

realtimepublishers.comtm

The Shortcut Guidetm To



Managing Certificate Lifecycles



Kevin Behr

Chapter 3: The Certificate Lifecycle.....40

Issuance.....40

 Contrasting Validation and Verification Procedures42

 Higher-Assurance Certificates49

 Managing Multiple Certificates50

Re-Issuance52

Expiry.....52

Renewal.....53

Revocation54

Summary.....55

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 3: The Certificate Lifecycle

The first two chapters focused on defining and exploring key elements of PKI and how the root certificates and infrastructure need to be managed. This chapter will cover the entire functional lifecycle of a digital certificate. The certificate lifecycle consists of five distinct phases: issuance, re-issuance, expiry, renewal, and revocation. This chapter is full of helpful hints, best practices, and resources that will save you time, help you avoid embarrassing and expensive site outages, and steer you towards the correct certificate product for your application. Let's start at the very beginning of the certificate lifecycle with issuance.

Issuance

This guide has defined digital certificates as the binding of a vetted identity (company, role, or person) to a pair of digital asymmetrical keys. Whether purchasing a certificate from a commercial CA or issuing your own certificates within your company or enterprise, the concept is the same. Because a digital certificate is a form of credential used to identify a person, company, or a role, it is crucial that a validation and verification process is sufficiently rigorous to indemnify the level of assurance provided by that credential. For example, if you were a relying party shopping on an e-commerce Web site for a new laptop computer that costs \$1500, you would want to know that the digital certificate presented to you by the Web site guaranteed that you were not being spoofed. You would hope that the CA had stringent standards to make the merchant prove it was who it purported to be. The first chapter discussed the differing levels of assurance offered by most commercial CAs. The levels of validation and the verification methods are more rigorous as the level of assurance provided by the certificate product escalates. Keeping with the focus on delivering useful shortcuts, let's break these types into functional categories that focus on their common usage rather than brand names and hype.

There are myriad uses for PKI and digital certificates; the following list highlights the most common uses:

- Securing communications with encryption to provide privacy and integrity
 - Secure Sockets Layer (SSL) encryption for externally facing Web applications—You want any personally identifiable information kept private, so you will need to encrypt the traffic between the Web server and the end user computer with asymmetrical keys. In this application, the focus is on providing assurance of privacy and data integrity to your customers and business partners.
 - SSL encryption for intranets—In this application, the focus is on intra-company use. Typical applications include intranets or Web-based email systems for remote use. The main focus is to keep your data secure from eavesdropping via encryption. This type of application is sometimes called *domain authorization* because the CA needs to verify the certificate requester's right to administer the domain and make the request on behalf of the company. Your users know who you are and already trust the company, so there is little need for stringent validation and authentication of the company itself.

- Email—Most email traverses the Internet much like a postcard. The message payload is typically not protected and potentially could be viewed by malicious eyes. By using PKI, you can safeguard the contents of your sensitive email by encrypting it with public/private keys and providing a high level of assurance that only the intended party can read the message in clear text.
- Providing authentication and integrity
 - Network and application authentication—Digital certificates can be used to prove identity, save users from having to memorize multiple passwords, and keep remote-login procedures simple. Certificates can provide critical assurance that the remote user is indeed who they say they are and reduce the need for multiple forms of credentials to just a few simple methods such as smart cards or secure biometric devices. Certificates can also be used as part of authentication for a virtual private network. VPNs allow use of the public Internet as a private network by encrypting all traffic that passes between the end user and the corporate network. Many VPN applications allow the user to function as if he or she were on the local corporate network.
 - Web site or company authentication—This application focuses on providing assurance to your clients that when they pull up your Web site, they are dealing with your legitimate site and not an imposter. The client's Web browser automatically verifies that the certificate presented by the Web server is valid and is the correct certificate for the server in question. If this information is correct and the certificate is valid, the lock symbol will appear on the bottom of the Web browser indicating the site is legitimate.
 - Software signing—For developers of commercial software products, signing the files that make up a software package with their digital certificate enables you, the end user, to be assured that the program you think you are installing is exactly that and nothing more. By leveraging the authentication and integrity functions of PKI, you can be assured that the software comes from the correct source because the CA validated and verified the company, and is the correct set of files and only the files the publisher intended for you to have (and therefore contains no viruses or malware added by others) because a digital checksum or hash is used.
- Non-Repudiation
 - Transactions—As Chapter 1 discussed, PKI provides merchants with the ability to prove that a particular user engaged in a transaction in the merchant's store. If customers could select items and have them shipped, then later claim that the transaction never occurred, business on the Web would be problematic. PKI allows the merchant to prove that a certain user transmitted a certain transaction. Additionally, the user can be assured that the transaction took place with the merchant that the user intended to do business with.
 - Software—Ensures that files signed by the private key of a software vendor did in fact come from that vendor.

Most of the common PKI applications hinge on effective vetting by a third party, as the issuance of faulty or fraudulent certificates could have disastrous effects. If successful, the malicious party, for example, could impersonate a reputable vendor on the Web or even have signed viruses, Trojan-horse software, or other malware as having originated from a trusted software company. Many users will accept software updates or patches if they appear to be from legitimate sources.

 For more information about fraudulent digital certificates, see <http://www.computerworld.com/softwaretopics/software/story/0,10801,58857,00.html>.

