

realtimepublishers.comtm

The Shortcut Guidetm To



Managing Certificate Lifecycles



Kevin Behr

Chapter 2: Root Management20

Certificate Policy and Certificate Practice Statements20

 The Components of Certificate Policies and CPSs.....25

 Other Documents26

 Do You Need to Develop a Certificate Policy and/or CPS?.....27

 Who Should Be Involved?.....28

 Access Restriction.....30

 Backing Up31

Audit35

Summary.....38

Copyright Statement

© 2006 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

Chapter 2: Root Management

This chapter will continue to build on the concepts outlined in Chapter 1 and extend them to common real-world scenarios. It will show you how to cut through the marketing hype and get to the bottom of the services provided by commercial CAs by introducing two documents that all commercial CAs produce. The chapter will then give you the inside track on methods you can use to manage your own certificate lifecycles by examining how commercial CAs manage their own

- Root keys
- Policy and procedures governing the keys
- End user agreements

Finally, the chapter will examine how the policies and procedures used by commercial CAs can map into your overall PKI management strategy, answering questions such as:

- How can you know what a CA does to secure their PKI?
- Who does the PKI serve?
- Is there a standard method you can use to compare different CAs?
- How are CAs audited?

This chapter will answer these questions as well as explore


- Access restriction,
- Backup of keys
- Auditing the environment to ensure operational integrity and reliability

Certificate Policy and Certificate Practice Statements

The first chapter mentioned that all commercial CAs are not the same as they have differing policies and procedures in place governing the lifecycle of the certificates that they issue and manage. Many CAs also have a range of certificate products that offer varying degrees of assurance and authentication based on the type of usage scenario required by the customer.

How do you best compare the products and services offered by various CAs? The answer is to look at what they actually do as opposed to what they market. The best way to understand the actual policies and procedures in use by a CA is to look at the two documents authored by CAs that describe how they manage their particular PKI. These documents are called the Certificate Policy and the Certificate Practice Statement (CPS). The Internet Engineering Task Force (IETF) PKIX working group, the group that is responsible for developing PKI standards, has created a standard document framework that CAs can use to make assertions about the practices and policies they use to issue and manage certificates.

These statements aren't just valuable for the prospective end subscriber of a CA; they are equally valuable to a relying party. In PKI, *relying party* refers to the person, company, or institution that relies on the information presented to them in the digital certificate. If you were to visit an e-commerce site to purchase something, you would be the party relying on the PKI to provide you with assurances of privacy via encryption and assurance of the authenticity of the Web site you are visiting via the information verified in the certificate presented to your Web browser.

 Remember, you can double-click the gold lock icon in the lower-right corner of your Web browser to see the contents of the digital certificate any time you are on a site for which the URL starts with https://.

The degree with which the relying party can depend on the accuracy of a digital certificate and its corresponding key is directly related to the particular policies and procedures of the issuing CA and the certificate holder (subject) of the certificate. The IETF RFC 3647 document authored by the PKIX working group serves as a framework for policies and practices documentation around the management of certificates. The Certificate Policy and the CPS and their suggested structures hold very valuable information that will come in handy when it is time to compare the practices of various CAs. The goal of the documents is to give interested parties a standard framework with which CA policies and practices can be compared.

 The IETF RFC 3647 is available at <http://www.ietf.org/rfc/rfc3647.txt> and the PKIX working group page is available at <http://www.ietf.org/html.charters/pkix-charter.html>.

According to the RFC, the Certificate Policy document is designed to act as a named collection of rules indicating the applicability of a digital certificate to a particular community of users. It can also refer to a specific application with common security requirements, such as which levels of verification are required by the CA for each certificate product it offers. Often these common requirements are tied to the monetary value of the transactions that will be authenticated by the certificate. The common requirements are not limited to commerce and can extend in to the types of end users or communities they support. These communities could be business units or academic research groups spanning multiple universities around the world. Whether evaluating a certificate created by an end subscriber or a certificate issued by a commercial CA, it is important to evaluate the assertions made by the CA to make sure that they match the application for which the certificate was presented. It is also very important that the procedures for validation and verification of the certificate subject are equal to the levels of assurance required by your particular application. If you are selling expensive items, you need to provide your customers with the highest level of assurance that you are authentic by purchasing the highest assurance certificate product from the appropriate CA.

When examining the various policy documents presented by a CA, you might find that there may in fact be several policies depending on the intended use scenario of the various certificate products offered. These differing policies reflect the needs of end-subscriber communities or corporate divisions. Inside of an enterprise banking network, for example, a one-size-policy-fits-all approach would not be the ideal approach. It would be wise to delineate the policy governing the management of certificates along the lines of risk and build separate policies for groups with differing risk profiles. For example, the bank's marketing personnel would certainly have different certificate needs than someone in banking operations that is responsible for transactional data. The bank's digital certificates could be managed with less transactional risk in marketing; therefore, the policies and procedures governing the certificate lifecycle can be much more lenient and geared to the speed of execution required by the business. This setup would be especially evident in the policies around issuance and verification of the certificate subject.

In the bank's operations group, the certificate lifecycle would be governed by stricter sets of controls around verification and issuance due to the increased risks associated with the processing of checks and payments.

The documentation framework outlined in RFC 3647 can also be used for creating documents besides the Certificate Policy and CPS. The format works well to construct relying party, subscriber, and other agreements outlined in a Certificate Policy or CPS (see Figure 2.1).

