How to Install SSL Certificates on Microsoft Servers

Realtime
publishers

Dan Sullivan

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

Chapter 1: Getting Started with SSL Certificates in Windows

We are constantly making use of SSL certificates, although we may not appreciate the frequency. When we navigate to a site using HTTPS, we are making use of an SSL certificate. When we encrypt a message to send to another party, we are depending on an SSL certificate. When we install software that has been signed by a trusted source, we are once again making use of SSL certificates. Their prevalence in IT environments indicates just how valuable they are in a number of applications. It is not surprising that sooner or later, many systems administrators, application managers, and other Windows professionals need to install and manage SSL certificates.

This book is designed to help you understand how to select an SSL certificate, install it in a Windows environment, manage multiple certificates, and use them with specialized applications, such as the SQL Server relational database. The guide is organized into four chapters.

This chapter starts with an assessment of why you would need an SSL certificate. Typical reasons include server authentication, client authentication, encryption, and code signing. The chapter also discusses how to choose among different types of SSL certificates, such as self-signed, third-party, and extended validation third-party certificates.

Chapter 2 delves into how to use the Microsoft Certificate Store. The Certificate Store is a central management tool for SSL certificates, and this chapter describes how to use it to add, remove, export, and renew certificates in a Windows environment.

Chapter 3 describes how to install SSL certificates in Internet Information Server (IIS) servers. IIS servers often deploy SSL certificates for server authentication. This gives users of the server evidence that they are actually using the server they think they are and not a spoofed or fraudulent server that only looks like a legitimate IIS server.

Chapter 4 describes how to install SSL certificates in other Microsoft applications that can make use of them: Microsoft Exchange Server, Microsoft SharePoint Server, and Microsoft SQL Server. All of these servers can provide essential functions to multi-tiered applications and distributed workflow. Application users need assurance that they are working with the correct servers, and SSL certificates for server authorization can do that. SSL certificates also support encrypted communication, which is essential for many business processes that make use of email, collaboration services, and relational databases.

This is a how-to guide. The goal is to provide you with the details you need to acquire, install, and maintain SSL certificates in a Windows environment. This book is not a guide on the theory behind SSL certificates, so there will be no long digressions on public key cryptography or on the business strategy for enterprise-level management of SSL certificates. These are valid and relevant topics; they are just outside the scope of this book.

Additional Resources on SSL Certificates

For the interested reader, there are several free SSL certificate resources that address topics we will only briefly touch on in this guide. See, for example, *The Shortcut Guide to Certificates in the Enterprise*, *The Shortcut Guide to Business Security Measure using SSL*, *The Shortcut Guide to Extended Validation SSL Certificates*, and *The Shortcut Guide to Subject Alternative Name Certificates*.

Although this book does not describe background information in great detail, it is not simply a rehash of operating system (OS) or application documentation. This guide is written from the perspective of someone who works in a Windows environment every day. It is written for someone who probably has responsibility for a mix of clients and servers, running some mix of Windows 7, Windows Vista, and Windows XP on the client side and various versions of Windows Server on the server side. Someone working in that kind of environment cannot simply work with a cookie-cutter guide that describes a complex process with a series of "Click here," "Select option," and "Enter password."

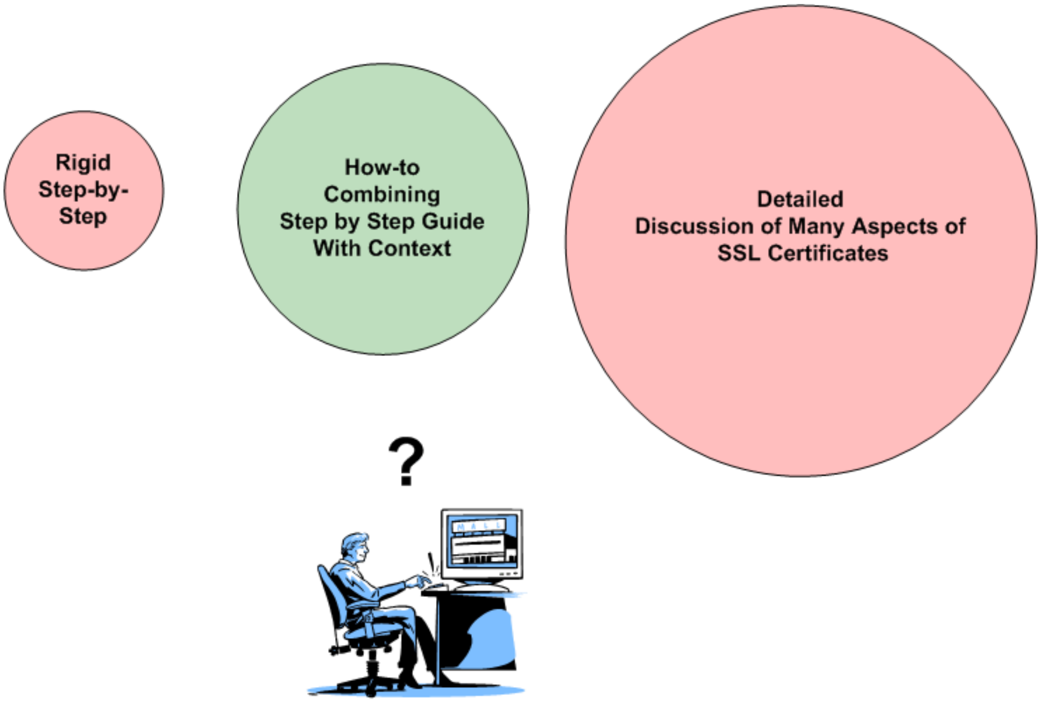

Rigid Step-by-Step
How-to Combining Step by Step Guide With Context
Detailed Discussion of Many Aspects of SSL Certificates
?

Figure 1.1: Step-by-step instructions tend to be brittle and break when dealing with different versions or configurations. Too much information slows the task at hand. The ideal how-to guide finds the balance between the two.

This book strikes a balance between too little and too much information. At one end of the spectrum, we have guides that do not provide the reader with enough background information to help adapt to slightly different requirements or troubleshoot when results are not identical to those in the guide. At the other end of the spectrum, we can delve too deeply into issues such as why is one encryption algorithm better than another for a given set of requirements.

This chapter is organized around several key tasks you need to do to start working with SSL certificates in the windows environment. They are:

- Knowing your reasons for using SSL certificates
- Acquiring an SSL certificate
- Choosing an SSL certificate
- Gathering the information needed to create an SSL certificate
- Generating a certificate signing request

It is often tempting to jump right into the technical details of a new project, but it pays to understand the business requirements driving the project. The same holds true for installing and managing SSL certificates.