To further illustrate the controls used during the validation of a certificate issuance request, let's look at two very popular certificate applications and contrast the information that maybe required by a CA to complete them.

Contrasting Validation and Verification Procedures

Many companies have leveraged intranets to act as a valuable information and resource repository for their employees. The intranet becomes such a part of daily operations that when users travel, they depend on remote access to the intranet to stay productive. A common approach is to make the intranet available to employees by creating VPNs through the public Internet. Certificates can help to alleviate many security concerns that arise when considering the prospect of making this information globally accessible to remote users. Namely, PKI can provide a credible means of proving that users attempting to access company resources are indeed employees of the company and are authorized to view or interact with the systems made available through the intranet. In addition, by offering SSL encryption, concerns of confidentiality and data integrity can be addressed.

Many CAs offer a commercial certificate product for intranet use. These products often feature a streamlined application process focused on quick turnaround. As a result of the reduced requirement for company authentication, as employees already trust their own company, the process instead focuses on command and control of the domain in question. The CA wants to be able to verify that the certificate requester is named by the company in a public record as having control over the domain for which the certificate is requested. This verification can often be performed with an automated search of a domain registrar's database.

It is important to note that if your organization has opted to use the private or anonymous registration features offered by some domain registrars, you will not be able to be automatically verified. This information must be publicly visible to be automatically checked. In addition, check to ensure that your CA differentiates intranet certificates that are visible via the intranet from internal-only intranets. Doing so will allow the CA to add another important control in the enrollment process. The additional check should be to verify that the host name or IP address of the host listed in the CSR designated for internal intranet use is not visible or publicly accessible from the Internet. A best practice of a CA is to check the IP address associated with the internal intranet host to make sure it falls within the specifications outline by the Internet Engineering Task Force (IETF) RFC 1918.


What Is the RFC 1918 Address Space?


The IETF is a standards body that creates proposed Internet standards through several working groups. The PKI standards were created by the PKIX working group at the IETF. RFC 1918 was created to allocate a range of IP addresses for internal organizational use. The addresses cannot be reached via the Web, as the routers on the Internet backbone know that they are not publicly routable. These addresses were reserved to encourage companies to conserve public IP address space by using a private IP address scheme behind their respective firewalls. The network allocations as outlined by the RFC 1918 include:


[10.0.0.0](#) - 10.255.255.255 (10/8 prefix)

[172.16.0.0](#) - 172.31.255.255 (172.16/12 prefix)

[192.168.0.0](#) - 192.168.255.255 (192.168/16 prefix)


 The complete text of RFC 1918 is available at <http://rfc.net/rfc1918.html>.

 The IETF can be found at <http://www.ietf.org/>.






 The PKIX working group at the IETF can be found at <http://www.ietf.org/html.charters/pkix-charter.html>

To request a commercial intranet (domain) authenticated certificate, you will need to create an email address or an email alias, which is an address that forwards all mail it receives to an existing email address that will act as an authorizing contact for certificate matters at your organization. Most CAs have established a predetermined list of authorizing contact email addresses that they want you to use. All future correspondence regarding your domain will need to use this address. If you are unclear as to what email address or alias to create, search the CA's site for a step-by-step registration or enrollment tutorial. If you can't find a document explaining the requirements for an authorized contact email address, you will need to call the CA to have your questions answered directly. Many CAs now offer online chat operators to answer these types of questions. Examples of predetermined email aliases include [webmaster@\(your-domain-name-here\).com](mailto:webmaster@(your-domain-name-here).com), [hostmaster@\(your-domain-name-here\).com](mailto:hostmaster@(your-domain-name-here).com), and [info@\(your-domain-name-here\).com](mailto:info@(your-domain-name-here).com). The key for many CAs is that the predetermined email address match an email address of a contact specified on the publicly visible domain registration.

You will need to generate a public and private key pair on the host on which you want to install your new certificate. To do so, it will be important to know which Web server software you are using. At the time of writing, Microsoft Internet Information Server (IIS) and the Apache Web server are the two most common Web servers in terms of actual visible installations on the Web. Microsoft's TechNet offers step-by-step instructions on how to generate key pairs and request certificates from commercial CAs as well as tutorials covering self-signed certificates for internal usage. The Apache project also has excellent online documentation for its HTTPD server that answers many of the common questions associated with setting up SSL and generation of key pairs.

 Both the public and private keys used to enable SSL functionality on your Web site will need to be created by your Web server software. The Web server software will also create a Certificate Signing Request (CSR), which you will present to the CA for them to sign with their own private key.

The private key generated by this process should be backed up immediately through a secure storage method such as a HSM or a protected disk or secure tape backup. Remember that if this key is ever compromised, so is the assurance associated with the site it protects!

-  More information about Microsoft IIS can be found at <http://www.microsoft.com/WindowsServer2003/iis/default.aspx>.
-  More information about the Apache Web server project can be found at <http://httpd.apache.org/>.
-  A report by Netcraft on the most common Web servers on the Web can be found at <http://survey.netcraft.com/Reports/0603/>.
-  Microsoft IIS TechNet articles are available at <http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/559bb9d5-0515-4397-83e0-c403c5ed86fe.mspx>.
-  Information about setting Apache HTTPD Version 2.2 servers for SSL can be found at http://httpd.apache.org/docs/2.2/ssl/ssl_faq.html#keyscerts.