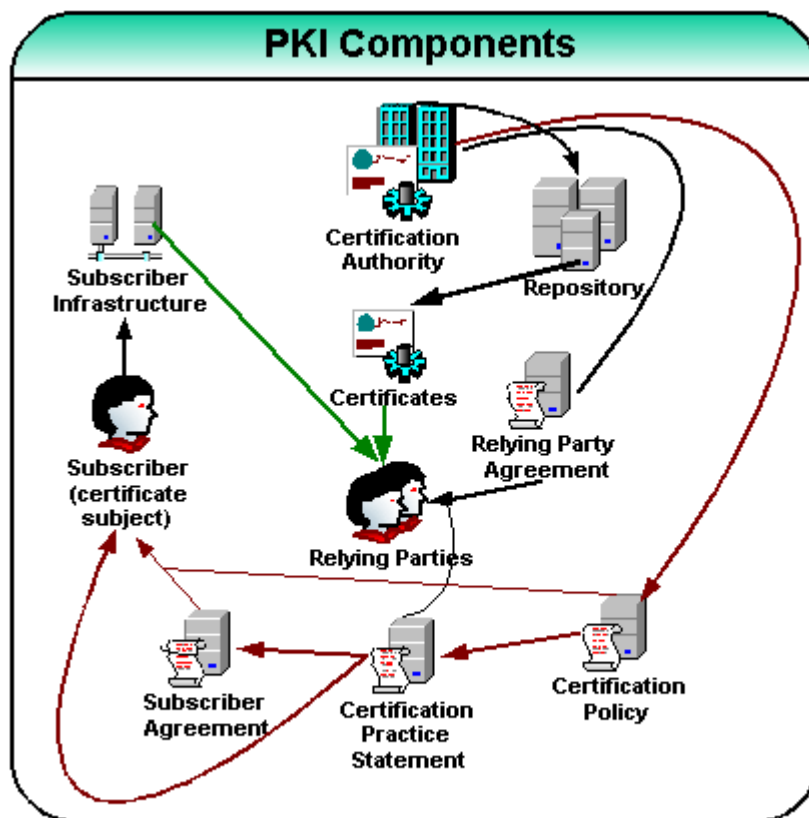



Figure 2.1: PKI components depicted with information flow. The green lines represent the flow of assurance from the certificate subscriber to the relying party. The red lines represent the flow of trust to the subscriber. The black lines represent the flow of trust from the CA to the relying party.

Think of the Certificate Policy as the basis for trust or accreditation in the issuing CA. When acting in the role of the relying party, it is wise to examine the certification policy associated with the certificate to make sure it matches the application for which it is being offered. For instance, when looking at the certificate type, it should match the type of transaction you are performing. If you are spending large sums or handling sensitive information, you want to be offered the highest level of assurance by a Class-3 certificate. If you are using a Web email service and just want basic security and privacy, a Level-1 or Level-2 certificate should be fine.

The CPS is an assertion by the CA covering the practices used by the CA to issue certificates. It is important to note that although the format of the document is outlined by an RFC, the actual content of the documents differ from CA to CA. The importance of understanding the very underpinnings of any network of trust cannot be overstated. The practices governing the issuance of certificates constitute the very cornerstone in the network of trust. If you are not comfortable that the CA can do what it purports to in its CPS, you need to consider another CA that offers services that match your needs more appropriately.

 A very sharp colleague recently shared such a scenario regarding the suspicious claims of a particular CA, which purported to automatically verify that the requester of a certificate was authorized to make changes to the domain name on their certificate application. The colleague pointed out that many domain name registrations commonly hide the names and information of the domain managers. So how could this information be verified automatically? The advantage of this automation was supposedly the speed of certificate issuance. Fast is not always the best—especially when dealing with security controls such as authentication. For high assurance applications of PKI, it is better to choose a CA that uses thorough checks, which might mean that they are performed manually by an actual person. It might take considerably longer to get your certificate and you might even have to mail or fax documents to the CA.

Key Terms in a Certificate Policy and a CPS

Activation data—Specific data values beyond the keys themselves that may be needed to activate cryptographic modules or access-control infrastructure. This data needs to be guarded, as it represents a security control in place to protect sensitive keys. The strength of the activation data and the strength of the access-control methods or devices must be commensurate with the sensitivity of the protected information.

CA certificate—A certificate for a particular CA's public key that has been issued by another CA.

Certification path—Certificates based on other certificates. These must follow an ordered, often hierarchical, path of certificates together with an initial certificate in the path that can be processed to validate the final certificate in the path (see Figure 2.2).

Certificate subject—The entity or end user that is requesting the certificate.

Issuing CA—The CA that issued the certificate, also referred to as the subject CA.

Policy qualifier—Information that accompanies an X.509 certificate in the form of a Certificate Policy identifier. The policy identifier is one of several data fields present in a digital certificate. This information might point to the URL at which a CA makes its CPS or Certificate Policy available.

Registration Authority—The entity that identifies and authenticates certificate subjects. This entity does not sign or issue certificates; the responsibility is usually delegated by a CA to perform these tasks on behalf of the CA.

Relying party—The party that receives the certificate and acts in reliance to the certificate directly or by other signatures verified by the certificate. This is also referred to as a being a certificate user.

The screenshot shows a Windows dialog box titled "Certificate" with three tabs: "General", "Details", and "Certification Path". The "Certification Path" tab is active, displaying a tree view of the certification path:

- DoD PKI Med Root CA (Root)
- Med CA-1 (Intermediate)
- ca-1.chamb.disa.mil (End Entity)

Arrows indicate the trust relationship from the intermediate and end entity certificates back to the root CA. A text box with a blue background and white text is overlaid on the path, explaining the browser's trust-checking process:

Your web browser will automatically check to see if it trusts the root certificate issuer. The browser ships with a list of all accepted root CAs. Before it will accept the certificate it is presented with it will check to see if it is in its listed of trusted root CAs. If it is not it will check to see who signed the certificate and check if that CA is listed. Your browser will traverse the entire path to see if it can trust anyone listed. If the browser can not find any of the CAs in its list it will present a dialogue box giving you the option to investigate the matter further.

