Realtime publishers

The Shortcut Guide™ To

Protecting Against Web Application Threats Using SSL

sponsored by

Dan Sullivan

Copyright Statement

Chapter 3: Planning, Deploying, and Maintaining SSL Certificates to Protect Against Information Loss and Build Customer Trust

SSL certificates can play an important role in securing Web applications but as with any IT system, especially security mechanisms, it pays to plan how you will deploy and maintain that system. In the previous chapters, we have examined how data loss can undermine customer trust and how SSL certificates can be used to protect online business and maintain customer trust. Now that we have covered the conceptual elements of what SSL certificates do and how they work, it is time to discuss implementation details.

This chapter will assume you understand the basic components of an SSL certificate and how it works, and are interested in implementing SSL certificates to protect your Web applications. This chapter is divided into four main sections:

- Planning for the use of SSL certificates
- Deploying SSL certificates
- Maintaining SSL certificates
- Choosing the right type of SSL certificate for your needs

This chapter will provide guidance to help you deploy SSL certificates in a way that can be sustained for the long term without creating undo management burdens. There will even be tips and instruction on how to do basic SSL certificate management tasks in Windows and Linux operating systems (OSs); however, this chapter is no substitute for system documentation.

Planning for the Use of SSL Certificates

The planning stage of deploying SSL certificates consists of two main tasks: identifying applications and servers that will benefit from having an SSL certificate and determining which type of SSL certificate is appropriate for each use case.

Process and Asset Inventory

This may sound strange, but for the next several paragraphs forget about SSL certificates. SSL certificates are tools—they are a means to an end. For the rest of this section, we are not interested in how SSL certificates can protect our Web applications. Instead, our sole focus is on what needs to be protected and why it needs to be protected.

To understand our needs, we will start with a few basic questions. First, what applications and servers are accessed by customers? These might include:

- Company Web site
- Online catalog
- Customer support services portal
- Customer feedback application
- A shipment tracking application
- Product documentation

This is a wide variety of application types and each has a different pattern of customer interaction. Consider how you would work with each of these if you were a customer.

The object of this exercise is to understand your risk tolerance with regards to using SSL certificates. In some cases, an organization may want to use SSL certificates on every server and workstation. This would be reasonable in cases where an unusually high level of security is required. A middle ground approach is to install SSL certificates on all Web accessible servers. An organization with a high tolerance for risk may pick and choose which of their Web facing servers warrant an SSL certificate. In the following sections, we will consider factors that may influence such a decision.

Company Web Site

The company Web site is the online public face of the company. It probably contains the usual information like a description of the company, news and events, product descriptions, and if you have physical locations, services such as store finders. It will likely include links to online catalogs, customer support, and other applications, but those are not considered part of the company Web site for our purposes. Those are substantial applications that have their own design, deployment, and maintenance life cycles independent of the company Web site. For this exercise, the company Web site provides the relatively static information about a company as well as links to other Web applications, such as an online catalog.

When customers or other users come to the company Web site, they are probably looking for basic information, such as contact names and email addresses, product information, locations, times of operations, etc. Businesses often take advantage of this customer interaction to collect information for mailing lists, surveys, and so on. If the site is not protected with SSL certificates, customers may be hesitant to provide personal information, leaving the business to pursue more costly means to collect that information. A company with conventional risk tolerance would want customers to be able to authenticate the company's Web site (see Figure 3.1).