Now you will need to generate a CSR on the Web server on which you will be installing the certificate. This process is also performed by your Web server software (see Figure 3.1). The CSR process will use the key pair generated in the last step. If you have questions about exactly how to configure your server to generate the CSR, check the references listed in the previous resource box for help with the Apache HTTPD and Microsoft IIS Web server software.

```

root@atlantis:~
[root@atlantis root]# openssl req -new -key www.mydomain.com.key -out www.mydomain.com.csr
Using configuration from /usr/share/ssl/openssl.cnf
Enter PEM pass phrase:
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:New York
Locality Name (eg, city) [Newbury]:New York
Organization Name (eg, company) [My Company Ltd]:My organization
Organizational Unit Name (eg, section) []:IS
Common Name (eg, your name or your server's hostname) []:www.mydomain.com
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@atlantis root]#

```

Figure 3.1: The CSR generation process on a host running the Apache HTTPD Web server.

As an alternative to wading through the potentially large amounts of technical documentation that came with your Web server software, you can look for help in the certificate enrollment guide from your CA. These guides tend to be targeted both at the specific software packages and the activities associated with the issuance process. If after consulting all these resources, you still need help, try pulling up your favorite search engine in your Web browser and entering the phrase “how to generate a CSR.” You will want to look for results from the domain name of your preferred CA first, as any CA specific instructions would be covered in their own documentation.

In most cases, the output of the CSR generation process will produce a text file of which the contents will look something like the example in the following sidebar (your characters will be different as the result of random key generation and your unique host information gathered during the CSR process).

What Does the Output of a CSR Look Like?

