Securing E-Commerce and Building Customer Confidence

Starfield Technologies Secure Certificate Services

Introduction

Recent numbers from the U.S. Department of Commerce show that online retail is continuing its rapid growth. However, fear of inadequate online security is causing online retailers to lose out on business as potential customers balk at buying online, worrying that their credit card information and other sensitive data will be abused or compromised.

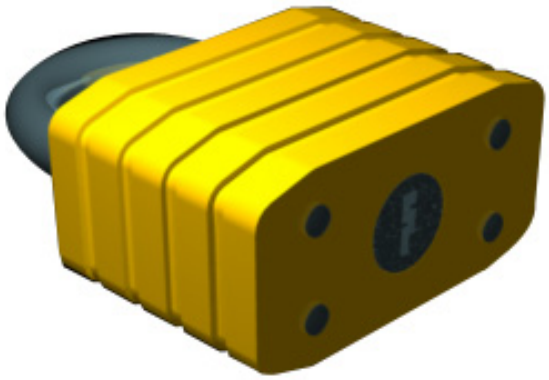
For e-businesses, the key is to build trust: Running a successful online business requires that your customers trust that your business effectively protects their sensitive information from intrusion and tampering.

Installing a 128-bit SSL Secure Certificate from the Starfield Technologies Certification Authority (CA) on your e-commerce Web site allows you to secure your online business and build customer confidence by encrypting all online transactions. A Secure SSL Certificate on your business's Web site will ensure that sensitive data is kept safe from prying eyes. With a Secure SSL Certificate, customers can trust your site.

Before issuing a certificate, the CA rigorously authenticates the requestor's domain control and, in the case of High Assurance SSL Certificates, the identity and, if applicable, the business records of the certificate-requesting entity. The authentication process ensures that customers and business partners can rest assured that a Web site protected with a Secure SSL Certificate can be trusted.

A Secure SSL Certificate from Starfield provides the security your business needs and the protection your customers deserve.

With a Secure SSL Certificate, customers will *know* that your site is secure.



Securing E-Commerce and Building Customer Confidence

Starfield Technologies Secure Certificate Services

Why You Need a Secure SSL Certificate

In the rapidly expanding world of electronic commerce, security is paramount. Despite booming Internet sales, widespread consumer fear that Internet shopping is not secure still keeps millions of potential shoppers from buying online. Only if your customers trust that their credit card numbers and personal information will be kept safe from tampering can you run a successful online business.

For online retailers, securing their shopping sites is paramount. If consumers perceive that their credit card information *might* be compromised online, they are unlikely to do their shopping on the Internet.

A Secure SSL Certificate enables you to build an impenetrable fortress around your customers' credit card information.

A Secure SSL Certificate provides an easy, cost-effective and secure means to protect customer information and build trust. A Secure SSL Certificate enables Secure Sockets Layer (SSL) encryption of your business' online transactions, allowing you to build an impenetrable fortress around your customers' credit card information.

SSL certificates from Starfield bring the highest level of trust to your online business. A Secure SSL Certificate ensures that all sensitive transactions are kept securely encrypted and safe from prying eyes, and rigorous authentication guarantees that Starfield certificates are issued only to entities whose existence and domains can be verified.

Secure SSL Certificates offer industry-leading security and versatility:

- ✓ Fully validated
- ✓ 128-bit encryption
- ✓ One- , two or three-year validity (Turbo SSL Certificates valid up to 10 years)
- ✓ 99% percent browser recognition
- ✓ Stringent authentication
- ✓ Around-the-clock customer support

Securing E-Commerce and Building Customer Confidence

Starfield Technologies Secure Certificate Services

What Is a Secure SSL Certificate?

A Secure SSL Certificate (aka "Web Server Certificate") is a digital certificate that authenticates the identity of a Web site to visiting browsers and encrypts information for the server via Secure Sockets Layer (SSL) technology. Encryption is the process of scrambling data into an undecipherable format — ciphertext —, which can only be returned to a readable format with the proper decryption key.