Below the path, a "Trust?" label is positioned near the arrows. At the bottom of the dialog, a "Certificate status:" section contains the following text:

This CA Root certificate is not trusted because it is not in the Trusted Root Certification Authorities store.

Buttons for "View Certificate...", "OK", and "Cancel" are visible at the bottom of the dialog.

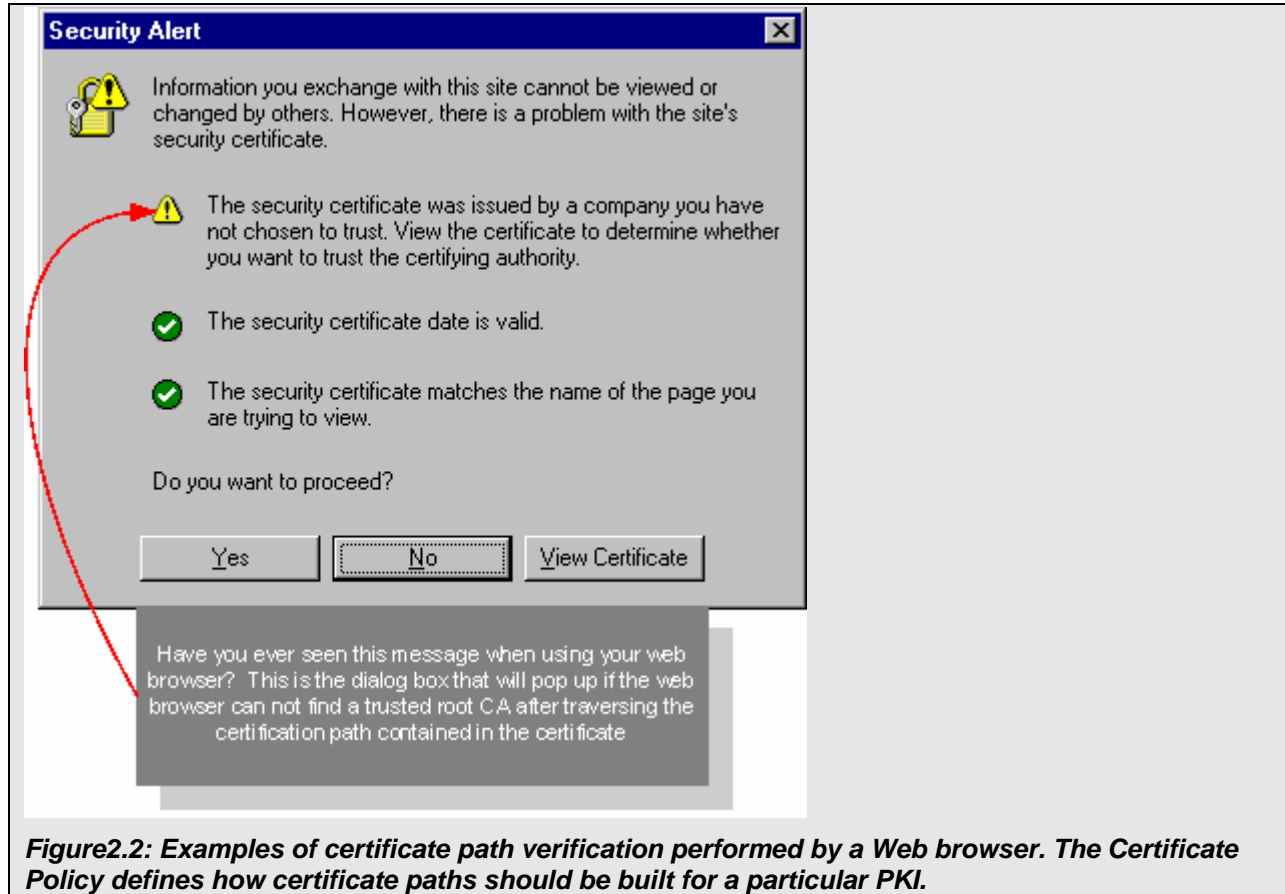


Figure 2.2: Examples of certificate path verification performed by a Web browser. The Certificate Policy defines how certificate paths should be built for a particular PKI.

The Components of Certificate Policies and CPSs


To find a Certificate Policy or a CPS from a CA, a good place to start is by visiting the CA's Web site. Most commercial and many private and community-specific CAs have links to their policy and CPS directly off their homepage. If you can't find the documents with ease, try using a search engine and query for the CA's name followed by CPS or Certification Practice Statement.

Once you have found the correct document, be sure to look at the date and version. The Web page on which CAs list their Certificate Policy documents and CPS usually have the latest document revisions at the top of the page in descending order with the older versions below. The CPS of many CAs is constantly evolving, so there are often several revisions.

The IETF RFC 3647 provides a basic framework or outline for the structure of these and other documents provided by CAs. The framework outlines nine basic elements. Not all elements are relevant to all CA applications or communities, so, in the course of reading documents authored by certain CAs, you might notice that some items are followed by the term *no-stipulation* for a specific element in the framework. In most cases, this simply highlights a provision that might not be applicable for that particular product or CA. This framework was designed to be used for all CA policy and procedure documents.

The RFC 3647 framework:

- Introduction
- Publication and Repository
- Identification and Authentication
- Certificate Lifecycle Operational Requirements
- Facilities, Management, and Operational Controls
- Technical Security Controls
- Certificate, CRL, and OCSP Profile
- Compliance Audit
- Other Business and Legal Matters

 More information about these nine elements is provided later in this chapter.

The main difference between the Certificate Policy and the CPS two documents has to do with their intended use. The Certification Policy document is intended to define the PKI and its community or application from a requirements standpoint. The point of this document is to instruct the PKI community members as to what they can or can't do within the confines of the PKI. Also the Certification Policy sets out the requirements and standards imposed by the CA on the PKI community. In contrast, the CPS focuses on how the CA and its participants must implement policy, procedures, and controls to meet the requirements that are spelled out in the Certificate Policy.

