Free Lunch!

No. FreeSSL.com

SSL GUIDE

Everything you need to know about SSL and securing your online business

For Control Panel based webservers

ensim PLESK cPanel SPHERE

Published by FreeSSL.com

FreeSSL.com US
600 17th Street, Suite 2800 South
Denver, Colorado, USA 80202
Tel: 720 359 1590
Fax: 720 528 8160

This Guide

Why is security required for the Internet?

The Internet has been a revolution to commerce and the transfer of data in general, which has developed new global business opportunities for all, including major enterprises, small to medium sized businesses and individuals alike. However e-commerce has inevitably attracted crime and developed a new breed of online criminals ranging from fraudsters and hackers to cyber terrorists. The growing concerns associated with conducting e-commerce have now resulted in the fact that security is an essential factor for online business success.

The market is now educated in the basics of online security and the majority of online users now expect security to be integrated into any online service they use and as a result they expect any details they provide via the Internet to remain confidential and secure.

This white paper explains how SSL can be utilized as the core security technology to protect customer's online transactions and informs users that the security of the online business is being taken seriously. In fact SSL provides proof of a digital identity and allows online customers to visibly see that their digital transaction will be confidential. These are essential factors in gaining customer confidence and remove the concerns and risks associated with sending sensitive data over the Internet.

SSL is essential to allow the true benefits of the Internet to be realised.

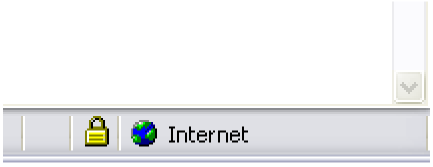
What is SSL?

SSL (Secure Sockets Layer) is a security technology that is commonly used for encrypting communications between users and e-commerce websites, thereby securing server to browser transactions. The SSL protocol utilizes encryption to prevent eavesdropping and tampering of the transmitted data, and is used to secure information passed by a browser (such as a customer's credit card number or password) to a webserver (such as an online store).

SSL protects data submitted over the Internet from being intercepted and viewed by unintended recipients and as used by hundreds of thousands of websites in the protection of their online transactions with their customers, SSL is the de-facto industry standard Internet transaction security technology.

How do website visitors know if a website is using SSL?

When a website visitor connects to a webserver using SSL they will see that the URL in the address bar begins with https:// rather than the usual http:// and also a small gold padlock will appear in their browser, e.g.



As seen by users of Internet Explorer

Whenever a browser connects to a webserver (website) over https:// - this signifies that the communication will be encrypted and secure. The actual complexities of the SSL protocol remain invisible to the end customer.

In summary, SSL is the de facto web transaction security technology. Webservers have been built to support it and web browsers have been built to use it. SSL provides the ability to secure customers transactions transparently without the customer having to do a thing!

What is required for a webserver (website) to use SSL?

In order for a website to use SSL a SSL Certificate is required (also known as Web Server Certificates and Secure Server Certificates). SSL Certificates are installed onto the webserver hosting the particular website and allow access to the security functionality of the webserver itself.

How is a SSL certificate installed onto a webserver?

When SSL is first activated on the webserver, the webserver requires information about the identity of the website including the website domain name and company details.
The webserver then creates two cryptographic keys – a Private Key and a Public Key. The Private Key is so called for a reason – this key must remain private and secure, only residing on the webserver. The Public Key does not need to be secret and is placed into a Certificate Signing Request (CSR) – a data file which also contains all the website credentials.