A certificate serves as an electronic "passport" that establishes an online entity's credentials when doing business on the Web. When an Internet user attempts to send confidential information to a Web server, the user's browser will access the server's digital certificate and establish a secure connection.

A certificate serves as an electronic "passport" that establishes an online entity's credentials when doing business on the Web.

A Web Server SSL Certificate contains the following information:

The certificate holder's name,
The certificate's serial number and expiration date,
Copy of the certificate holder's public key,
The digital signature of the certificate-issuing authority.

In order to obtain an SSL certificate, you must generate and submit a Certificate Signing Request (CSR) to a trusted Certification Authority, such as Starfield Technologies, which will authenticate the requestor's identity, existence and domain registration ownership before issuing a certificate.

Public and Private Keys

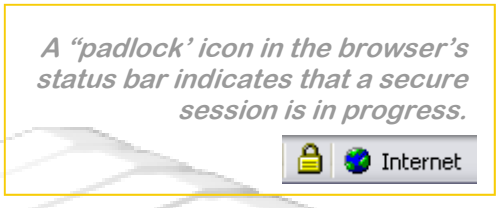
When you create a CSR, the Web server software with which the request is being generated, creates two unique cryptographic keys: A *public* key, which is used to encrypt messages to your (i.e., the certificate holder's) server and is contained in your certificate, and a *private* key, which is stored on your local computer and "decrypts" the secure messages so they can be read by your server. In order to establish an encrypted link between your Web site and your customer's Web browser your Web server will match your issued SSL certificate to your private key. Because only the Web server has access to its private key, only the server can decrypt SSL-encrypted data.

Securing E-Commerce and Building Customer Confidence

Starfield Technologies Secure Certificate Services

Enabling Safe and Convenient Online Shopping

A Secure SSL Certificate secures safe, easy and convenient Internet shopping. Once an Internet user enters a secure area — by entering credit card information, e-mail address or other personal data, for example — the shopping site's SSL certificate enables the browser and Web server to build a secure, encrypted connection. The SSL "handshake" process, which establishes the secure session, takes place discreetly behind the scenes, ensuring an uninterrupted shopping experience for the consumer. A "padlock" icon in the browser's status bar and the "https://" prefix in the URL are the only visible indications of a secure session in progress.



A "padlock' icon in the browser's status bar indicates that a secure session is in progress.

By contrast, if a user attempts to submit personal information to an unsecured Web site (i.e., a site that is not protected with a valid SSL certificate), the browser's built-in security mechanism will trigger a warning to the user, reminding him/her that the site is not secure and that sensitive data might be intercepted by third parties. Faced with such a warning most Internet users likely will look elsewhere to make a purchase.

128-Bit Encryption

Secure SSL Certificates from Starfield use 128-bit SSL encryption to secure online transactions. Virtually unbreakable, 128-bit encryption is used by all banking infrastructures to safeguard sensitive data.

Encryption strength is measured in key length — number of bits in the key. To decipher an SSL communication, one needs to generate the correct decoding key. Mathematically speaking, 2^n possible values exist for an *n*-bit key. Thus, 40-bit encryption involves 2^{40} possible values. 3-bit encryption involves eight possible values, 4-bit encryption 16 possible values, and so on. A 128-bit key involves a staggering 2^{128} possible combinations, rendering 128-bit encrypted data de facto impervious to intrusion. Even with a *brute-force attack* (the process of systematically trying all possible combinations until the right one is found) cracking a 128-bit encryption is computationally unfeasible.

128-bit encryption is expected to provide sufficient encryption strength for Internet purposes for at least the next ten years.

Securing E-Commerce and Building Customer Confidence

Stringent Authentication — A Matter of Trust

Before Starfield issues a Secure SSL Certificate, the applicant's company or personal information undergoes a rigorous authentication procedure that serves to pre-empt online theft and to verify the domain control and, if applicable, the existence and identity of the requesting entity. Only through thorough validation of submitted data can the online customer rest assured that online businesses that utilize SSL certificates from this CA indeed are to be trusted.

A High Assurance certificate guarantees that the entity that owns the certificate is who it claims to be and has a legal right to use the domain from which it operates.

