Straightforward Explanation of SSL and HTTPS.

How does SSL work?
Quick SSL Fact:
Getting your own SSL certificate usually requires some coordination with your web host. A *"certificate signing request"* needs to be generated on your hosting server. This is normally done by the hosting company staff.

How does SSL work?
Quick SSL Fact 2:
Using an SSL certificate on your account requires the hosting account to have it's own IP address. Many hosting companies charge extra for this or only have IP addresses included in their higher packages. If you plan to use your own SSL certificate be sure your hosting package includes an IP address. (see our our hosting recommendations)

Shared SSL Certificates:
Some web site hosting companies have "shared" SSL certificates available. Using shared SSL certificates can be a good alternative to

How does SSL work Navigation

How does ssl work?

Simplified SSL - About Secure Sockets Layer and HTTPS

Information regarding specific SSL certificate providers can be found by clicking here.

Processing transactions securely on the web means that we need to be able to transmit information between the web site and the customer in a manner that makes it difficult for other people to intercept and read. SSL, or Secure Sockets Layer, takes care of this for us and it works through a combination of programs and encryption/decryption routines that exist on the web hosting computer and in browser programs (like Netscape and Internet Explorer) used by the internet public.

See the left side panel for information on how ***shared*** secure certificates work.

SSL Overview from the Customer's Browser viewpoint

1. Browser checks the certificate to make sure that the site you are connecting to is the real site and not someone intercepting.
2. Determine encryption types that the browser and web site server can both use to understand each other.
3. Browser and Server send each other unique codes to use when scrambling (or encrypting) the information that will be sent.
4. The browser and Server start talking using the encryption, the web browser shows the encrypting icon, and web pages are processed secured.

Detailed SSL/HTTPS:
See our **detailed step-by-step** *SSL walk-through* including diagrams and sidebars on items like cyphers and man-in-the-middle attacks.

Are you looking for a comparison of the primary SSL certificate providers?

Click here to take see our SSL Provider Summary.

About Merchant and Gateway Accounts
Selecting a web host

having your own. They can usually be easily integrated into your shopping cart and can save site owners the expense and effort of getting their own certificates. For more information on **shared SSL certificates** click here.

SSL web site hosting companies: Most hosting companies allow for hosting your own SSL certificate. There is often an additional charge added to your monthly web site hosting fee for this. Our e-commerce web site hosting companies recommendations include SSL hosting with all packages at no additional cost other that a small setup fee.

Be sure to check SSL hosting fees before selecting an e-commerce web site hosting company.

More Resources: If you want more detail on items such as the cyphers used and how the behind the scenes validation works, click here to view Netscape papers or here for our detailed description.

Click here for our detailed SSL/HTTPS walk through >>

About IP addresses and SSL: Though your SSL certificate is bound to your fully qualified domain name (encrypted into the certificate request and registerd when you purchase your certificate) web servers link the certificate to the IP address. The result is that if you attempt to have more than one SSL certificate associated with the same IP address (in the case of virtual hosting) you may get undesired results.

Typically the certificate that will be used for the IP address, no matter which domain you attempt to access, will be the first one in the web server's configuration file. This is important to note for the web site owner because many of the budget and free web hosting services do not give you your own IP address.

Getting a unique IP address for an SSL certificate is usually the main factor in extra pricing for secure hosting on the budget web hosts and can often increase your pricing past that of a full service host. Even with full service web hosts if you need seperate certificates for multiple domains you will often need to open individual accounts for each so that they have their own IP addresses. On the other hand, since the certificate itself is not linked to the IP address you can usually move the certificate from one web host to another (as long as you have a unique IP address at the new host).

Our Detailed How does SSL work pages include additional IP address notes in the sidebars.

What does the typical merchant need to know about how SSL works?

