SSL Certificates

Using OpenSSL [1] we are able to implement the Secure Sockets Layer [2] (SSL v2/v3) and Transport Layer Security [3] (TLS v1) protocols as well as a full-strength general purpose cryptography library. Using the mod_ssl [4] we can apply the strong cryptography of openssl for the Apache [5] webserver via the Secure Sockets Layer [2] (SSL v2/v3) and Transport Layer Security [6] (TLS v1) protocols by the help of the Open Source [7] SSL/TLS toolkit OpenSSL [1]

We can setup certificates that are signed by yourself or a third party you choose like verisign [8] or tucows. [9] For companies we are not an authorized reseller a labor charge will apply for setup.

We accept many forms of payments including credit cards, e-gold, gold grams and other digital gold currencies. Call or email us with your questions, certs@cocoavillagepublishing.com [10]

	QuickSSL™	QuickSSL Premium™	True BusinessID™	True BusinessID™ Wildcard
Verification of Entity	Domain	Domain	Organization & Domain	Organization & Domain
Documentation Required for Authentication	Domain Authorized E-mail	Domain Authorized E-mail	Proof of Organization or DUNS Number and WHOIS	Proof of Organization or DUNS Number and WHOIS
Included in Product	Certificate only	Certificate & Site Seal	Certificate & Site Seal	Certificate & Site Seal
Name in Seal	N/A	Domain Name	Organization & Domain Name	Organization & Domain Name
Terms	1-3yrs	1-3yrs	1-3yrs	1-3yrs
Retail Price	$149 – 1 year $261 – 2 years $372 – 3 years	$199 - 1 year $348 – 2 years $498 – 3 years	$249 – 1 year $436 – 2 years $622 – 3 years	$799 – 1 year $1,223– 2 years $1,748 – 3 years

The following applies in general, but in specific to certificates resold from tucows:

Web Certificates Sample Frequently Asked Questions

This section provides the answers to the most commonly asked questions about our web certificates.

What is a Web-Certificate?

A Web Server Certificate permits securer communication between a client and a server (say a customer's browser and a web retailer's server) or two servers (any servers who want to "talk" securely amongst themselves). Simply stated, a web-certificate is a digital document that has unique codes to identify the holder of the certificate to the person accessing the site.

A Personal Certificate is issued to individuals to certify their identity. One can use them to digitally sign email, documents, jar files etc. to prove that they were the author, and that the files have not been tampered with.

Cocoa Village Publishing offers web certificates. As an authorized TUCOWS reseller if available we may also offer their Personal Certificates along with other security products.

How does a web-certificate work?

A Web-certificate functions as follows:

- Whenever anybody transacts with a "secure" web-site, their browser (or server) authenticates the identity of the web-site using the web-certificate
- If the site's certificate is not valid, a warning is issued to the user, otherwise the web-cert creates an SSL (Secure Server Layer) session and encrypts any information exchanged during that session
- This prevents communication from being intercepted and deciphered by nefarious people on the Internet.

Can you explain "how a web certificate works" in "Plain English"?

Basically, when two parties (say a customer and the Amazon.com web-site) wish to "talk" securely (transfer the customer's credit-card number to Amazon.com), then a web-certificate sets up a "secure" session that first verifies the true identity of the party that requests data transfer (Amazon.com).

If a certificate is valid, the other party (the customer) gets a message saying that its OK to "talk" to them (Amazon.com), as they are who they say they are. The other party (customer) then transfers the info (CC number) securely, without fear of any nefarious elements intercepting the data.

If the certificate is invalid, a message pops up saying so. Transactions can still occur, but at the risk of counter party fraud (It may be joesbooks.com tying to appear as Amazon.com)

How can someone tell whether a website is using a web certificate or not?

The pages of a web-site which are secured by a web-certificate are characterized by the following traits:

- The URL of the secure web-pages change from http://... to https://
- A lock symbol appears in the lower left-hand (right hand) status bar in Netscape Navigator (Internet Explorer).

If one wants to view and verify the encryption information of the secure pages, onw should simply undertake the following:

- In Netscape - click on the lock symbol above and select "View Certificate" button
- In Internet Explorer - double-click on the lock in the lower right-hand status bar.

How are your web certificates trusted by the browsers?
Our web certificates are automatically and transparently trusted by browsers. This trust is established because our supplier's Root Certificate has been embedded in all major browsers.

What browsers will my web certificate work with?
That depends upon who issues the certificate, the root certificate of authoriaty (root ca). Even VeriSign, the first company contacted by Netscape to first do web site certificates, may have problems with expiration dates on old browsers.

Tucows security products are provisioned from GeoTrust and are backed with Root Certification Authority. The Root Authority is embedded in all the leading browsers, enabling seamless connectivity to sites secured with these digital certificates. The specific browser recognition properties are outlined in the table below:

Browser	Support Level
AOL Browser 6.x	Fully supported
AOL Browser 7.x	Fully supported
Microsoft Internet Explorer 6.x	Fully supported
Microsoft Internet Explorer 5.01+	Fully supported
Netscape 6.X	Fully supported
Netscape Navigator 4.51X and higher	Fully supported
Opera 5	Fully supported

How long does it take to get a web certificate?
Companies will usually receive a web certificate within three business days after the verification has been complete. The verification period varies and relies greatly on the information provided by the company during the application process.