Other Documents

Although the Certification Policy and CPS are the central documents used to enumerate the policy and practice requirements of CAs, there are often several other documents that are very important. Not all Certification Policies or CPS are presented as legal contracts or even legally binding statements. Often contracts are handled in standalone documents that may be referenced in a CPS or Certification Policy. Other documents that may be referenced or even included within the Certificate Policy or CPS include:

- Subscriber agreements—These are the agreements that govern the purchase of certificates
- Relying party agreements—The agreements that stipulate what assurance guaranty is being provided to the person trusting a certificate by the issuing CA
- Security policies—The security policy documents for a particular CA
- Operational or training manuals—Documents that describe how to use the PKI of a particular CA
- Other standard documents from the IETF, ISO, other CAs, or a corporate entity
- Policies governing the use of email for subscribers and relying parties
- Key management planning documents—Templates that provide guidance and describe lifecycle considerations for certificate subscribers
- Employee manuals and guides—The internal Human Resources documents used by CAs
- A CPS abstract—An abbreviated version of a CPS that may omit sensitive or confidential information

The American Bar Association's Digital Signatures Guidelines Tutorial

The American Bar Association's section of Science and Technology Law has developed a free tutorial that can be accessed on its Web site at <http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>. The tutorial covers the basics of digital signatures and PKI as well as takes a broad look at the various legal implications of these technologies. Background into the nature of electronic commerce and a solid method for evaluating certificates are just two reasons to visit this great site. In addition, the guidebook can be downloaded in several document formats.

Do You Need to Develop a Certificate Policy and/or CPS?

If your organization is going to depend on digital certificates to deliver goods or services or issue them to employees or other business partners, you will need to develop a Certificate Policy and/or CPS. The RFC 3647 framework is a great place to start your efforts. As mentioned earlier, the RFC outlines nine sections that can be addressed depending on the scope of your PKI implementation. Are you running an e-commerce site and just need a certificate to provide assurance to your customers or business partners? If so, your documentation requirements will not be as elaborate and need not address certificate issuance, for example. If you plan to use PKI to issue certificates to all your employees, you will need to address the full certificate lifecycle in your documents:

- Introduction—This section is used to describe the company and how it intends to use PKI
- Publication and Repository—This section will answer the questions: How will you publish your public keys and how will you store the certificates you issue?
- Identification and Authentication—This section will answer the questions: What are the processes and controls you will use to authenticate certificate requesters?
- Certificate Lifecycle Operational Requirements—This section will answer the questions: How will you manage the infrastructure, policies, procedures, and controls around your PKI? Who will be responsible for what?
- Facilities, Management, and Operational Controls—This section describes what systems of controls you will build around physical and logical access to the facilities and infrastructure that house your PKI.
- Technical Security Controls—Use this section to describe the preventive, detective, and corrective controls that keep your certificates safe from others. For example, describe how you separate your production PKI network from your test and development networks and limit access to it. Also describe your defense-in-depth strategy for protecting the information assets in your PKI.
- Certificate, CRL, and OCSP Profile—Use this section to describe how you will publish a list of expired or revoked certificates to your PKI users.
- Compliance Audit—Describe your audit partner and frequency. Offer a brief description of the audit plan and objectives used as well as how the user can obtain a copy of the audit results.
- Other Business and Legal Matters—This section is used for general comments and/or items you might want to cover outside of the other sections.

Who Should Be Involved?

Assemble a working team comprised of the stakeholders in your organization that are involved with and affected by the use of PKI. Often the team will be lead by your security organization, as PKI is often part of a larger security policy or roadmap:

- IT operations—The ops staff can speak to technical and infrastructure questions that may arise.
- Sales/marketing—What is the business value of this technology and what business processes depend on PKI?
- Liaison to business partners—Often IT organizations have someone designated to address the concerns of business with IT and vice-versa.
- Legal council—They are crucial for offering decisions about what risks are acceptable in a general business context.
- Finance—If you are going to put dollar and cent values on the business processes that PKI enables, you will want their buy-in.
- Relevant division heads—Which business groups will depend on PKI? Whether they know it or not they need to have a voice and be part of the process.
- IT security—At most companies, PKI is a subset of a broader security policy framework. Security must be present to make sure that the PKI policy and procedures are integrated into this framework and that the provisions outlined in the documentation are consistent with the broader security roadmap. IT security may act as the PKI team lead.
- Physical security—It is very important to involve those in charge of physical building and area access. Commercial CAs use multiple levels of physical security to provide assurance that only authorized staff have access to systems used to issue or modify certificates. This is an important control consideration for enterprise use as well.
- Internal audit—It never hurts to bring your most knowledgeable control experts in if they have the time.
- Human Resources—If your PKI is used to authenticate employees or contractors, you will want HR at the table to make sure that the policies and procedures are consistent with employee manuals.
- Corporate compliance (HIPPA, GLBA, CFR11, FISMA, PCI, SOX) team leader—If your company is regulated, they will need to integrate any relevant policy and procedures into their control documentation.
- Business continuity/disaster recovery team lead—If PKI is going to affect your company's ability to maintain business continuity, you will need to integrate your work with the overarching business continuity and disaster recovery plans.

This group is also an effective team to determine the operational and corporate risks involving the use of PKI and certificates. The documents you create will most likely work with existing documents such as Human Resource employee handbooks, IT security policy, and IT change management or other operational run books. This is also a great team to classify the methods used to store and backup the certificates. Are the certificates so sensitive and mission critical that they need special protection? Ask questions to determine whether the certificates will be required to ensure business continuity. If third-party business partners utilize your certificates, you might want to consider authoring a CPS abstract that is an abbreviated CPS that contains only information that is relevant to business partners but does not disclose sensitive information regarding your security or HR policies.

