Understanding SSL Certificates

Understanding SSL Certificates

Secure Socket Layer (SSL) certificates are widely used to help secure and authenticate communications both on the Internet and within organizational intranets. Thawte is a leading global provider of SSL certificates. By making use of Thawte SSL certificates on your organization's web servers, you can securely collect sensitive information online and give your customers and users confidence that their communications with you are protected.

This guide provides an introduction to SSL security, covering the basics of how SSL functions. You will also find a discussion of the various applications of SSL certificates, along with information on their proper deployment and details of how you may test SSL certificates on your web server.

What Is SSL and What Are SSL Certificates?

SSL is a protocol developed by Netscape in 1995, which quickly became the preferred method for securing data transmissions across the Internet.

SSL is built into every major web server and web browser and makes use of public-private key encryption techniques originally developed by RSA. To make an SSL connection, a web server must have a digital certificate installed; this certificate utilizes the public and private keys used for encryption, and the certificate uniquely and positively identifies the server. You can think of digital certificates as a kind of electronic identification card, not unlike a driver's license or national identity card, which authenticates the server to the client before establishing an encrypted communications channel.

Typically, digital certificates are issued by an independent, trusted third-party to ensure their validity and broad acceptance. The issuer of a certificate is also known as a Certification Authority (CA). For example, Thawte is a commonly used global CA.

Features of SSL

People tend to associate SSL with encryption, but in fact, an SSL certificate provides four distinct features, all of which are critical to ensuring the privacy and security customers and users demand: encryption, integrity, authentication, and non-repudiation.

ENCRYPTION

Encryption utilizes mathematical algorithms to transform data so that it can only be read by the intended parties. In the case of SSL, the private and public keys provided as part of the server's digital certificate play an important role in securing data sent to and from the web browser.

INTEGRITY

By encrypting data so that only the intended parties can read it, SSL certificates also ensure the integrity of that data. In other words, if nobody else can successfully read the data, the data cannot be modified in transit. Modifying the encrypted data would render it useless, and the intended parties would then know that someone had tried to tamper with the data.

AUTHENTICATION

One of the primary roles of the CA in issuing a digital certificate is to validate the identity of the organization, or person, requesting the certificate. SSL certificates are tied to an Internet domain name, and by verifying ownership of that name, a CA ensures that users know with whom they are dealing at a basic level. For example, when you connect to an SSL-enabled web site, such as Amazon.com, the certificate identifies its owner as Amazon, Inc., and you can be sure that you are dealing with Amazon.

NON-REPUDIATION

Encryption, integrity, and authentication combine to establish non-repudiation, which means that neither party in a secured transaction can legitimately state that their communications came from someone other than themselves. This feature removes the option for one party to repudiate, or "take back," information that they have communicated online.

Applications of SSL

SSL can be used in many ways and for different purposes:

- Browser-to-server communications – Most commonly, SSL is used to secure communications between a web server and a web browser, often when sensitive information is being transmitted. This information may relate to an online purchase, a patient's medical data, or banking details. SSL helps ensure that the user of the web browser knows to whom their information is being sent and that only the intended recipient can access the information.

- Server-to-server communications – SSL can also be used to secure communications between two servers, such as two businesses that transact with one another. In this scenario, both servers usually have a certificate, mutually authenticating them to each other as well as securing the communications between them.

- Compliance with legislative and industry requirements – Many legal and industry requirements call for levels of authentication and privacy that SSL certificates provide. The Payment Card Industry Data Security Standard (PCI DSS), for example, requires the use of authentication and encryption technologies during any online payment transaction.

The SSL Experience for Users

When users visit a web site that has been secured with an SSL certificate, their web browser provides visual cues to let them know that SSL is working. One prominent cue is the address displayed in the browser's address field, which will start with https:// for an SSL-secured connection, and http:// for non-secured connections.