How strong are Tucows server certificates?
Tucows server certificates are 1024 bit capable and support 128 bit browsers.

The strength of the public key in the certificate is defined by you when you generate the key pair for your server. If you generate a 1024-bit key pair and submit the associated CSR (Certificate Signing Request), then the certificate you receive contains the 1024-bit public key. If you generate a 512-bit key pair then the certificate contains the 512-bit public key.

Is my web certificate tied to my IP address?
No, server certificates do not contain any information about IP addresses. However, the domain name listed in the server certificate must match the domain name of the server on which the Web server certificate is installed. The domain name can be mapped to any IP address.

I am using several servers in a load-balancing configuration. How many web certificates do I need?
You will need one web certificate for each of your secure servers (including any virtual servers).

How do I correct information on my web certificate after it has been issued to me?
You must issue a request to correct your information on your web server certificate. You can request one replacement web server certificate within 30 days of the certificate being issued without being charged. Any requests made after the 30-day period, or any requests outside the primary request, will require you to purchase a new web server certificate. If a processing error occurs, we will issue a new web server certificate at no cost to you.

In order to change any information, we must re-issue a new web certificate with the correct information and re-sign it - this preserves the integrity of the web certificate. All our web certificates are electronically signed by the Root Certificate. This electronic signature ensures that none of the information contained in the web server certificate has been modified or tampered with. See http://www.certificateregistration.com/ [15]

How will I know if my enrollment was successful?
The Technical Contact, Authorized Contact and Bill Contact will receive an e-mail when your order has been processed. This e-mail includes a link to your request status page and links to each of the Web server certificates that have been issued. If any of your server certificate requests have not been approved the status page explains why.

With the recent partnership of GEO Trust and Tucows/Opensrs the feature of "True Site" is possible,

True Site FAQ

What is True Site?
True Site provides a simple way for your customers to view your validated organization information via a trusted third party. True Site will increase transactions and revenue by giving your customers the confidence and assurance to trust the identity of your web site. The result- a substantial increase in consumer confidence regarding your web site information, services, and/or products. Even if you don't have a web site brand name, True Site will let your customers know you are legitimate.

True Site, a patent pending "smart icon" that resides on a web page(s), independently identifies a website is legitimate, authentic, and validated via a trusted third party. For more information, please see our True Site white paper.

Why do I need True Site?
In a sea of over 30 million websites and over 1 billion web pages, it is very difficult for people to know who is legitimate and who is not. Most organizations on the web today do not have a brand name to overcome the odds of being 1 out of 30 million. True Site is a tool that your organization can use to substantially reduce these odds and set your web site apart from the crowd.

Organizations enrolled in True Site use their online identities to send these messages:

- Owner is known and associated with the web site
- Consumers know that your organization is legitimate
- Consumers know that your web site is genuine
- Smart icon has company and time/date stamp embedded. If a user tries to recreate a static image, it will not update with the current time and date.

True Site sets your web site apart, resulting in:

- Increased customer traffic
- More time spent browsing the trusted content on your web site
- Improved probability of a customer transaction

If you are serious about your web site, you should consider True Site.

How does True Site Work?
True Site uses patent pending technology to create a "smart icon" that actively displays the identity of the organization behind the web site. When a customer clicks on the True Site "smart icon," the server performs a domain name lookup to verify that the user is clicking on a legitimate icon. Consumers, seeking to know and trust the web domains they visit, will know from the icon if the web site owner is a True Site member.

How do I install True Site?
Once you have enrolled in True Site, installation is simply adding a few lines of JavaScipt to each web page on which you want the True Site seal to appear. Click here [16] for the full instructions.

What do I get with True Site?
True Site comes with annual unlimited use for each fully qualified domain name purchased for your organization.

How do I get True Site?
Contact your Tucows OpenSRS Reseller, Cocoa Village Publishing.

Source URL: https://cocoavillagepublishing.com/services/ssl_certificates/index.html#comment-0

Links
[1] http://www.openssl.org/
[2] http://www.netscape.com/eng/ssl3/
[3] http://www.consensus.com/ietf-tls/ietf-tls-home.html
[4] http://www.modssl.org/
[5] http://www.apache.org/
[6] http://www.ietf.org/rfc/rfc2246.txt
[7] http://www.opensource.org/
[8] http://www.verisign.com/
[9] http://www.opensrs.net/
[10] mailto:certs@cocoavillagepublishing.com
[11] http://resellers.tucows.com/opensrs/certificates/certs_techspecs#qssl
[12] http://resellers.tucows.com/opensrs/certificates/certs_techspecs#qsslpre
[13] http://resellers.tucows.com/opensrs/certificates/certs_techspecs#trubiz
[14] http://resellers.tucows.com/opensrs/certificates/certs_techspecs#trubizwild
[15] http://www.certificateregistration.com/
[16] http://www.geotrust.com/true_site/install.htm