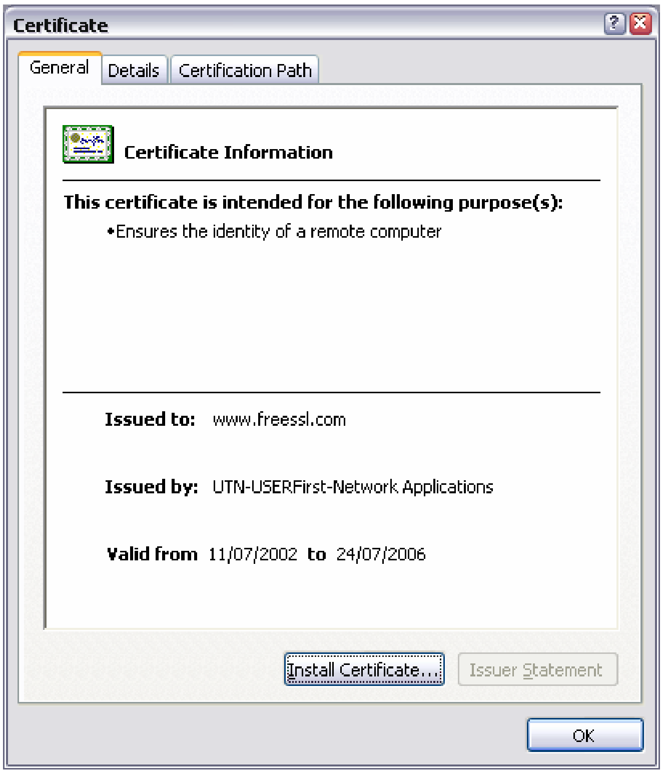
The Private and Public keys are used in the encryption process, so that the data passing between the webserver (website) and the customer's browser remains confidential and secure.

The CSR generated is submitted to Certification Authorities during the SSL Certificate application process. The Certification Authority then validates the website credentials and issues an SSL Certificate containing the digital identity of the website, binding the domain name to the company details.

The webserver will match the issued SSL Certificate to the associated Private Key and allows the webserver to establish encrypted links between the website and customer's browsers.

What does a SSL certificate look like?

SSL certificates can be seen by simply double clicking on the padlock symbol when displayed in the browser. A typical certificate will look like this;



Certificate Information

This certificate is intended for the following purpose(s):
- Ensures the identity of a remote computer

Issued to: www.freessl.com

Issued by: UTN-USERFirst-Network Applications

Valid from 11/07/2002 to 24/07/2006

All SSL Certificates are issued to either companies or legally accountable individuals. Typically SSL Certificates contain the domain name, the company name, the address i.e. city, state and 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, that 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.

What is a Certification Authority (CA)?

Not just anybody can issue trusted SSL Certificates. If they could then there would be no trust in SSL - and it could no longer be used commercially. Instead only Certification Authorities, or CAs as they are commonly known, can issue trusted SSL Certificates.

CAs have generally invested in establishing the technology, support, legal and commercial infrastructures associated with providing SSL certificates. Even though CAs are essentially self-regulated, the nearest to a regulatory body is the WebTrust compliancy program operated by AICPA/CICA. The majority of CAs comply to the WebTrust principles, however some CAs do not have WebTrust compliance. Those CAs who are WebTrust compliant display the WebTrust Seal, as seen below.

CERTIFICATION AUTHORITIES
WebTrust
ERNST & YOUNG

The WebTrust Seal of assurance for Certification Authorities symbolizes to potential relying parties [e.g. to the end customer] that a qualified practitioner has evaluated the CA's business practices and controls to determine whether they are in conformity with the AICPA/CICA WebTrust for Certification Authorities Principles and Criteria. An unqualified opinion from the practitioner indicates that such principles are being followed in conformity with the WebTrust for Certification Authorities Criteria. These principles and criteria reflect fundamental standards for the establishment and on-going operation of a Certification Authority organization or function.

Who are the CAs and why are there so many providers of SSL?

There are actually less than 10 CAs issuing commercially available SSL certificates. The Appendix contains the full list of CAs. Until recently the SSL market has been monopolized by Verisign and Thawte. In 1999 Verisign acquired Thawte, and it became a Verisign subsidiary. In recent years, new global players providing enterprise class solutions such as GeoTrust (formerly Equifax Certificate Services) have also established themselves in the enterprise security market. In the last few months, other companies providing solutions for small to medium sized businesses have also started providing SSL certificates.

There is however confusion in the market because all CAs have reseller programs. Resellers are organizations that will resell the SSL CA’s certificates, often at different prices to the SSL CA themselves. Resellers are a great way to sometimes save money through discounted pricing, but are also an easy way to be overcharged for SSL!