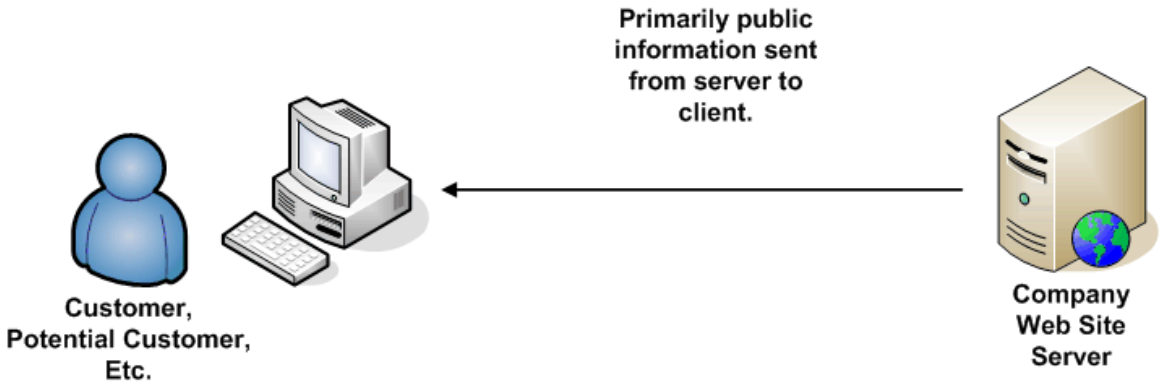

Figure 3.1: SSL certificate protection is not required when primarily public information is exchanged but there is a need to authenticate the server when collecting customer data, such as names and addresses.

Online Catalog

The online catalog allows customers to browse and search for products, collect sets of items to buy, pay for them, and then have them shipped. There is probably some type of database application behind this Web site as well as links to supporting services such as credit card processing services. The user's interactions with an online catalog are substantially different from those with a company Web site. For example, a customer is likely to:

- Browse a particular type of product or search for a specific product
- Review multiple products
- Read descriptions, reviews, and other material about products
- Select items for purchase
- Provide personal information including names, addresses, and credit card numbers

The interactions in this case includes both getting information from the application, similar to what we saw with the company Web site, and providing information to the application.

The fact that the customer is providing information to the business is a fundamental difference among applications. When it comes to personal information, such as names, addresses, and payment account information, it is probably a good bet to assume that the customer wants to keep that private. As your customer, I may have no problem sharing my credit card number with you, but I don't want anyone else to have access to it.

Depending on the size of the transaction (and the credit limit on the payment card), customers may be particularly cautious about providing payment card information to an unfamiliar company. If the customer is shopping at the online store for a national retail chain, she may feel confident that the site and the business behind it are legitimate. If this is the first time the customer has visited this site or it is not well known, major brand there may be some hesitation about trusting this site.

This application collects confidential information, so the Web and application servers supporting it should be authenticated with SSL certificates (see Figure 3.2). They would also be used to enable encrypted communication between the application and the customer. The business should consider and Extended Validation (EV) SSL certificate to demonstrate compliance with stricter identity verification standards.

