Network Solutions® nsProtect™ Secure SSL Certificate Services

Realize Greater Profits As An Authorized Reseller Of Network Solutions® nsProtect Secure SSL Certificates

The Federal Trade Commission (FTC) estimates that 3.2 million US citizens every year are victims of identity theft. Even though the lion's share of fraud takes place offline, many view online transactions as especially risky. To reassure prospective customers, online merchants must exhibit trustworthy security credentials.

With growing concerns about I.D. theft and fraud on the increase…opportunity knocks. By providing SSL certificates, you can help your customers establish themselves as reliable organizations that safeguard customer data through secure transactions.

Not only will you be helping your customers, but you'll be creating higher value orders, establishing a reoccurring revenue stream and strengthening customer retention.

Network Solutions is now offering our Partners the chance to sell nsProtect™ Secure SSL Certificates to their customers. To help you get started, here's an overview of Network Solutions nsProtect Secure SSL products and how they work.

Introducing Reseller SSL Certificates

When it comes to SSL Security, Network Solutions offers the best value and the highest guarantee in the marketplace. We offer four types of SSL certificates (nsProtect Secure Basic, Advanced, Wildcard and Extended Validation, as well as an nsProtect Assured Site Seal).

- **nsProtect Secure Basic SSL Certificate** provides a reasonably priced way for your customers to secure a Web site for online transactions.
- **nsProtect Secure Advanced SSL Certificate** offers the best certificate value available.
- **nsProtect Secure Wildcard Certificate** enables your customers to create an unlimited number of sub-domain certificates from a primary domain registration.
- **nsProtect Extended Validation SSL Certificate** provides the highest level of authentication and turns the browser address bar green — an additional sign that your site is secure.
- **nsProtect Assured Site Seal** establishes credibility for a Web site by validating that it is operating as a legitimate company.

The table below provides a high level snapshot of our products.

nsProtect™ Secure Basic SSL Certificate	nsProtect™ Secure Advanced SSL Certificate	nsProtect™ Secure Wildcard SSL Certificate	nsProtect™ Secure Extended Validation SSL Certificate	nsProtect™ Assured Site Seal
Cost effective $50K Guarantee Identity Assurance Issued in 2-4 business days Secure Site Seal	Secured by a well-trusted and recognized brand $1 Million Guarantee Identity Assurance Issued in 1 business day Secure Site Seal	Create an unlimited number of SSL Certificates from a single domain $1 Million Guarantee Identity Assurance Issued in 1 business day Secure Site Seal	Turns the browser address bar green $1 Million Guarantee Strongest Identity Assurance Secure Site Seal	Establish identity as a legitimate company $50K Guarantee Issued in 2-4 business days SSL encryption not included

Why Choose Network Solutions® nsProtect Secure SSL Certificates?

Some resellers charge considerably more for SSL certificates with similar features. You'll find that Network Solutions' prices enable you to be both competitive and profitable selling SSL certificates.

On the other end of the spectrum, some companies issue discounted SSL certificates which are less robust, for example, they provide weaker security or are compatible with fewer browsers. The result is a product that doesn't meet customer needs.

Let's take a look at which features customers consider important when choosing SSL certificates and examine how nsProtect Secure SSL Certificates stand out when it comes to:

- Secure transactions
- Identity assurance
- Browser compatibility
- Trusted seal

Secure Web Site Transactions

SSL (Secure Sockets Layer) is the transaction security protocol used by Web sites to protect online communications. The most common use of SSL is to provide protection for confidential data, such as entering personal details or credit card information into a Web site. This protocol provides two primary functions: encryption of data and identity assurance.

- Encryption allows data to be transmitted over computer networks in a secure manner.
- Identity assurance allows the business running the site to 'prove' that they are who they claim to be (the most robust level of identity assurance is offered through nsProtect Secure Extended Validation).

Encryption

Encryption allows data to be transmitted over computer networks in a secure manner by using a technique which scrambles the readable information into an unreadable format. SSL is the industry 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 remains private and integral. SSL is used by hundreds of thousands of Web sites in the protection of their online transactions with their customers.

This technology is based on the use of SSL certificates (also known as digital certificates or digital certs). The certificate contains an encryption key and information about the server it was issued for, the person(s) who requested the certificate, the dates the certificate is valid between, and the Certificate Authority (CA) who issued the certificate.

