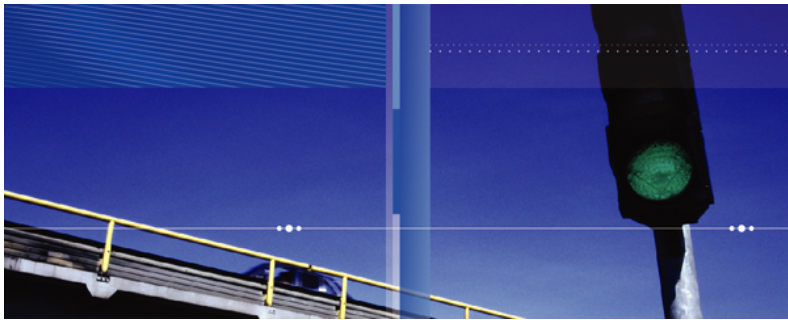


**Entrust**<sup>®</sup> Securing Digital Identities & Information



**Securing Your  
Digital Life**

***Understanding Digital Certificates & Secure Sockets Layer***  
A Fundamental Requirement for Internet Transactions

May 2007

Entrust is a registered trademark of Entrust, Inc. in the United States and certain other countries. Entrust is a registered trademark of Entrust Limited in Canada. 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. You should not act or abstain from acting based upon such information without first consulting a professional. 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 AND/OR WARRANTIES OF ANY KIND, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, AND/OR WARRANTIES OF MERCHANTABILITY, SATISFACTORY QUALITY, NON-INFRINGEMENT, OR FITNESS FOR A SPECIFIC PURPOSE.

© Copyright 2007 Entrust. All rights reserved.

## Table of Contents

<b>1 The Landscape .....</b>	<b>3</b>
<b>2 What Are Digital Certificates? .....</b>	<b>4</b>
<b>3 What Is SSL? .....</b>	<b>5</b>
How Is SSL Encryption Strength Determined? .....	5
What Are SSL Certificates? .....	6
Public Trust .....	8
<b>4 Entrust SSL Certificates .....</b>	<b>10</b>
Entrust Certificate Management Service .....	10
<b>5 Conclusion.....</b>	<b>11</b>
<b>6 About Entrust .....</b>	<b>11</b>

## 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 making security integral, organizations not only gain customer trust, but also can increase revenue by adding more services online.

## 2 What Are Digital Certificates?

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 holder's 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 standard 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), which 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 (e.g., 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 What Is SSL?

Secure Sockets Layer (SSL) technology is a security protocol that is today's de-facto standard for securing communications and transactions across the Internet. SSL has been implemented in all 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.

#### How Is 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 is limited to 128-bit encryption, then only a 128-bit session will be established, even if the Web server supports 256-bit sessions. If both the browser and server support 256-bit encryption, then a 256-bit session can be established.

#### Is Server-Gated Cryptography (SGC) Required?

At one time, the export of 128-bit browsers outside of North America was regulated. Prior to changes in these U.S. export regulations, the use of "step-up" encryption or Server-Gated Cryptography ("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. Organizations want 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.

Since 2000, 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. The primary browser version that would benefit from SGC is a non-updated installation of Internet Explorer 5.01. An update to 128-bit encryption has been available for many years on Microsoft's Windows Update service, along with many other important security updates. Deployed browser statistics are contentious, but according to at least one source, as of April 2007, Internet Explorer 5.01 and Internet Explorer 4 have a combined total market share of .33 percent<sup>1</sup>, and that does not take into account the number of IE 5.01 installations that may have updated to 128-bit encryption.

For high-traffic sites where even 0.3 percent of users represent a real concern, organizations need to consider the security ramifications of conducting secure transactions with a user who has not patched their browser or operating system for most of the 21st century.