Know the Reasons for Using SSL Certificates

It may seem obvious, but we need to start by understanding why you need an SSL certificate. There are different uses for SSL certificates, and you should be clear which of the reasons applies to you. The three main uses for SSL certificates are:

- Authentication
- Encryption
- Code signing

How we will use a certificate will influence what type we will use and how many we will need, which will ultimately determine the total cost of providing those certificates.

Authentication

SSL certificates for authentication are a means for assuring the identity of a device or a person. (We are not discussing personal SSL certificates here, however). This kind of assurance is useful for both server and client devices. In the case of servers, users want to know that they are dealing with a legitimate server and not a fraudulent server set up to steal credentials or perpetrate a scam.

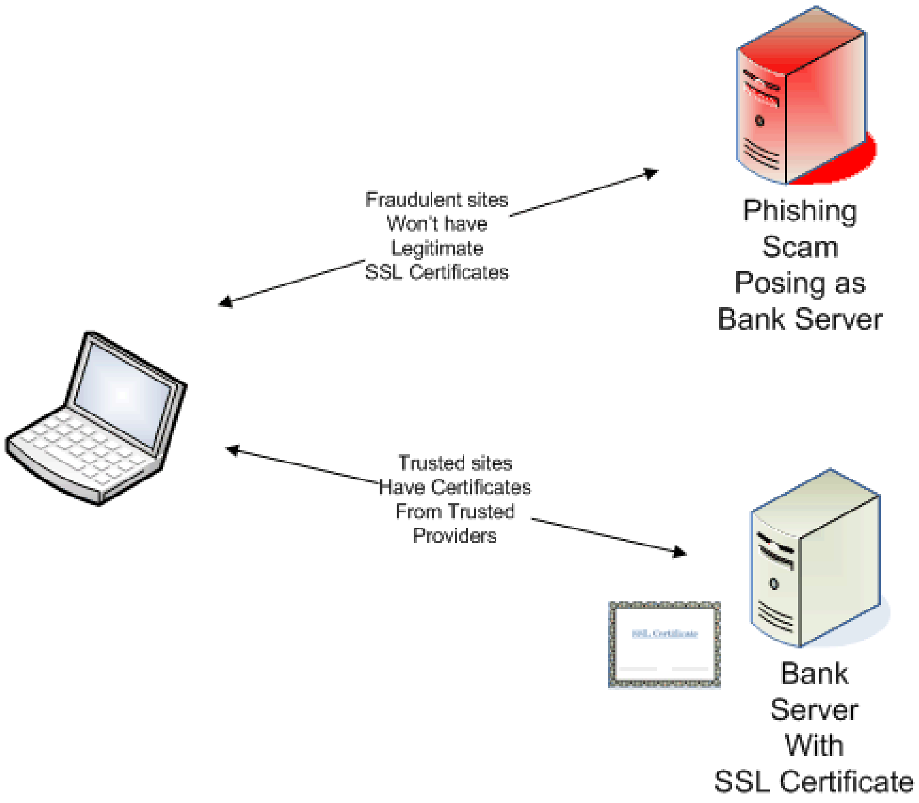


Figure 1.2: Servers are authenticated with SSL certificates that are provided by trusted third-party SSL certificate providers. Servers used in scams might have an SSL certificate but it will either (1) not be from a trusted source or (2) not have details of a legitimate business.

Certainly online banking and other commerce customers will want to know they are dealing with servers of legitimate businesses. There are times when businesses will want to know who they are dealing with as well. Banks and online retailers can authenticate users with account numbers, passwords, and credit card information. That is sufficient for many types of transactions but not all. For example, consider a remote laptop that is trying to connect to a company's network and use that company's compute and storage services. Prudent network and systems administrators are going to want to make sure that laptop is a trusted device. SSL certificates for client authentication do just that.

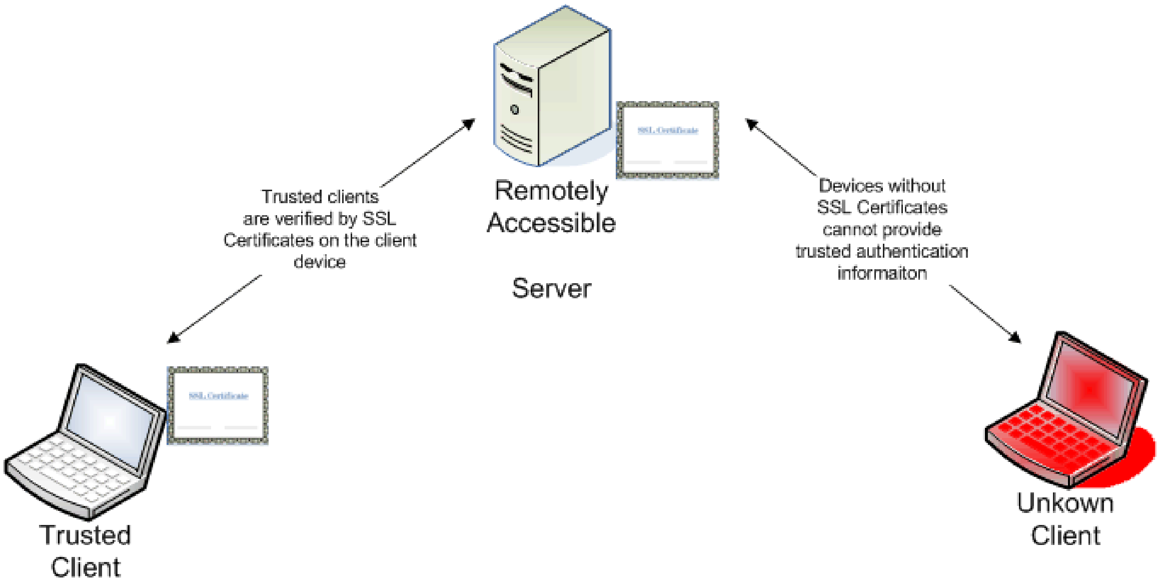
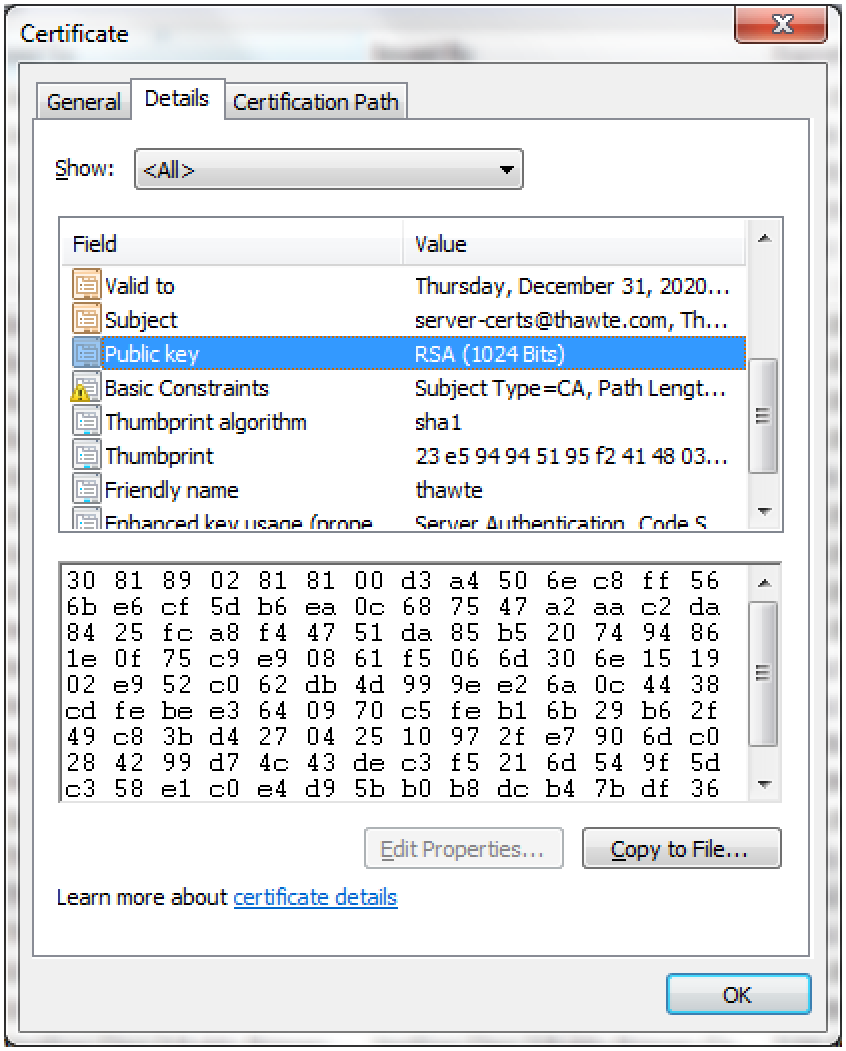