Though it is good to answer the "How does SSL work?" question (see the steps on the following pages) the typical merchant really needs to only be concerned with how to get a secure certificate and making sure that he/she is using a valid and current ssl certificate (step 2.03) and what URL to use when creating secure links. SSL certificates are purchased from various certificate vendors and it requires a CSR (Certificate Signing Request) to be generated on the web server. This usually involves getting in touch with the hosting company and asking them to generate the CSR for you. After your receive the CSR (which looks like an encrypted block of undecipherable text) you can order your certificate from the SSL certificate provider. Once you receive the SSL certifcate back from the certificate authority, you will normally need the hosting company to install it for you.

You also need to be sure that your hosting account will allow an SSL certificate. The primary factor is a unique IP address (as stated above). If not documented on your web host's web site, it is a good idea to contact them directly. You want to know a) whether or not your account can handle its own certificate and b) what additional costs are involved.

After the web host installs the new certificate on the web server the merchant/designer will need to be sure that the desired secure pages

are called using "https://" in their links. All components on the page should either use a relative path (without https or http) or "https://" in order to avoid browser messages saying that some items are not secure. Addressing additional page items (such as images) using a relative path will default to the same protocol used when the page was displayed.

Some web hosting companies have "shared" SSL certificates that you can use under their domain name. This eliminates the need for you to get your own. As an example, if OurShop.com were a web hosting company and xyz.com had an account there, they could use the shared certificate with a URL something like "https://xyz.ourshop.com". A merchant that prefers to have their secure processing under their own domain name will need to get their own SSL certificate. **Click Here** for our *How does shared ssl work?* page.

Our SSL certificate provider recommendation page can help you understand which SSL certificate provider is right for you. This page can be found by clicking here.

How Does SSL Work? - Detail Step 1 >

SSL Certificate Provider Recommendations >

Recommended books about SSL and encryption >

Not finding the SSL answer you need?
Enter your secure certificate question here and we'll try to add it.

Submit Comment

[OurShop.com Web Site Hosting Resources for E-commerce Companies - Home]

[Site Map]

Quick SSL Fact:

SSL authentication assures authentication on both ends. It not only encrypts the data but determines whether or not each party (server and client) has the expected authentication.

Though secure certificates can be created independently, getting a secure certificate from a validated certificate authority helps to ensure the parties are trusted.

Can I get an SSL Certificate for an IP address?

This question comes up from time to time where a site would like to have secure access but does not want to use a domain name.

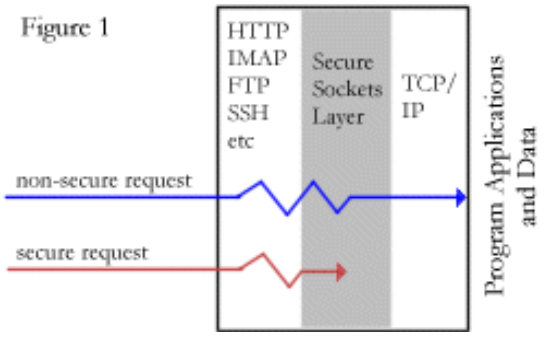
The answer we have at this time is that you can get an SSL certificate for an IP address (entering the IP address anywhere that it asks for FQDN) ***however*** the IP address must be registered to the entity requesting the certificate. This means that you most likely would not be able to do this with a Web Trust approved certificate authority

How does ssl work?

Detailed SSL - Step 1 Determine Secure Communication

(updated 2004-01-15)

This is page 2 of our SSL articles. You can go back to the SSL overview by clicking here.



Internet communication typically runs through multiple program layers on a server before getting to the requested data such as a web page or cgi scripts.

The outer layer is the first to be hit by the request. This is the high level protocols such as HTTP (web server), IMAP (mail server), and FTP (file transfer).

Determining which outer layer protocol will handle the request depends on the type of request made by the client. This high level protocol then processes the request through the Secure Sockets Layer. If the request is for a non-secure connection it passes through to the TCP/IP layer and the server application or data.

