

Securing Your Web Server Identity

FIPS 140-2 Certified



TECHNOLOGY GUIDE



Hardware Protected SSL Certificate

Internet communication now plays a central role in the business strategy of today's organizations. Compromise of the sensitive customer data that a Web server, Application server or VPN gateway handles can result in devastating financial losses, liability for the disclosure of private information, and the disruption of key business activities and relationships.

With a VeriSign Hardware Protected SSL Certificate, you can benefit from the highest level of security available today to protect your sensitive Web transactions and promote this implementation of preventative best practice security as a competitive differentiator.

Web Authentication

Trust is central to customer loyalty and the growth of online business, and therefore security at the edge of your network infrastructure is paramount. Now firmly established, the SSL (Secure Sockets Layer) standard for secure Web based communications uses encryption and digital certificates to confirm the identity of parties and to enable delivery of encrypted information.

2000 to 2001 saw a 100% rise in the number of Web sites using encrypted transactions, and in January 2003 the number of sites with SSL certificates was recorded at 187,000.¹

The secure underpinnings of SSL digital certificates are the private SSL encryption keys used to establish secure sessions. It is therefore critical that SSL private keys are kept safe to ensure the privacy of online transactions. Effectively, the Web server's certificate cannot be trusted unless the associated private key is kept secret.

FIPS 140-2 (Federal Information Processing Standard) is a benchmark industry standard that outlines security requirements for cryptographic modules. FIPS 140-2 Level 2 defines that the private keys used in the encryption process be created and managed in a dedicated tamper evident cryptographic module. In the case of mission critical and sensitive data, FIPS 140-2 certified hardware security is a mandatory requirement for U.S. and Canadian federal agencies and commercial sectors too are increasingly subject to such operational mandates.

Evolving Threats—How vulnerable is your Web server?

Many organizations make the mistake of leaving their SSL keys exposed, relying on the security properties of the operating system. This approach is vulnerable to 'Key finding attacks'² from increasingly sophisticated attackers or internal abuse. Exposing cryptographic keys in this way can be equated to installing the best lock on your front door and then leaving the key under the mat. (Refer also to the Gartner independent report of June 2002: Software Security Is Soft Security: Hardware Is Required, by John Pescatore.)

Consequences of compromised Web server keys include:

- Data theft - Encrypted information to and from your Web site can be decrypted off-line and read by an attacker without your knowledge.
- Spoofing - with your server's private key an attacker can create a fake Web site that appears to be legitimate and through which your customers may trust their private information.
- Unauthorized access - Decryption of user login credentials sent over an SSL link allows the attacker to gain unauthorized access to sensitive data on the site by impersonating valid users.

¹ NetCraft Secure Server Survey, January 2003

² "Playing hide and seek with stored keys," http://www.ncipher.com/resources/downloads/files/white_papers/keyhide2.pdf

Hardware Protected Certificates—The new standard for industry best practice

VeriSign, the name behind the vast majority of all SSL certificates issued, and nCipher, the market leader in FIPS certified SSL acceleration hardware, have joined forces to counter the threat to Web server security with the Hardware Protected SSL Certificate. This new, premium grade VeriSign SSL certificate raises the bar for Web site security. By protecting the SSL private key in a FIPS 140 certified Hardware Security Module (HSM) throughout its lifecycle, from generation to destruction, the certificate's authenticity can be assured. For the first time a commercial SSL certificate has been created specifically for organizations that have taken the extra steps necessary to strengthen secure their use of SSL—by protecting the SSL server key in a FIPS validated hardware security module (HSM). The Hardware Protected SSL Certificate establishes a best practice security model, as recommended by consultants and security practitioners.

nCipher's nForce™ and nShield™ tamper-resistant hardware modules create a protective subsystem within your server where the SSL private keys are generated and managed in a physically protected environment. nCipher hardware modules used with the Hardware Protected SSL Certificate are certified to the international standard FIPS 140-2 Level 2 or greater, and the unique nCipher key management architecture creates a traceable infrastructure, ensuring secrecy and integrity of the cryptographic keys associated with SSL server certificates.

The high level of security provided by the Hardware Protected SSL Certificate is backed by the highest level of NetSure protection that VeriSign provides.

The NetSureSM Plan provides protection against certain occurrences, such as loss, theft, modification, or unauthorized access to your Private Key that corresponds to the public key in the VeriSign certificate. The Plan also protects you against Unauthorized Revocation, Loss of Use, and the Erroneous Issuance of Certificates and Impersonation.

Promoting Security for Competitive Advantage

The ability to show your customers that their privacy is your priority and that you take this responsibility seriously is crucial. The VeriSign Secure Site Seal is the visual assurance to a user that a Web site takes their security seriously. In fact it can be a competitive advantage when a company can demonstrate they are an industry leader, providing a more secure service when working with credit card numbers, health records, PIN numbers or other private data. The ability to prove an advanced level of on-line security not only helps secure your business, it can also help to grow your business. The Secure Site Seal will visibly differentiate the Hardware Protected SSL Certificate from other VeriSign SSL certificates. Prominently featuring this seal on your site will help inspire the highest level of confidence.