SSL Certificate
Remotely Accessible
Server
Trusted clients are verified by SSL Certificates on the client device
Devices without SSL Certificates cannot provide trusted authentication informaiton
SSL Certificate
Trusted Client
Unkown Client

Figure 1.3: A client device authenticates to servers with SSL certificates.

Encryption

SSL certificates allow us to send information between devices in an encrypted form. One of the challenges with encryption is managing keys used to encrypt data. Without going into too many details, SSL certificates help with this because they include a public key. Anyone who wants to send the holder of that certificate encrypted information can use that key.

If we need to ensure our communications remain confidential, we will want to encrypt them. This is such a common requirement that encryption is embedded into frequently-used Internet protocols. When we use the HTTPS protocol, we are using encryption thanks to an SSL certificate. When we transfer files securely using encrypted protocols, we are making use of SSL certificates.



Field	Value
Valid to	Thursday, December 31, 2020...
Subject	server-certs@thawte.com, Th...
Public key	RSA (1024 Bits)
Basic Constraints	Subject Type=CA, Path Lengt...
Thumbprint algorithm	sha1
Thumbprint	23 e5 94 94 51 95 f2 41 48 03...
Friendly name	thawte
Enhanced key usage (prope	Server Authentication, Code S

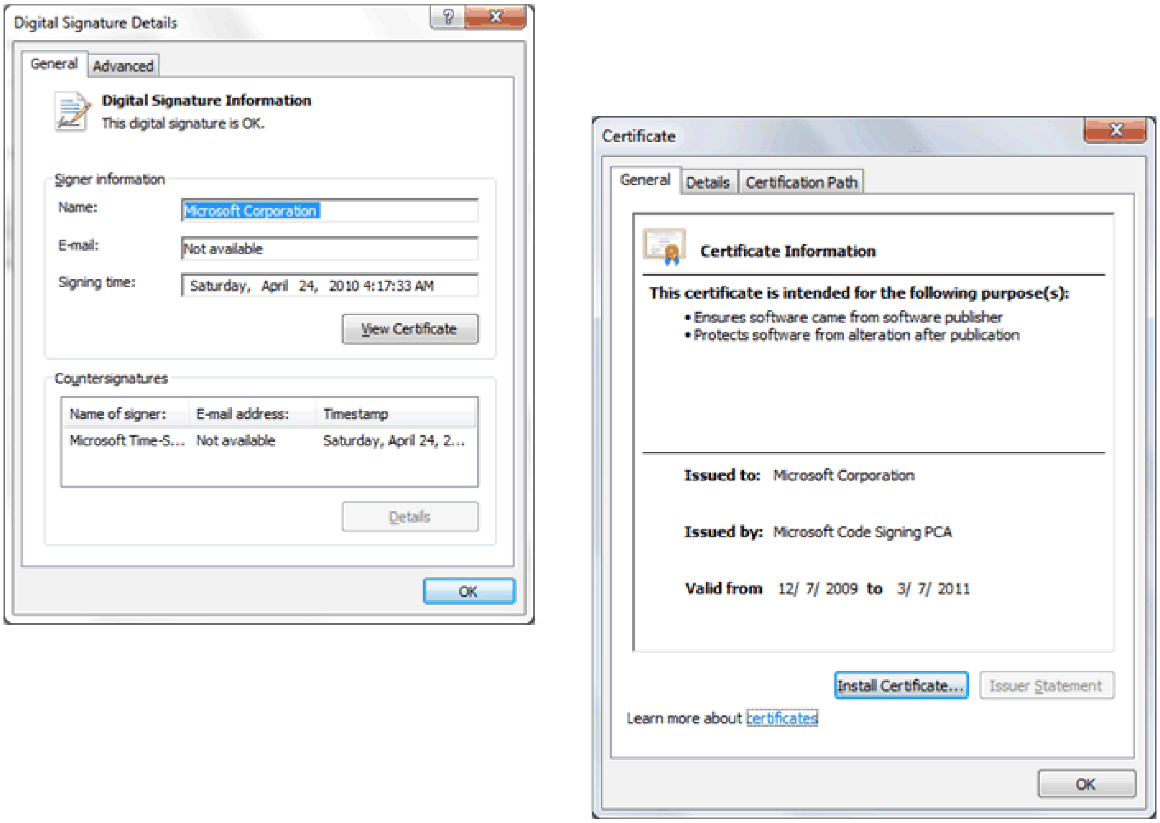
```
30 81 89 02 81 81 00 d3 a4 50 6e c8 ff 56
6b e6 cf 5d b6 ea 0c 68 75 47 a2 aa c2 da
84 25 fc a8 f4 47 51 da 85 b5 20 74 94 86
1e 0f 75 c9 e9 08 61 f5 06 6d 30 6e 15 19
02 e9 52 c0 62 db 4d 99 9e e2 6a 0c 44 38
cd fe be e3 64 09 70 c5 fe b1 6b 29 b6 2f
49 c8 3b d4 27 04 25 10 97 2f e7 90 6d c0
28 42 99 d7 4c 43 de c3 f5 21 6d 54 9f 5d
c3 58 e1 c0 e4 d9 5b b0 b8 dc b4 7b df 36
```