When your Web server software generates a CSR, it will generate the private/public key pairs that will be signed by the CA you have selected. To present this information to your CA, the Web server software will gather information such as the organization name and several other details that it will combine with the public key; it will then encrypt it all with the newly generated private key. This process produces an encrypted text blob that can be pasted directly into the CA's enrollment form. The CA then uses the public key in the blob to decrypt the contents of the CSR, and in doing so, verifies that you are in possession of the private key, as you used it to encrypt the whole CSR. The following example shows CSR output:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBzDCCATUCAQAwYsxHDAaBgNVBAMTE3d3dy50aGlzaXNhdGVzdC5jb20xCzAJ
BgNVBAYTAipBMRkwFwYDVQQIExBXZXN0ZXJlIFByb3ZpbmNIMRlwEAYDVQQHEWID
YXBIIFRvd24xEjAQBgNVBAoTCVRlc3QgQ29ycDEbMBkGA1UECxMSVGVzZdGluZyBE
ZXBhcnRtZW50MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDvzfmv7vJ9bOyQ
dxMLIgtDIEFz7MWsOUoZOPTq3qsTTXPW61q01jY8eQfs96I5xPjxALPeT4m74cce
UtYxldG7pLJiB3SGU94yvyvHDiyV+6mV/e++KWT2ql0Jv1emmobmAGdUxdx2pW9C
Epr0DmcVny6VGWAI36bG0NdYrNix4QIDAQABoAAwDQYJKoZIhvcNAQEEBQADgYEA
BfSHgDr9Vc460YG+IAiWuVWEife8B4QOojiV8oUxJJdqA2CEEmXLWfa7/mfUtd5
EQd6voLDT8axpXPbOrmwa3kzEZvQZhg+QvKEylfncqdWbDUK71tO0fVafBKwRQfE
73J/THmVABZuz9T6X3+KWGxGDiYw0sY3bE7OjBCwr14=
-----END CERTIFICATE REQUEST-----
```

When unencrypted by the CA, this example CSR contains the following information:

Server domain name:	www.thisisatest.com
Country code:	ZA
State / province:	Western Province
Town / city:	Cape Town
Organization:	Test Corp
Organizational unit:	Testing Department

The CSR process uses the private key to encrypt and sign the information collected during the CSR generation process, thus binding the key pair to the host. This request is what the CA will sign with its private key and incorporate into the certificate the CA issues to you following successful verification and validation of your credentials. This process is very similar to the process used by organizations that issue credentials such as a state driver's license and a passport. In this scenario, you must complete an application and supply credentials to prove your identity. Once the agency has been satisfied, it takes the information you supplied on the registration form and incorporates it into an official license and signs it with the credentials of the particular agency to, in essence, vouch for the information you have provided.

A very important and often-overlooked part of the CSR process is the designation of what is referred to in PKI as a common name. During the process of actually generating the CSR, you will be asked to fill in several information fields as (see Figure 3.2):

- Organization (O)
- Organizational Unit (OU)
- Country (C)
- State (S) (do not abbreviate)
- Locality (L)
- Common Name (CN)

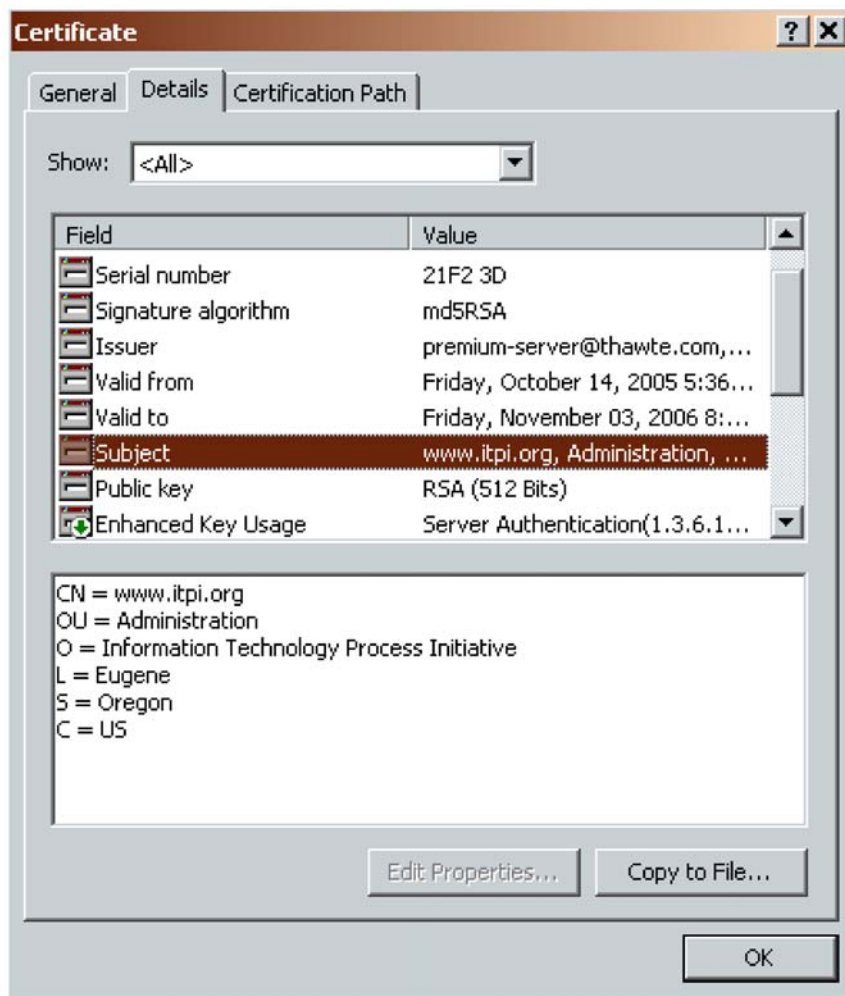


Figure 3.2: When on a site using SSL, double-click the lock symbol at the bottom of your Web browser and the certificate properties window will appear. By selecting the Details tab, you will see a list of fields present in the certificate. Select the subject field, which stores the value you entered during the process of generating your CSR.

The Common Name (CN) specification can be a bit tricky if you are new to generating a CSR. Typically, the common name is comprised of the host name that the CSR was generated on appended to the domain name `yourhostname.(your-domain-name-here).com` (see Figure 3.3). If the name you enter as the common name is just your domain name, your site visitors will likely receive a pop-up window alerting them that the actual secure site hostname you are logged onto is different than the name specified on the digital certificate. This message is hardly comforting, and users will often shy away from using a site that causes their browser to display warning messages. When specifying a common name for an internal-only facing intranet site, simply specify the host name by itself as one word. When it is external facing, you will need to use the hostname plus domain name format mentioned earlier. This format is often called a Fully Qualified Domain Name (FQDN), as it contains all the information an application would need to reach this host from the Internet (providing your DNS is set up correctly).

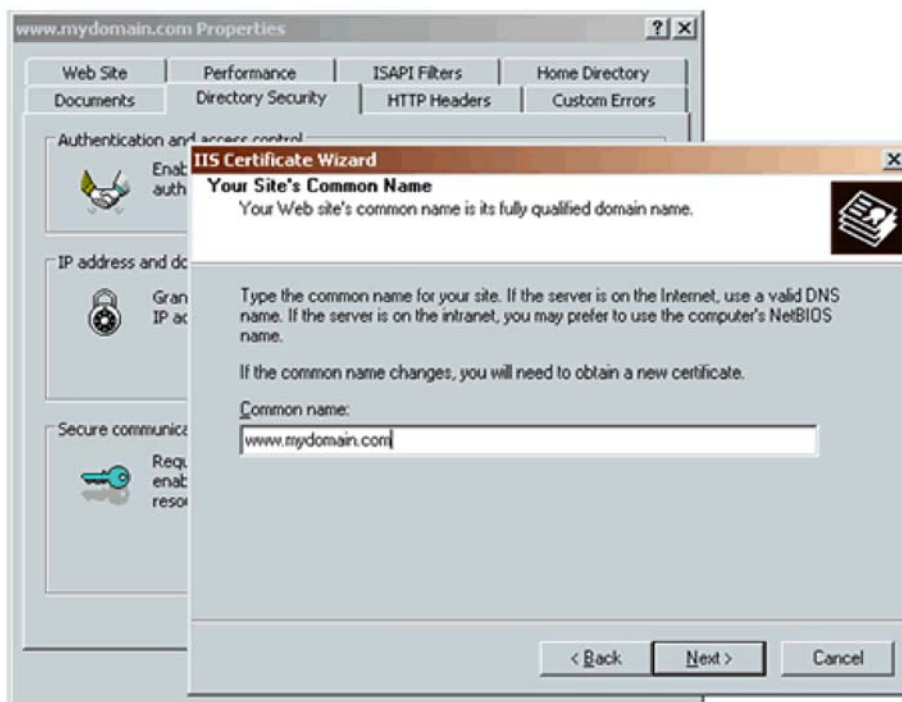


Figure 3.3: The Microsoft IIS Certificate Wizard prompts for the entry of a common name. Notice that the domain name `mydomain.com` is combined with a host name `www`.

Another piece of information that you will be prompted for is the location or *Geographic location* as it is sometimes called. This parameter refers to the state in which the organization resides. It is very important to spell out the state name completely rather than abbreviate it (see Figure 3.4). If you abbreviate the name of the state, your resulting certificate may not work.

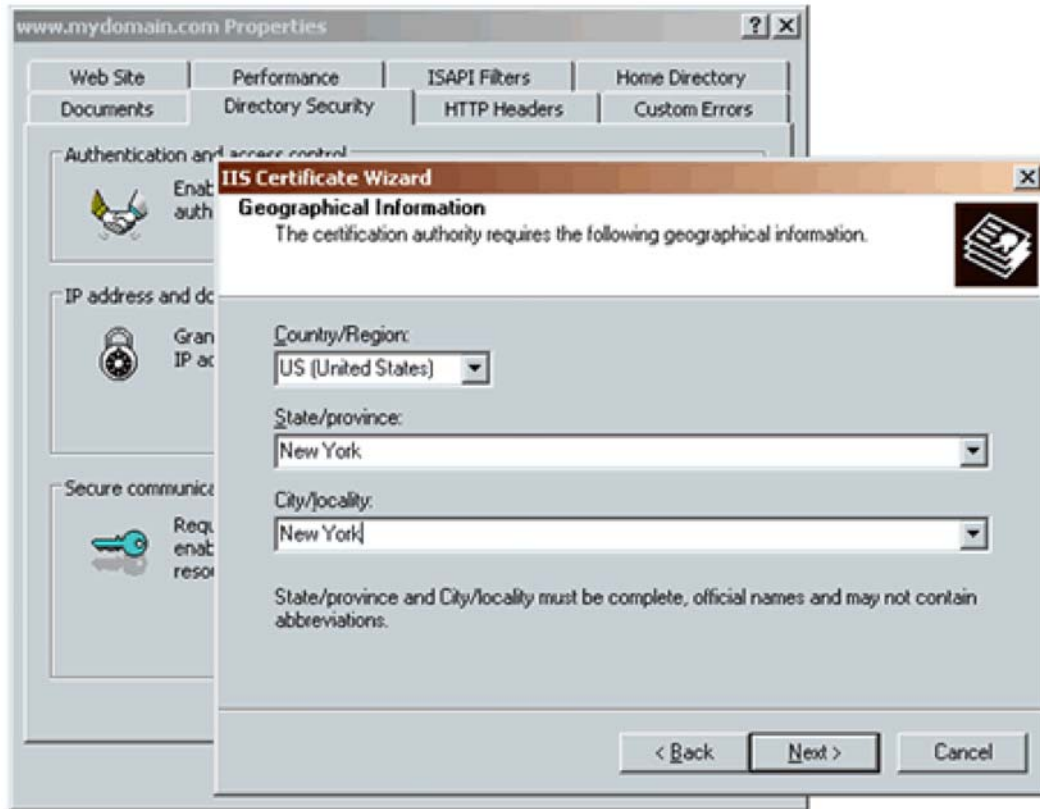


Figure 3.4: The Microsoft IIS Certificate Wizard prompting for location information during the generation of a CSR. Notice that the State New York is not abbreviated but spelled out completely. If you abbreviate your state name the resulting certificate may not function correctly.