---

<sup>1</sup> ["Browser Version By Market Share," March 2007, Net Applications](#)

## What Are SSL Certificates?

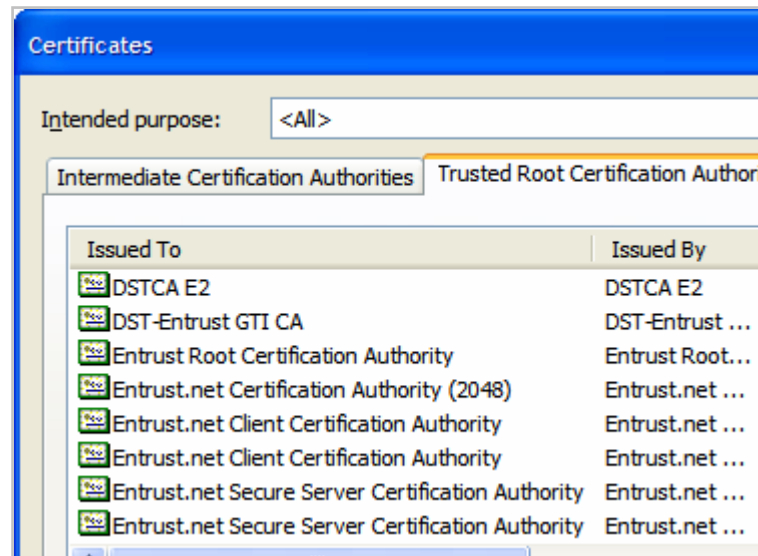
An SSL Web server certificate authenticates the identity of a Web site to browser users and enables encrypted communications using Secure Sockets Layer (SSL). When a browser user wants to send confidential information to a Web server, the browser will access the server's digital certificate and obtain 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- or 256-bit SSL connection works:



**The client verifies the signature to determine if he/she should trust the certificate. As long as the certificate is signed by one of the client's Trusted Root Certification Authorities, no trust dialogs are presented to the user and the secure connection starts seamlessly.**



## 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 Certification 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.
- 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" is 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 appears 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.