Figure 1.4: SSL certificates include a number of properties, including a public key that can be used to send the holder of the certificate encrypted data.

Code Signing

We want to trust the servers we connect to but we also want to trust the software we install on our devices. Code signing is a method by which software developers acquire SSL certificates from a trusted third party and associate those certificates with their application. If we trust the third party that signed the SSL certificate, we can trust that the software provider listed on the certificate actually produced the code. Of course, an SSL certificate is only used to validate the origin of the software, not the quality.

Software developers are the primary users of code-signing SSL certificates. Systems and application administrators are more likely to require SSL certificates for authentication and encryption. As the latter is the focus of this how-to book, we will concentrate on those uses for the rest of this guide.



Digital Signature Details

General | Advanced

Digital Signature Information

This digital signature is OK.

Signer information

Name: Microsoft Corporation

E-mail: Not available

Signing time: Saturday, April 24, 2010 4:17:33 AM

View Certificate

Countersignatures

Name of signer:	E-mail address:	Timestamp
Microsoft Time-S...	Not available	Saturday, April 24, 2...

Details

OK

Certificate

General | Details | Certification Path

Certificate Information

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

- Ensures software came from software publisher
- Protects software from alteration after publication

Issued to: Microsoft Corporation

Issued by: Microsoft Code Signing PCA

Valid from 12/ 7/ 2009 **to** 3/ 7/ 2011

Install Certificate... | Issuer Statement

Learn more about certificates

OK

Figure 1.5: Applications can be signed with SSL certificates to authenticate the software vendor or other group that produced the application.

The first step to working with SSL certificates is to understand what the certificates are used for. SSL certificates are fundamentally about trust. We trust third-party providers to verify the identity of servers, Web sites, software developers, and others. We trust servers that hold SSL certificates from trusted providers. We trust software when we can verify it comes from a trusted application developer. When you want customers, users, business partners, or others to trust your services, it's time to get SSL certificates.

Steps to Acquiring an SSL Certificate

Acquiring an SSL certificate is a multi-step process. It begins with identifying the purpose of the certificate followed by determining the best type of SSL certificate for your needs. Although all SSL certificates are fundamentally similar, there are important differences in the level of trust users are likely to have in the various types.