All nsProtect™ Secure SSL Certificates from Network Solutions are encrypted up to 256 bits. Additionally, Network Solutions® SSL Certificates also support lesser encryption levels as determined by the Web server or browser, in other words, if the Web server or browser is configured to only support 40 or 56-bit encryption, then a secure session can still be established at that encryption level.

Network Solutions issues 256-bit certificates. 256-bit encryption means that the data cryptographically encoded during an SSL session is at the highest level currently available, and nearly impossible to break. Some certificates are issued as low as 40 bit or 56 bit. With computing power available today, these lower-bit certificates are at risk of being cracked. Compared to a 40-bit encrypted SSL certificate, a 256-bit is many septillion times stronger.

With computing power growing exponentially, it is always wise to purchase as strong a certificate as is available so that online transmissions remain secure.

Identity Assurance

SSL does not just provide encryption – it offers another important feature, that of Identity Assurance. Having data encrypted so it cannot be intercepted is very useful, but it is equally critical that there is some assurance that the party receiving the data is actually who they claim to be.

Certificate Authorities are the organizations that issue SSLs and provide identity assurance. Browsers, such as Microsoft and Netscape, come with a pre-installed list of trusted Certification Authorities, known as the Trusted Root CA store. As a result of their "trusted" status, Certification Authorities are responsible for only issuing SSL certificates to legitimate companies. This is achieved by putting in place and following rigorous validation processes.

Before the SSL Certificate Authority agrees to sign and issue the certificate, they should first do a background check on the person or company requesting the certificate. This will verify that the entity is legitimate. Then, a check is done to ensure that they also own the domain-name or IP address (via the WHOIS register)

In addition, an SSL certificate also verifies the business or individual who owns the Web site that they are, in fact, who they claim to be. This is accomplished by manually checking credentials such as D-U-N-S number, articles of incorporation, WHOIS, passport, driver's license, etc.

Once all the details match and can be proven, the certificate is signed and issued. The certificate will then only function properly when used by the correct people on the correct server to which the certificate was issued.

As the SSL certificate provides Identity Assurance as well as the encryption, good strong validation procedures are essential from any Certificate Authority who issues SSL certificates.

All Network Solutions® security services include a limited guarantee for site visitors to provide extra assurance that a site is safe to conduct online business. This guarantee is limited to $1,000 per transaction, and the aggregate guarantee amount per security service is based on the following:

- **nsProtect™ Secure Advanced, Wildcard and Extended Validation certificate aggregate guarantee amount is $1,000,000**
- **nsProtect™ Secure Basic certificate and the nsProtect Assured Site Seal aggregate guarantee amount is $50,000**

For terms and conditions of our Relying Party Guarantee, please contact your Partner Support Representative or e-mail us at premiersupport@ networksolutions.com.

An SSL guarantee is an insurance policy put in place to back-up the strength of a Certificate Authority's validation techniques. The Certificate Authority should validate all certificates to the highest possible standard. If they do not, and the certificate is issued by mistake to a company or individual who is not entitled to it, and they then go on to defraud the public – the warranty can provide compensation in this instance. nsProtect™ Secure SSL Certificates are backed by the best guarantee on the market – up to $1 Million for nsProtect Secure Advanced, Wildcard and Extended Validation Certificates.

It is vital that you consider the validation process and guarantees that will work best for your business.

Browser Compatibility

Another important aspect to consider when evaluating an SSL certificate is its browser compatibility.

Browsers and operating systems come with a pre-installed list of trusted Certification Authorities, known as the Trusted Root CA store. As Microsoft and Netscape provide the major operating systems and browsers, they have elected whether to include the Certification Authority into the Trusted Root CA store, thereby giving trusted status.

A Certification Authority (CA) is a trusted third party organization that issues SSL Certificates. The role of the CA is to verify and thus guarantee the individual or entity applying for the certificate is who they claim to be. To fulfill its role, the CA will follow a set of steps designed to categorically validate the identity of the requestor.

