

**Using PeaceTrust SSL to boost
Customer Confidence in your web services**

For Apache based Webservers

www.peacetrust.net

A Security Service provided by:
PEACE 2000 INSTITUTE
Reykjavik – London – Las Vegas

Marketed world wide by a network
of independent associates working
with our subsidiary company:
Earthchild Inc

support@earthchild.net
Document delivery by FAX:



Fax Reykjavik: +354 557 1000

Fax: London: +44 870 164 3718



Fax: Las Vegas +1 (801) 740-3532

Why you need **security** for your website

The Internet has created many new global business opportunities for enterprises conducting online commerce. However, the many security risks associated with conducting e-commerce have resulted in security becoming a major factor for online success or failure.

Over the past 7 years, consumer magazines, industry bodies and security providers have educated the market on the basics of online security. The majority of consumers now expect security to be integrated into any online service they use, as a result they expect any details they provide via the Internet to remain confidential and integral. For many customers, the only time they will ever consider buying your products or services online is when they are satisfied their details are secure.

This guide explains how you can utilize PeaceTrustSSL to activate the core security technology available on your existing webserver. You will also learn how PeaceTrustSSL allows you to protect your customer's transactions and provide visitors with proof of your digital identity – essential factors in gaining confidence in your services and identity.

Using PeaceTrustSSL Certificates to secure your online transactions tells your customers you take their security seriously. They will visibly see that their online transaction will be secure, confidential and integral and give them the confidence that you have removed the risk associated with trading over the Internet.

Using Security helps you realize the benefits of online commerce:

- Cost effectiveness of online operations and delivery
- Open global markets – gain customers from all over the world
- New and exciting ways of marketing directly to your customers
- Offer new data products and services via the Web

Only if you have visibly secured your site with SSL security technology will your customers have confidence in your online operations. Read on to learn how SSL helps you achieve the confidence essential to successful e-commerce.

What is SSL?

Secure Sockets Layer, SSL, is the standard security technology for creating an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browser remain private and integral. SSL is an industry standard and is used by millions of websites in the protection of their online transactions with their customers. In order to be able to generate an SSL link, a web server requires an SSL Certificate.

When you choose to activate SSL on your webserver you will be prompted to complete a number of questions about the identity of your website (e.g. your website's URL) and your company (e.g. your company's name and location). Your webserver then creates two cryptographic keys – a Private Key and a Public Key. Your Private Key is so called for a reason – it must remain private and secure. The Public Key does not need to be secret and is placed into a Certificate Signing Request (CSR) – a data file also containing your details. You should then submit the CSR during the SSL Certificate application process Comodo, the PeaceTrustSSL Certification Authority, who will validate your details and issue an SSL Certificate containing your details and allowing you to use SSL.

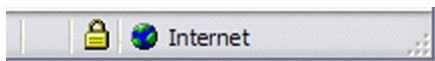
Your webserver will match your issued SSL Certificate to your Private Key. Your webserver will then be able to establish an encrypted link between the website and your customer's web browser.

For detailed application and installation instructions please refer to section "Step by step instructions to set up SSL on your webserver" of this guide.

“SSL is the de facto web transaction security technology. Webservers have been built to support it; web browsers have been built to use it. Secure your customers transactions transparently without your customers having to do a thing!”

