoD Class 3 certificate. The difference is that the private key material and certificate are exported from the user's hard disk to a hardware token, such as a USB token. The movement of the private key to a hardware device increases the security of the private key.

Once the private key is successfully transferred to a hardware device, the private key should be deleted from the computer's hard drive to prevent unauthorized access.

DoD Class 4.

- A DoD Class 4 certificate requires presentation of the same photo identification as the DoD Class 3 and DoD Class 3 Hardware certificates. The difference is that the private key pair is not generated on the local hard disk but on a hardware two-factor device, such as a smart card. The increased security of the key pair associated with the certificate results in the certificate being valid for high-value transactions on public networks.

DoD Class 5.

- Currently, there is no PKI that meets the subject-identification requirements for a DoD Class 5 certificate. In the future, a DoD Class 5 certificate will require biometric validation of the certificate's subject. This can include retinal scans, fingerprint matches, or even DNA matching. A DoD Class 5 certificate can be used to secure classified materials on public networks. .

The DoD classifications do not assign actual values to low-value, medium-value or high-value transactions. Rather than providing predetermined values that can become dated, general terms are used to allow value modification without requiring certificate policy modification

Comparing Certificate Policies

Sometimes it is valuable to compare different available certificate policies when you are developing the certificate policies for your organization. As mentioned earlier in this chapter, the US Federal Bridge CA also defines a certificate policy.

When you compare the policies to the DOD certificate policies, you can see a definite similarity between the assurance levels.

The Federal Bridge defines a Rudimentary assurance level that relies on the subscriber providing an email address to receive a certificate. This is very close to the DOD Class 1 definition.

Likewise, the FBCA Low, Medium, and High Assurance levels map pretty much 1-to-1 with the DOD Class 2, DOD Class 3, and DOD Class 4 definitions. This really should not come as a surprise though. The DOD is one of the organizations participating in the Federal Bridge!

Brian Komar

Co-Author of the cross-certification white paper

Certification Practice Statement (CPS)

A CPS defines the measures taken to secure CA operations and the management of CA-issued certificates. You can consider a CPS to be an agreement between the organization managing the CA and the people relying on the certificates issued by the CA.

By reviewing a CA's CPS—a public document that should be readily available to all participants on the Internet—a relying party can determine whether the certificates issued by that CA meet its security requirements. The CPS contains the following information:

- How the CA will enforce the measures necessary to validate the certificate's subject, as required by the certificate policy.
- The liability of the organization in the event that an act of fraud is performed against the service protected by the certificate and the fault is found to be associated with the certificate.
- The circumstances under which a certificate can be revoked before its expiration.

When a certificate is issued by a CA that follows a CPS, the CA's certificate (or that of its parent CA) includes a URL pointer to the CPS. In the CA's certificate, the CPS is viewed by clicking the Issuer Statement button on the General tab of the certificate, as shown in Figure 3-2.



Figure 3-2 A CA certificate that references a CPS

When a CPS is included in a CA certificate, it is applicable to that CA and all subordinate CAs in the CA hierarchy. This means that the practices defined in the CPS must be implemented by that CA and all subordinate CAs.

RFC 3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," available at www.ietf.org/rfc/rfc3647.txt, recommends a standard CPS format to ensure compatibility between organizations and promote a stronger degree of trust of an organization's CPS by other companies. The RFC recommends the following nine sections:

- Introduction
- Publication and Repository Responsibilities
- Identification and Authentication (I&A)
- Certificate Life-Cycle Operational Requirements
- Facility, Management, and Operational Controls
- Technical Security Controls
- Certificate, CRL, and OCSP Profiles
- Compliance Audit and Other Assessment
- Other Business and Legal Matters

RFC 3647 recommends that the same format be used for both certificate policies and CPSs. The X.509 certificate policies for both the United States Department of Defense and the US Federal Bridge implement the nine sections discussed here. Differences between the certificate policy and the CPS are mainly related to the documents' focus. A certificate policy focuses on subject validation and is often compared between organizations to find similar policies, whereas a CPS describes the operations of the CA to enforce the implemented certificate policies.

CPS Section: Introduction

The introduction of a CPS provides an overview of the CA, as well as the types of users, computers, network devices, or services that will receive certificates. The introduction also includes information on certificate usage. This includes what types of applications can consume certificates issued under the CP or CPS and what types of applications are explicitly prohibited from consuming the CA's certificates. Should another organization have any questions regarding the information published in the CPS, the introduction also provides contact information.

CPS Section: Publication and Repository Responsibilities

The publication and repository responsibilities section contains details regarding who operates the components of the public key infrastructure. This section also includes describes the responsibilities for publishing the CP/CPS, whether the CP/CPS will be publicly available, whether portions of the CP or CPS will remain private, and descriptions of access controls on published information. The published information includes CPs, CPSs, certificates, certificate status information, and CRLs.