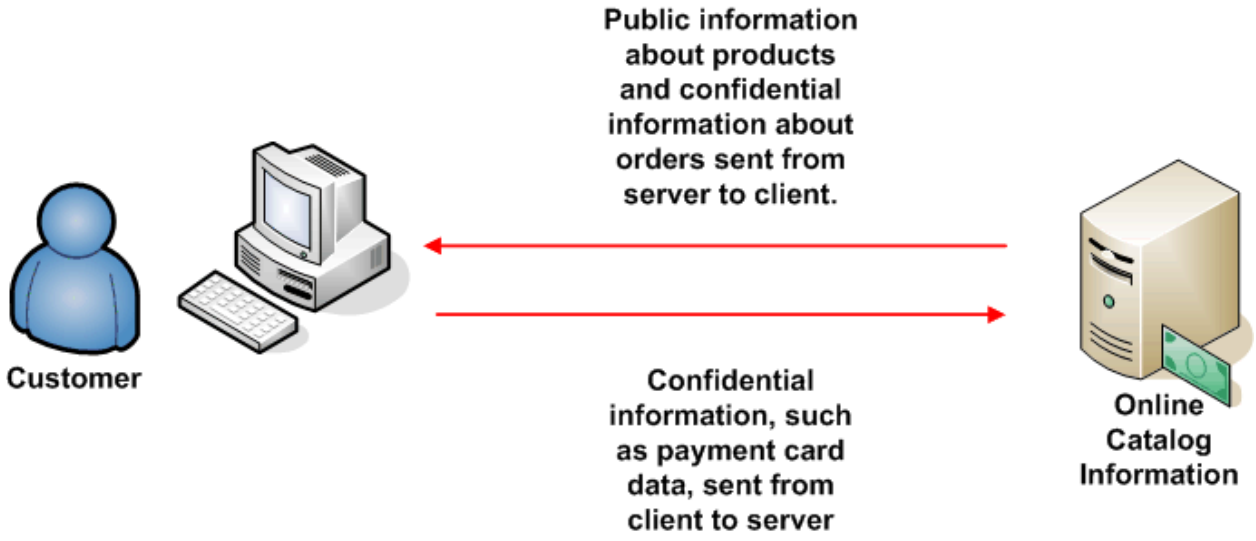

Figure 3.2: Confidential information is exchanged, so there is a need to authenticate the server and provided encrypted communications. An SSL certificate is required in this scenario even for highly risk tolerant organizations.

Customer Service Support Portal

The customer service support portal is a Web application designed to allow customers to manage their accounts, review past purchases and invoices, and set preferences, such as shipping and billing methods. Customers will want to keep their information private, so access controls are in place and customers will have access only to their account information. These access controls will keep customer data private when it is stored in the application database but does not help when data is transmitted from the application to the customer, so encryption is required for all transmitted data.

This application collects confidential information, so the Web and application servers supporting it should be authenticated with SSL certificates. They would also be used to enable encrypted communication between the application and the customer.

Customer Feedback Application

The customer feedback application collects comments and emails them to a special email account created to track such messages. These comments should be considered private and confidential because the business would want to collect frank and clear comments, which a customer might not want to disclose to others. This application should be protected with SSL certificates to ensure data is encrypted during transmission. The authentication service enabled by the SSL certificate will help assure the customer that she is working with a legitimate application. Here again, risk-adverse organizations will use SSL certificates to authenticate their company's applications.

Track Shipment Application

In some cases, a track shipment application is a relatively simple application that acts as a front-end to services provided by the major shippers used by the company. Customers enter an order number and the application looks up the shipping company for that order, contacts that company's tracking Web service, and displays the results. In more complex tracking systems, customers may provide feedback, which should be considered confidential, so SSL-based encryption should be used.

SSL certificates are not required for simple track shipment applications in highly risk-tolerant organizations, but for moderate-risk tolerance profiles or in cases where confidential information is exchanged, SSL certificates should be used. In addition, the shipping companies should use SSL certificates for their servers so that companies such as the one described here can authenticate the server they are communicating with.

Product Documentation

A product documentation application allows customers and employees to search a database of content of user manuals, technical documents, and other material to help customers and employees use products sold by the company. Product documentation is often considered proprietary information and should be protected as such.

In this scenario, the company is concerned about maintaining the confidentiality and integrity of the documentation. They have established strict access controls to mitigate the risk of incorrect documentation being placed in the database. There is some concern that if a malicious prankster spoofed the site and lured customers to a fake version of the site, the company's reputation could be damaged.