Most browsers also display some kind of lock icon (see Figure 1), although the location and appearance will vary from browser to browser.
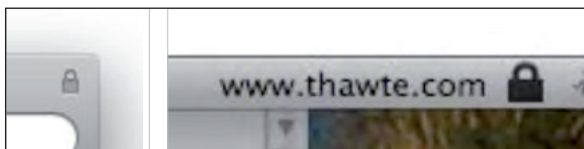

Figure 1: A lock icon displayed by a web browser.

Browsers may also allow the user to click the lock icon to view more information about the certificate. For example, Firefox™ displays a dialog box similar to the one in Figure 2, with details about the certificate, who owns it, and who issued it.
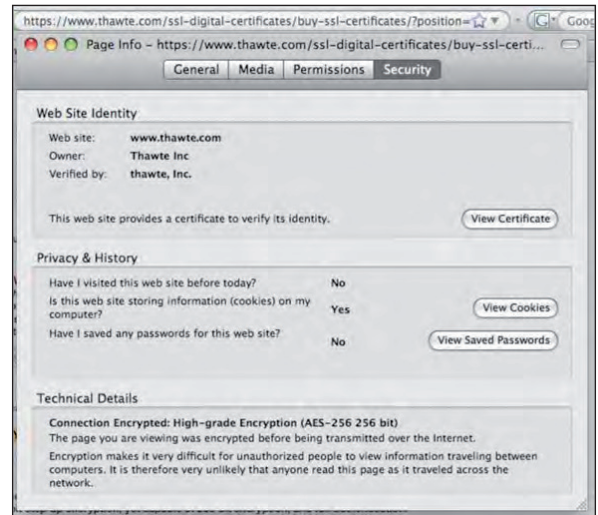

Figure 2: Details about a certificate, including the owner and the issuer.

Clicking "View Certificate" provides additional details, including its expiration date, verification fingerprints, and so forth (Figure 3).
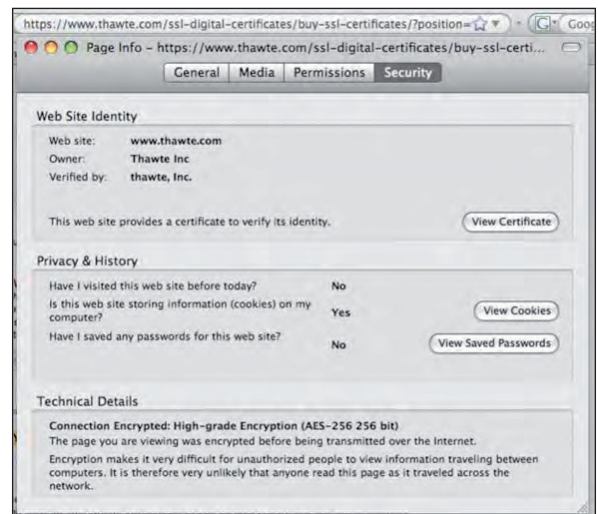

Figure 3: Additional details about a certificate.

3

There are several key pieces of information provided:

- The name of the domain to which the certificate was issued. The certificate is only valid when used with this domain; a browser will reject a request if it is presented along with a different domain name.

- The owner of the certificate, allowing users to see the name of the entity with which they are dealing.

- The validity period of the certificate – the date on which certificate validity begins and ends. Like most other forms of identification, digital certificates expire and must be renewed, allowing the CA to re-verify the identity of the certificate owner.

SSL vs. Extended Validation (EV) Certificates

The stringent identity verification process that, as a matter of best practice, is required to issue SSL certificates, is expensive for CAs to maintain. As a result, SSL certificates originally carried a price that reflected the quality of that verification process. Some SSL customers, pressured CAs for a lower-cost product and many CAs responded by offering "domain validation only" certificates. These lower-priced certificates only verify the domain name to which they are issued, and do not include more extensive identity validation of the domain's owner company. While less expensive, these SSL certificates also provide less assurance to the end user. These certificates are often ideal for low-security applications, when the stronger validation required to issue a traditional SSL certificate is not necessary.