SSL Acceleration—Lowering Infrastructure Costs

Adding servers isn't the most effective approach to scaling Web site capacity and managing growth: adding servers is expensive, adds administrative overhead, and provides limited SSL processing capacity.

In addition to the security benefits, the nCipher HSM provides SSL acceleration. SSL operations put an extremely heavy load on server resources, and can slow server performance to a crawl under even moderate traffic conditions dramatically impacting overall system capacity. The HSM's powerful acceleration co-processors free the server's CPU to respond to more customer requests.

Benefits of Hardware Protected SSL Certificate:

- Best Practice Security: proof that the private SSL keys were created and have subsequently been managed within a FIPS 140-2 validated HSM, one of the most stringent standards in the IT security industry
- Prevent online attacks involving stolen private keys: data theft, Web site spoofing, and unauthorized access
- Web server SSL acceleration (up to 400 transactions per second), via the HSM
- Highest level of VeriSign NetSure liability protection
- Competitive advantage through promotion of Web site security via the VeriSign Secure Site Seal

Technical Specifications*

VeriSign Hardware Protected SSL Certificate Characteristics

- SSL private key protected in FIPS 140-2 level 2 validated hardware
- Powerful 128-bit SSL Encryption
- VeriSign Authentication Service
- VeriSign Secure Site Seal
- VeriSign NetSure protection up to \$500,000
- Plus all other features bundled with the VeriSign Secure Site Pro certificate

nCipher Hardware Security Module Characteristics

The VeriSign Hardware Protected SSL Certificate is supported on all of nCipher's nForce and nShield HSMs. These HSMs are available in multiple physical form factors, SSL performance levels and FIPS 140 validation levels. For technical specifications of the nCipher HSMs, please refer to the nCipher Web site at <http://www.ncipher.com/products/index.html>.

For a limited time only beginning May 2003, the Hardware Protected SSL Certificate bundled with an nForce150 PCI card is available from nCipher at a promotional price in North America. Contact nCipher for details.

SSL-enabled Application Software Supported

- Apache Web Server v1.3.9 or later
- BEA Weblogic 8.1 (when released)
- IBM WebSphere Application Server 5.0
- IBM HTTP Server 1.3.26 and 2.0
- IBM Tivoli Access Manager 4.1
- Microsoft IIS 4, IIS 5
- Microsoft ISA Server
- Reactivity (XML) Service Firewall v1.1
- RedHat Stronghold 3.0
- SunONE (formerly iPlanet) Directory Server 4.1
- SunONE (formerly iPlanet) Proxy Server 3.6
- SunONE (formerly iPlanet) Web Server v. 6.0, 4.1
- VeriSign Trust Gateway 1.0 (when released)
- webMethods B2Bi 3.5

The most comprehensive up-to-date technical specifications for the VeriSign Hardware Protected SSL Certificate can be found at: www.ncipher.com/hardwarecert

Every effort has been made to ensure the information included in this data sheet is true and correct at the time of going to press. However, the products and services described herein are subject to continuous development and improvement, and the right is reserved to change their specifications at any time. The most up-to-date technical specifications for the VeriSign Hardware Protected SSL Certificate can be found at: www.ncipher.com/TBC.

For Information regarding the Hardware Protected SSL Certificate contact:
Contact a VeriSign Sales Representative with questions about Hardware Protected SSL Certificates at (650) 426-5112 or (866) 893-6565 or send an e-mail message to internetsales@verisign.com

North America
nCipher Inc., 500 Unicorn Park Drive, Woburn, MA 01801, United States
Tel: +1 781 994 4000, E-mail: ussales@ncipher.com

Europe & International
nCipher Corporation Ltd., Jupiter House, Station Road, Cambridge, CB1 2JD, U.K.
Tel: +44 (0)1223 723600, E-mail: int-sales@ncipher.com

Asia Pacific
nCipher Corporation Ltd., 15th Floor, Cerulean Tower, 26-1 Shakuragaoka-cho, Shibuya-ku, Tokyo 150 8512 Japan
Tel: +81 3 5456 5484, E-mail: int-sales@ncipher.com

About VeriSign, Inc.

VeriSign's (Nasdaq:VRSN) critical infrastructure services deliver an unmatched level of security and reliability to Internet and telecommunications customers around the world. Nearly all of the Fortune companies 500, governmental bodies and other organizations, hundreds of thousands of small businesses and hundreds of service providers rely on VeriSign to engage in digital commerce and communications. VeriSign's core services include Security, Telecommunication, and Registry Services.



© 2003 VeriSign, Inc. All rights reserved.

VeriSign, the VeriSign logo, The Value of Trust, and other trademarks, service marks, and logos are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. nCipher Corporation Ltd., nCipher and nCipher Security World are trademarks or registered trademarks of nCipher Corporation Ltd. All other trademarks contained herein are the property of their respective holders. 4/03