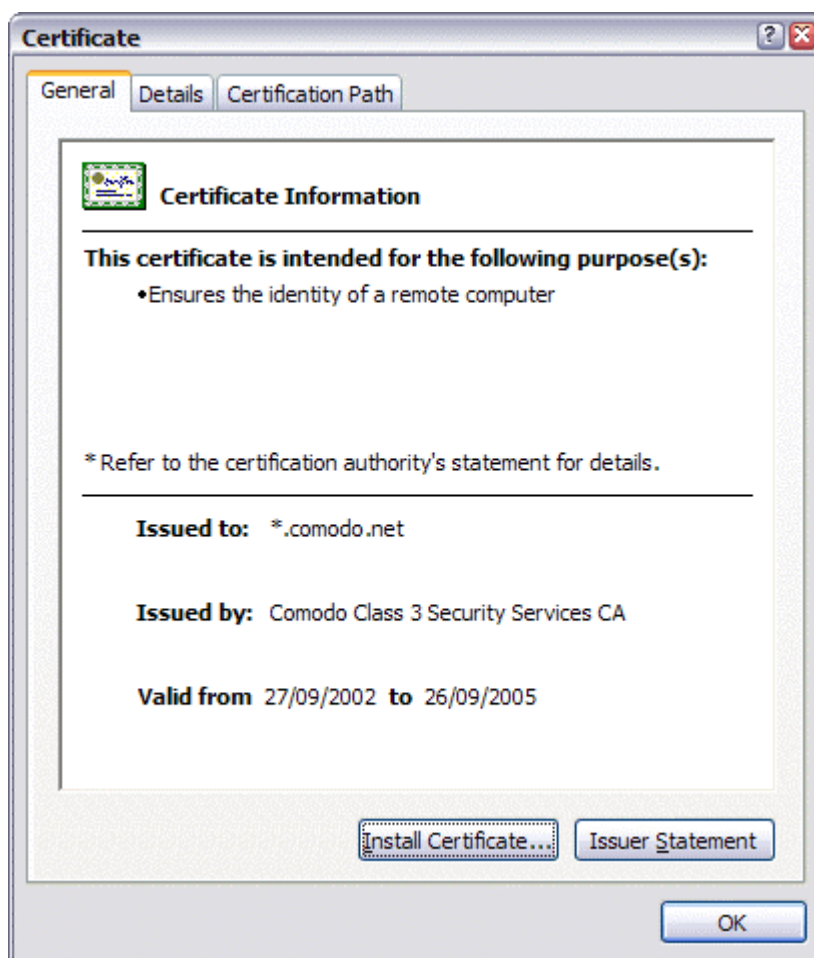
Displaying the **SSL secure padlock**

The complexities of the SSL protocol remain invisible to your customers. Instead their browsers provide them with a key indicator to let them know they are currently protected by an SSL encrypted session – the Padlock:



As seen by users of Internet Explorer

Clicking on the Padlock displays your SSL Certificate and your details:



As seen by users of Internet Explorer

All SSL Certificates are issued to either companies or legally accountable individuals. Typically an SSL Certificate will contain your domain name, your company name, your address, your city, your state and your country. It will also contain the expiry date of the Certificate and details of the Certification Authority responsible for the issuance of the Certificate.

When a browser connects to a secure site it will retrieve the site's SSL Certificate and check that it has not expired, it has been issued by a Certification Authority the browser trusts, and that it is being used by the website for which it has been issued. If it fails on any one of these checks the browser will display a warning to the end user.

Why should you use an **InstantSSL Certificate**?

“Starting at only \$49 per year per Certificate, with additional bulk and multi-year discounts available, InstantSSL provide the most cost effective fully validated and fully supported Certificates available.”

Comodo, the Certification Authority behind PeaceTrustSSL, is the fastest growing SSL Provider in the world. Unlike other Certification Authorities, Comodo does not just provide SSL Certificates – they are a world-renowned security and cryptography service provider. When you are a customer of Comodo, you can feel safe knowing that your website security is provided by experts.

PeaceTrustSSL Certificates are the most cost-effective fully validated and fully supported 128 bit SSL Certificates you can buy today! You can contact the technical support team between 3am- 7pm EST (soon to be 24 hours). You can also feel safe in the knowledge that Comodo will validate your application in accordance with the latest digital signature legislation pertaining to Qualified Certificates. This validation is done effectively and quickly, ensuring you need not wait the traditional 3 working days normally associated with a fully validated SSL Certificate.

PeaceTrustSSL boasts industry leading browser ubiquity – comparable to Verisign and Thawte, however without the costs associated with other SSL Providers. PeaceTrustSSL Certificates are compatible with over 99% of browsers – including Internet Explorer 5.00 and above, Netscape 4.5 and above, AOL 6 and above and Opera 5.00 and above.

PeaceTrustSSL benefits summary:

PeaceTrustSSL Certificates are the most cost effective SSL Certificates you can buy which include:

- Full validation conducted quickly – in many cases you can expect your SSL Certificate to be issued within minutes
- Telephone, email, web support available 3am – 7pm EST
- Over 99% browser compatibility
- 128 bit strong encryption security
- Backed by warranties ranging from \$50 to \$10,000

PeaceTrustSSL Certificates provide you with the key to successfully using SSL on your webserver.

Testing your webserver before you buy – Try a Trial SSL Certificate for FREE

“Only InstantSSL offers free fully functional, validated and supported 30 day trial Certificates, giving you the unique opportunity to fully test the Certificate and your webserver configuration before going live.”

Trial SSL Certificates provide full SSL functionality for 30 days and are fully supported by our expert technical support staff. Unlike test Certificates from other CAs, PeaceTrustSSL trial Certificates are issued using the same Trusted Root CA that issues our end-entity SSL Certificates and provides 99% browser ubiquity, and NOT by a different test CA. This unique service helps you fully test your system prior to your live roll out.

Trial SSL Certificates are ideal for anyone requiring proof of ease of installation, confirmation of high quality technical support and also confirmation of compatibility with the majority of the browsers that exist today. Trial SSL Certificates are also ideal for practicing with Certificates and learning about SSL implementation before committing to installing a Certificate on your live system.