Eventually, end users became confused about the differences between SSL certificates and began demanding a way to distinguish between these less-expensive certificates and certificates that provide greater identity verification and assurance. In response, the CA/Browser Forum, an independent industry group, produced guidelines for an Extended Validation (EV) certificate.

An EV certificate is an SSL certificate where the issuing CA must take more rigorous steps to validate the identity of the certificate requestor. CAs must also pass an independent audit of their validation procedures in order to continue offering EV certificates, meaning EV certificates tend to only be available from top-tier, highly-trusted CAs, such as Thawte.

Web browsers display different visual cues for web sites with EV certificates, along with extended, more easily-accessible identity information (see Figure 4).
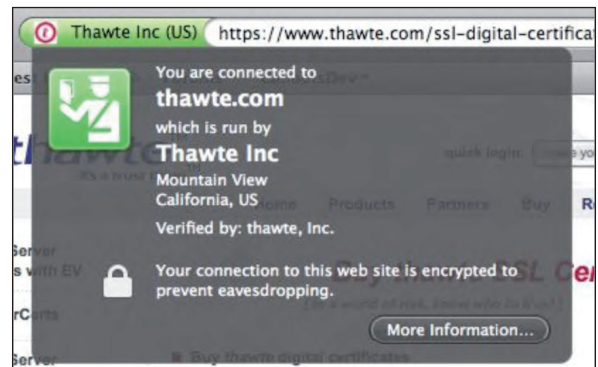

Figure 4: Visual cues associated with an EV certificate.

These enhanced visual cues (e.g., green-tinted URL bars) help provide users with a clearer distinction for more highly-trusted certificates in high-security applications making it easier for users to positively confirm with whom they are communicating (see Figure 5).
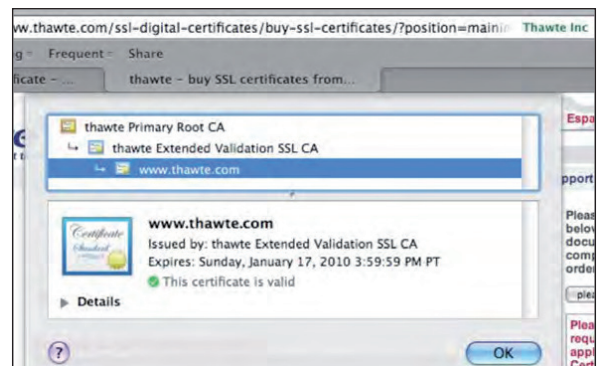

Figure 5: Gaining information from an EV certificate.

How SSL Works

SSL is a reasonably straightforward protocol, despite the advanced math that makes it work.

PUBLIC AND PRIVATE KEYS

SSL uses public and private encryption keys. When a digital certificate is issued for a web server, that certificate contains two keys: one that is privately held by the web server ("private key"), and another that is made publicly available to anyone who requests it ("public key"). These two keys are asymmetric, which means:

- Data encrypted by the private key can only be decrypted by the public key

- Data encrypted by the public key can only be decrypted by the private key

For example, to ensure the privacy of communications, a web browser retrieves the server's public key. The browser then uses that key to encrypt the information to be transmitted, since only the web server holds the private key necessary to decrypt that information. Note that in practice the encryption process may also rely on randomly-generated, short-term session keys that are exchanged between the browser and server. This is because, in most cases, the browser does not possess its own digital certificate and key pair.

HOW IS AN SSL SESSION CREATED?