It is also wise to establish an update plan that will address changing needs and scenarios and incorporate them into the documentation. A good rule of thumb is to make the evaluation of your PKI policy and procedure documents a part of an annual security policy review. If your PKI implementation will be used to protect email or enable secure e-commerce activities, it will be wise to construct an appropriate privacy statement for your employees, business partners, and customers; this statement is best handled in the context of your overall security policy framework.

As policy and procedure are meant to be living documents that are changed to reflect actual evolving practices, you will do well to consider revisions, distribution, and notification out of the gate:

- How often will this team or a smaller subset revisit the documentation to determine whether it still meets the needs of the business?
- How will your business partners or employees be notified regarding changes and updates to the various documents your company publishes?
- How will they know whether they are looking at the latest version?
- Where will these documents be stored?

These questions represent the belief that your PKI implementation will evolve as your business needs and partnerships change.

Rather than force everything into one huge documentation set you might want to consider each PKI use case as a separate implementation and create separate documentation. It does create a larger document base to maintain, but, if your organization is extending its PKI implementation beyond the walls of your company and into other companies, this will prove to be important. By the very nature of the Certification Policy and CPS documents, you might opt to protect sensitive references to internal security policy, authentication, and escalation methods from the eyes of anyone outside of your company. Abstracts of briefs can be prepared for each community or use case and should be represented by an internal-master Certification Policy that documents any and all certification policies and practice statements and the entities to which they pertain. This way, a regular review will cover both internal and external versions and all the documentation will receive the periodic scrutiny necessary to make sure the documents are still relevant.

Access Restriction

Another topic covered in most CPS documents is the policy of limiting access to PKI production systems, such as servers and network infrastructure that store and serve certificates to users. Many IT organizations have become very comfortable with pervasive server access by IT support personnel. This is often provided with customer service in mind. The rationale is that the less hurdles a systems administrator has to go through to solve a problem, the better. When it comes to access to live production systems containing digital signatures, this logic does not hold up. There have been several studies showing that the largest single cause of system outages is human error. By reducing the field of suspects, it is much easier to eliminate change or human error as a causal factor if something goes awry. If your PKI implementation is critical to the flow of business, you will want to consider removing persistent account access to the PKI servers and implementing a limited functional access only via approval. When the approved work is complete, access is then removed. Typically, during an effective IT audit, the auditors (internal or external) will want to see a list of user accounts on mission-critical servers. Make sure that you can account for every access account and answer why each account is enabled. Also consider the roles and responsibilities of your IT engineers. Do any of their official responsibilities make it more difficult for them to follow procedure and process?

Separation of Duties

CAs make sure that the roles and responsibilities of its employees do not compromise their ability to adhere to policy and procedure. A classic example in finance is the old rule about being able to add vendors to the accounting system and being able to print checks. This check and balance was instilled to prevent the AP clerk from adding a new “mystery” vendor and then printing the checks only to steal the funds for themselves. Checks and balances can also include signing limits or dual signatures for checks over \$500.00.

Preventing Unilateral Changes and Transactions

One of the largest causal factors behind IT service outages is change. Eighty percent of the time it takes to resolve an outage is spent determining just what changed! Many security breaches happen as a result of firefighting problems, as access controls are often bypassed to expedite troubleshooting efforts. Commercial CAs know that accountability for changes is key to preventing disasters and security incidents. For these reasons, commercial CAs have developed elaborate systems of control to prevent a single person from compromising the entire PKI.

CAs utilize security controls around the signing and storage of certificates and private keys. As CAs must protect their private keys at all cost, a formal signing ceremony of sorts is usually designed to reduce the risk of collusion or unilateral decisions that could prove to be fatal to a PKI. The next chapter will address the roles and responsibilities of those managing a PKI infrastructure, as the chapter looks at the certificate lifecycle components and what must be managed at each stage.

Strong Change Management Integration

Any proposed changes involving certificates or PKI should most likely involve security personnel. As the effects of PKI can be felt everywhere, on many corporate networks it is wise to vet all proposed modifications through a rigorous change management process. At a minimum, the change manager must obtain the appropriate approvals from the potentially affected business customers. If PKI is used by your sales and marketing team to sell on the Web, this is even more important, as any certificate modification or installation has the ability to affect the viability of e-commerce sites or employee network access.

Backing Up

If you have read some of the CPSs issued by CAs, you might have noticed that there is often a section that mentions that all critical keys are backed up in case of hardware failure and to address disaster recovery requirements. The documents state that they only back up their own certificates not those that belong to end subscribers. If your certificates are important to the everyday operation of your company, a plan to provide continuity of service should be put in place immediately. It is wise to inventory all the software and systems that depend on certificates to operate and make a list. If your organization has a business continuity and disaster recovery plan, find out how these systems and software are addressed. It is a great idea to look for underpinnings or new dependencies that might have cropped up due to changing requirements. A meeting with the person in charge of the overall disaster recovery/business continuity plan to discuss the role that certificates play in business operations would be a great place to start. Make sure that they understand that digital certificates may take days to provision and make sure that any documents used in the validation process with your CA are available in the event of a disaster so that if it is necessary you can re-validate your organization.

The most common form of backup in many organizations is the magnetic tape. Whether your organization relies on tape or other media for backup, be sure to understand who has access to this media. I have heard stories from more than one security professional that has casually lifted a backup tape out of the tape library and found certificates complete with private keys on the tape with absolutely no security. If someone is able to obtain your private key, they can issue certificates signed by your organization! This can prove disastrous, which is why backups of digital certificates must be subject to a system of controls that is designed to meet the assurance requirements of your company.