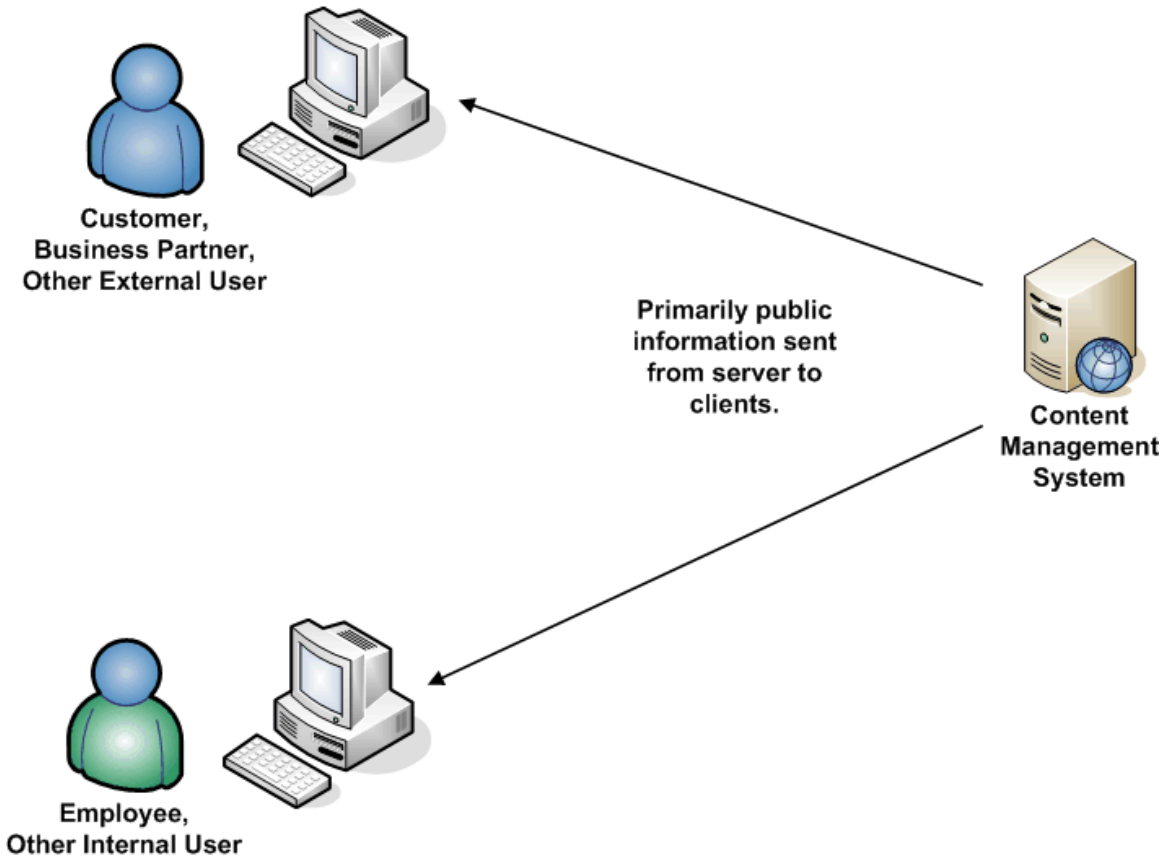

Figure 3.3: Public information distributed to both internal and external users does not require SSL certificate protection.

SSL certificate protection is required for encryption and authentication. If the perceived risk is high and the expected impact of a possible spoofing attack is great enough, an SSL certificate should be used for authentication.

Multi-Tier Applications

Having completed the application-based assessment of our SSL certificate requirements, we next have to delve into server-level requirements. In cases of simple applications that run on a single server, one would only need a certificate for that server. Many business applications, however, require multiple servers such as Web servers, application servers, and database servers.