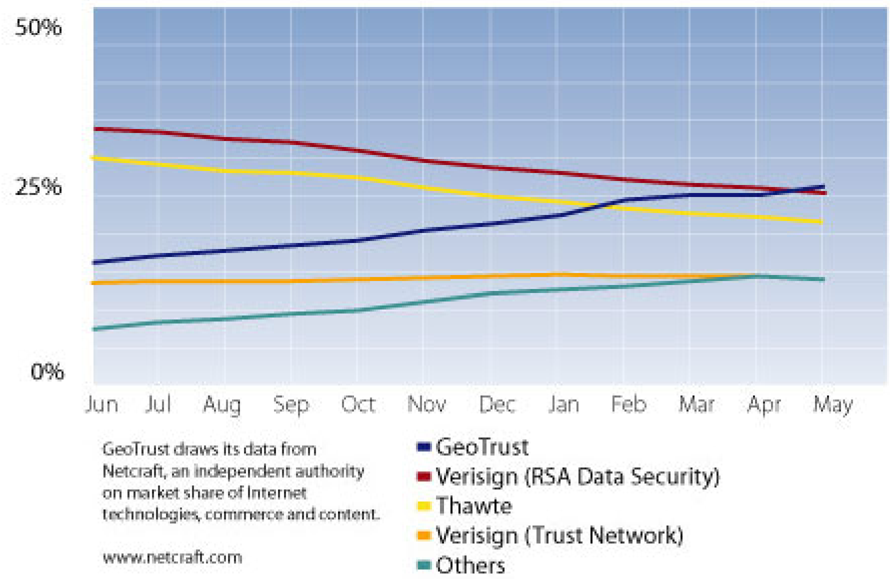
Be aware that some resellers will "re-brand" the CA’s certificate, thereby masking who actually issues the certificate and then offer their own re-branded certificates at inflated prices above the SRP of the CA themselves.

Don't be fooled by unknown brands - if an SSL Certificate is being sold under a brand that is not contained in the attached Appendix, the buyer should examine one of the reseller's example certificates before purchase. It is very likely that the certificate has been issued by a CA featured in this white paper and will probably be available directly from the CA at a different cost, maybe even lower than the reseller offers it.

Resellers provide exactly the same certificate and features provided by the CA themselves, so it is essential for buyers to know which CA that will issue the SSL certificate before purchasing through a reseller!

Who are the top 2 CAs?

Each month Netcraft (www.netcraft.com) publishes the market share of each CA. The following chart summarizes the market share of the top 2 enterprise players in the .net market, namely Verisign and GeoTrust. The chart also shows the market share of Thawte (Thawte is a Verisign company).



GeoTrust draws its data from Netcraft, an independent authority on market share of Internet technologies, commerce and content.

www.netcraft.com

What do I need to consider when purchasing a SSL certificate?

The following 10 considerations must be taken into account before deciding which CA and which type of SSL certificate to purchase? Each point will be discussed in more detail later.

1. **What type of web site application. Low volume, professional or development?**
2. **How credible and stable is the CA issuing the SSL certificate?**
3. **What browser recognition is required?**
4. **Do I require a single root or intermediate SSL certificate?**
5. **What certificate strength is required?**
6. **Is technical support available from the CA for installation or CSR issues?**
7. **Do I need warranty?**
8. **What type of validation is required?**
9. **How fast do I want my certificate?**
10. **What budget do I have for my certificate?**

Lets look at each point in turn.

1. What type of web site application. Low volume, professional or development?

Perhaps the most important differentiation between all the SSL certificates available on the market today, is the strength of the brand behind the SSL technology. SSL technology besides ensuring secure transmission of data, is an essential element in providing online customers with the confidence to buy or use a product or service.

For example, the greater the number of users visiting a website, the greater the probability that some customers may not complete a transaction, simply because they do not recognise or trust the brand behind the SSL technology.

Inevitably the well known brands from the credible long standing CAs are the most expensive SSL certificates on the market. If you have a low volume or development website and you decide that your customer's confidence is not affected at all by the brand behind the SSL certificate or the volume of customers that would have an issue are insignificant in number then the choice of CA and certificate is increased. Low volume websites can therefore enjoy significant savings on the SSL purchases by purchasing the lesser known brands of SSL certificates.

We suggest as a guide that if a website is performing more than 50 transactions per week then, it is advisable to use a known SSL brand.

Another important consideration is the typical or average transaction value that a website will process. If customers are expected to pay high amounts online the greater the probability that some customers may not complete a transaction because they do not trust the brand behind the SSL technology.