Next, find the certificate enrollment or registration page for your chosen CA. Before you actually begin the enrollment process, check to determine whether the CA has an online CSR test page. A CSR test page will allow you to paste the contents of your CSR into a text box. You can then click a submit button and the page will display the contents of your CSR in readable text so that you can verify that the CSR contains all the correct information before you submit it.

Once you have generated your CSR and feel comfortable that it contains accurate information about your host and company, complete the online certificate application by completing the relevant contact information, designating an authorizing contact, selecting the certificate product you want, specifying the type of Web server software you are using on the host, and providing the number of host licenses you will need. Unless you are using a load balancer that is spreading server traffic across several Web servers, you will need only one host license. The final step in the enrollment process is to provide payment, which is usually done with a credit card.

Once the certificate has been processed by the CA, it will typically notify the authorizing contact via email that they can download the certificate. Typically, this download is done by providing a URL and a PIN code to be used as a login credential. Once the authorizing contact has logged in to the CA's site, the contact will be able to download the signed certificate.


Once the certificate is in the possession of the authorizing contact, they will need to follow the steps outlined in the documentation for the particular Web server software being used to install the certificate for the site. This point is a good time to verify that the methods used to back up and protect the corresponding private key have been effective.

Higher-Assurance Certificates

For domain authenticated certificates, most CAs verify that the person generating the CSR is authorized by the company listed as the owner of the domain to administer the domain and request certificates on behalf of the domain. For company-authenticated certificates, the CA needs to authenticate the right to administer the domain and the right to request and manage certificates on its behalf—but it needs to go much further. Make sure that your CA validates at least two and preferably three additional points.

For a high-level assurance certificate used for e-commerce transactions or code signing, read your CA's Certification Practice Statement (CPS) to ensure your CA checks the following points:

- Company name validation—Does the company actually exist and is it licensed to do business? Sometimes the CA will request copies of the articles of incorporation or other legal documents that vouch for the legitimacy of the company.
- Does the company have the right to use the domain name?
- Is the telephone number on the application linkable to a published company phone number? Some CAs will call a published number or send a letter through the postal system to verify that the certificate requester is a legitimate employee at the company and that they are authorized to request the certificate on behalf of the company.
- The CA must prove that the subscriber has a legitimate copy of the private key associated with the public key included in the CSR. In most cases, the CA will spell out this method in its CPS. Often, for security reasons, the description of exactly how a CA does this may be a bit vague and open-ended.
- Make sure that your CA splits the authentication and verification duties in their company by examining the CPS section that spells out separation of duties policy. A good application of this process is to have one CA staff member authenticate the domain and the right to control the domain by the authorizing contacts listed on the certificate application. This task can be performed by pulling up the domain information using a service called Whois at the Internic (see Figure 3.5). Verification would then be handled by another CA staff member and should entail calling the organization listed in the certificate application and verifying that the authorizing contact is both employed by the organization listed and that the listed contact has the right to request and manage certificates on behalf of the organization. If both the authentication and verification processes determine that everything checks out, the certificate application will be approved as long as the CSR is valid.

 The Internic Whois domain query tool can be found at <http://www.internic.com/whois.html>.

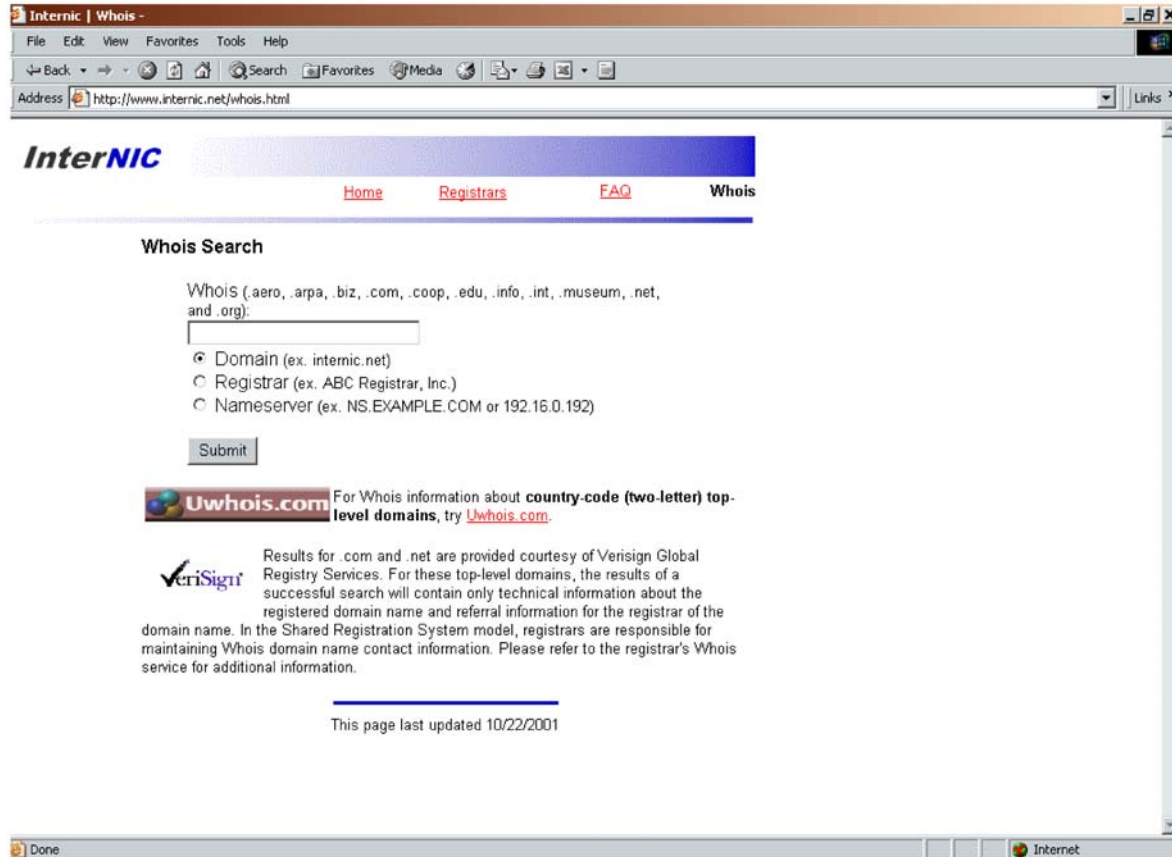



Figure 3.5: The InterNIC Whois domain query tool.

Managing Multiple Certificates

Many CAs offer solutions for the organization that needs to manage multiple certificates. Even relatively small organizations that start out with a single Web server and just need a single certificate find themselves in the position of having multiple servers and thus the need to manage multiple certificates in short order. If your venture is successful, it makes sense that you will need to scale your infrastructure.