It is crucial to build a policy for the backup and safe storage of your certificates. Special provisions may need to be made to safeguard your high assurance for Class-3 certificates. When building this policy, make a concerted effort to quantify the damage possible if your certificate were to be compromised. The American Bar Association offers a wealth of information in a free PKI tutorial on their Web site that will prove helpful in identifying your risks (<http://www.abanet.org/scitech/ec/isc/dsg-tutorial.html>). Would there be a dollar loss or would the certificate give someone the magic keys to sensitive corporate data? Once you have a feel for the risks, it is much easier to design a protection plan that is commensurate with risk. For high-value certificates, you might want to consider some or all of the following controls:

- Consider the use of a FIPS-approved Hardware Security Module (HSM) to store your most sensitive keys (rather than a general-purpose server). It is a great idea to purchase a backup HSM in addition to your primary HSM. As HSMs typically cost thousands and can cost tens of thousands of dollars, they are most appropriate for high-risk scenarios or to protect very sensitive keys (see Figure 2.3).
- Use an offline backup server to store root or sensitive certificates. Control access to this server.
- Use change detection software such as Tripwire or Solidcore to monitor the integrity of your certificates. These types of software can create a fingerprint of your certificates and alert you if they are changed in any way.
- Encrypt your certificates and keys if they must be stored on a shared server.
- If certificates must be stored on tape, utilize tape encryption and control the physical storage of the tapes. The tapes should be kept in safe deposit boxes or controlled access scenario. Make sure that retention policies for longevity of storage and destruction are well thought out for these valuable items.

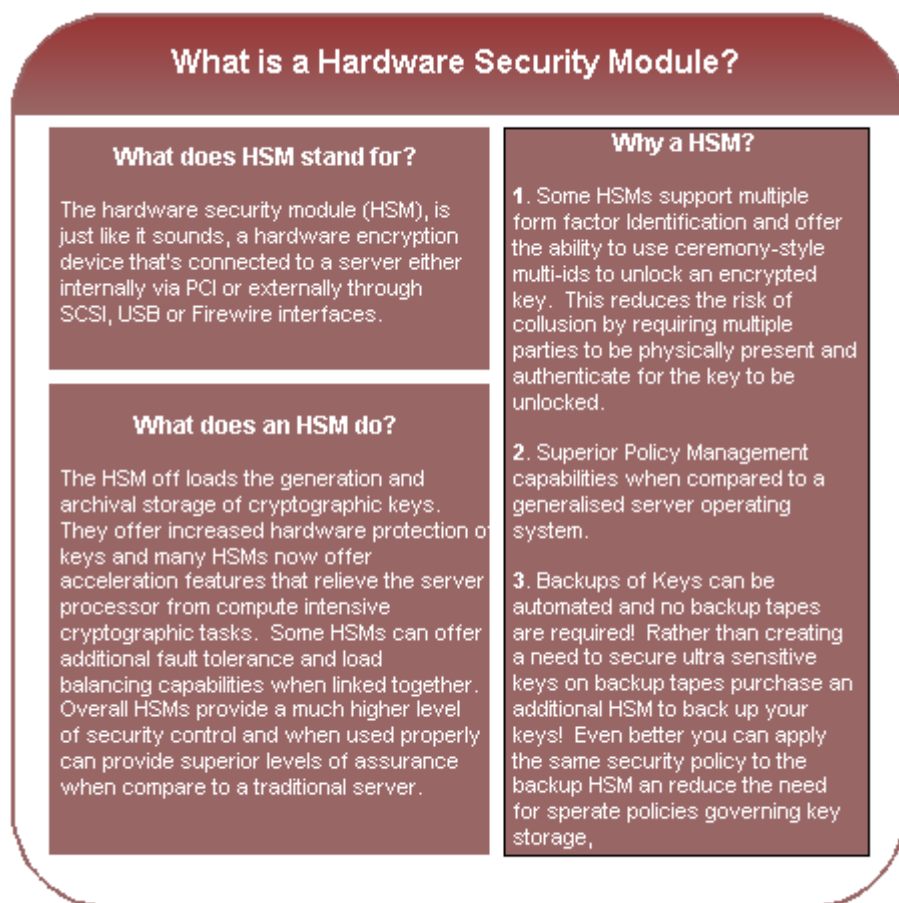


Figure 2.3: The definition and key reasons to use an HSM.

What is FIPS Certification?

The National Institute of Standards (NIST) has developed guidelines for security hardware manufactures and FIPS 140-2 (<http://csrc.nist.gov/cryptval/140-2.htm>) is the current specification for security requirements for HSM. Manufacturers must comply with the guidelines in order to sell their respective products to the United States federal government.

The specifications are dovetailed with a standardized testing methodology and an approved testing lab list. Once a vendor's hardware has been successfully tested by one of the approved labs, it is added to a list of approved solutions at the NIST Web site (<http://csrc.nist.gov/cryptval/>). This list is a helpful way to start evaluating competing HSM solutions.

It makes sense that commercial CAs go to great lengths to protect their private keys. If a commercial CA's private key were compromised, its entire PKI trust hierarchy could be destroyed—not to mention all the end subscribers validated by that particular CA (see Figure 2.4). Most commercial CAs go to very elaborate lengths to make sure that their private keys stay private. This is accomplished through the judicious implementation of security controls.

Controls common to commercial CAs:

- HSMs are used—Many CAs use HSMs to create and store their critical keys. These modules are capable of encrypting the keys and require an authorization process to be completed before the keys can be unencrypted and transferred to another device or server. In many cases, these HSMs are not statically connected to a network or, if they are, they are connected to an isolated production-only network with access granted only to those with an approved need.
- Backups are controlled—Backing up critical keys is a very serious business at CAs, and these backups are subject to rigorous controls and regular auditing to guaranty that this information is available only to authorized personnel. Limits are placed on retention and backups are audited regularly.
- Ceremony—Requiring multiple parties to be present with their part of the overall secret is called a ceremony. Many CAs use this same control method to guard the generation and signing of certificates and keys. This method makes it more difficult to compromise keys and certificates due to an increased number of people involved (reducing the risk for collusion).

