Securing Your Website Using SSL

The purpose of this paper is to explain how to secure your website using SSL. It is mostly targeted at business rather than technical readers.

How does an SSL certificate benefit my business?

There are two main reasons to use an SSL certificate. The first is to **protect people who use your website.** It stops hackers from being able to eavesdrop, steal and even modify your users' data while it is being transmitted between the website and web browser. This might be financial, personal or confidential information. The second reason is to **encourage people to use your website** by having a trusted 3rd party verify that your website is legitimate.

The only downside, apart from the cost, is that due to the encryption, your website will run a little more slowly.

What is an SSL certificate?

Secure Sockets Layer (SSL) certificates are used to encrypt data that is sent between a web browser and a website. Only these two parties have access to the data and any hackers will not see anything intelligible. When a website is secured by SSL, the user of the website will see a notification in the browser address bar such as a padlock or a green colour. Another indication is that the address of the website is preceded with https rather than http.

A traditional analogy is with the postal system. The postman and anyone else who handles your mail can read your postcard. It can be easily stolen from your letter box and the message on it could even be changed. You would not write your credit card number on a postcard and you would not write personal information.

Two keys are used to set up an SSL connection: a private key and a public key. A key is just a long string of data that is analogous to the teeth on your front door key. The public key is freely given out but the private key is kept secure by the web-server. The public key can be used to lock up (encrypt) data but only the private key can unlock (decrypt) it.

When a secured page is requested, the web-server will return the certificate and the public key. The browser will check the certificate for validity before displaying content. When a user enters data in a form, the browser will encrypt the data using the public key and send it to the web-server. The web-server will decrypt it with the private key and process the data.

This explanation is simplified but this should serve to illustrate the idea.

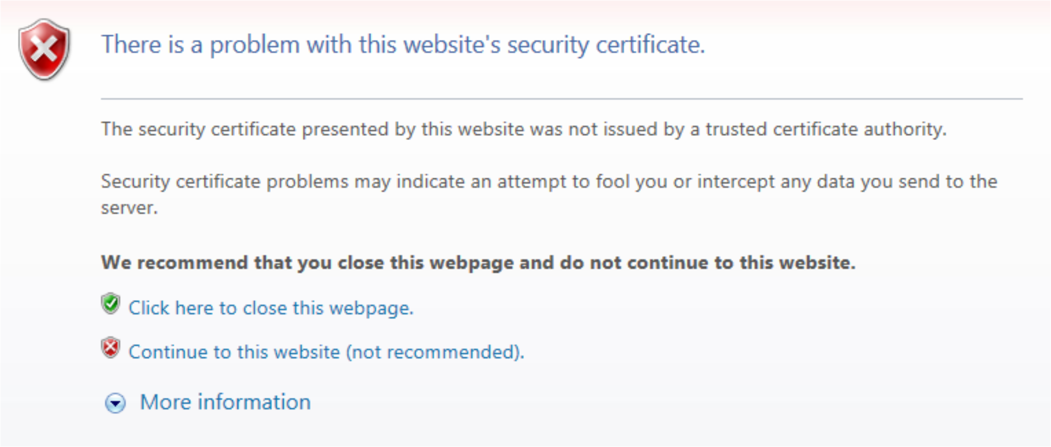
SSL certificates are created by trusted third parties called Certificate Authorities (CA). One of their responsibilities is to confidently assure us that the buyer, the organisation and the website is legitimate. Actually anyone can create an SSL Certificate so it's important to get one that is issued by an official authority. A CA will check out your application before they issue the certificate to ensure that they are not issuing to a hacker.

Different types of SSL certificate

There are different types of SSL certificate with different costs. Due to the difference in the depth of the initial verification procedure, the time taken to obtain a certificate varies from almost immediate to 10 days.

Self- Signed

Anyone can create their own "self-signed" certificate. There is no cost to this but it is fairly useless as a means to protecting your website. This is because no trusted 3rd party verified the authenticity of the certificate. However it can be useful to ensure that your new website will work correctly once a proper certificate is purchased. In theory it can be used for an intranet that is only accessible from within the firewall. However staff will not appreciate the message that browsers display when accessing a website that uses a "self-signed" certificate:



There is a problem with this website's security certificate.

The security certificate presented by this website was not issued by a trusted certificate authority.

Security certificate problems may indicate an attempt to fool you or intercept any data you send to the server.

We recommend that you close this webpage and do not continue to this website.

Click here to close this webpage.
Continue to this website (not recommended).
More information

Domain Validated

Also known as Low Assurance certificates, these are the most basic certificate provided by a 3rd party. It is used to verify the website domain. It does not verify the organisation that operates the website. The issuer will verify that the applicant has registered the domain name to which the certificate will be associated. It provides basic security but a hacker can still gain access to your customers' information.

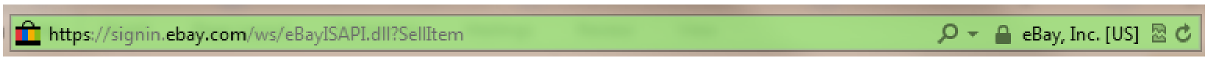
Organizationally Validated (OV)

Also known as High Assurance certificates, these certificates verify that the applicant's business is correct, as well as their domain name.

Extended Validation (EV)

Before an EV certificate is issued, the issuer will check the person applying, their organisation and the domain.

The result is the highly trusted green bar and company name being displayed in the browser. This will give ultimate confidence to customers to finalise their transaction.



More Information

These links may help you to choose a Certificate Authorities to purchase from. Note that there are plenty of resellers that sometimes offer discounts. You may wish to try eWay, SecurePay or your domain name supplier.

Saving money on SSL certificates:

http://www.sslshopper.com/article-top-10-ways-to-save-money-on-ssl-certificates.html

Compare issuers:

http://www.sslshopper.com/ssl-certificate-wizard.html

http://www.sslshopper.com/free-trial-ssl-certificates.html

Purchasing a certificate:

http://www.sslshopper.com/how-to-order-an-ssl-certificate.html