If the client requested a secure connection the ssl layer initiates a handshake to begin the secure communication process. Depending on the SSL setup on the server, it may *require* that a secure connection be made before allowing communication to pass through to the TCP/IP layer in which case a non-secure request will send back an error asking for them to retry securely (or simply deny the non-secure connection).

This is a good time to answer a question we periodically get: ***"what does ssl encrypt?"***

This question is usually geared toward whether or not the path and query string is encrypted in an HTTPS "get" request (this is where form field responses or program variables are tagged on to the end of the url). These fields *are* stripped off of the URL when creating the routing information in the https packaging process by the browser and are included in the encrypted data block.

The page data (form, text, and query string) are passed in the encrypted block *after* the encryption methods are determined and the handshake completes.

A related issue that frequently comes up is whether or not form data is transmited with encryption if the blank form is displayed without https. If the form "action" is set to use https then the ssl handshake will take place before the data is sent. Whether or not the original form is displayed using https has little to do with the

since most web site hosting companies have their IP addresses registered to them (the hosting company). Contact your hosting company to discuss IP ownership. You may also want to look into generating your own non-CA certificate.

form submission unless the form action uses a relative path, in which case the default will be to use the protocol that was used to display the form.

This applies to both the request *and* the response.

Next >> Initiate the SSL Handshake >

SSL Certificate Provider Recommendations >

Recommended books on SSL and Encryption >

Back to How Does SSL Work? Overview >

[OurShop.com Web Site Hosting Resources for E-commerce Companies - Home]

[Site Map]

Quick SSL Fact 2:

Man-in-the-middle attacks occur when the communication is intercepted en route. This is where an unauthorized program sends its own certificate back to the client and makes a client request to the server. Rather than the client and server validating with each other they are validating with the unauthorized program.

Using (*and expecting*) certificates from valid certificate authorities minimizes this risk.

SSL Performance Issues:

Latency is increased with SSL connection since as shown in these "hand shake" steps there are additional round trips added in order to establish authentication. *This is only a fraction of a second for each connection so it wouldn't be noticible on most small or medium businesses*. For large business processing numerous transactions per minute this can add up, especially if "client authentication" is required.

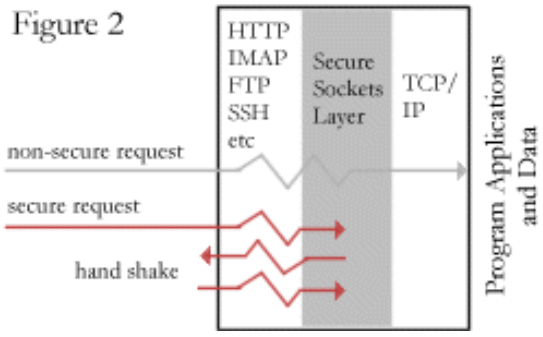
How does ssl work?

Detailed SSL - Step 2 The SSL Hand shake

(updated 2004-01-16)

This is page 3 of our SSL articles. You can go back to the SSL overview by clicking here.

The handshake is the most complicated phase in the process and though our example specifically uses HTTPS (web based security) the same items apply to other protocols.



The "handshake" syncs the server and the client up with the encryption methods and keys that will be used for the remainder of the communications. This is also where the server authentication is determined (and client authentication if required by the server).

Typically it is enough to know that server and client establish a secure connection but the following is a summary of what happens (again, using https and "web browser" as an example):

1. The customer's web browser sends the web site server it's methods of encrypting data. This includes the encryption type, some random data that the encryption programs on both sides can use in the scrambling routines, and other ssl related data.

2. The server returns it's own random data to be used for encryption as well as other secure sockets layer information (including it's ssl certificate with a long string of characters called a public key) that the browser will need in step 4 (step 1 on next page).

3. The customer's browser checks the information it recieved and compares it to the domain it was trying to connect securely with. If the secure certificate information on the web site doesn't match the domain name the browser will notify the customer that there is a problem. **The certificate expiration date and valid certificate authority are also checked at this point.**

   Validating the Certificate Authority is important to prevent "man in the middle" attacks (see left side panel). The CA assures that the certificate was generated by an acceptable entity.

