

Securing Your Digital Life

Understanding Digital Certificates & Secure Sockets Layer (SSL): A Fundamental Requirement for Internet Transactions

February 2005

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. In Canada, Entrust is a registered trademark of Entrust Limited. All Entrust product names are trademarks of Entrust, Inc. or Entrust Limited. All other company and product names are trademarks or registered trademarks of their respective owners.

The material provided in this document is for information purposes only. It is not intended to be advice. ENTRUST DOES NOT WARRANT THE QUALITY, ACCURACY OR COMPLETENESS OF THE INFORMATION CONTAINED IN THIS ARTICLE. SUCH INFORMATION IS PROVIDED "AS IS" WITHOUT ANY REPRESENTATIONS, WARRANTIES AND/OR CONDITIONS OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, WARRANTIES AND/OR CONDITIONS OF MERCHANTABILITY, SATISFACTORY QUALITY, TITLE, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

TABLE OF CONTENTS


1. THE LANDSCAPE.....	1
2. DIGITAL CERTIFICATES.....	2
2.1 WHAT ARE THEY?	2
3. SSL CERTIFICATES.....	3
3.1 WHAT ARE THEY?	3
4. SECURE SOCKET LAYER (SSL).....	4
4.1 WHAT IS SSL?	4
4.2 HOW IS THE SSL ENCRYPTION STRENGTH DETERMINED?	4
4.3 IS SERVER GATED CRYPTO (SCG) REQUIRED?.....	4
4.4 HOW CERTIFICATES ARE USED IN AN SSL TRANSACTION	5
4.5 ENTRUST SSL CERTIFICATES	5
5. ENTRUST CERTIFICATE SERVICES	7
6. CONCLUSION	8

1. THE LANDSCAPE

The Internet is your gateway to millions of potential new customers. Moving your business online provides the convenience and accessibility your customers and partners demand, helping you to stand out from the competition.

As organizations provide more services and transactions online, security becomes a necessity. Customers need to be confident that sensitive information such as a credit card number is going to a legitimate online business. Organizations need to keep customer information private and secure.

In today's environment with identity theft and fraud, it is imperative that businesses provide a secure way of conducting online transactions. By providing security to an online presence, organizations not only gain customer trust, but also can increase revenue by adding more services online.



"SSL acceleration and SSL digital certificates will be a key first step to Web services security."

Source: Gartner "Security Strategies for Enterprises Using Web Services," May 2003

2. DIGITAL CERTIFICATES

2.1 WHAT ARE THEY?

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

When you travel to another country, your passport provides a way to establish your identity and gain entry. Digital certificates provide similar identification in the electronic world. Certificates are issued by 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 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.

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 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 packaging—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.

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 or decrypted with the corresponding private key, and vice-versa.

A digital certificate can securely bind your identity, as verified by a trusted third party, with your public key.