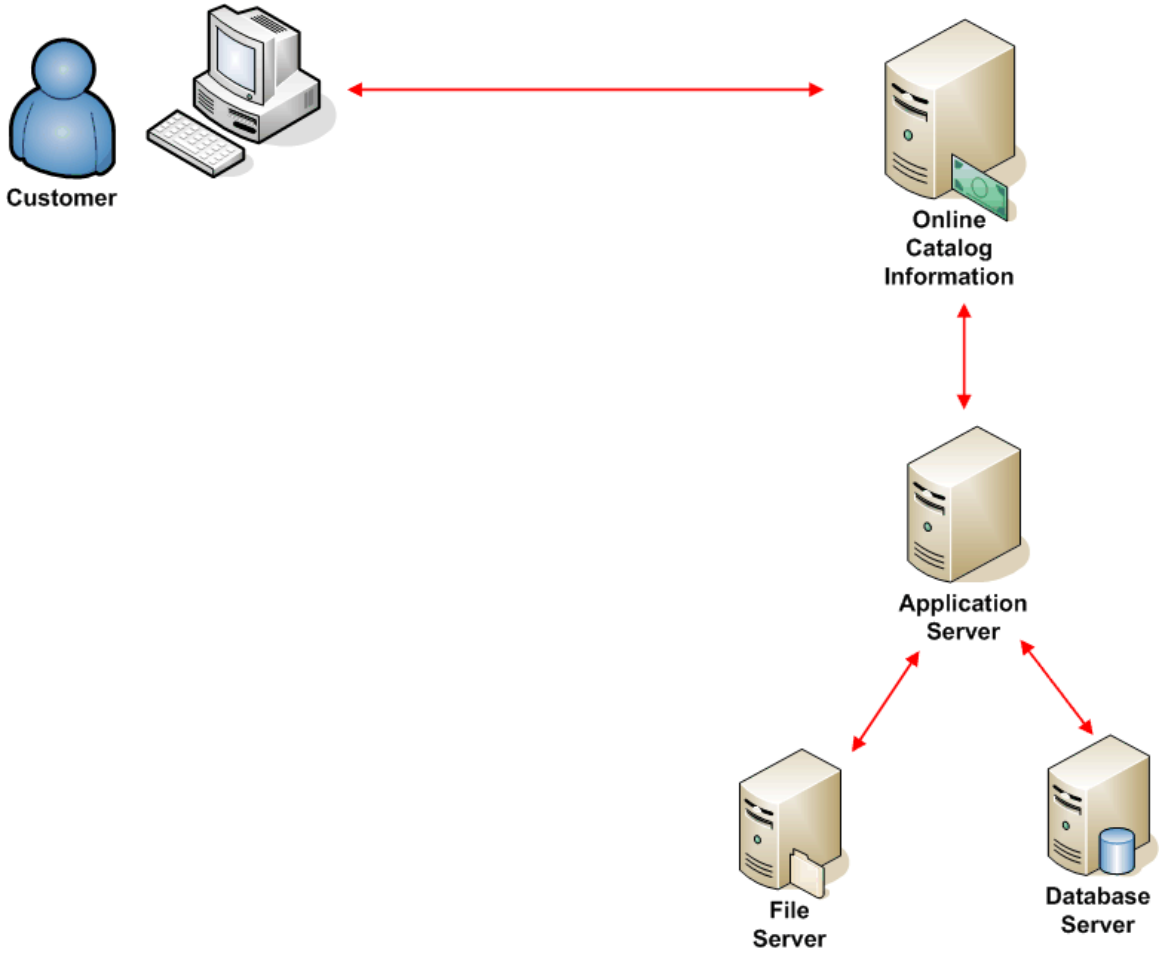

Figure 3.4: Multi-tier applications depend on multiple servers. If the application requires SSL certificates, then usually all servers will require SSL certificates.

Figure 3.4 shows a multi-tiered application. In this scenario, confidential data, such as payment data or customer account data, moves through several servers. The trust that a customer has in the application has to build on trust in the servers that implement the application. In such cases, the most secure option is to use SSL certificates on all servers in the multi-tier architecture. It is conceivable that there may be a server providing some basic function that never receives or processes confidential information. In such a case, one could argue against authenticating that server via an SSL certificate; however, given that requirements might change and that consistency often eases management burdens, it might be worthwhile using SSL certificates on all servers in the architecture.

In general, the planning process consists of a similar exercise to the one described earlier. Assess the way private and confidential information flows from the business to customers and from servers and devices implementing the application. Specifically, be sure to ask the following questions:

- What applications and servers are accessed by customers?
- What applications and servers are accessed by other trusted applications?
- What applications access confidential, private, or sensitive data?

With answers to these questions, we can determine which applications and servers need SSL certificate protection. The next question to address is what type of SSL certificate should be used.

Determining the Type of SSL Certificate Required

Although all SSL certificates are fundamentally the same in terms of form and function, there are differences. There are certificates for single servers, for multiple servers within a domain, and there are even some that work especially well with email servers. Let's look at criteria for choosing between these.