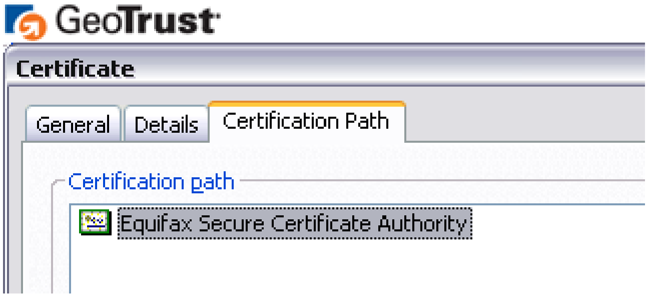
We suggest as a guide that if a website has an average transaction of greater than 50 USD, it is advisable to use a known SSL brand from a reputable CA.

2. How credible and stable is the CA issuing the SSL certificate?

Clearly for any SSL certificate to be taken seriously, it is important to ensure that the CA issuing the SSL certificate is well established and credible. The best way of determining the credibility of a CA is by simply establishing whether the CA in question owns its own trusted root i.e. does the CA own a root that is already present in all popular browsers?

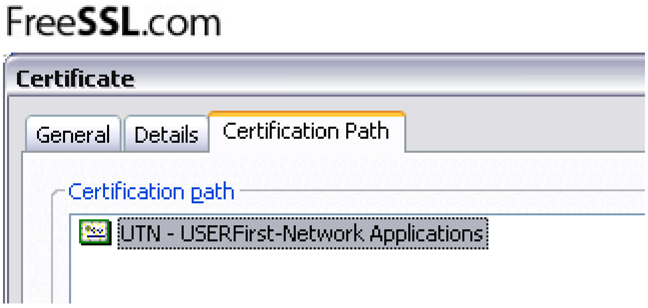
You can examine trusted root ownership by double clicking the padlock seen in the browser during an SSL connection with a webserver. When the SSL Certificate appears, simply click the "Certification Path" tab to see which trusted root CA certificate issued the SSL certificate.

It is also possible to see the trusted roots referenced in a browser e.g. for IE6, go to “Tools”, “Internet Options” and select “Content”, “Certificates” and then the tab “Trusted Root Certification Authorities”.



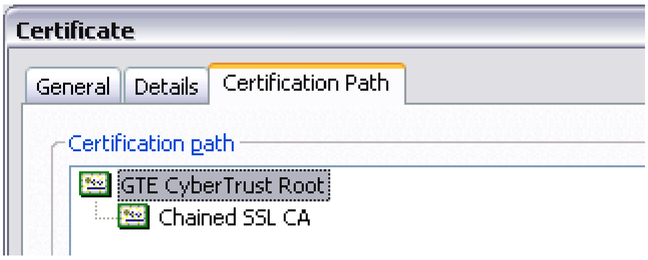
Equifax Secure Certificate Authority

GeoTrust owns the Equifax root (Equifax Digital Certificate services became GeoTrust in 2001).



UTN - USERFirst-Network Applications

FreeSSL.com's StarterSSL and FreeSSL product owns its own root. FreeSSL.com purchased the USERTrust Network root a number of years ago.



FreeSSL.com's ChainedSSL Wildcard product uses an intermediate certificate issued by the USERTrust Network root. FreeSSL.com purchased the USERTrust Network root a number of years ago, making it the only stable chained root certificate available on the market today.

Business stability is also an essential component when selecting any supplier. Whilst we do not examine financial stability of each CA in detail in this white paper, enterprise class accounts are advised to conduct their own due diligence into each CA, as well as examine the root CA certificate ownership.

When selecting a CA, always therefore consider the long term stability of the CA, especially if a longer term enterprise solution is required.

If the CA relies on an intermediate certificate - consider the long-term stability of the CA supplying the intermediate, and obviously the stability of the supplier relationship between the two CAs.

Clearly it is very advisable to ensure the integrity of the CA and to establish which CA is issuing the SSL certificate to be used.

3. What browser recognition is required?

Browser recognition or ubiquity is the term used in the industry to describe the estimated percentage of Internet users that will inherently trust an SSL certificate.

Certification Authorities who own their own roots, have what are known as Root CA Certificates. These root CA certificates are added into releases of all the major browsers such as Internet Explorer, Netscape, Opera, etc by the browser vendor (such as Microsoft). When a browser is used, it automatically relies on a "list" of root CA certificates that the browser vendor has deemed trustworthy. If a SSL certificate is issued by one of the trusted root CAs, then the browser will inherently trust the SSL certificate and the gold padlock will appear transparently during secure sessions.