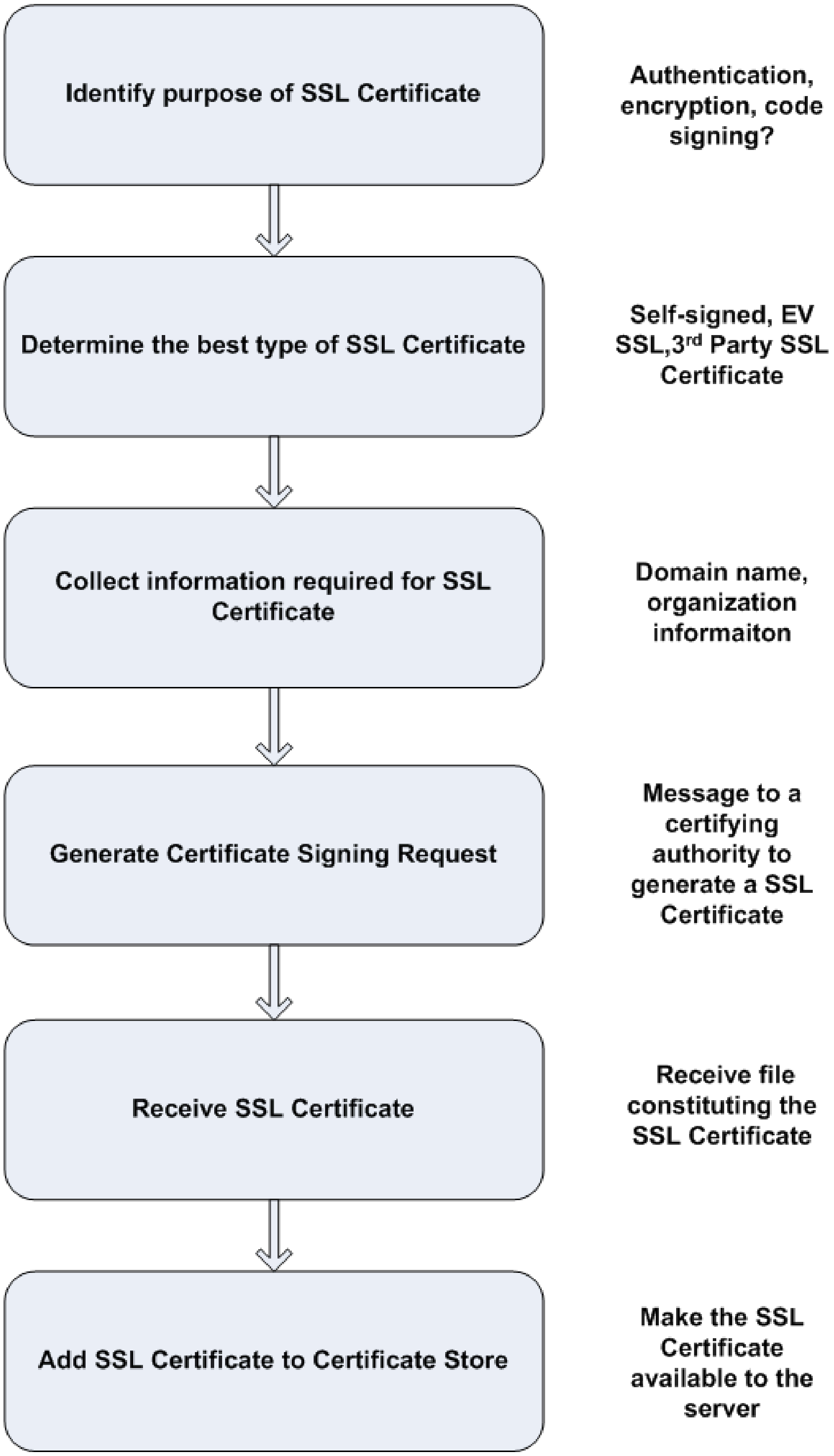

Identify purpose of SSL Certificate
Authentication, encryption, code signing?
Determine the best type of SSL Certificate
Self-signed, EV SSL,3rd Party SSL Certificate
Collect information required for SSL Certificate
Domain name, organization informaiton
Generate Certificate Signing Request
Message to a certifying authority to generate a SSL Certificate
Receive SSL Certificate
Receive file constituting the SSL Certificate
Add SSL Certificate to Certificate Store
Make the SSL Certificate available to the server

Figure 1.6: Steps to acquiring an SSL certificate.

In the next section, we will discuss, in detail, the different types of SSL certificates and the advantages and disadvantages of each.

After we have determined the appropriate type of certificate, we need to collect the necessary information to generate the certificate. With that information, we can generate a message to a certifying authority. This message, known as a certificate signing request (CSR), is highly structured and allows a certifying authority to create an SSL certificate. The certificate is then sent from the certifying authority to the requestor in the form of a structured file. The file is imported into the Microsoft Certificate Store where it is managed from there as needed. Assuming we have determined we need an SSL certificate for authentication and encryption and not code signing, we proceed to choose one of three types of SSL certificates.

Choosing a Type of SSL Certificates

There are different types of SSL certificates in the sense that some are generally more trusted than others. All SSL certificates are the same in terms of their structure and function. For example, SSL certificates have common attributes:

- Common name of the party holding the certificate
- Common name of the party issuing the certificate
- Valid date range
- Public key algorithm
- Public key
- Certificate signature algorithm
- Certificate signature value

If the basic nuts and bolts of certificates are all the same, why do we care about which certificate we use? The answer is that there are tradeoffs and, not surprisingly, cost is one of those factors.

The three types of certificates we're considering are:

- Self-signed
- Standard third-party SSL certificates
- Extended validation (EV) SSL certificates

Each has different levels of verification associated with it. The greater the verification, the greater the costs.

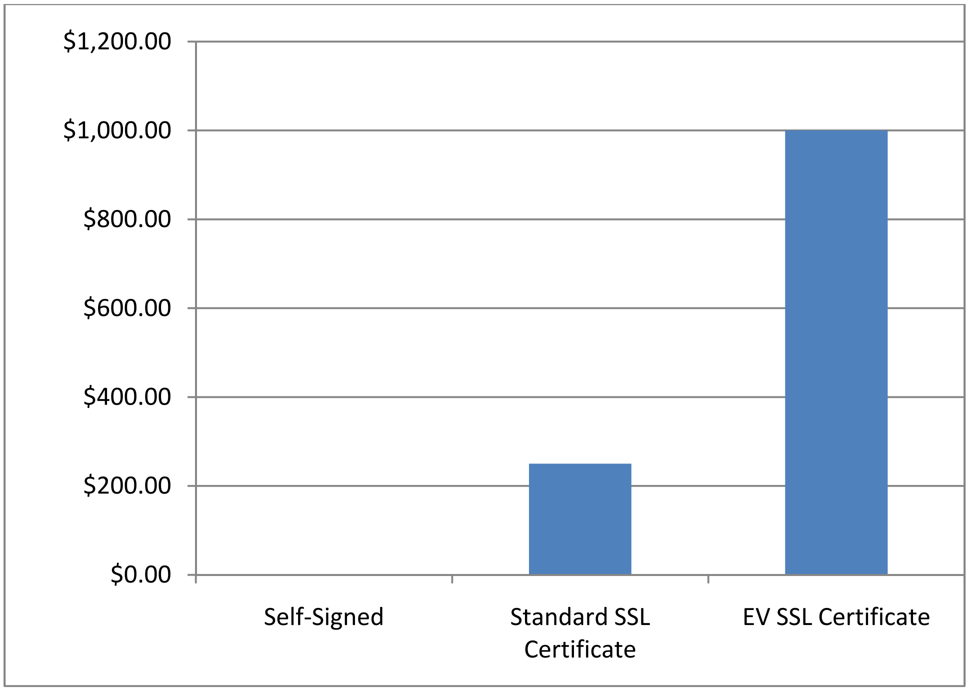


Figure 1.7: Relative costs of different types of SSL certificates.

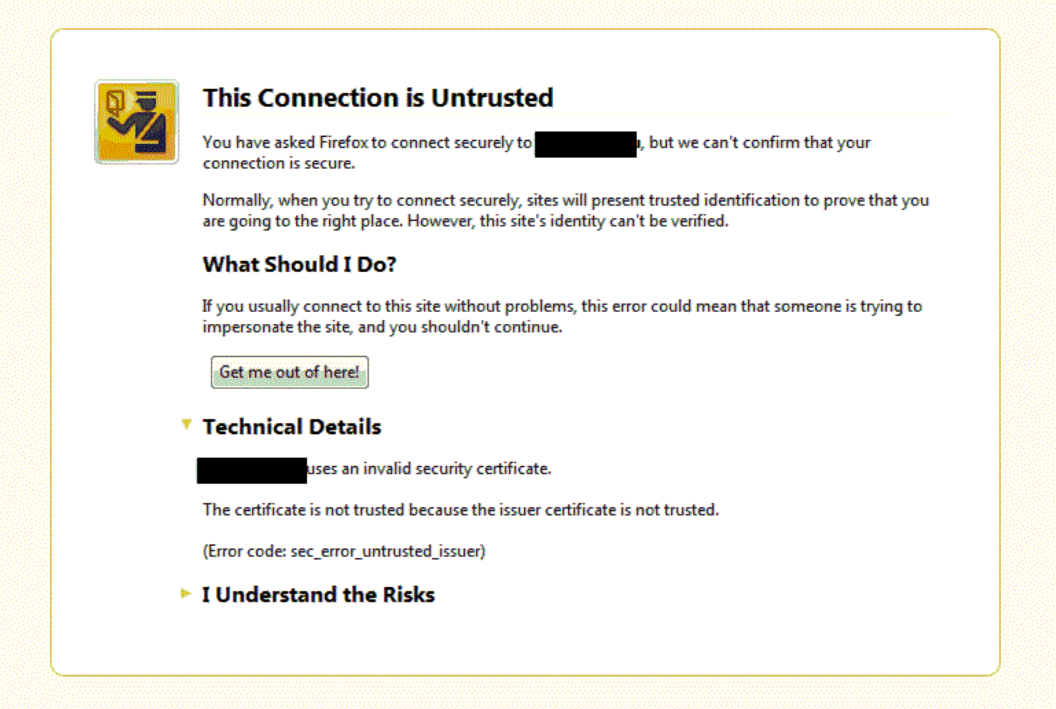
SSL certificates have information about two parties: the party to whom the certificate is issued and the certifying authority. The certifying authority is the organization that vouches for the truthfulness of the information contained in the certificate. The organizations that offer certifying authority services have an obvious vested interest in protecting their reputation. They will take care to verify the information included in the certificates that they issue. As a general rule of thumb, the greater the effort required to verify information, the greater the costs.