CPS Section: Identification and Authentication

This section describes the name formats assigned used in certificates issued by the CA. The section will also define whether the names must be unique, meaningful, allow nicknames, and so on. The section's main focus is on the measures taken to validate a requestor's identity prior to certificate issuance. The section describes the certificate policy and assurance levels implemented at the CA and detail identification procedures for:

Initial registration for a certificate.

- The measures taken to validate the identity of the certificate requestor.

Renewal of a certificate.

- Are the measures used for initial registration repeated when a certificate is renewed? In some cases, possession of an existing certificate and private key is sufficient proof of identity to receive a new certificate at renewal time.

Requests for revocation.

- When a certificate must be revoked, what measures will be taken to ensure that the requestor is authorized to request revocation of a certificate?

A CA can implement more than one assurance levels, as long as the CA's procedures and operations allow enforcement of each assurance level. To implement multiple assurance levels within a certificate policy, separate subsections can be defined, one for each assurance level.

CPS Section: Certificate Life-Cycle Operational Requirements

This section defines the operating procedures for CA management, issuance of certificates, and management of issued certificates. It is detailed in the description of the management tasks. Operating procedures described in this section can include the following:

Certificate application.

- The application process for each certificate policy supported by a CA should be described. Applications can range from the use of autoenrollment to distribute certificates automatically to users or computers, to a detailed procedure that pends certificate requests until the requestor's identity is proven through ID inspection and background checks.

Certificate application processing

- Once the application is received by the registration authorities, the application must be processed. This section describes what must be done to ensure that the subscriber is who they say they are. The section can include what forms of identification must be performed, whether background checks are required, and whether there are time limits set on processing the application. The section may include recommendations on when to approve or deny a request.

Certificate issuance.

- Once the identity of a certificate requestor is validated, what is the procedure to issue the certificate? The process can range from simply issuing the certificate in the CA console to recording the certificate requestor's submitted identification in a separate database maintained by an RA.

Certificate acceptance.

- When a certificate is issued to a computer or user, what procedures must be performed to install the certificate on the user's computer or a certificate-bearing device, such as a smart card?

Key pair and certificate usage.

- Once a certificate is issued, the parties involved in the usage of the certificate must understand when and how the certificate may be used. The section describes responsibilities for the certificate subscriber and relying parties when the certificate is used.

Certificate Renewal.

- When a certificate reaches its end of lifetime, the certificate can be renewed with a the same key pair. The section provides details on when you can renew with the same key pair, who can initiate the request, what measures must be taken to verify the subscriber's identity (these are typically less stringent than initial enrollment).

Certificate Re-key.

- Alternatively, when a certificate reaches its end of lifetime, the certificate can be renewed with a new key pair. The section provides details on when you must renew with a new key pair, who can initiate the request, what measures must be taken to verify the subscriber's identity (these are typically the same as initial enrollment).

Setting a schedule for renewal and rekey is an important task in this section. For example, some defence contractors only allow renewal for a period of seven years for medium assurance or DOD Class 3 certificates. The subscriber's identity during renewal is validated by the subscriber signing the request with their previous certificate (since the subscriber is the holder of the private key). In the seventh year, the subscriber must re-key and undergo the vetting process to re-establish their identity.

Certificate modification.

- Sometimes, a certificate must be re-issued due to the subscriber's name change or change in administrative role. This section describes *when* you can modify a certificate and how the registration process proceeds for the modification of the certificate.

Technically, it is not a modification. You cannot modify a certificate as it is a signed object. Think of it more as a replacement of a certificate.

Certificate revocation and suspension.

- Under which circumstances will the issuing party revoke or suspend an issued certificate? This section should detail the obligations of the certificate holder, as well as actions that can lead to certificate revocation. The section also includes information on what revocation mechanism are supported by the CA. If CRLs are used, the section describes the publication schedule for the CRLs. If online revocation and status checking is implemented, the URL of the web site hosting the web site is provided.

Certificate status services.

- If the CA implements certificate status checking services, this section provide operational characteristics of the service and the availability of the services.

End of subscription.

- If a subscriber wishes to terminate their subscription, this section provides details on how the certificate is revoked. There may be multiple recommendations in this section detailing the different reason that may require a subscriber to end their subscription. For example, an organization may choose to process the revocation request differently if an employee is terminated versus an employee that retires.

Key escrow and recovery.

- If the CA provides private key escrow services for encryption certificate, this section describes the policies and practices governing the key archival and recovery procedures. The section will typically reference other policies and standards defined by the organization.

