

Chapter 3

Policies and PKI

A public key infrastructure (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 PKI design:

- **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.



Warning 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. (See Figure 3-1.)

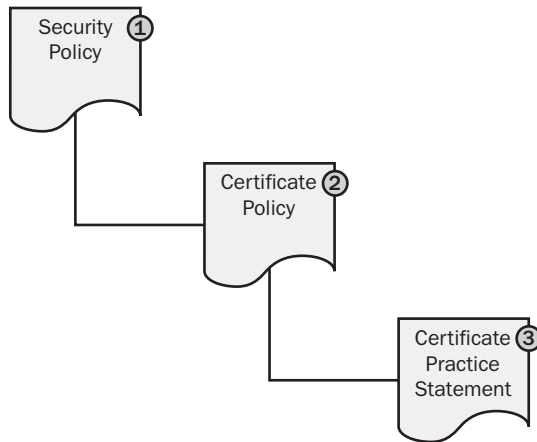


Figure 3-1 The dependency between the security policy, certificate policy, and certificate practice statement (CPS)

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.



Note 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.



Note 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 whether 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."



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

ISO 17799, available for purchase at <https://www.bspsl.com/secure/iso17799/software/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.

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 providing certificate enrollment access through controlling network interfaces on the CA, 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 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 conjunction with 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 archiving 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 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 www.defenselink.mil/nii/org/sio/ia/pki/DoD_CP_V60_31May2002.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 a 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.



Note 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.



Note 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.

Certificate 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



Note 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 2527, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework,” available at www.ietf.org/rfc/rfc2527.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 eight sections:

- Introduction
- General Provisions
- Identification and Authentication
- Operational Requirements
- Physical, Procedural, and Personnel Security Controls
- Technical Security Controls
- Certificate and Certificate Revocation List (CRL) Profiles
- Specification Administration



Note RFC 2527 recommends that the same format be used for both certificate policies and CPSSs. The X.509 certificate policy for the United States Department of Defense implements the eight 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: Introduction

The introduction provides an overview of the CA, as well as the types of users, computers, network devices, or services that will receive certificates. Should another organization have any questions regarding the information published in the CPS, the introduction also provides contact information.

CPS: General Provisions

The general provisions provide legal definitions for:

- **The obligations of the company managing the CA, as well as the obligations of the certificate holders.** These obligations can include who is responsible for the private key material and the measures taken to identify the subject of the certificate.
- **The liability of the organization that manages the CA.** The liability defines the maximum value of transactions for which the CA-issued certificates can be used. For example, if the liability is defined as \$1,000, transactions for a greater value are insured only up to the maximum value of \$1,000.
- **The laws applicable to the operation and management of the CA.** For example, a CA can enforce the laws of the state of Nevada, rather than the state of New York. This defines how certain actions might be interpreted if brought to litigation.
- **The fees required to receive a certificate issued by the CA.** Some commercial CAs have a fee scale for the issuance of a certificate. If fees are involved, this section should detail the associated fees for each class of certificate offered by the CA.
- **How audits of the CA are performed to ensure that the CPS-defined tasks and measures are performed.** For example, if an independent auditing firm is brought in once a year to evaluate PKI-related processes, the CPS should define how often audits are performed and what tests are performed by the auditing firm.

CPS: Identification and Authentication

This section describes the measures taken to validate a requestor's identity prior to certificate issuance. It must reflect the certificate policy or policies 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.
- **Replacement of a revoked certificate.** If a certificate must be replaced because of key compromise, such as a stolen laptop, what measures will be taken to ensure that the authorized user, not the person who stole the laptop, receives a new certificate?

- **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?



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

CPS: 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 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 a registration.
- **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?
- **Certificate suspension and revocation.** Under what 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.
- **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 responsi-

bilities 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 termination.** What actions are taken when the CA is removed from the network? This section can include information about the CA's expected lifetime.

CPS: Physical, Procedural, and Personnel Security Controls

This section describes physical, procedural, and personnel security controls implemented at the CA for key generation, subject authentication, certificate issuance, certificate revocation, audit, and archiving. 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.

CPS: 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.



Warning 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: Certificate and Certificate Revocation List (CRL) Profiles

This section is used to specify two 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 publication.** This section should provide information about how frequently a CRL is published and whether delta CRLs are implemented. If the CA implements Online Certificate Status Protocol (OCSP), configuration information should be detailed here.

CPS: Specification Administration

This section specifies ongoing maintenance of the CPS. For example, what circumstances drive the modification of the CPS? If the CPS is modified, who approves the 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.



Note 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.

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?
2. In what document would you define the methods used to identify the new hires when they start with Fabrikam?
3. Will the identification validation requirements for existing employees differ from those implemented for new employees of Fabrikam?
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?
5. You are considering modeling your certificate policies after the United States Department of Defense certificate policies. What certificate class would best match your deployment of 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) (www.defenselink.mil/nii/org/sio/ia/pki/DoD_CP_V60_31May2002.pdf)
- RFC 2527, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework” (www.ietf.org/rfc/rfc2527.txt)
- The Information Security Policies/Computer Security Policies Directory (<http://www.information-security-policies-and-standards.com>)