Self-Signed Certificates

Self-signed certificates are the least costly of the three types we consider. As the name implies, the certifying authority is the same as the issuer. In other words, we vouch for ourselves when we generate self-signed certificates.

The advantage of self-signed certificates is that we can generate them ourselves. There are several tools readily available for generating self-signed SSL certificates in Windows and other platforms. For example, the commonly used OpenSSL package and the IIS 6.0 Resource Kit both include programs for generating this type of certificate.

Self-signed certificates are free and easy to generate. How can you beat that? The drawbacks stem from the fact that SSL certificates generate trust with users because we trust the certifying authority. Browsers typically warn users when a site uses an SSL certificate that is not signed by a known, trusted certifying authority.



This Connection is Untrusted

You have asked Firefox to connect securely to [redacted], but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

Technical Details

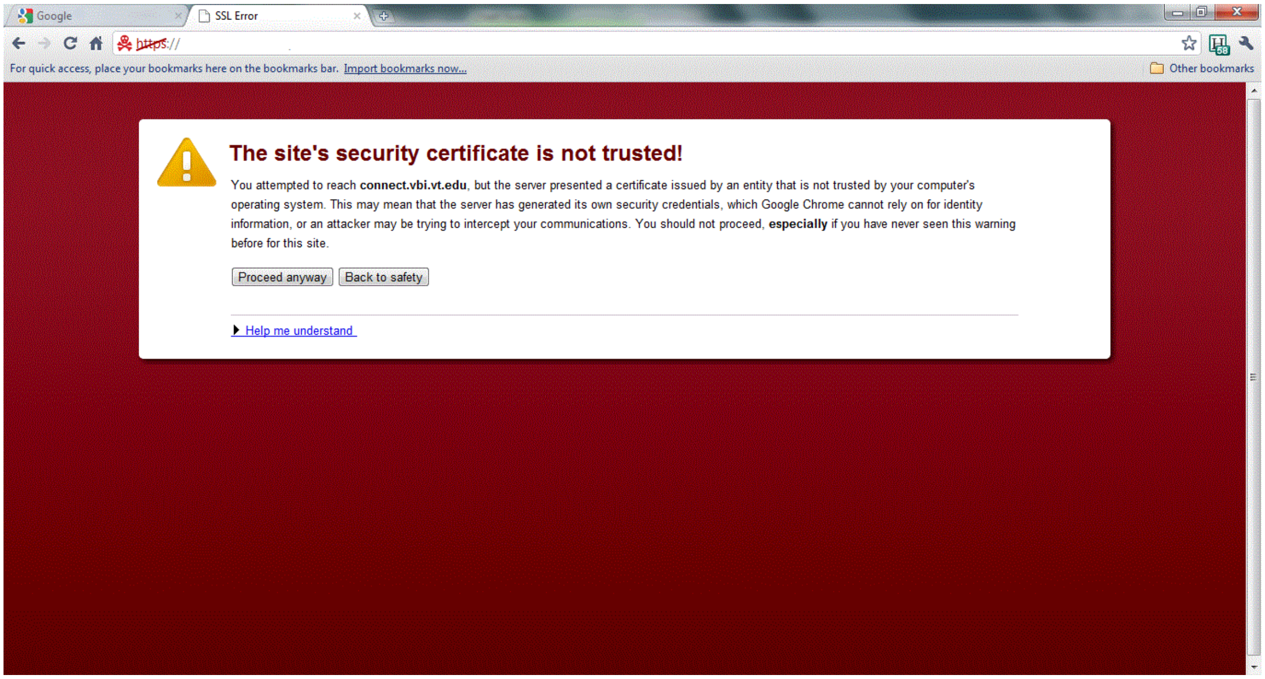
[redacted] uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is not trusted.

(Error code: sec_error_untrusted_issuer)

I Understand the Risks

Firefox reacts to self-signed sites with a warning that the site cannot be trusted because the issuer of the certificate is not trusted.



Google
SSL Error
~~https~~://
For quick access, place your bookmarks here on the bookmarks bar. Import bookmarks now...
Other bookmarks

The site's security certificate is not trusted!

You attempted to reach **connect.vbi.vt.edu**, but the server presented a certificate issued by an entity that is not trusted by your computer's operating system. This may mean that the server has generated its own security credentials, which Google Chrome cannot rely on for identity information, or an attacker may be trying to intercept your communications. You should not proceed, **especially** if you have never seen this warning before for this site.

