

NetNames SSL certificates

powered by VeriSign

Data from Cambridge-based brand monitoring specialist Envisional[®] shows that the volume of phishing mail targeting banks in the first six months of 2008 was 26% greater than that received in the first six months of 2007. This increases the numbers of online banking customers visiting unsecure and fraudulent pages.

Visitors to your website need to trust your site and know that their information is safe. The only way to validate this trust is through the use of a Secure Socket Layer (SSL) certificate.

What are Secure Socket Layer (SSL) certificates?

When information or data travels across online networks without SSL encryption, that data is in full view of potential scammers and is not secure. Secure Socket Layer certificates are a way of hiding information, so that only the authorised contact is able to access and use the data.

A SSL certificate is created for a particular server in a specific domain and is verified against a particular business entity. It acts like a passport or a driving licence and can only be issued by a trusted authority (such as VeriSign).

How do SSL certificates work?

A SSL certificate consists of a public key and a private key. A public key is used to encrypt information and a private key is used to decipher it.

When a browser points a user to a secured domain, a SSL handshake authenticates between the server and the client, and establishes both an encryption method and a unique session key. The user can then begin a secure session that guarantees message privacy and integrity.

NetNames SSL certificates containing Server-Gated Cryptography (SGC) encryption (with 128-bit or 256-bit SSL encryption) allows website owners to provide the most powerful SSL encryption available in the industry for their websites.

Visible evidence of online security for your website:



Once a website is secured through a SSL certificate, your site will carry the 'golden padlock' sign which is a well-known symbol of trust.

Also, when you buy NetNames SSL certificates, you will additionally receive the VeriSign Secured Seal (a seal that demonstrates that the SSL certificates are the most secure in the industry) to place on your website.

Tangible returns for your business:

The VeriSign Secured Seal not only provides customers with peace of mind, but also directly impacts your organisation's bottom line:

"We posted the VeriSign Secured Seal on the payment pages and found that completed sales rose by approximately 10% in comparison to the previous weeks results."

Warren Jonas, Head of Service Management, Opodo.

Free SSL certificate audits through NetNames:

If you are already using SSL certificates to protect your business and would like to check the status of those certificates, NetNames offers you a no obligation SSL certificate audit, which will highlight the following:

- > The number of SSL certificates on your websites (on external sites only)
- > Current providers of your SSL certificates
- > When the certificates will expire

If you would like to transfer your SSL certificates to NetNames following the above audit, all you need to do is contact NetNames and we will run through the simple process with you. >>>



Choose from two highly secure SSL certificate options:

Secure Site Pro certificate

- Secures sensitive information during online transactions with a minimum of 128-bit encryption
- \$250,000 warranty
- VeriSign Secured Seal

Extended Validation (EV) certificate

- Provision of a special certificate that offers a competitive advantage for your website, building customer confidence by securing the highest levels of trust
- Includes all benefits offered by the Secure Site Pro certificate

Why choose Extended Validation (EV) SSL certificates?

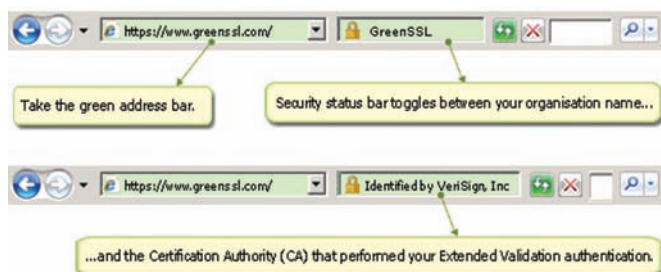
Extended Validation (EV) certificates offer websites a green address bar indicator, which displays both the strongest validation, and the highest visibility of security on a website.

1. The green address bar

If an EV certificate is in place for a website on Microsoft® Internet Explorer 7 (IE7), the website address bar will turn green, and the name of the EV certificate owner will be displayed. If the site does not have an Extended Validation, the website address bar will remain white, displaying a very visible indication of the level of security.

Having a green address bar in IE7 when your competitors don't, provides a true advantage for your business, making your site a trusted and legitimate entity.

All of the major financial institutions and e-commerce websites have EV SSLs in place. As consumers are becoming familiar with the 'green bar' indicator, EV certificates are expected to become an industry standard.



Partnering with world leaders

NetNames is the only Gold VeriSign partner in Northern Europe. This unique partnership positions NetNames as the market leader in corporate managed domain services, partnering with the world's number one SSL certificate specialist.

This partnership offers NetNames Platinum Service customers quick and easy access to VeriSign SSL certification, cost efficiencies during upgrades or new purchases, and a single point of contact for online security needs.

2. Applying for Extended Validation (EV)

To qualify for an EV certificate, the organisation requesting the certificate must be registered with the appropriate government agency in its country of jurisdiction (country of registration).

The following registration requirements need to be confirmed through the company registration database (SOS) or a registration document (POR):

1. Organisation's registration number
2. Organisation's date of registration/incorporation
3. Organisation's registered/agents address
4. Organisation's status

An Extended Validation certificate complies with the CA/Browser Forum Extended Validation Certificate Standard.

For further information on obtaining SSL certificates from NetNames, please contact:

NetNames®
platinum@netnames.com
www.netnames.com