Many Internet Service Providers (ISPs) and Managed Service Providers (MSPs) manage large server and network infrastructures that require management of digital certificates. In these types of arrangements, service providers are looking to add value to their existing lines of business by assuming the management of the certificate lifecycle for their client base.

 The next chapter will take a close look at the decision process around outsourcing PKI lifecycle management and whether managing certificates in-house makes sense for your organization.

If you find that you need to manage multiple certificates, most commercial CAs offer a multi-certificate management service. This service can be useful for many reasons:

- If you want a consolidated view of all certificates in your possession—complete with expiry and host information.
- If you want to receive the best volume pricing on all your certificate purchases.
- If you want the ability to request certificates on your clients' behalf.
- If you want expedited turnaround time from the CA on all certificate requests.
- If your clients want you to manage everything for them including the CSR and enrollment process.

A key benefit with these programs is that they require validation and verification up front, which once completed, permits authorized account users to request certificates with significantly reduced issuance times based on the initial authentication. It is also usually possible to add domains to your account at any stage, with the CA performing the necessary authentication procedures in each instance. Be sure to carefully read the subscriber agreement for these types of product offerings. It is a good idea to develop a permissions hierarchy for all staff involved in the process that dictates exactly whom will be responsible for managing requests and approvals for certificates. In some cases, extra staff might be required to create a workable separation-of-duty schema. Processes such as change and configuration management will need to be reviewed to make sure they adequately address the increased risk associated with handling sensitive customer information such as private keys. A look at your organization's privacy policy may be in order due to brokering contact- and security-related information on behalf of your clients—not to mention the special infrastructure you may need for the backup and storage of private keys for your clients. Physical security may also be a concern for this additional infrastructure.

 It is a best practice to have any agreements that legally bind you or your organization analyzed by your legal counsel to make sure you are not biting off more than you are willing to chew contractually.

Re-Issuance

Once you have secured and installed your certificate, there are several scenarios that might occur that cause the need for a re-issuance of the certificate. One of the most common is the loss of the private key. Make sure that your CA will re-authenticate your request from scratch in the event of a private key loss. Otherwise, it will be much easier for people with malicious intent to hijack your certificates. The extra steps involved in re-authentication and verification are trivial compared with the damage that can come from an unauthorized party controlling your private key.

Other situations that might necessitate a re-issuance are changes to the version of your Web-software, contact information, or the hostname of the server housing the certificate. Any changes required to the information in the CSR will most likely trigger re-authentication and verification processes as well. It is important to plan for the time that these processes may consume when considering changes to any of these parameters. The CA will not operate on your timetable for verification. Most likely, the re-issuance process will go smoothly, but make sure you have carefully planned for these types of changes and have allowed for potential time delays if your request will require re-authentication and verification. When considering a CA, be sure that you understand what triggers the need for re-authentication. It pays to inquire up front and have a full understanding of your CAs practices. This information is available in the CPS published by all commercial CAs. If it is difficult for you to understand the rules and practices your CA has outlined in the CPS, by all means, engage a sales support person directly and get answers to your specific questions. If after talking directly with the CA you still have confusion, you might want to look at the policies of another CA to determine if they are more inline with your expectations.

Expiry

With all the work required to properly authenticate and verify digital certificates, some people may ask “Why even have an expiration date?” Certificates expire in order to allow companies to manage risk over time. By forcing periodic re-authentication and verification, the PKI is continually cleansing itself of outdated or outmoded information that could be used to increase risk of key theft or key revocation due to inaccurate information in the certificate. The same logic used for state- or country-issued credentials such as drivers licenses and passports apply. By periodically forcing all certificate subjects to re-prove their identity and having that information verified, both the CA and the certificate are subject to reduced risk of fraud. It is very important to understand your CA’s policy with regard to expiry in order to minimize the risk associated with unexpected termination of your certificate and to understand what the timeline of a potential certificate renewal may look like.