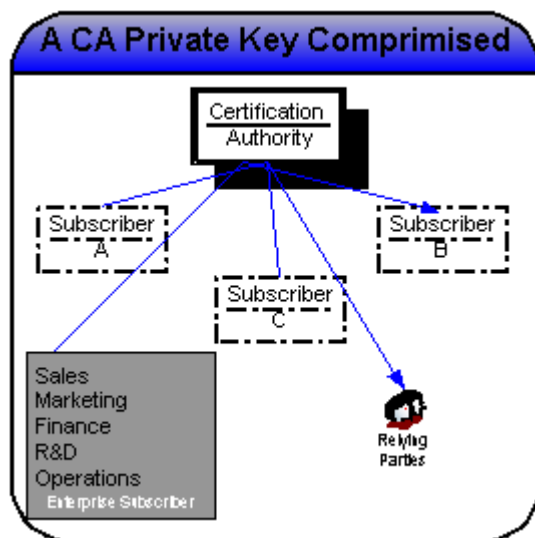


Figure 2.4: Everyone below the root CA in the PKI hierarchy is exposed if the CA's private key is compromised. In cases in which the compromised CA is a root CA, other CAs could even be compromised without their knowledge.

Audit

One of the most misunderstood terms among IT security professionals is audit. Many believe it means simply to check up on things or to investigate. Even worse, I have talked to many IT staffers that believe controls belong to the auditors. Controls are owned by the business. To be effective over the long-haul, high-performing IT organizations design controls to act as sensors that indicate whether current performance is furthering the goals of the business (keeping risk in check) or impeding them. In other words, controls are management. Audit is not a management function; rather, it provides an ongoing commentary on the effectiveness of controls in place and a list of controls that are missing (see Figure 2.5).

IT audit can be a critical part of managing adherence to critical controls such as policy and procedure. However, don't leave the development of policy, procedure, and controls to auditors—that is not their job! That is not to say that audits shouldn't review documentation. There are few people in the business world with a better grasp on process and controls than auditors, so leverage their expertise. Although you are gleaning from their knowledge, do yourself a tremendous favor and read up on control theory and IT audit frameworks such as Control Objectives for IT (COBIT—<http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=55&ContentID=7981>), which is published by the Information Systems Audit and Control Association (ISACA). Audit is best performed by trained auditors that have adequate independence from day-to-day operations and projects. In fact, the auditor ideally should report to a completely separate management chain. Independence gives the auditor an unbiased viewpoint from which to judge adherence with an organization's stated policies, procedures, and controls.

Controls 101

Preventive—Preventive controls focus on what can be done before an undesired action or condition occurs. A classic example of a preventive control is a lock on a door. In the case of systems control, functional access based on approved work is a preventive control. When compared with static access, functional access can drastically reduce the amount of unauthorized changes. If you can't access the server, it is much more difficult to implement a change on it. In PKI, a preventive control is the validation of a certificate applicant's identity preventing the applicant from falsely representing themselves.

Detective—Detective controls monitor an environment or a process and look for a certain set of conditions to occur, then generate a notification or alert that the condition indeed occurred. A great example of a detective control is a fire alarm. When a certain threshold of smoke and heat are met, the alarm emits a piercing sound to warn the building's occupants that there is a fire. In PKI, a detective control could be used to protect the integrity of a key by monitoring it against a baseline to detect any modifications to the certificate.

Corrective—Somehow an undesired behavior occurred and now you need to remediate the situation so that you can get back to performing as if nothing ever happened. A classic example of a corrective control is a steering wheel. Data backups are an example of a corrective control. If a certificate is corrupted or lost due to a hardware failure, the certificate can be restored from a backup.

Commercial CAs that are licensed are required to have their operations audited. The audits in the United States and Canada are performed under an AICPA/Chartered Accounts of Canada coauthored document called the Webtrust Program for Certification Authorities (this document is available at http://ftp.webtrust.org/webtrust_public/tpafile7-8-03fortheweb.doc). The basic principles serve as an excellent mechanism with which any organization can evaluate its performance against its intentions or policy assertions. Often, service providers and CAs will also undergo a Statement on Auditing Standards for Service Providers (SAS70) audit to validate the broader system of controls in place around their IT environments. The SAS70 was designed to make a public statement about a service provider's controls and what the auditor found to be true or untrue about those public assertions. Although the SAS70 and Webtrust audit programs do not serve as an effective method to compare one CA to another, as they will most likely have different assertions regarding their own system of internal controls, it is important that they successfully pass these audits. The main difference between the two audits is that the Webtrust audit has a defined framework and control set that is audited and the SAS70 that audits the service provider's control assertions and has no predefined framework. The SAS70 audit focuses on the control assertions that the service provider has decided to make public.

The main categories of Webtrust audit evaluation are:

- CA Business Practice Disclosure
 - Identify the Certificate Policy and CPS under which the CA issues certificates
 - What are the CAs certificate lifecycle practices?
 - Does the supplied documentation disclose all this information to subscribers and relying parties?
- Service Integrity
 - Does the authentication method employed by the CA effectively screen applicants in a repeatable fashion?
 - Does the CA effectively protect the keys and certificates it is responsible for managing throughout their lifecycle?
 - Does the CA publish revocation lists in a timely and accurate manner?
- Environmental Controls
 - Subscriber Personally Identifiable Information (PII) is kept confidential and is used in a way that is consistent with the promises and warranties outlined in the CA's privacy statement.
 - Operational integrity and continuity are sufficiently maintained
 - Systems are maintained only by authorized personnel performing work that has been authorized and vetted by appropriate control processes such as change management
 - Any software or systems developed are built using repeatable and authorized processes

