

This technical information may contain copyright materials of Digital Marketing Solutions LLC. It's only provided to the owner of this website for the sole purpose of training. Any third party use of this material requires written permission from its owner DMS.

## **E-COMMERCE SECURITY FOR DMS CUSTOMERS**

### **WHAT IS SSL?**

#### **Secure Sockets Layer (SSL)**

Secure Sockets Layer ([SSL](#)) technology protects your Web site and makes it easy for your Web site visitors to trust you in three essential ways:

1. An SSL Certificate enables **encryption** of sensitive information during online transactions.
2. Each SSL Certificate contains unique, **authenticated** information about the certificate owner.
3. A Certificate Authority **verifies** the identity of the certificate owner when it is issued.

#### **You need SSL if...**

you have an online store or accept online orders and credit cards

you offer a login or sign in on your site

you process sensitive data such as address, birth date, license, or ID numbers

you need to comply with privacy and security requirements

**you value privacy and expect others to trust you.**

### **How It Works**

#### **How Encryption Works**

Imagine sending mail through the postal system in a clear envelope. Anyone with access to it can see the data. If it looks valuable, they might take it or change it. An [SSL Certificate](#) establishes a private communication channel enabling encryption of the data during transmission. Encryption scrambles the data, essentially creating an envelope for message privacy.

Each SSL Certificate consists of a **public key and a private key**. The public key is used to encrypt information and the private key is used to decipher it. When a Web browser points to a secured domain, a Secure Sockets Layer handshake authenticates the server (Web site) and the client (Web browser). An encryption method is established with a unique session key and secure transmission can begin. [True 128-bit SSL Certificates](#) enable every site visitor to experience the strongest SSL encryption available to them.

#### **How Authentication Works**

Imagine receiving an envelope with no return address and a form asking for your bank account number. Every VeriSign® SSL Certificate is created for a particular server in a specific domain for a verified business entity. When the SSL handshake occurs, the browser requires authentication information from the server. By clicking the closed padlock in the browser window or certain SSL trust marks (such as the VeriSign Secured® Seal), the Web site visitor sees the authenticated organization name. In high-security browsers, the authenticated organization name is prominently displayed and the address bar turns green when an Extended Validation SSL Certificate is detected. If the information does not match or the certificate has expired, the browser displays an error message or warning.

#### **Why Authentication Matters**

Like a passport or a driver's license, an SSL Certificate is issued by a trusted source, known as the **Certificate Authority (CA)**. Many CAs simply verify the domain name and issue the certificate. VeriSign verifies the existence of your business, the ownership of your domain name, and your authority to apply for the certificate, a **higher standard of authentication**.

VeriSign **Extended Validation (EV) SSL Certificates** meet the highest standard in the Internet security industry for Web site authentication as required by CA/Browser Forum. EV SSL Certificates give high-security Web browsers information to clearly display a Web site's organizational identity. The high-security Web browser's address bar turns green and reveals the name of the organization that owns the SSL Certificate and the SSL Certificate Authority that

This technical information may contains copyright materials of Digital Marketing Solutions LLC. It's only provided to the owner of this website for the sole purpose of training. Any third party use of this material requires written permission from its owner DMS.

issued it. Because **VeriSign is the most recognized name in online security**, VeriSign SSL Certificates with Extended Validation will give Web site visitors an easy and reliable way to establish trust online.

[Click here for more information about online securities](#) or <http://www.verisign.com/ssl/ssl-information-center/ssl-resources/index.html>

### **PUBLIC SSL vs. PRIVATE SSL**

Most payment gateway providers such as Paypal, Google Checkout, Verisign, Authorize.net provide the SSL as a payment gateway services without you having to buy a private one.

Example 1:

<https://www.paypal.com/us/cgi-bin/webscr?cmd=flow&SESSION=dsBGfUk1QCo5TwJcGAjbClm7Cy02i0UfnDgueC41LNKcHbqRMAjrnuDGwIS&dispatch=50a222a57771920b6a3d7b606239e4d529b525e0b7e69bf0224adecfb0124e9bed5d628c85727479b1b92b132a6281aab8c2c6f2ee34f0a1>

I got to the above link after I hit "Submit Order". It took me from the website [www.computrainsolutions.com](http://www.computrainsolutions.com) to the Paypal payment gateway. Please notice the "https:", it means that there is a SSL protection on this page. Here is where I can safely enter my credit card info and submit it without fearing the content of the submission is being stolen away. Without the "https" or with only the "http", your submission can be stolen by the online thief(s) because that submission is transported in a "transparent envelop".

### **When do you need a private SSL?**

1. Some payment gateway providers especially the "cheap" ones do not provide SSL.
2. You have a need to store customer's credit card info on your own database for later payment processing or other purposes.
3. You want to keep your customer within your domain (not having to go to <https://www.paypal.com> for an example to enter the payment)

This means that your customers now enter their credit card info under your own domain name such as <https://www.computrainsolutions.com> assuming that [www.computrainsolutions.com](http://www.computrainsolutions.com) is your domain or in share domain name that is outside of the payment gateway provider. In such case, your web developer Digital Marketing Solutions LLC has to purchase a SSL and a private IP address for you.

### **The risk of having a private SSL.**

In addition to the extra costs of having a private SSL, there is a great risk of having to constantly protect your private and confidential data such as credit card numbers that belong to your customers. The risk here is more of an internal risk. Let say one of your employees has access to the login ID and password to your database and decided to steal the information for illegal purposes, you as the owner of the website can be held responsible for your employee's illegal act. Furthermore, our server is as secured as it can be but there is no absolute 100% security proof. We made no claim that our server is 100% error free or 100% security proof. There is no such thing in the IT world.

### **Recommendation**

We recommend that by all means you should choose a payment provider that provides SSL service. This put the responsibility of protecting your customer's confidential info on them instead of you. Digital Marketing Solutions LLC is a web design and web developing firm. We are not in the business of "data security" service provider. All responsibility of protecting your customer's confidential data is on you and only you.

I, \_\_\_\_\_, (Customer), have read, understood and agreed the above E-COMMERCE SECURITY. Signed \_\_\_\_\_ Date \_\_\_\_\_