SSL certificates will only be trusted by a browser if the Root Certificate of the Certification Authority is present within the trusted Root Certificates store of the browser. The level of compatibility is determined by which browsers contain the Root Certificate as a default. Anyone can generate a root CA certificate; but that certificate won't be installed and trusted by the root stores of Web browsers. Without going through a browser-recognized Certificate Authority, an alert box displays a warning that the certificate is not issued by a recognized authority.

As a result of their "trusted" status, Certification Authorities have a responsibility to ensure they only issue SSL certificates to legitimate companies. This is achieved by adhering to stringent validation processes.

Most of the major Certificate Authorities have their roots in the default Windows store and Netscape store. With alternate browsing software, such as Opera and Foxfire, becoming more popular, it makes sense to select an SSL provider with a high browser acceptance level in order to serve as many end users possible.

Network Solutions® nsProtect Secure SSL certificates are trusted by over 99% of the browsers used on the Internet today, including:

- **Microsoft Internet Explorer® 5.01+**
- **Mozilla Firefox® 1.0+**
- **Mozilla 0.6+**
- **Google™ Chrome**
- **KDE® Konqueror**
- **Netscape® 4.77 +**
- **Opera 7.0+**
- **Apple® Safari 1.2 +**
- **Camino® 1.0+**
- **AOL® 5+**

You should opt for an SSL provider with high browser coverage.

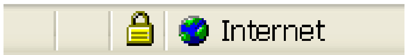
Trusted Seal from a Reputable Company

Web sites that are secured by SSL can easily be recognized by well-known markers, such as the URL that begins with "https://" instead of the usual "http://" or a small padlock icon in the corner of the Web browser.

Displaying the SSL Secure Padlock

The complexities of the SSL protocol remain invisible to end users. Instead, their browsers provide them with a key indicator to let them know they are currently protected by an SSL encrypted session. Visual indicators vary somewhat depending on the end user's browser.

For users of Internet Explorer SSL protection is displayed as a Padlock:



SSL Certificate Details

Clicking on the Padlock displays the details behind the SSL Certificate.

All SSL certificates are issued to validated companies or legally accountable individuals. Typically, an SSL certificate will contain, the following information: domain name, company name, address, city, state and country. It will also contain the expiration date of the certificate and details of the Certification Authority responsible for the issuance of the certificate.

Network Solutions® is at the forefront of providing fully qualified SSL certificates. Network Solutions will validate each application in accordance with the latest digital signature legislation pertaining to Qualified Certificates.

When a browser connects to a secure site, it will check to see that the site's SSL certificate has not expired, that it has been issued by a Certification Authority the browser trusts, and that it is being used by the Web site 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.

Most Internet users will refuse to provide personal information or conduct transactions on sites that are not protected by SSL.

Display of Critical Identification Information

Digital signature legislation is catching up to how SSL certificates are used commercially. At Network Solutions, we are already complying with the next generation of stricter legislation aimed at safeguarding online identities and transactions by including the following validated critical identification information within the SSL certificate:

- Common Name – the Fully Qualified Domain Name (FQDN) for which the SSL certificate is to be used
- Organization Name
- Organization Unit
- Street Address
- City/Town
- State/Province
- Country
- Zip/Postal Code

All the above information is validated quickly and efficiently by Network Solutions, ensuring customers receive their certificate quickly.

Site Seals

Many organizations want to proactively provide visitors with proof of their digital identity. Site seals can be used to foster confidence in a Web site's services and identity by promoting its "secure site" status to customers.

A site seal is a secure image appearing on a Web site that enables visitors to visibly tell that their online transaction will be secure, confidential and integral. Clicking or hovering the mouse over a site seal provides a real-time identity request of the company behind this Web site. Many SSL providers charge extra for site seals.

With Network Solutions as the Certification Authority behind nsProtect Secure SSL, customers can feel safe knowing that a Web site security is provided by reputable, trusted experts.

When reselling SSL certificates, put yourself in your customer's shoes. To maximize revenues, your customers must be able to deliver a sense of security and piece of mind to their customers. nsProtect Secure SSL Certificates come with a site seal from a company that is recognized and trusted.

As a Network Solutions® Partner, you can be the one to deliver the most cost-effective, highly trusted SSL products available. Take advantage of our low reseller pricing and discounted terms and sign up to profit with Network Solutions® Reseller SSL Certificates.