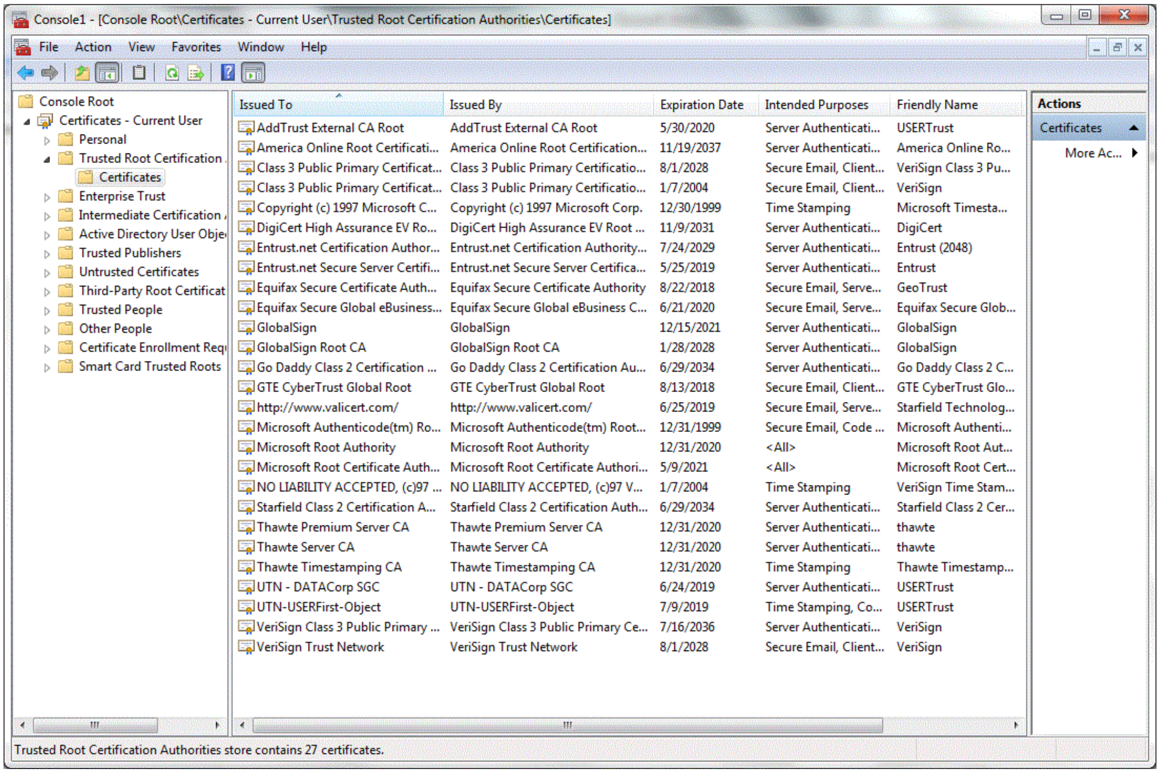
Chrome drives home the point about trustworthiness with colors that make it hard to miss the message.

Figure 1.8: When a site is not trusted—for example, because it uses a self-signed certificate—site visitors will see warning messages.

Standard Third-Party Certificates

When we use certificates from trusted certifying authorities, we do not have to worry about customers or other Web site users seeing warning messages (such as those shown in Figure 1.8—actually, they could see such messages if they deleted the certifying authority certificate that is stored in their browser, but we'll ignore that possibility for our purposes).

The distinguishing characteristic of an SSL certificate from a trusted certifying authority is that most browsers ship with certificates for the major certifying authorities. Browsers use the information in certifying authority certificates to verify the information in Web site certificates that claim to be issued by that authority.


Console1 - [Console Root\Certificates - Current User\Trusted Root Certification Authorities\Certificates]
File
Action
View
Favorites
Window
Help
Console Root
Certificates - Current User
Personal
Trusted Root Certification
Certificates
Enterprise Trust
Intermediate Certification
Active Directory User Obje
Trusted Publishers
Untrusted Certificates
Third-Party Root Certificat
Trusted People
Other People
Certificate Enrollment Requ
Smart Card Trusted Roots
Actions
Certificates
More Ac...

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name
AddTrust External CA Root	AddTrust External CA Root	5/30/2020	Server Authenticati...	USERTrust
America Online Root Certificati...	America Online Root Certification...	11/19/2037	Server Authenticati...	America Online Ro...
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	8/1/2028	Secure Email, Client...	VeriSign Class 3 Pu...
Class 3 Public Primary Certificat...	Class 3 Public Primary Certificatio...	1/7/2004	Secure Email, Client...	VeriSign
Copyright (c) 1997 Microsoft C...	Copyright (c) 1997 Microsoft Corp.	12/30/1999	Time Stamping	Microsoft Timesta...
DigiCert High Assurance EV Ro...	DigiCert High Assurance EV Root ...	11/9/2031	Server Authenticati...	DigiCert
Entrust.net Certification Author...	Entrust.net Certification Authority...	7/24/2029	Server Authenticati...	Entrust (2048)
Entrust.net Secure Server Certifi...	Entrust.net Secure Server Certifica...	5/25/2019	Server Authenticati...	Entrust
Equifax Secure Certificate Auth...	Equifax Secure Certificate Authority	8/22/2018	Secure Email, Serve...	GeoTrust
Equifax Secure Global eBusiness...	Equifax Secure Global eBusiness C...	6/21/2020	Secure Email, Serve...	Equifax Secure Glob...
GlobalSign	GlobalSign	12/15/2021	Server Authenticati...	GlobalSign
GlobalSign Root CA	GlobalSign Root CA	1/28/2028	Server Authenticati...	GlobalSign
Go Daddy Class 2 Certification ...	Go Daddy Class 2 Certification Au...	6/29/2034	Server Authenticati...	Go Daddy Class 2 C...
GTE CyberTrust Global Root	GTE CyberTrust Global Root	8/13/2018	Secure Email, Client...	GTE CyberTrust Glo...
http://www.valicert.com/	http://www.valicert.com/	6/25/2019	Secure Email, Serve...	Starfield Technolog...
Microsoft Authenticode(tm) Ro...	Microsoft Authenticode(tm) Root...	12/31/1999	Secure Email, Code ...	Microsoft Authenti...
Microsoft Root Authority	Microsoft Root Authority	12/31/2020	<All>	Microsoft Root Aut...
Microsoft Root Certificate Auth...	Microsoft Root Certificate Authori...	5/9/2021	<All>	Microsoft Root Cert...
NO LIABILITY ACCEPTED, (c)97 ...	NO LIABILITY ACCEPTED, (c)97 V...	1/7/2004	Time Stamping	VeriSign Time Stam...
Starfield Class 2 Certification A...	Starfield Class 2 Certification Auth...	6/29/2034	Server Authenticati...	Starfield Class 2 Cer...
Thawte Premium Server CA	Thawte Premium Server CA	12/31/2020	Server Authenticati...	thawte
Thawte Server CA	Thawte Server CA	12/31/2020	Server Authenticati...	thawte
Thawte Timestamping CA	Thawte Timestamping CA	12/31/2020	Time Stamping	Thawte Timestamp...
UTN - DATACorp SGC	UTN - DATACorp SGC	6/24/2019	Server Authenticati...	USERTrust
UTN-USERFirst-Object	UTN-USERFirst-Object	7/9/2019	Time Stamping, Co...	USERTrust
VeriSign Class 3 Public Primary ...	VeriSign Class 3 Public Primary Ce...	7/16/2036	Server Authenticati...	VeriSign
VeriSign Trust Network	VeriSign Trust Network	8/1/2028	Secure Email, Client...	VeriSign

Trusted Root Certification Authorities store contains 27 certificates.