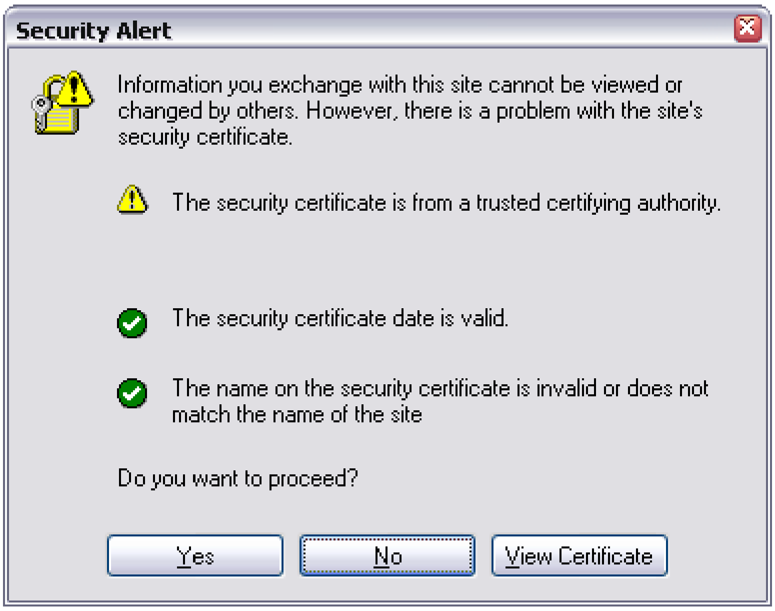
The browser stores the CA roots that can be trusted, therefore if a browser encounters a website using a SSL certificate issued by a CA root it does not trust, the browser will display warning messages to the website visitor. The lower the browser ubiquity, the less people will trust a certificate - clearly, a commercial site will require as many people as possible to trust a SSL certificate.

The general rule is that any SSL certificate with over 95% browser ubiquity is acceptable for a commercial site.

As with any form of statistics, browser ubiquity is open to interpretation, hence in the Appendix, the table does not place a great deal of validity in presenting browser recognition "percentages", instead it simply concludes whether a SSL Certificate is acceptable for commercial sites.

Why is browser recognition important?

If a website visitor is using a browser that does not contain the root CA certificate used to issue the SSL certificate, they will be prompted with a security warning:



Security Alert

Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate.

⚠ The security certificate is from a trusted certifying authority.

✓ The security certificate date is valid.

✓ The name on the security certificate is invalid or does not match the name of the site

Do you want to proceed?

The ⚠ signifies that the SSL Certificate has been issued by a CA that the browser does not trust. As more people upgrade their old browsers, this message becomes less frequent. It is also worth noting that people who do not upgrade their browsers are less technically and security savvy and hence are less likely to purchase from websites.

Another consideration often overlooked concerning the overall ubiquity of a SSL certificate is the issue over Webserver Compatibility. The SSL Certificate is required to be installed onto a webserver. Generally, all webservers accept all SSL certificates currently available but it is recommended to check with the CA to be sure. Webservers such as Apache (including the website control panel variants), IIS, Webstar, Website Pro, Java based, iPlanet, Zeus, Netscape server, Cobalt support the certificates of all SSL certificates featured in this whitepaper.

There are few webservers still in use that do not support the use of intermediate certificates. Such webservers are not SSL v3 compliant. If your webserver does not support SSL v3, then you will need to select a CA that issues certificates directly off its root such as GeoTrust and FreeSSL.com.

4. Do I require a single root or intermediate SSL certificate?

Some certificates are issued directly by a Trusted Root CA certificate e.g. GeoTrust. The Trusted Root CA certificate is already contained within all popular browsers, and hence is already trusted. Some Certification Authorities do not have a Trusted Root CA certificate present in browsers, therefore they need a "chained root" in order for their certificates to be trusted.

Both FreeSSL.com's ChainedSSL Wildcard product and Comodo's InstantSSL product are chained root certificates. However FreeSSL.com own the trusted CA root used to issue ChainedSSL Wildcard and are therefore the only stable chained root provider. Comodo do not own the BeTrusted root used to issue InstantSSL certificates and therefore cannot offer the stability of ChainedSSL Wildcard.

Both StarterSSL and all of the Professional Level Certificates offered by FreeSSL.com are single root certificates.