Most CAs offer both a 1-year and 2-year certificate product. The 2-year pricing is usually more attractive and should be considered. The main reason is less administrative overhead on your team’s part. When you factor in that the 2-year option is cheaper and requires less work, it is usually the best route to take.

Renewal

When submitting your first certificate request, renewal is a distant thought. But to prevent costly outages and prevent your clients from getting scary messages about your certificate being expired, schedule your renewal the instant you complete the issuance process.

I wish I had a dollar for every horror story I have heard from systems administrators about unknowingly letting domains and certificates expire. Even with the auto-notification emails used by most CAs and registrars, domains and certificate renewal often get put off to the last minute. It is both embarrassing and costly in many cases to let a certificate expire. When your users pull up your secure Web site and are about to pay for their goods, they will see an ugly message from their Web browser telling them that your certificate has a problem and that the date is no longer valid. The user will be presented with the option of choosing to trust the certificate in spite of its date. Many users will not choose to trust an outdated certificate. This situation sends out the message that the site is not well managed—not to mention that it may have been compromised!

Many IT organizations depend on a change management process to protect their critical services from interruption and security breaches from risky unauthorized changes. Typically, the change management process handles the approval and scheduling of IT infrastructure changes. This scheduling is often committed to a master calendar, which serves many purposes. Primarily, it acts as a control to deter change-related collisions and to notify users of changes that may affect them.

One effective way of making sure that certificate renewal does not get lost in the operational shuffle is to put in a change request for the certificate renewal and schedule the work to be done 1 or 2 months prior to the certificate expiry date. This method eliminates the need to put the reminder for renewal in an individual's schedule or task list.

Another effective method is to leverage a Configuration Management Database (CMDB) as spelled out by the standard for IT service management, the IT Infrastructure Library (ITIL). The CMDB is designed to contain all relevant information about the IT infrastructure and its relationships and dependencies. This database is not limited to hardware and software; it also may contain documentation, policy and procedure information, and depictions of network and security architecture.

 The ITIL is a registered trademark of the United Kingdom Office of Government and Commerce. More information can be found at <http://www.itilpeople.com/>.

In my tenure as CTO and CIO at several organizations, I have used a CMDB to keep track of important information about domain and certificate expiry. A simple report run on a daily basis can illuminate which domains and certificates need to be renewed long before a crisis is looming.

Integration of renewal with change management and configuration management processes can also alert authorizing contacts to changes that might need to be made to the certificate itself. It is very important to understand what types of changes your CA will allow to your renewal. A good CA will have firm boundaries around exactly what can and cannot be changed under the renewal process. For example, you should not be able to change any details contained in the CSR. Details such as contact information, the email address of the authorizing contact, or the business contact can be changed without the need for re-issuance. These changes may trigger validation and verification efforts to provide assurance that your certificate is not being hijacked by an unauthorized party.

If any of the details in the CSR must change, re-issuance rather than renewal will be required by your CA. Most likely, your CA will then need to re-authenticate and re-validate your information. This can add time delay to the process—especially if there is inaccurate information in your original certificate request.

Renewal is also a perfect time to consider the quality of service your CA has provided you during your subscription period. Have you been satisfied with their performance? Were they available to answer your questions in a reasonable timeframe? In today's global economy, you might find that you are dealing with a company an ocean away. Do they have support hours that match your region or time zone and native language? It is important to look at their offering in light of new products and pricing from other vendors. Are their prices and service quality in line? If not, consider switching to another CA. I highly recommend checking for changes and updates to both the subscriber agreement and CPS to determine whether you have gained or lost any rights or assurances that might be important to you.