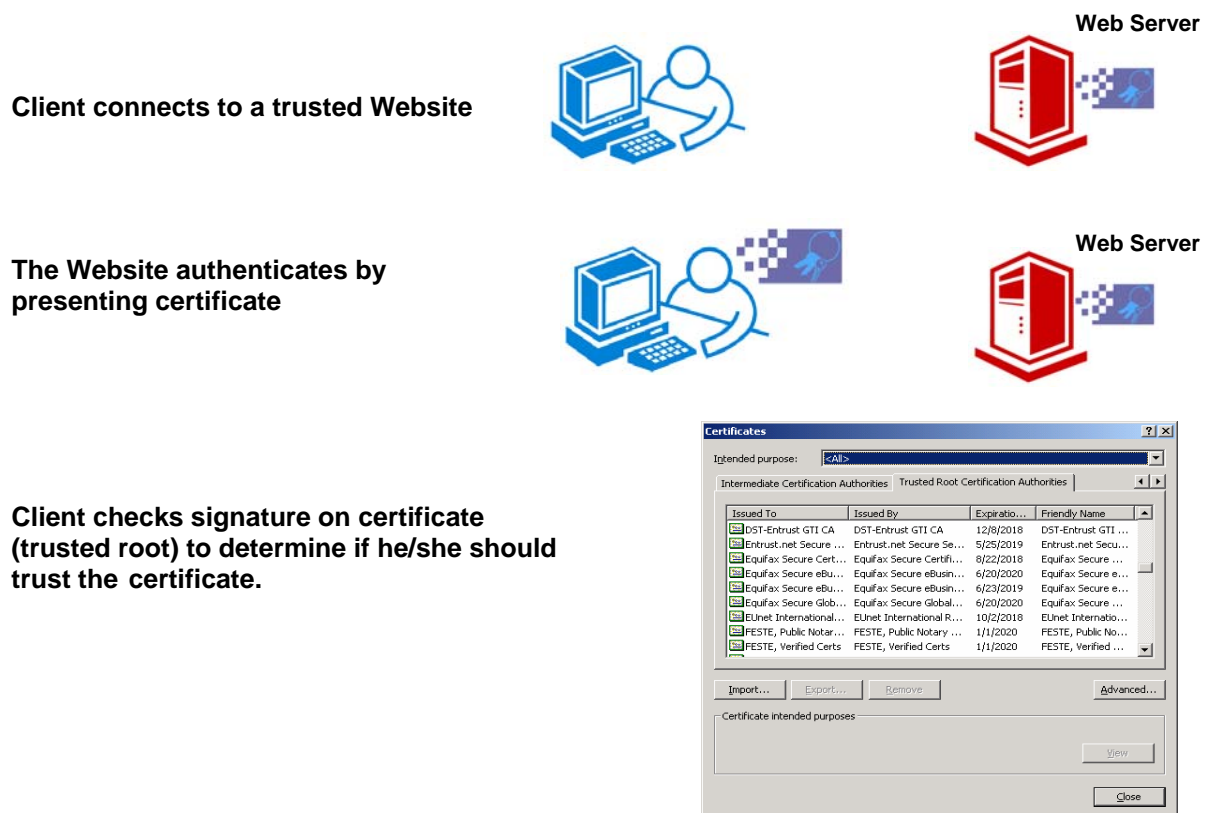
3. SSL CERTIFICATES

3.1 WHAT ARE THEY?

An SSL Web server certificate is a certificate that authenticates the identity of a Web site to browser users and enables encrypted communications using Secure Sockets Layer (SSL). When a browser user wants to send confidential information to a Web server, the browser will access the server's digital certificate and obtain its public key to encrypt the data.

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.

The following diagram illustrates how a 128-bit SSL connection works:



4. SECURE SOCKET LAYER (SSL)

4.1 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 cannot 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.

"Through 2008, nearly all trading communities will use SSL to meet diverse trading-partner requirements."

Gartner, B2B Security Patterns: Finding the Perfect Combination, August 2003

4.2 HOW IS THE SSL ENCRYPTION STRENGTH DETERMINED?

Although the information sent between the browser and the Web server is encrypted, it is a common misunderstanding that the certificate dictates the strength of the encryption. The strength of the SSL session is actually a function of the strength of the browser and the capabilities of the server. If the browser only supports 40-bit encryption, then only a 40-bit session will be established, even if the Web server supports 128-bit sessions. If the browser supports 128-bit encryption, then a 128-bit session will be established.

4.3 IS SERVER GATED CRYPTO (SCG) REQUIRED?

At one time, the export of 128-bit browsers outside North America was regulated. Prior to changes in these U.S. Export Regulations, the use of "step-up" encryption or Server-gated Crypto ("SGC") was the only way for organizations dealing with consumers outside the U.S. and Canada to secure communications between Web browsers and web servers using 128-bit encryption. Because Microsoft and Netscape were restricted to only exporting 40-bit encryption browsers, enterprises with international customers were forced to purchase expensive "step-up" certificates in order to secure 128-bit encryption for their Web site users.

Everyone wants the highest level of security available today, but at a reasonable cost. If you are using SGC certificates, you should understand that in the majority of cases, these certificates are no longer necessary. For more than 2 years, U.S. export regulations have permitted the export of 128-bit encryption-enabled browsers and upgrades for existing browsers to all countries except those under U.S. embargo. According to browser usage statistics cited on an industry Web site*, 97.43% of browsers in use today support SSLv2 (128-bit encryption). For this reason, premium priced "step-up" Web server certificates are no longer necessary.

*Source: www.securityspace.com

4.4 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 Certificate Authority (CA) like Entrust, whose certificate is in the browser's database or that has been cross certified by a root 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 certificate is 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 confident about two things:

- The Web site she is communicating with has been vetted to confirm the identity of the organization requesting the certificate and the domain on which the server has been established, and
- Only Alice's browser and the Web server have a copy of the session key.

Once the SSL "handshake" is complete, then a secure communications "pipe" will have 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 protected. 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 or is not present. Once an SSL connection has been established, the key becomes whole, or the padlock becomes closed or appears, indicating that the browser is now in "secure" mode.

4.5 ENTRUST SSL CERTIFICATES

Using Entrust SSL Certificates not only provides security and trust to your Web site, but they are also easier to deploy. Entrust is a recognized and trusted brand. Entrust has a certified CA and its CA's roots are embedded in most major browsers or have been cross certified by a root embedded in those browsers.

When a Web site does not have an SSL Certificate signed by a certificate authority whose root is embedded in the browser or that has been cross certified by one of the roots embedded in the browser, most internet browsers, will show a warning dialogue box similar to that shown in Figure 1, which may lead the customer to question the trustworthiness of the site.