Figure 1.9: The Certificate snap-in for the Microsoft Management Console displays trusted certifying authorities on a Windows device.

It should be noted that SSL certificate vendors may offer different options with SSL certificates and charge accordingly. Major vendors, for example, may offer additional features such as phone-based customer support, email reminders about certificate expiration, and other extras. These are all potentially helpful additions depending on your requirements, but they do not fundamentally alter what we describe as "standard" SSL certificates. They all require the same amount of work to verify the identity of the organization receiving the certificate.

EV SSL Certificates

For many purposes, a standard SSL certificate provides the right level of confidence to a customer. For example, someone purchasing a $20 t-shirt from an online retailer will probably want to make sure the retailer:

- Looks legitimate
- Provides an encrypted communications channel, indicated by a lock in the Web address bar or similar visual cue
- Accepts your preferred method of payment, especially credit cards or other payment methods with fraud protection
- Does not prompt your system to display warning messages (see Figure 1.8)

There is some risk of losing $20 on a fraudulent purchase, but for many of us, standard SSL certificates provide enough assurance that we continue with the transaction without giving it much more thought. This is not the case for higher-value transactions.

Banks are common targets of phishing scams. If a phisher can lure a customer to a fake site and collect the customer's login credentials, the customer's real account can be compromised. Banks and other businesses that are common targets of phishing scams can now use EV SSL certificates to provide additional assurance to their customers.

Again, the structure and function of an EV SSL certificate is the same as that of a standard SSL certificate, but there are additional requirements to getting and EV SSL certificate. Getting an SSL certificate for a domain can entail fairly limited checks, for example, verifying the owner of a domain by checking publically available registries. If the requirement for getting a low-cost SSL certificate is to have an email address matching the domain name in the InterNIC database, one can imagine a scenario where a phisher compromises a site, creates an email account, and applies for an SSL certificate for that domain. This may sound extreme, but if you are a criminal targeting a top bank in the US, Europe, or Asia, the payoff could be well worth it. It is understandable that some businesses will want to demonstrate higher levels of validation than simple database lookups; this is where EV SSL certificates come in.

To get an EV SSL certificate, businesses or other organizations have to provide substantial documentation to verify their identity. To get an EV SSL certificate, one has to demonstrate:

- The business is duly licensed or charter by ruling governments
- The business maintains a physical establishment, such as a store or office
- An officer or other principal for the business can vouch for information about the business
- Non-business organizations must be legally established according to laws of the jurisdiction

In addition, to get an EV SSL certificate, one needs to provide signatures from a certificate requestor who submits the request, an approver who has authority to confirm the request made by the requestor, and a contract signer who has the authority to enter into legal contracts. There are also requirements on certifying authorities to maintain proper levels of governance and compliance with sound business practices to protect the integrity of the EV SSL certificate process. This combination of requirements reduces the likelihood that a fly-by-night operator will start selling EV SSL certificates or a phisher will easily get hold of an EV SSL certificate.

Resource

For more information about EV SSL Certificates, see *The Shortcut Guide to Extended Validation Certificates*.

Which Type of SSL Certificate Is Right for Your Requirements?

The different types of SSL certificates are suited for different requirements. If the set of users of a Web site is limited and the users have strong reason to trust a self-signed certificate, that is a reasonable option. These situations are typically limited to development and test environments or sites that are only accessed by internal users for low-risk activities.

When external users are using a Web site and they need assurance that the site is actually the site run by a legitimate business or organization, at least the standard SSL certificate is required. This type of certificate meets a broad set of requirements and is less costly than an EV SSL certificate. If a business is the target of phishing scams or deploys applications in which customers or others perform high-value transactions, the business should consider and EV SSL certificate.

At this point, we have discussed the first two steps outlined in Figure 1.6: identifying the purpose of an SSL certificate and determining the appropriate type for our needs. The next step is to collect the information needed to request an SSL certificate from a certifying authority.

Information Needed to Create a SSL Certificate

The information requirements for a self-signed or standard SSL certificate are minimal. The requirements for an EV SSL certificate are more extensive, and we will not discuss those here. For most cases, the following information is needed to start the SSL certificate process:

- An email address associated with the business requesting the certificate
- The subject name, also known as the common name, of the server using the SSL certificate; this is the fully qualified domain name
- Organization name and organization unit, such as department
- City, state, and country

You might also need to specify key size; use 2048, which is likely the default in the program you will use to generate a certificate request.

One of the variations on the standard SSL certificates we referred to earlier is known as a Subject Alternative Names (SAN) certificate. A SAN certificate can be used to authenticate a group of servers, not just a single server. These are especially popular in Microsoft Exchange environments because the email server supports the use of SAN certificates.

> **Resource**
> For more information about SAN certificates, see *The Shortcut Guide to Subject Alternate Name Certificates*.

Generating a Certificate Signing Request

At this point, we have all the information we need to request a certificate. Fortunately, the process of requesting a certificate is well structured and many applications that make use of SSL certificates have tools for generating properly formatted requests, also known as CSRs. In Windows environments, CSRs can be generated using Microsoft IIS or Microsoft Exchange. The freely available OpenSSL package (http://www.openssl.org/) provides command-line tools for creating a CSR.

The basic steps to generating a CSR are as follows:

1. Generate a private key. This requires a pass phrase, which you will need to remember.
2. Submit the information listed in the previous section to the CSR generation program along with the key file generated in Step 1.
3. The file generated in Step 2 contains the CSR, which is submitted to the certifying authority.

The certifying authority will generate an SSL certificate and return it to you for installation. In the following chapters, we will describe how to use Microsoft IIS and other programs to generate CSRs, install SSL certificates, and test them in your environment.

Summary

SSL certificates function as a means of developing trust relationships. SSL certificates authenticate servers and client devices and allow developers to sign their application code. We users of Web sites and applications trust those resources because we trust the certifying authority that issued the certificate.

The first part of the installation and management process is to understand how an SSL certificate will be used and what level of trust we require. These requirements can range from very low trust requirements, for example, for internal development and test servers, to the demanding requirements of banks and other financial institutions.

SSL certificate generation is a standardized process. Most applications that make use of SSL certificates provide the means to create CSRs, which are then sent to certifying authorities. In the next chapter, we will examine how to manage SSL certificates using Microsoft Certificate Store.

Download Additional Books 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 book to be informative, we encourage you to download more of our industry-leading technology books and video guides at Realtime Nexus. Please visit http://nexus.realtimepublishers.com.