Secure SSL Certificates are only issued to entities whose domain control and, depending on certificate type, business credentials and contact information have been verified. Thus, a Secure SSL Certificate guarantees that the entity that owns the certificate is who it claims to be and has a legal right to use the domain from which it operates.

Starfield issues three types of Secure SSL Certificates, each of which relies on authentication of a number of elements:

High Assurance Certificate — Corporate: The CA will authenticate that:

- The certificate is being issued to an organization that is currently registered with a government authority.
- The requesting entity controls the domain in the request.
- The requesting entity is associated with the organization named in the certificate.

High Assurance Certificate — Small Business/Sole Proprietor The CA will authenticate that:

- The individual named in the certificate is the individual who requested the certificate.
- The requesting individual controls the domain in the request.

Medium Assurance (i.e., Turbo SSL) certificate — The CA will authenticate that:

- The requesting entity controls the domain in the request.

Securing E-Commerce and Building Customer Confidence

Establishing a Secure Connection — How SSL Works

A secure, SSL-encrypted connection is established via the SSL "handshake" process, which transpires within seconds — transparently to the end user. In essence, the SSL "handshake" works thus:

- When accessing an SSL-secured Web site area, the visitor's browser requests a secure session from the Web server.
- The server responds by sending the visitor's browser its server certificate.
- The browser verifies that the server's certificate is valid, is being used by the Web site for which it has been issued, and has been issued by a Certificate Authority that the browser trusts.
- If the certificate is validated, the browser generates a one-time "session" key and encrypts it with the server's public key.
- The visitor's browser sends the encrypted session key to the server so that both server and browser have a copy.
- The server decrypts the session key using its private key.
- The SSL "handshake" process is complete, and a secure SSL connection has been established.
- A padlock icon appears in the browser's status bar, indicating that a secure session is under way.

Securing E-Commerce and Building Customer Confidence

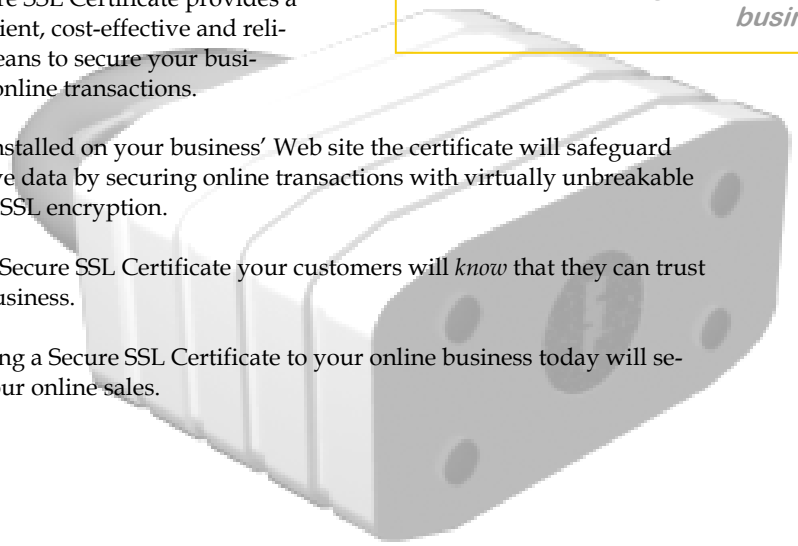
Conclusion — The Key to Online Security

Demand for reliable online security is increasing. Despite booming online sales many consumers continue to believe that shopping online is less safe than doing so at old-fashioned brick-and-mortar stores.

The key to establishing a successful online business is to build customer trust. Only when potential customers trust that their credit card information and personal data is safe with your business, will they consider making purchases on the Internet.

With a Secure SSL Certificate your customers will know that they can trust your business.

A Secure SSL Certificate provides a convenient, cost-effective and reliable means to secure your business's online transactions.



Once installed on your business' Web site the certificate will safeguard sensitive data by securing online transactions with virtually unbreakable 128-bit SSL encryption.

With a Secure SSL Certificate your customers will *know* that they can trust your business.

Applying a Secure SSL Certificate to your online business today will secure your online sales.