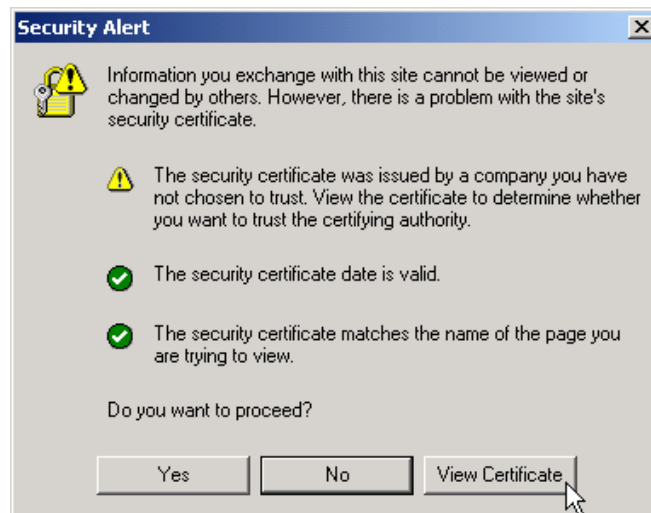


Figure 1: Warning dialogue box

In contrast, if a user submits credit card or other information to a site with a valid SSL Certificate and an SSL connection, the warning does not appear. The secure connection is seamless, making the online shopping experience more pleasant.

In order to conduct transactions over the internet every organization requires SSL Security as a basic minimum. To gain the trust of your customers, partners and employees, it is imperative that your business identity be verified with an SSL Web Server Certificate. Entrust certificates provide trust through a strong verification process, 128-bit compatible encryption technology, and easy to use, low cost SSL certificate life-cycle management.

Entrust will only issue an SSL Certificate to your online business after it has performed the following verification procedures:

- Verifying your identity against third-party databases and confirming that your organization is listed in these databases
- Confirming that that your organization has the right to use the domain name included in the certificate request
- Verifying that the individual who requested the SSL certificate on behalf of the organization was authorized to do so and is employed with that organization.

Entrust was the first certificate authority (CA) in the world to earn the WebTrust for Certificate Authorities (CAs) Seal of Assurance from the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA). A WebTrust Seal provides you with assurance and confidence in the security of a public key infrastructure (PKI).



5. ENTRUST CERTIFICATE SERVICES

Entrust Certificate Services is designed to help customers take advantage of the operational efficiencies that electronic commerce has to offer, while securing online transactions. By protecting communications between browsers and Web servers, Entrust SSL Certificates enable increased consumer confidence and transparent Web security for end-users and administrators. Entrust Certificate Services are automated so that the administrator doesn't have to worry about unnecessary certificate expiry and loss of service.

The solution consists of the following products and services:

Entrust Certificate Management Service – Standard Edition

Entrust SSL Certificates enable 128-bit SSL encryption between Web servers and browsers. Customers can purchase one-year or two-year certificates and be confident that they are purchasing a trusted brand whose root is embedded in or has been cross certified by a root embedded in the most common browsers. Entrust SSL Certificates help you to prevent service disruptions and reduce your monitoring costs by delivering automatic notification of upcoming certificate expiration and around the clock online support.

Entrust Certificate Management Service – Enhance Edition

The Entrust Certificate Administrator Service streamlines the procurement and administration of one-year and two-year Web server certificates, acting as a centrally managed, self-service system. The Certificate Administrator Service reduces administrative hassles and helps lessen the risk of inadvertent certificate expiration by allowing customers to synchronize and control the timing of certificate expiration. The Entrust Certificate Administrator Service enables administrators to "re-use" or "re-cycle" their certificates for improved usage.

Entrust Certificate Management Service – Premium Edition

Along with offerings of the Enhanced edition, customers will benefit from reduced costs and complexity through the automation of certificate lifecycle management. The Certificate Manager software included in the Premium edition, automates the installation and renewal of certificates to provide customers managing large pools of SSL certificates with the greatest potential savings.

Entrust Certificate Enrollment Service for Web Hosters

The Entrust Certificate Enrollment Service for Web Hosters has been designed to provide Web Hosters with an opportunity to more easily deliver security services to their customers. This program offers a convenient and cost-effective solution to deliver SSL certificates using a simplified, on-line certificate request process.

6. CONCLUSION

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. By protecting the security of online payments, businesses can reduce risk and reach a larger market. SSL security is a standard and a minimum requirement for those that conduct transactions online. Almost all legitimate and trustworthy businesses use SSL security to secure their Web site.

Entrust Certificate Services helps organizations secure their online transactions quickly and efficiently with limited effort required by the user or administrator. By using Entrust SSL Certificates, organizations can be confident that communications are secure and that their online presence is a trusted one, thereby increasing customer confidence and reducing security risks.

To learn more about Entrust Certificate Services and how it can help your business grow, please refer to the Entrust Web site at http://www.entrust.com/certificate_services/index.htm

7. ABOUT ENTRUST

Entrust, Inc. [NASDAQ: ENTU] is a world-leader in securing digital identities and information. Over 1,400 enterprises and government agencies in more than 50 countries rely on Entrust solutions to help secure the digital lives of their citizens, customers, employees and partners. Our proven software and services help customers achieve regulatory and corporate compliance, while turning security challenges such as identity theft and e-mail security into business opportunities. For more information on how Entrust can secure your digital life, please visit: www.entrust.com.