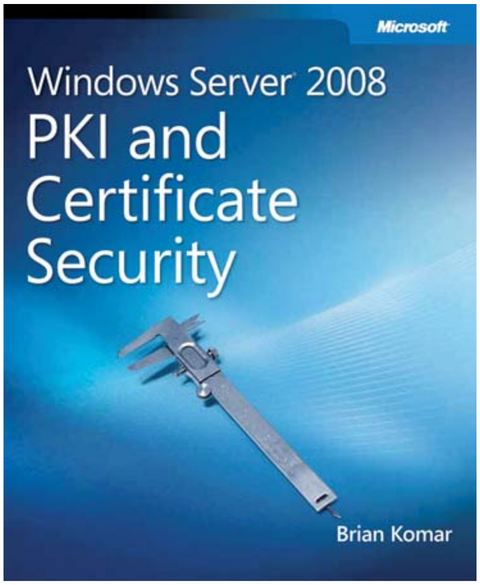


Windows Server® 2008 PKI and Certificate Security

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

Table of Contents

3 Policies and PKI

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 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.

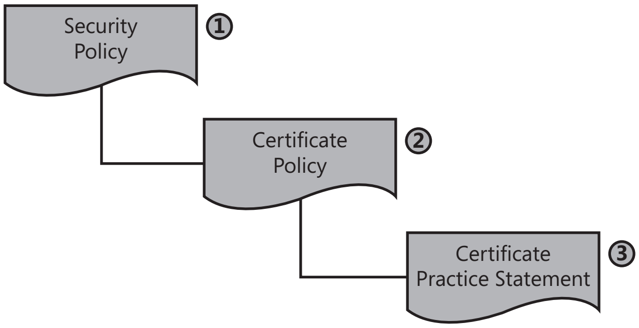


Figure 3-1 The dependency between the security policy, certificate policy, and certificate practice statement (CPS)

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 includemanually 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

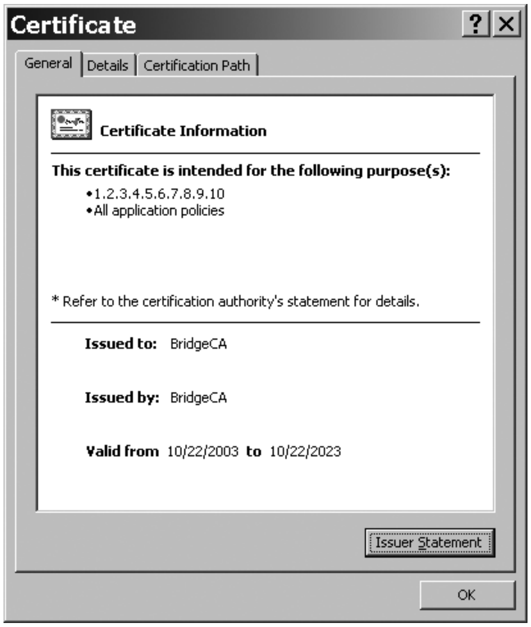
Certification Practice Statement (CPS)

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.



Certificate Information

This certificate is intended for the following purpose(s):

- 1.2.3.4.5.6.7.8.9.10
- All application policies

* Refer to the certification authority's statement for details.

Issued to: BridgeCA

Issued by: BridgeCA

Valid from 10/22/2003 **to** 10/22/2023

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 authorites, 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 includes what forms of identification must be performed, whether back ground 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 strigent 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. The 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 typical 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 (*https://www.bspsl.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.mspx)
- 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*)