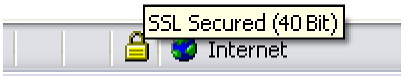
Compared to single root installations, chained root certificates require additional webserver installation steps. If a CA is chosen that requires the installation of more than one certificate, then it is advisable to ensure that the necessary technical expertise or resources to be able to perform the installation are available. Loading and managing multiple certificates per installation, especially in an enterprise environment, can be costly and cumbersome.

Certification Authorities (CAs) that own their own roots are long-time security providers who have long term relationships with the browser vendors for the inclusion of their Trusted Root CA certificates. For this reason, such CAs are seen as being considerably more credible and stable than chained root certificate providers.

5. What certificate strength is required?

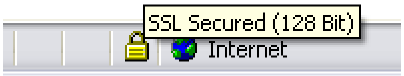
Generally there are two strengths of certificate in existence - 40 bit & 128 bit.

The bit size indicates the length of the key size used for the encryption during a secure SSL session. Hovering the mouse over the gold padlock will detail the current strength of encryption being used:



SSL Secured (40 Bit)

Internet



SSL Secured (128 Bit)

Internet

Why is encryption strength important?
The bigger the number, the longer it takes for computer(s) to crack or break the code.

- 40 bit: It is computationally feasible to crack a 40 bit key. For this reason 40 bit encryption is rarely used.
- 128 bit: It is computationally unfeasible to crack a 128 bit key. All banking infrastructures use 128 bit encryption.

We strongly recommend the use of 128 bit SSL encryption for any application or website.

6. Is technical support available from the CA should I need it?

Installing a SSL certificate can sometimes be tricky – you will need to first generate a CSR and then install your issued certificate. For this reason it is essential that the CA provides sufficient and timely support.

All CAs provide some level of support, even if it is only email and web based. Most issues can easily be solved using the expansive online resources and knowledge bases provided by the CA. However, should an issue arise, it is highly recommended that there is access to technical support staff, therefore make sure the CA clearly publishes a technical support telephone number. Also, be aware that some CAs charge extra for telephone support.

7. Do I need warranty?

The warranty level is the financial protection awarded to end customers against the CA misissuing an SSL Certificate. If a customer relies on the information within a misissued SSL Certificate and suffers financial loss as a direct result of relying on the certificate, the CA will hold insurance to cover claims made by the customer against the CA. Effectively, the warranty is the insurance taken out by the CA to protect itself in the event it makes a mistake.

Verisign offers a more advanced insurance policy in that it will also provide insurance against a compromise of a private key or loss of certificate - but such insurance comes at a price.

How likely is a missisuance?
It is highly unlikely that a WebTrust compliant CA will mississue a certificate. All WebTrust compliant CAs have passed certification to ensure that procedures and policies are in place that make misissuance improbable. For this reason, many WebTrust compliant CAs do not offer a warranty at all.

CAs that are not WebTrust compliant will often offer the warranty as a means of adding perceived value to their SSL certificates.

8. What type of validation is required?

A trust hierarchy demands that entities "vouch" for each other. Companies that issue SSL certificates are in the business of establishing that entities on the web are, in fact, who they claim to be. The potential for criminal activity on the web (in relevance to SSL anyway), is in online ‘hijacking’ of sites or connections to siphon encrypted data. Persons so inclined can easily "copy" web site interfaces and pose as well known vendors, simply to collect these data.

SSL certificates work to prevent this through ensuring that www.abc.com is, in fact, ABC Co. In the “real world” we use identification procedures like photo ids, telephone calls and papers of incorporation to know with whom we are dealing. If products or services are defective, buyers can seek recourse. In the “online world”, companies wishing to use SSL certificates must prove to the certificate authority that they have the right to present themselves online as ABC Co.

This is done through a variety of means in different SSL products. For the sake of simplicity, consider the method started and championed by Verisign, as the ‘traditional’ model. The process involves certificate petitioners faxing in their articles of incorporation, and then waiting several days to be granted a certificate to do business online under that name. There is a fair amount of overhead related to this task, as these credentials are examined and reviewed, and full-service products in this arena can cost hundreds of dollars.