A single server certificate is appropriate for a server that is managed and deployed relatively independently of other servers. A domain wildcard certificate allows multiple servers to use the same certificate. These servers use a subjects such as "*.example.com" which matches any server in the example domain. This is useful when a number of servers in a domain require certificates. Use these carefully, though. This certificate can be copied and used on any server in the domain, which could result in either unauthorized use and/or difficult-to-manage certificates if they are not properly tracked.

EV SSL certificates are appropriate for customer-facing Web sites and applications that will process high-value private and confidential information, such as bank account information or personal health care information. Businesses and organizations that may be targets for cybercriminals should consider the value of having an EV SSL certificate and the corresponding visual cues presented to customers. This is one way to help customers distinguish between a legitimate site and a fraudulent one.

At the other end of the trust spectrum from EV SSL certificates are self-signed certificates. These certificates do not involve a trusted third party as a certifying authority—instead someone within a company creates an SSL certificate himself. There is not much point in having an SSL certificate that asserts "Trust me because I say so" on a public-facing Web site. External-facing applications need an SSL certificate that asserts "Trust me because a trusted third party has vouched for my identity." Self-signed certificates are used for internal purposes such as development and testing.

Self-signed certificates have a number of advantages for development and testing:

- They can be created quickly
- They incur minimal, if any, cost
- They can be customized to meet specific needs; for example, validation periods, wild card subjects, etc.
- They are managed completely internally and do not depend on interactions with a third party

Planning SSL certificate deployments is a critical step that allows you to identify which applications and servers need SSL certificates. This step in turn allows you then to select the best type of SSL certificates for your requirements. The next step to follow after this process is to actually deploy the SSL certificates to your servers.

Key Points About Choosing and Deploying SSL Certificates

As you are planning, deploying, and managing SSL certificates, keep in mind several key points about choosing and deploying them. SSL certificates are used for two security operations: securing communications and authenticating systems.

Secure communications are required for when confidential or private information is exchanged. This is certainly the case when data such as credit card numbers are exchanged, but this is not the only scenario. Sometimes attackers can piece together information incrementally over time. There may be no case where a single transaction had all the details the attacker needed to steal information or compromise a system, but if the attacker has access to multiple transactions or data exchanges, it is possible to cull useful information to further the attacker's objectives.

Authentication with SSL certificates allows client devices to verify that the server they are working with possesses a certificate from a trusted third party created for use on only that server (or set of servers in the case of wildcard or SAN certificates).Confidence you are working with a legitimate server is a building block to something more important: building the trust between a customer and a business.

We use SSL certificates to mitigate the risk that users will be lured into using illegitimate or otherwise malicious devices. Customers have visual cues, such as locks and green bar indicators that reinforce the idea that particular security measures are in place to protect this customer. Ideally, customers will understand that lack of such cues on sites that usually have them is an indicator of a potential problem.

SSL certificates are like any IT asset, they require maintenance. Fortunately, this is minimal. The key things we need to keep in mind once we have selected the appropriate type of certificate is to monitor the valid dates of use and to track the use of wildcard certificates so that they are not used on servers for which they are not intended. Also consider whether you have special requirements that might necessitate a SAN SSL certificate.

Summary

Web applications often require the use of SSL certificates in order to enable basic authentication and encryption services. Planning how to best deploy SSL certificates begins with assessing the kinds of operations performed by applications. Do they exchange private or confidential data, such as credit card information? If so, then SSL certificates should be used to enable encryption and preserve confidentiality. Is there a risk of customers being lured to malicious sites that appear to be one of your business' sites? If so, then SSL certificates are needed for authentication.

Deploying SSL certificates is not difficult, but the process is often specific to your OS or application. Some applications, such as Microsoft IIS, have specialized tools for managing SSL certificates. Fortunately, once SSL certificates are deployed, they have relatively low-maintenance requirements.