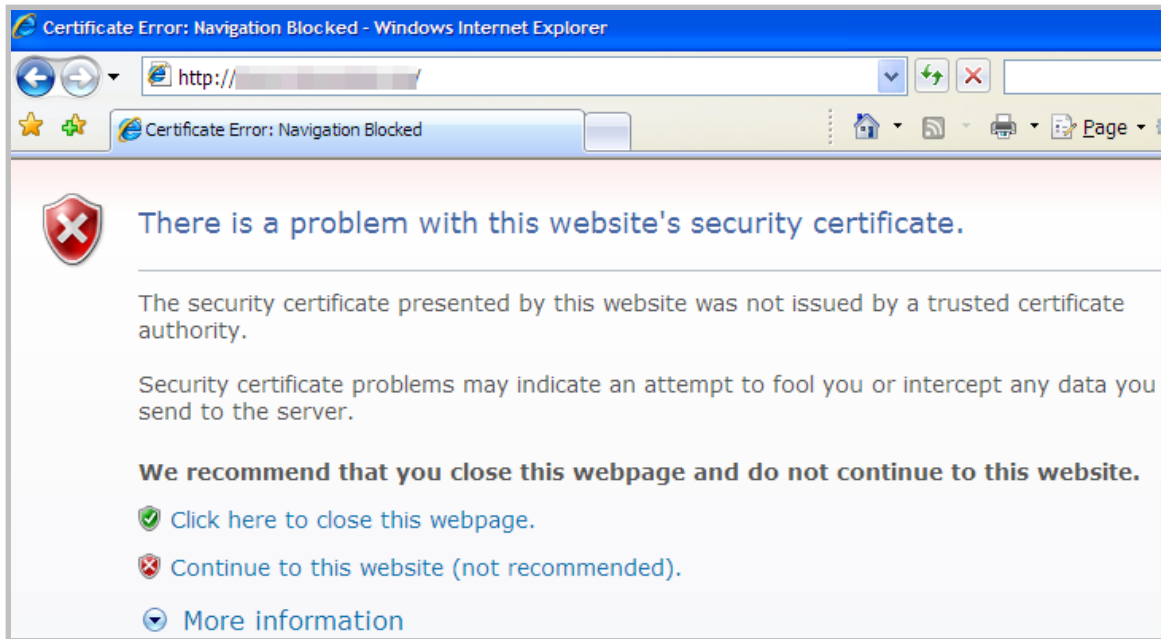
## Public Trust

Public Trust is not a widely used term, but it is a useful concept. In this context, we define it as trust relationships built using certificates issued from CAs whose public keys are embedded in applications such as Web browsers. Without these embedded keys, consumers and end-users need to go to much more effort to establish basic trust in online services.

When a Web site does not have an SSL certificate signed by a CA whose root key is embedded in the browser, most Internet browsers will display a warning dialog box similar to that shown in Figure 1, which may lead the customer to question the trustworthiness of the site and abandon their transaction.



**Figure 1: Warning dialog box, Internet Explorer 6**



**Figure 2: Warning dialog box, Internet Explorer 7**

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.

Before browser vendors will embed a CA's public key (or 'root key') into their browser, they typically require the CA to be certified for compliance with the Web Trust for Certification Authorities audit criteria. A WebTrust Seal provides you with assurance and confidence in the security of a public key infrastructure (PKI).

Entrust was the first certification authority (CA) in the world to earn the WebTrust for Certification Authorities (CAs) Seal of Assurance in 2001 from the American Institute of Certified Public Accountants (AICPA) and the Canadian Institute of Chartered Accountants (CICA).

As examples of processes and procedures audited under WebTrust, Entrust will only issue an SSL certificate to your online business after it has performed the following verification procedures:

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

## 4 Entrust SSL Certificates

Entrust's range of SSL certificate offerings are designed to help customers take advantage of the operational efficiencies that electronic commerce has to offer, while concurrently 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.

Using Entrust SSL Certificates not only provide security and trust to your Web site, but they are also easier to deploy. Entrust has been in the security business since the early 1990s and its Certification Authority (CA) root keys have been embedded in major browsers since the late '90s, which means your users will have a secure and positive experience.

Entrust SSL Certificates enable up to 256-bit SSL encryption between Web servers and browsers. Customers can purchase one- or two-year certificates and be confident that they are acquiring a trusted brand whose root key is embedded in the most common browsers and applications for a seamless user experience. Entrust SSL Certificates help you prevent service disruptions and reduce monitoring costs by delivering automatic notification of upcoming certificate expiration and around-the-clock online support.

Entrust offers a complete range of certificate products, including the new Extended Validation and Unified Communications certificates.

### Entrust Certificate Management Service

As customers manage more certificates, the account administration interface of the Entrust Certificate Management Service solution makes it simple to order, deploy and manage SSL certificates. The certificate-recycling feature allows customers to redistribute their certificate inventory to where it is needed at any time within their subscription period (e.g., if a group of Web servers is decommissioned, the certificates from those servers can be redeployed on another set of Web servers at no additional cost). Administrative delegation better fits how SSL certificates are managed within the organization by distributing certificate management functions across subsidiaries, departments or geographic boundaries.

The Entrust Certificate Management Service is not only suitable for enterprises, but also for **outsourcers and Web hosters**. The powerful management tools allow these organizations to conveniently manage large numbers of certificates on behalf of their clients and provide flexible reporting tools to facilitate billing.

## 5 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.

The Entrust Certificate Management Service helps organizations secure their online transactions quickly and efficiently with limited effort required by the user or administrator. By leveraging 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 the Entrust Certificate Management Service and how it can help your business grow, please refer to the Entrust Web site at [www.entrust.net](http://www.entrust.net)

## 6 About Entrust

Entrust, Inc. [NASDAQ: ENTU] is a world leader in securing digital identities and information. More than 1,650 enterprises and government agencies in more than 60 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.