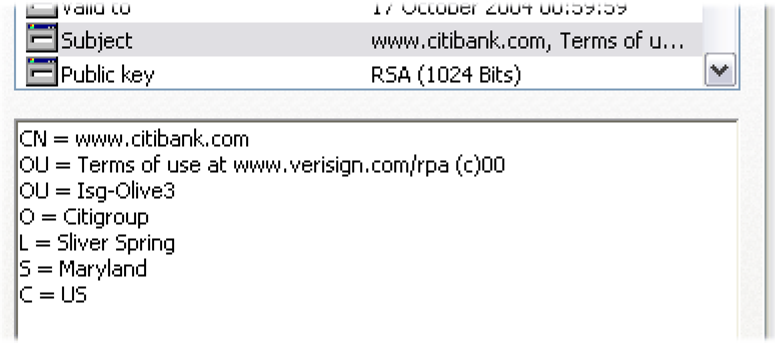
There are newer, lower-cost alternatives in which certificates are issued more quickly. These certificates verify that the certificate holder is the owner of that domain, ensuring customers that domain name “owners” are who they claim to be.

There are also other validation options, like two-way, real-time telephony. Certificate applicants are required to provide telephone numbers, and certificate authorities call to verify basic information, yet another way to seek recourse in the event of problems.

So there are essentially two types of validation available, manual and automated.

Manual Validation.
Involves the validation of domain name ownership and business legitimacy using humans. This process is traditionally slow and takes up to two working days, often longer.

A manually validated certificate usually contains the following information within the certificate:

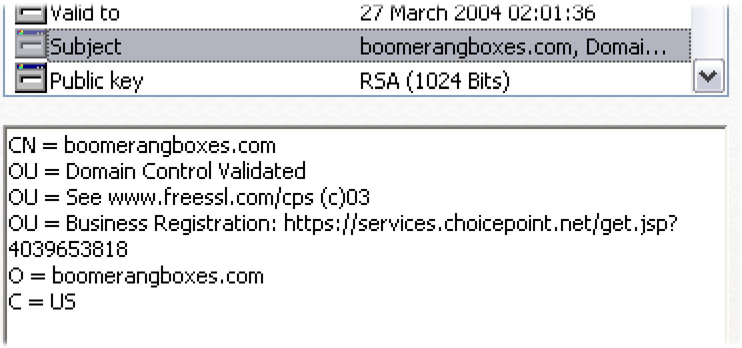


Valid to 17 October 2004 00:59:59
Subject www.citibank.com, Terms of u...
Public key RSA (1024 Bits)

CN = www.citibank.com
OU = Terms of use at www.verisign.com/rpa (c)00
OU = Isg-Olive3
O = Citigroup
L = Sliver Spring
S = Maryland
C = US

Auto-Validation.
Computers, databases and automated routines validate domain name ownership and business legitimacy. The process takes minutes rather than days. The GeoTrust QuickSSL product and FreeSSL.com FreeSSL and ChainedSSL products use automated validation to issue SSL certificates within 10 minutes. Their automated validation processes are WebTrust compliant and use Domain Control validation and ChoicePoint (equivalent to Dun & Bradstreet) to validate the applicant before issuing the certificate.

An automatically validated certificate, such as the GeoTrust or FreeSSL.com certificates, contain the following information within the certificate:



Valid to 27 March 2004 02:01:36
Subject boomerangboxes.com, Domai...
Public key RSA (1024 Bits)

CN = boomerangboxes.com
OU = Domain Control Validated
OU = See www.freessl.com/cps (c)03
OU = Business Registration: https://services.choicepoint.net/get.jsp?4039653818
O = boomerangboxes.com
C = US

Note: If a CA is not WebTrust compliant its validation processes will not have been audited and accredited as being satisfactory and inline with the WebTrust guidelines for CAs.

9. How fast do I want my certificate?

The principal delay associated with the issuance process of SSL is the validation process adopted.

For fast issuance of certificates, it is advisable to use automated methods of validation.

Be very careful when confirming the issuance time with a CA. Some may suggest immediate delivery once they have obtained all your company documentation in the format required and have initiated the validation. This process may still take up to 2 days from start to finish.

10. What budget do I have for my certificate?

Certificates range dramatically in price from one CA to another. The highest prices are 40 times the lowest prices!

This white paper has examined numerous points of consideration in determining which SSL certificate to purchase.

The correct choice of SSL certificate is principally dependent on the application type and on whether there is a need for a well known brand of SSL that has been issued from a highly trusted and credible CA.

There are however significant savings available for websites conducting low volume/ low value transactions. Some SSL certificate types are perfect for development environments, whilst other certificate types suit professional requirements. Buyers are therefore urged to carefully consider their choice of CA before purchasing.