More performance issues on next page.

Next >> Complete the SSL Hand Shake Process >

SSL Certificate Provider Recommendations >

Recommended books on SSL and Encryption >

Back to SSL Certificate Overview >

[OurShop.com Home]

[Site Map]

Quick SSL Fact:

There are a number of different encryption methods that can be employed to assure the data is not readable by anyone interecepting the communication. These "Cyphers" include:

- DES - Digital Encryption Standard
- DSA - Digital Signature Algorithm
- KEA - Key Exchange Algorithm
- MD5 - Message Digest algorithm
- RC2 - Rivest encryption cipher
- RC4 - Rivest encryption cipher
- SHA-1 - Secure Hash Algorithm
- Triple DES - DES used 3 times
- Others

RC2 and RC4 support 128bit encryption. 128 bit encryption allows for 3.4 * 10^{38} (34 with 37 zeros to the left of the decimal place) possible keys. These are extremely hard to crack while 40bit encryption allows for 1.1 * 10^{12} possible keys.

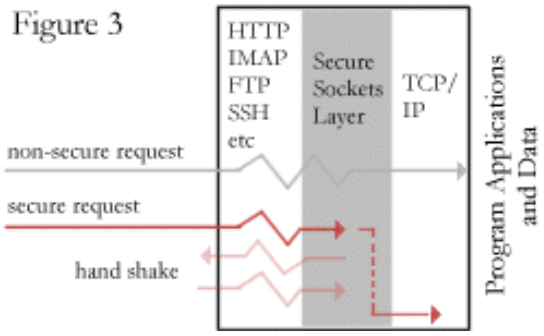
SSL Performance Issues:

Bandwidth considerations are not an issue for most small or medium sized businesses.

How does ssl work?

Detailed SSL - Step 3 Completing The SSL Hand Shake

(updated 2004-01-16)



The handshake finally creates the new key that the remainder of the connection will be using. The end product is then a transmission encrypted based on a calculated key that is based on a combination of verified certificates.

1. The browser now creates a "premaster secret" that will be used to encrypt the rest of the session. This is a random key that it encrypts using the agreed upon encryption method (see left side panel) combined with the server's public key string that it recieved and sends the new encrypted secret string back to the server

   > If the server requires client authentication, it is done at this point using the same steps as those on the preceding page but looking for a certificate on the client side rather than on the server side. Typically this is done in corporate environments.

2. With the new "premaster secret" string, both the browser and the web site server create a new "master secret" string and use it to create session keys (long strings of generated characters) that their encryption programs use for the rest of the session to scramble and descramble (or encrypt/decrypt) all transmissions for the rest of the session. With the Master Secret key in place, both sides are also able to verify that the data didn't change in route.

3. The browser now has the information it needs to establish secure communication and it sends a message to the server saying that it will start using the new session key.

4. The browser (now talking in the encrypted format) verifies to the web server that it is finished locking / securing it's part of the session.

5. The web server then sends a message to the browser saying that it too will start using the new session key.

6. The web server (now talking in the encrypted format) verifies to the browser that it is finished locking / securing it's part of the session.

SSL transactions can however increase by about 1k bytes each which would typically only be a concern when large numbers of transactions are ocurring.

Processor Usage *is* increased with SSL connections but again, this should only be a concern on servers running numerous transactions per minute. Processor usage can also be minimized by using the most processor effeicient encryption methods (RC4 and MD5 are much less processor intensive than DES or Triple DES).

The remainder of the SSL session gets processed between the browser and the web server using the agreed upon encryption with the master secret phrase as the key.

Back - To SSL Overview >

Recommended books on SSL and Encryption >

SSL Certificate Provider Recommendations >

Not finding the secure certificate answer you need?

Enter your secure certificate question here and we'll try to add it.

Submit Quesiton or Comment

[OurShop.com Web Site Hosting Resources for E-commerce Companies - Home]

[Site Map]