Get your free 30 day trial SSL Certificate from
www.peacetrust.com/products/trialssl.html

Step by step instructions to set up SSL on your Apache webserver

There are four stages to setting up SSL on your Microsoft IIS 5x webserver:

1. Create a Certificate Signing Request (CSR)
2. Apply online
3. Installing your Certificate
4. Displaying your Secure Site Seal

1. Generating a Certificate Signing Request (CSR)

A CSR is a file containing your certificate application information, including your Public Key. Generate your CSR and then copy and paste the CSR file into the webform in the enrollment process:

Generate keys and certificate:

To generate a pair of private key and public Certificate Signing Request (CSR) for a webserver, "server", use the following command :

```
openssl req -new -nodes -keyout myserver.key -out server.csr
```

This creates a two files. The file myserver.key contains a private key; do not disclose this file to anyone. Carefully protect the private key.

In particular, be sure to backup the private key, as there is no means to recover it should it be lost. The private key is used as input in the command to generate a Certificate Signing Request (CSR).

You will now be asked to enter details to be entered into your CSR

.

What you are about to enter is what is called a Distinguished Name or a DN.

For some fields there will be a default value, If you enter '.', the field will be left blank.

```
-----
Country Name (2 letter code) [AU]: GB
State or Province Name (full name) [Some-State]: Yorks
Locality Name (eg, city) []: York
Organization Name (eg, company) [Internet Widgits Pty Ltd]: MyCompany
Ltd
Organizational Unit Name (eg, section) []: IT
Common Name (eg, YOUR name) []: mysubdomain.mydomain.com
Email Address []:
```

Please enter the following 'extra' attributes to be sent with your certificate request

```
A challenge password []:
An optional company name []:
```

Use the name of the webserver as Common Name (CN). If the domain name is mydomain.com append the domain to the hostname (use the fully qualified domain name).

The fields email address, optional company name and challenge password can be left blank for a webserver certificate.

Your CSR will now have been created. Open the server.csr in a text editor and copy and paste the contents into the online enrollment form when requested.

2. Applying for your PeaceTrustSSL Certificate Online

Visit www.peacetrust.net and select your SSL Certificate product type. You will be required to submit the CSR into a webform. When you make your application, make sure you include the CSR in its entirety into the appropriate section of the enrollment form. When you view your CSR it will appear something like:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDVjCCAr8CAQAwezEdMBSGAlUEAxMUD3d3Lm15ZG9tYwLubmFtZS5jb20xDDAK
BgNVBAsTAldlYjEAMBgGA1UEChMRWW91ciBDb2lwYW55IE5hbWUxEDA0BgNVBACr
B015IENpdHkxETAPBgNVBAGTCE15IFN0YXRlMQswCQYDVQQGEwJVUzCBnzANBjkq
hkiG9w0BAQEFAAOBjQAwGyKCGYEAuev9LnSRX/6u5Iz7ckpt0IG4DwnAF/lsksj0
n5r9w1EK9Np5/OJEt72r5es3nie5rTKo304yvsLovkS0vqT+i0IEZv15B4mXTEPw
fDLjEcwcnb8SCJ4ArUahHKJWHDKJHDKDA6587568gfhjfjFHGFHFHsgGHJGJjhhj
HFD^TGFryTrYTrfGHI&DHJKDHkjjwkkAgcwgYlKoZlhvcNHKJHFrytDETR$456
AwcEwYDVR01BAwwGyKCGYEAuev9LnSRX/6u5Iz7ckpt0IG4DwnAF/lsksj0n5r9w1
WgBNAGkAYwByAG8AZwByAGEAcABoAGkAYwAgFAAACgBvAHYAaQBKAGUAcgOBiQCq
QwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgFAAACgBvAHYAaQBKAGUAcgOBiQCq
EH3QppP7Ewuz6oh4EUXMbKdqieAcBQ52iFSXqQ/nlxAtEpVUfjIM3exr42EhyYlr
1V7cpUKbSr/eQ6c/hjiUi17EpvleBBV0BkFWsWzJoShx0BmOKvDnKINNQC3Jya+M
N/t9axyuCwdUYJiLglNnjbLsXl/6hovXNDLuCLgMAAAAAAAAAAAMA0GCSqGSIb3
DQEBBQUAA4GBAEQT6Pwj0BHeOUw+AR0GAT30q+1OYNkr341CouM6M7Kq1KgVZDV
tRes4uz1Yf8+WRcutVvDByrey+CdgzJzHvHqS61Aj2swx8QadclVWokZfH//k/KE
1Mi0Eb6c3Mp1ECorjIm+HRN20Qga+dnDBOowyRyn7Vz+Nkar88mrJwk/
-----END NEW CERTIFICATE REQUEST-----
```

Be sure to copy the CSR text in its entirety into the application form, including the:

```
-----BEGIN CERTIFICATE REQUEST----- and -----END CERTIFICATE REQUEST-----
```

3. Installing your PeaceTrustSSL Certificate

Step one: Copy your certificate to file

You will receive an email from Comodo Security Services with the certificate in the email (**yourdomainname.crt**). When viewed in a text editor, your certificate will look something like:

```
-----BEGIN CERTIFICATE-----
MIIDVjCCAr8CAQAwezEdMBSGAlUEAxMUD3d3Lm15ZG9tYwLubmFtZS5jb20xDDAK
BgNVBAsTAldlYjEAMBgGA1UEChMRWW91ciBDb2lwYW55IE5hbWUxEDA0BgNVBACr
B015IENpdHkxETAPBgNVBAGTCE15IFN0YXRlMQswCQYDVQQGEwJVUzCBnzANBjkq
hkiG9w0BAQEFAAOBjQAwGyKCGYEAuev9LnSRX/6u5Iz7ckpt0IG4DwnAF/lsksj0
n5r9w1EK9Np5/OJEt72r5es3nie5rTKo304yvsLovkS0vqT+i0IEZv15B4mXTEPw
fDLjEcwcnb8SCJ4ArUahHKJWHDKJHDKDA6587568gfhjfjFHGFHFHsgGHJGJjhhj
HFD^TGFryTrYTrfGHI&DHJKDHkjjwkkAgcwgYlKoZlhvcNHKJHFrytDETR$456
AwcEwYDVR01BAwwGyKCGYEAuev9LnSRX/6u5Iz7ckpt0IG4DwnAF/lsksj0n5r9w1
WgBNAGkAYwByAG8AZwByAGEAcABoAGkAYwAgFAAACgBvAHYAaQBKAGUAcgOBiQCq
QwByAHkAcAB0AG8AZwByAGEAcABoAGkAYwAgFAAACgBvAHYAaQBKAGUAcgOBiQCq
EH3QppP7Ewuz6oh4EUXMbKdqieAcBQ52iFSXqQ/nlxAtEpVUfjIM3exr42EhyYlr
1V7cpUKbSr/eQ6c/hjiUi17EpvleBBV0BkFWsWzJoShx0BmOKvDnKINNQC3Jya+M
N/t9axyuCwdUYJiLglNnjbLsXl/6hovXNDLuCLgMAAAAAAAAAAAMA0GCSqGSIb3
DQEBBQUAA4GBAEQT6Pwj0BHeOUw+AR0GAT30q+1OYNkr341CouM6M7Kq1KgVZDV
tRes4uz1Yf8+WRcutVvDByrey+CdgzJzHvHqS61Aj2swx8QadclVWokZfH//k/KE
1Mi0Eb6c3Mp1ECorjIm+HRN20Qga+dnDBOowyRyn7Vz+Nkar88mrJwk/
-----END CERTIFICATE-----
```


2. Add the following line to SSL section of the httpd.conf (assuming /etc/httpd/conf is the directory to where you have copied the ca.txt file). if the line already exists amend it to read the following:

```
SSLCACertificateFile /etc/httpd/conf/ca-bundle/ca.txt
```

If you are using a different location and certificate file names you will need to change the path and filename to reflect your server.

The SSL section of the updated httpd config file should now read similar to this example (depending on your naming and directories used):

```
SSLCertificateFile /etc/ssl/crt/yourdomainname.crt  
SSLCertificateKeyFile /etc/ssl/crt/private.key  
SSLCACertificateFile /etc/httpd/conf/ca-bundle/ca_new.txt
```

Save your **httpd.conf** file and restart Apache.

4. Displaying your Secure Site Seal

As a valued PeaceTrustSSL customer we encourage you to display the PeaceTrustSSL secure site seal to help promote your **secure** site to customers. The secure site seal is free to all PeaceTrustSSL customers.

Contact us to discuss our TrustLogo technology and how providing real-time identity assurance to customers to help establish even more confidence and trust with your customers.

Fast, cost-effective [SSL Security](#) for your webserver...

The Internet is a revolutionary medium for you to improve your sales and online services for customers. PeaceTrustSSL is the perfect solution to securing your webserver with SSL quickly, easily and cost-effectively.

Contact us to discuss your individual security requirements

Contact us between 3am and 7pm EST to discuss how PeaceTrustSSL can help you:

support@earthchild.net

sales@earthchild.net

PeaceTrust.net

Marketed worldwide through the independent associates of Earthchild.net
a marketing program by Peace 2000

For contact information visit: www.earthchild.net