Give me 10 reasons why I should buy from FreeSSL.com?

1. **A Complete Range of SSL Certificates.**
   FreeSSL.com offers a range of certificates suitable for low volume/ low transaction value, Professional level and Development applications.

2. **Credibility.**
   FreeSSL.com is a subsidiary of GeoTrust, a highly trusted, credible and long standing CA with an Internationally recognized brand. GeoTrust own the Equifax roots that are already present in all popular browsers and used to issue the Professional Level certificates. FreeSSL.com also owns the UTN root used to issue StarterSSL, FreeSSL and ChainedSSL Wildcard certificates. GeoTrust is a WebTrust compliant CA and holds the WebTrust Seal.

3. **Browser recognition.**
   FreeSSL.com certificate range offers browser recognition rates from 96 to 99 percent suitable for both test/development, lite ecommerce and high volume / high transaction value ecommerce.

4. **Single root not Chained root.**
   FreeSSL.com offers SSL certificates utilizing single roots (owned by FreeSSL.com and GeoTrust) making installation far quicker and simpler than chained root certificate installations. **Issued in minutes, installed in seconds!**

5. **Certificate strength.**
   All certificates offered through FreeSSL.com use 128 bit industry standard SSL encryption.

6. **Industry Leading Expert Support.**
   Both telephone, web and email support is available for all certificates sold through FreeSSL.com, covering 1am to 9pm EST, 6am -2am Europe. Unlike some of our competitors, FreeSSL.com does not charge extra for technical support.

7. **Warranty.**
   All certificates are issued from a WebTrust compliant CA. Our automated validation processes have been audited as part of WebTrust compliance, making mis-issuance extremely unlikely. Do not be fooled by other SSL Providers offering "mis-issuance warranty". There has never been a recorded case of a mis-issuance warranty being used ever, so beware of paying inflated prices for additional warranty.

8. **Automated Online Validation.**
   Our validation system is conducted online and is completely automated. There is no faxing or documentation required and we complete the online validation in only minutes.

   As part of the provisioning process with both StarterSSL, ChainedSSL and FreeSSL, businesses are registered with ChoicePoint and assigned a ChoicePoint Unique Identifier (CUI) - equivalent to a DUNS number. The CUI provides a corporate profile to the Internet users through information imbedded in to the certificate. With the ChoicePoint Unique Identifier, industry-recognized domain control authentication, and two-factor telephony authentication, FreeSSL.com offers the strongest real-time authentication process on the market today.

9. **Issuance speed.**
   FreeSSL.com's 2nd generation validation and issuance infrastructure allows certificates to be issued immediately 24 hours per day, 7 days per week, 365 days each year.

10. **Lowest cost.**
    FreeSSL.com is the lowest cost provider of SSL certificates in the market today and offers the lowest priced certificates suitable for all application categories namely, low volume /low transaction value, Professional Level and test/development.

In summary…

There is absolutely no reason why buyers of SSL should have to;

- **Pay more for their certificates irrespective whether the application is for low volume, professional or development**
- **Wait more than 10 minutes for their SSL certificate to be issued**
- **Buy a certificate that cannot be installed in seconds (such as a chained root / intermediate certificate)**
- **Buy from SSL Providers who DO NOT own their own root**
- **Not enjoy FREE excellent customer service levels**

FreeSSL.com has a very simple mission in life and that is;

- **To be focused on providing small to medium sized businesses (SMB) and entry level web sites with strong 128bit encryption, industry standard SSL certificates**
- **To be dedicated to being the lowest cost provider of SSL to the SMB market place**
- **To deliver the ultimate customer service through fast issuance and leading customer care**
- **A commitment to quality in all aspects of the business through meeting the industries most stringent Certification Authority quality standards**

Secure your webserver with a **SSL Certificate** at FreeSSL.com. The **lowest cost** provider of highly trusted stable & single root **128 bit SSL Certificates** (we own all our own root certificates!) suitable for lite and professional level ecommerce - fully supported and delivered immediately!

Support Files

ensim	Generate a CSR – click here Install a SSL Certificate - click here
PLESK	Generate a CSR - click here Install a SSL Certificate - click here
cPanel	Generate a CSR - click here Install a SSL Certificate - click here
SPHERE	Generate a CSR - click here Install a SSL Certificate - click here