Revocation

Why do you need revocation? If your private key is somehow compromised, you would want it revoked. If your organization is found to be engaged in illegal activities, your key will be revoked for you. Despite all the best practices and best efforts of your staff and the fully vetted, background-checked dedicated team at your CA, mistakes can happen. When they do, it is good to know that there is a way to stop a bad certificate from deceiving non-suspecting relying parties. The revocation concept is not new. Most state and federal law enforcement agencies have databases of credentials such as state issued driver's licenses. They can run the numbers against the database to make sure the license hasn't been altered and is in good standing. Credit card companies use the same principle to prevent stolen or missing credit cards from being used once their disappearance has been reported.

In PKI, these lists are called Certificate Revocation Lists. A CRL is a signed, time-stamped blacklist of revoked but unexpired certificates and is issued by a CA periodically (usually daily). CRLs are a commonly recognized standard (as spelled out in the X.509 RFC) and are deemed by many organizations as acceptable for use in non-online or low-value commercial applications. The largest issue for security-sensitive organizations is that the data might not be current enough if the CA publishes the list only once a day. The other main issue with CRLs is that they can become impressively large and unwieldy over time. To address the size issue, the Delta CRL mechanism, which only contains the changes since the last CRL was issued, was developed.

The CRL Distribution Point (CDP) mechanism was established to tackle the issue of large list sizes by partitioning the CRL into relevant PKI communities. CDP partitions have their own designators or pointers that are embedded in the certificate so as to point the query to the correct CRL partition.

In the financial services world in which large transactions such as funds transfers require an online check of the certificate's status as of that exact moment, the Online Certificate Status Protocol (OCSP) was developed. OSCP has since become the successor to CRL; although many Web browsers still use CRL, it is commonly disabled by default. As new releases of Web browsers become available with OSCP enabled, it will completely replace CRL. OCSP was enabled to allow for nearly instantaneous checking of a certificate's real-time status with a digitally stamped and signed result making it suitable for high-value/high-assurance transactional scenarios. One downside to OCSP is its performance. Due to the fact the requests are happening in real time and the results must be stamped and signed by the CA, the performance can fluctuate greatly and can be problematic for Online Analytical Processing environments or high-volume commerce. When choosing a PKI provider, ask questions about their investment in the OSCP infrastructure. Have they built their plans around OCSP becoming the standard or have they built their infrastructure to support the older standard and have adopted a wait-and-see approach with OSCP? Like CRL and CDP, OCSP was also spelled out by the PKIX working group at the IETF and is part of the X.509 standard.

Summary

This chapter has covered a lot of ground, starting with issuance and working to revocation. Along the way, it covered best practices that will speed you along the certificate application process and help you obtain a certificate that will function seamlessly for your end users. Answering the question "Just how do you generate a CSR?" allowed for a look at the CSR and what it contains. The chapter revealed that you as the certificate subscriber are responsible for generating the public/private key pair that the CA will ultimately verify, validate, and sign with the CA's private key.

Tools such as online multi-certificate management programs from CAs were presented as a potentially effective solution for managing certificates for multiple clients or for a single-user multi-certificate environment. This chapter made sure to tip you as to what changes could be made in the re-issue and renewal processes that wouldn't require you to be re-validated and re-authenticated to avoid introducing additional delays in the process.

The next chapter will look at whether it makes sense to outsource PKI functions to PKI service providers. It will also examine the enterprise CA model to determine whether there is any benefit to becoming your own CA and issuing your own certificates for your employees and internal applications. With all the flexibility that being your own CA offers, there is a major tradeoff in complexity. But not to fear, the chapter will cover the processes controls and key practices you will need to know to make an informed decision.

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>.