CPS Section: Management, Operational, and Physical Controls

This section describes physical, procedural, and personnel controls implemented at the CA for key generation, subject authentication, certificate issuance, certificate revocation, audit, and archival. These controls can range from limiting which personnel can physically access the CA to ensuring that an employee is assigned only a single PKI management role. For a relying party, these controls are critical in the decision to trust certificates

because poor procedures can result in a PKI that is more easily compromised without the issuing organization recognizing the compromise.

This section also provides details on other controls implemented in the management of the PKI. These include:

Security audit procedures.

- What actions are audited at the CA and what managerial roles are capable of reviewing the audit logs for the CA?

Records archival.

- What information is archived by the CA? This can include configuration information, as well as information about encryption private keys archived in the CA database. This section should detail the process necessary to recover private key material. For example, if the roles of certificate manager and key recovery agent are separated, a description of the roles and responsibilities of each role should be provided so the certificate holder is aware that a single person cannot perform private key recovery.

Key changeover.

- What is the lifetime of the CA's certificate and how often is it renewed? This section should detail information about the certificate and its associated key pair. For example, is the key pair changed every time the CA's certificate is renewed, or only when the original validity period of the CA certificate elapses?

Compromise and disaster recovery.

- What measures are taken to protect the CA from compromise? Likewise, if a CA fails, what measures are in place to ensure a quick recovery of the CA and its CA database?

CA or RA termination.

- What actions are taken when the CA or registration authority is removed from the network? This section can include information about the CA's expected lifetime.

CPS Section: Technical Security Controls

This section defines the security measures taken by the CA to protect its cryptographic keys and activation data. For example, is the key pair for the CA stored on the local machine profile on a two-factor device, such as a smart card, or on a FIPS 140-2 Level 2 or Level 3 hardware device, such as a hardware security module (HSM)? When a decision is made to trust another organization's certificates, the critical factor is often the security provided for the CA's private key.

This section can also include technical security control information regarding key generation, user validation, certificate revocation, archival of encryption private keys, and auditing.

The technical security control section should only provide high-level information to the reader and not serve as a guide to an attacker regarding potential weaknesses in the CA's configuration. For example, is it safe to disclose that the CA's key pair is stored on a FIPS 140-2 Level 2 or Level 3 HSM? It is not safe to describe the CA's management team members or provide specific vendor information about the HSM.

CPS Section: Certificate Certificate Revocation List (CRL), and OCSP Profiles

This section is used to specify three types of information:

Information about the types of certificates issued by the CA.

- For example, are CA-issued certificates for user authentication, EFS, or code signing?

Information about CRL contents.

- This section should provide about the version numbers supported for CRLs and what extensions are populated in the CRL objects.

OCSP Profile

- This section should provide information on what versions of OCSP are used (for example, what RFCs are supported by the OCSP implementation), and what OCSP extensions are populated in issued certificates.

CPS Section: Compliance Audit and Other Assessment

This section is relevant if the CP or CPS is used by a CA that issues certificates that are consumed by entities outside of your organization. The section details what is checked during a compliance audit, how often the compliance audit must be performed, who will perform the audit (is the audit performed by internal audit or by a third-party), what actions must be taken if the CA fails the audit, and who is allowed to inspect the final audit report.

CPS Section: Other Business and Legal Matters

This section specifies general business and legal matters regarding the CP and CPS. The business matters include fees for services and the financial responsibilities of the participants in the PKI. The section also details legal matters such as privacy of personal information recorded by the PKI, intellectual property rights, warranties, disclaimers, limitations on liabilities, and indemnities.

Finally, the section describes the practices for maintenance of the CPS. For example, what circumstances drive the modification of the CPS? If the CPS is modified, who approves the recommended changes? In addition, this section should specify how the modified CPS's contents are published and how the public is notified that the contents are modified.

In some cases, the actual modifications are slight, such as a recommended rewording by an organization's legal department. In these cases, the URL referencing the CPS need not be changed, just the wording of the documents referenced by the URL.

So What if my Current CP/CPS is based on RFC 2527

Many of your organizations may have a CP or CPS based on RFC 2527 (the predecessor to RFC 3647), there is no immediate need to rewrite the CP or CPS to match the section names in RFC 3647. On the other hand, if you are in the process of drafting your CP or CPS now, I do recommend that you write based on the section names in RFC 3647.

Either way, RFC 3647 does provide a great cheat sheet for you as you start your copy and paste adventure. Section 7 "Comparison to RFC 2527" provides a detailed table that shows the mappings between sections in RFC 2527 and RFC 3647. For example, in RFC 2527, Compliance Auditing is described in section 2.7 and its subsections. In RFC 3647, the same subsections exist, but are now recorded in section 8. The table below summarizes the remapping of the sections regarding Compliance Auditing.