An SSL session begins when a web browser sends a request to a web server using the https:// protocol (see Figure 6).
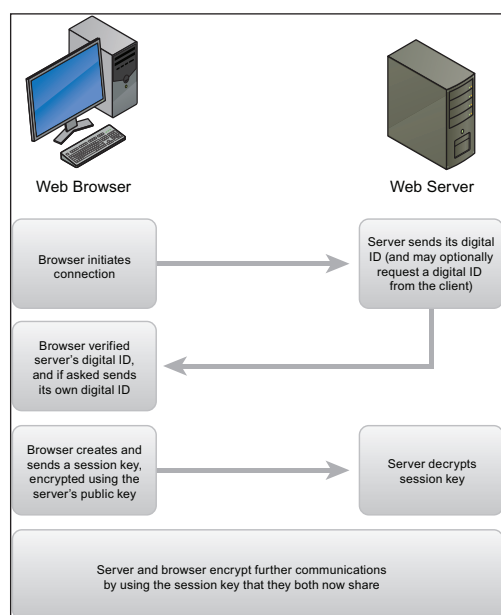

Figure 6: The creation of an SSL session.

The web server responds with its digital ID, which includes its public encryption key. The web browser verifies the digital ID, which may include an online check with the CA as well as a

check of the certificate itself for validity dates and other details. Once verified, the browser generates a session key, encrypts the session key using the server's public key, and sends the package back to the server.

The server decrypts the session key by using the server's private encryption key, which only the server possesses. This ensures that only the browser and the server possess the session key, and they can use that shared key to encrypt further communications between them. Servers usually discard session keys after several minutes of inactivity.

SSL Solutions from Thawte

Thawte offers a number of SSL certificate products. Each of Thawte's certificate products are designed for specific business scenarios:

- **SSL Web Server Certificate with EV** is an Extended Validation certificate capable of very high (256-bit) encryption. It includes detailed identity verification procedures to assure the highest level of trust in high-security web sites and web applications.

- **SGC SuperCert** is a premium SSL certificate capable of up to 256-bit encryption and full authentication. These certificates provide automatic 128-bit step-up encryption for certain older web browsers.

- **SSL Web Server Certificate** is a standard SSL certificate with full authentication capable of up to 256-bit encryption.

- **SSL123 Certificate** is a domain validation-only certificate capable of being issued within minutes, and capable of up to 256-bit encryption.

- **Wildcard SSL Certificates** can be used to secure multiple sub-domains on the same fully-qualified top-level domain with a single certificate, offering up to 256-bit encryption.

Consult a Thawte sales representative for information about these and other certificate products.

THE THAWTE TRUSTED SITE SEAL

All **SSL Web Server Certificate, SGC SuperCert,** and **SSL Web Server Certificate with EV** customers may display the **Secured by Thawte Trusted Site Seal** on their web sites (see Figure 7). This seal is a secure image, generated by Thawte, which provides visible proof of your site's trusted status. It is available in various languages and sizes, allowing for easy integration into your existing site design.

SECURED
BY
ⓣ thawte®
2005-00-00

Figure 7: The Secured by Thawte Trusted Site Seal.

Testing SSL on Your web Server

To gain a practical understanding of SSL certificates, you might want to download a Thawte SSL Trial Certificate for test and evaluation purposes. These certificates are valid for 21 days and will allow you to familiarize yourself with the installation process as well as to ensure compatibility with your web server software. To request your free SSL Trial Certificate, click here: https://ssl-certificate-center.thawte.com/process/retail/thawte_trial_initial

Useful Links

You may find the following URLs useful:

- More details about Thawte's SSL Web Server Certificates can be found at: http://www.thawte.com/ssl/

- Common problems experiences with SSL certificates, and the solutions to those problems, are detailed in the Thawte Knowledge Base at: https://search.thawte.com

- You can purchase Thawte SSL certificates at: https://www.thawte.com/buy/

To learn more, contact our sales advisors:

- Via phone
  - **US toll-free: +1 888 484 2983**
  - **UK: +44 203 450 5486**
  - **South Africa: +27 21 819 2800**
  - **Germany: +49 69 3807 89081**
  - **France: +33 1 57 32 42 68**

- Email **sales@thawte.com**
- Visit our website at **https://www.thawte.com/log-in**

Protect your business and translate trust to your customers with high-assurance digital certificates from Thawte, the world's first international specialist in online security. Backed by a 17-year track record of stability and reliability, a proven infrastructure, and world-class customer support, Thawte is the international partner of choice for businesses worldwide.