Entrust®
Securing the Internet

Understanding Digital Certificates and Secure Sockets Layer (SSL)

Author: Peter Robinson
January 2001
Version 1.1

Digital Certificates

What are they?

Digital certificates are electronic files that are used to uniquely identify people and resources over networks such as the Internet. Digital certificates also enable secure, confidential communication between two parties.

When you travel to another country, your passport provides a universal way to establish your identity and gain entry. Digital certificates provide similar identification in the electronic world. Certificates are issued by a trusted third party called a Certification Authority (CA). Much like the role of the passport office, the role of the CA is to validate the certificate holders' identity and to "sign" the certificate so that it cannot be forged or tampered with. Once a CA has signed a certificate, the holder can present their certificate to people, Web sites, and network resources to prove their identity and establish encrypted, confidential communications.

For more information on trust, refer to the White Paper *The Concept of Trust in Network Security*, available at: http://www.entrust.com/resourcecenter/whitepapers.htm

A certificate typically includes a variety of information pertaining to its owner and to the CA that issued it, such as:

- The name of the holder and other identification information required to uniquely identify the holder, such as the URL of the Web server using the certificate, or an individual's e-mail address;
- The holder's public key (more on this below). The public key can be used to encrypt sensitive information for the certificate holder;
- The name of the Certification Authority that issued the certificate;
- A serial number;
- The validity period (or lifetime) of the certificate (a start and an end date).

In creating the certificate, this information is digitally signed by the issuing CA. The CA's signature on the certificate is like a tamper-detection seal on a bottle of pills – any tampering with the contents is easily detected.

Digital certificates are based on public-key cryptography, which uses a pair of keys for encryption and decryption. With public-key cryptography, keys work in pairs of matched "public" and "private" keys. In cryptographic systems, the term key refers to a numerical value used by an algorithm to alter information, making that information secure and visible only to individuals who have the corresponding key to recover the information.

For more information on public-key cryptography, refer to the White Paper *An Introduction to Cryptography,* available at: http://www.entrust.com/resourcecenter/whitepapers.htm

The public key can be freely distributed without compromising the private key, which must be kept secret by its owner. Since these keys only work as a pair, an operation (for example encryption) done with the public key can only be undone (decrypted) with the corresponding private key, and vice-versa.

A digital certificate securely binds your identity, as verified by a trusted third party (a CA), with your public key.

Web server certificates

A Web server certificate is a certificate that authenticates the identity of a Web site to visiting browsers. When a browser user wants to send confidential information to a Web server, the browser will access the server's digital certificate. The certificate, which contains the Web server's public key, will be used by the browser to:

- authenticate the identity of the Web server (the Web site), and
- encrypt information for the server using Secure Sockets Layer (SSL) technology (more on SSL below).

Since the Web server is the only one with access to its private key, only the server can decrypt the information. This is how the information remains confidential and tamper-proof while in transit across the Internet.

CA certificates

A CA certificate is a certificate that identifies a Certification Authority. CA certificates are just like other digital certificates except that they are self-signed. CA certificates are used to determine whether to trust certificates issued by the CA.

In the case of a passport, a passport control officer will verify the validity and authenticity of your passport and determine whether to permit you entry. Similarly, the CA certificate is used to authenticate and validate the Web server certificate. When a Web server certificate is presented to a browser, the browser uses the CA certificate to determine whether to trust the Web server's certificate. If the server certificate is valid and trusted, the browser and Web server will establish an SSL connection. If the server certificate is not valid, the server certificate is rejected and the SSL session is stopped.

CA certificates come pre-installed on most popular Web browsers, including those from Microsoft® and Netscape®.

Secure Sockets Layer (SSL)

What is SSL?

Secure Sockets Layer (SSL) technology is a security protocol. It is today's de-facto standard for securing communications and transactions across the Internet. SSL has been implemented in all the major browsers and Web servers, and as such, plays a major role in today's e-commerce and e-business activities on the Web.

The SSL protocol uses digital certificates to create a secure, confidential communications "pipe" between two entities. Data transmitted over an SSL connection can not be tampered with or forged without the two parties becoming immediately aware of the tampering. The newest version of the SSL standard has been renamed TLS (Transport Layer Security). You will often see these terms used interchangeably. Since the term SSL is more commonly understood, we will continue to use it throughout this paper.

How certificates are used in an SSL transaction

Suppose Alice wants to connect to a secure Web site to buy something online:

- When Alice visits a Web site secured with SSL (typically indicated by a URL that begins with "https:"), her browser sends a "Client Hello" message to the Web server indicating that a secure session (SSL) is requested.
- The Web server responds by sending Alice its server certificate (which includes its public key).
- Alice's browser will verify that the server's certificate is valid and has been signed by a CA whose certificate is in the browser's database (and who Alice trusts). It will also verify that the CA certificate has not expired.
- If the certificates are all valid, Alice's browser will generate a one-time, unique "session" key and encrypt it with the server's public key. Her browser will then send the encrypted session key to the server so that they will both have a copy.
- The server will decrypt the message using its private key and recover the session key.

At this point Alice can be assured of two things:

- the Web site she is communicating with is really the one it claims to be (its identity has been verified), and
- only Alice's browser and the Web server have a copy of the session key.

The SSL "handshake" - the process of identifying the two parties that want to establish an SSL connection - is complete and a secure communications "pipe" has been established. Alice's browser and the Web server can now use the session key to send encrypted information back and forth, knowing that their communications are confidential and tamper-proof. The entire process of establishing the SSL connection typically happens transparently to the user and takes only seconds.

A key or padlock icon in the lower corner of the browser window identifies the security mode of a browser. When the browser is running in "normal" mode, the key looks broken or the padlock looks open. Once an SSL connection has been established, the key becomes whole, or the padlock becomes closed, indicating that the browser is now in "secure" mode.

SSL is supported in the vast majority of browsers, which means that almost anyone with a browser can reap the benefits of SSL encryption. SSL is also incorporated into most Web servers on the market.

What's Next?

The Internet, Intranets, Extranets and wireless networks are re-defining how companies communicate and do business. As the value of business relationships and transactions increase, so do the associated risks and security requirements. Entrust provides the world's most advanced security solutions for protecting business relationships and transactions with a full range of products based on public-key infrastructure (PKI) technology. To learn more about PKI and how it can help your business grow, please refer to the Entrust Web site at http://www.entrust.com