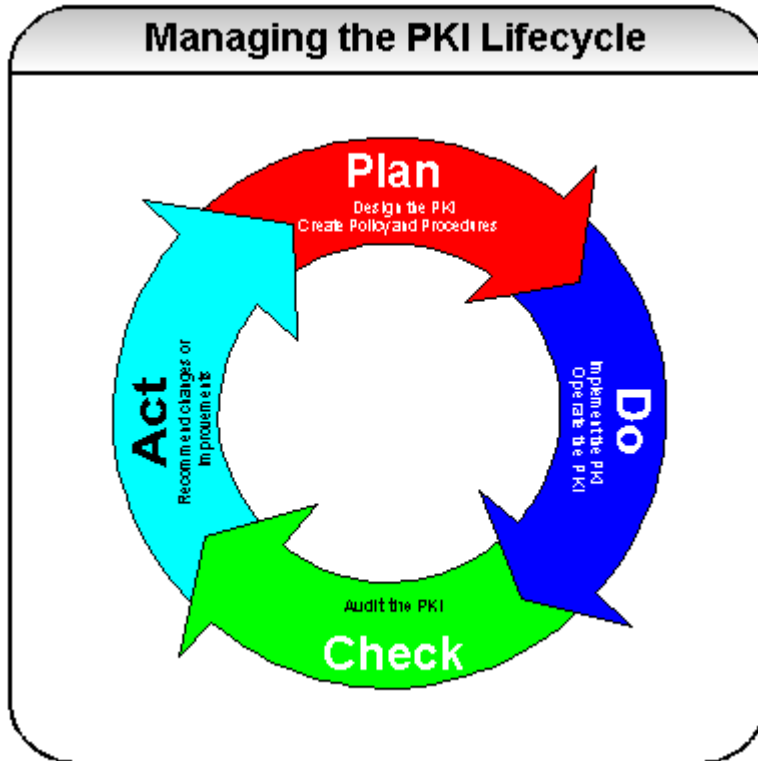


Figure 2.5: Audit represents a critical component in a successful PKI implementation. Audit verifies that the foundation of trust promised by a CA is actually delivered.

In addition to the Webtrust (<http://www.ansi.org/>) checklist, there are a variety of sources for audit and control objective guidance. The ANSI X.9.79:2000 standard codifies the control objectives highlighted in the Webtrust CA audit into its PKI Practices and Policy Framework. There is no shortage of audit guidance from organizations such as the Information Systems Audit and Control Association (ISACA—<http://www.isaca.org>). There is much guidance available on their Web site free of charge. Simply use the search bar and enter PKI to get a great list of articles and guidance to peruse through. ISACA members also have access to a wide variety of audit checklists and specific audit guidance around security and PKI.

If your organization does not have a full-time internal audit staff, you might want to consider hiring or contracting with a third-party organization to audit your PKI implementation annually to make sure the policy, procedure, and controls you have invested in are in fact being followed every day.

Summary

This chapter has covered quite a bit of ground building on the PKI concepts covered in the first chapter, moving beyond basic certificate and digital signature technologies to how certificates are actually provided and looking at what needs to be done once a certificate is purchased. It is easy to get overwhelmed by the wealth of information and seemingly steep learning curve associated with the purchase of a digital certificate. The real work begins when it is time to depend on PKI. Building a dependable PKI solution requires serious thought and effort around policy, procedure, and controls. Implementation of digital certificates is not where the heavy lifting is done. Building out an effective system of controls to support the goals of the business requires involvement from many stakeholders and often represents the bulk of the work. Making sure that the digital certificate lifecycle is understood and effectively managed doesn't require a technical certification or advanced Computer Science degree but rather a focus on the goal of the business and how digital certificates can diminish constraints around commerce and security and open up a whole new avenues of business.

By choosing to see digital certificates in the context of a lifecycle, you are now free to focus on management, metrics, and controls in an enabling manner. Rather than view certificates and PKI as something you buy, implement, and forget about until a disaster occurs and strips your organization of its ability to derive e-commerce revenue through theft, fraud, or reputation loss, why not tackle policy, procedure, and audit when it is least expensive, both in monetary and emotional capital, early in the lifecycle. Nothing hurts worse than failures, outages, or miscues shortly after the fanfare of a new rollout. The common misconception of business and IT executives alike is that the steepest curve in any new IT project is getting the new technology to work. Seasoned IT operations engineers know that most common incidents could and should be prevented with simple controls designed into the project before it is ever starts. Nearly 80 percent of all IT outages are caused by people and process issues, according to research performed by Gartner.

Using the standardized policy and procedure document framework (RFC 3647) built by the IETF's PKIX working group, it is possible to compare critical components of the Certificate Policies and CPSs issued by commercial CAs. This chapter covered that a CA can actually issue several policies and practice statements depending on the PKI community they are addressing. As with the commercial CAs, it is important for you to consider whether abridged or specialized versions of your documentation should be developed for use with business partners or customers so as no to reveal confidential security practices and controls beyond the confines of your trusted company staff.

With a better understanding of the makeup of the Certificate Policy and CPS, it is also easier to make more informed decisions as a relying party. Especially when you can slice and dice the issuing CA's CPS to verify that the certificate you are presented with is the correct type for the application in use. Knowing how to strip all the marketing hype away and get to the bottom of the validation and verification methods employed by a particular CA not only helps you decide whether to trust a certificate but also helps you decide whether a CA's practices line up with the requirements of your application. By using the CPS as your guide to what a CA really does in the way of validation and verification, you can steer clear of misunderstandings and get the level of assurances you really need.

The next chapter will leverage these concepts and explore the different phases of the certificate lifecycle. It will explore how CAs manage these phases differently—some CAs provide adequate verification policies and practices but lack in other areas such as reissue or revocation.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.