Section Title	RFC 2527 Section	RFC 3647 Section
Compliance Audit	2.7	8.
Frequency of Entity Compliance Audit	2.7.1	8.1
Identity/Qualifications of Auditor	2.7.2	8.2
Auditor's Relationship to Audited Party	2.7.3	8.3
Topics Covered by Audit	2.7.4	8.4
Actions Taken as a Result of Deficiency	2.7.5	8.5
Communication of Results	2.7.6	8.6

Brian Komar

Amateur CP/CPS Author

Case Study: Planning Policy Documents

You are the head of security for Fabrikam Inc., a large manufacturing company. Your IT department has several PKI-related initiatives planned for the next 18 months, and you are responsible for the drafting of all related policy documents.

Design Requirements

One of the applications planned by the IT department is the deployment of smart cards for both local and VPN authentication by all employees. During research for the smart card deployment, the IT department gathered the following information that will affect the policies you draft:

- Each employee will be issued a smart card on his or her first day with Fabrikam Inc.
- Existing employees will receive their smart cards on an office-by-office basis. Members of the IT department will travel to each major regional office and deliver the smart cards to all employees in that region.
- Fabrikam has a high employee turnover. In any given month, as many as 1,000 employees leave Fabrikam and are replaced with roughly 1,200 new employees.

Case Study Questions

1. What is the relationship between a CPS, certificate policy, and security policy?

A security policy defines an organization's security standards. The contents of an organization's security policy provides the input to the definition of a certificate policy. The certificate policy defines how a PKI will enforce the organization's security policies. Finally, the certificate practice statement defines the operating rules for the PKI in the enforcement of any defined certificate policies.

2. In what document would you define the methods used to identify the new hires when they start with Fabrikam?

The methods of identifying the subject of a certificate are defined in a certificate policy. The certificate policy will define the exact measures, such as different types of ID, required to validate the subject's identity before issuing a certificate.

3. Will the identification validation requirements for existing employees differ from those implemented for new employees of Fabrikam?

Not necessarily. The answer depends on what measures are taken by the organization to identify employees when they are originally hired by the company. For example, if similar measures were taken before providing employees with photo ID cards, the employees could just show their existing employee card as an equivalent form of identification, rather than show all the identification required for new employees.

4. The high turnover of employees must be addressed in the CPS. Specifically, what sections must be updated to define the measures taken when an employee is terminated or resigns from Fabrikam?

The sections of the CPS that define the revocation policies of the organization are "Identification and Authentication," which is where you define how requests for revocation are submitted to a revocation authority, and "Certificate Life-Cycle Operational Requirements," which is where you define the circumstances under which a certificate is revoked (such as termination or resignation). Although tempting, the "Certificate, CRL and OCSP Profiles" section is related to the format of CRLs, not the actual revocation of certificates.

5. You are considering modeling your certificate policies after the United States Federal Bridge certificate policy. What certificate class would best match your deployment of smart cards?

The Federal Bridge High Assurance certificate. The Federal Bridge High Assurance certificate describes certificates stored on two-factor authentication devices, such as smart cards.

Additional Information

- Microsoft Official Curriculum, course 2821: "Designing and Managing a Windows Public Key Infrastructure" (www.microsoft.com/traincert/syllabi/2821afinal.asp)
- ISO 17799 - Code of Practice for Information Security Management (<http://www.bspl.com/secure/iso17799software/cvm.cfm>)
- RFC 2196 - The Site Security Handbook (www.ietf.org/rfc/rfc2196.txt)
- X.509 Certificate Policy for the United States Department of Defense (DoD) (<http://iase.disa.mil/pki/dod-cp-v90-final-9-feb-05-signed.pdf>)
- RFC 2527 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (www.ietf.org/rfc/rfc2527.txt)
- RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (www.ietf.org/rfc/rfc3647.txt)
- The Information Security Policies / Computer Security Policies Directory (<http://www.information-security-policies-and-standards.com>)
- Homeland Security Presidential Directive (HSPD)- 12 (<http://csrc.nist.gov/policies/Presidential-Directive-Hspd-12.html>)
- Federal Bridge CA Certificate Policy (http://www.cio.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf)
- "Planning and Implementing Cross-Certification and Qualified Subordination Using Windows Server 2003" (<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/security/ws03qswp.msp>)
- Certipath (<http://www.certipath.com/>)
- FIPS-201 - Personal Identity Verification (PIV) of Federal Employees and Contractors (<http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf>)
- RFC 3739 - Internet X.509 Public Key Infrastructure Qualified Certificates Profile (www.ietf.org/rfc/rfc3739.txt)