VeriSign®

White Paper

Strong Security in Multiple Server Environments

VeriSign® OnSite® for Server IDs

Contents

1. Introduction

In today's businesses, electronic communication is a central part of the everyday flow of information, and privacy is a top priority. Whether your company conducts sales over the Internet or hosts a company-specific network, you want to know that your communications are safe from unauthorized interference.

For information exchange between servers and client browsers and server-to-server, load balancing devices and SSL accelerators, Secure Server IDs from VeriSign, Inc. have become recognized as the bottom line in security. Working with the Secure Sockets Layer (SSL) protocol for encryption, Secure Server IDs protect businesses against site spoofing, data corruption, and repudiation of agreements. They assure customers that it is safe to submit personal information, and provide colleagues with the trust they need to share sensitive business information.

For companies with multiple servers and load balancing devices in their network, VeriSign now offers the option of locally managing your own Server IDs with OnSite for Secure Server IDs. If you need to secure five or more servers, enrollments and cancellations can become cumbersome when managed one by one. With OnSite for Secure Server IDs, you save money by purchasing your Server IDs in bulk, then save time by issuing your own IDs to servers and load balancing devices within your organization. You can customize your end-user support to meet your company-specific needs, and integrate your server and client security systems. With OnSite for Secure Server IDs, VeriSign provides the technical tools and back-end support you need, while an administrator at your site manages your secure network from day to day. In other words, you get VeriSign-strength security within your own control.

This paper provides you with a basic introduction to Digital ID technology and Server IDs from VeriSign. It then describes the reasons that you would want to consider OnSite for Server IDs as an alternative to one-by-one purchasing. Finally, it will present the features you can expect if you decide OnSite for Server IDs is right for your organization.

2. Security Solutions: The Digital ID System

Given the security risks involved in conducting business on-line, what does it take to make your Internet transactions and company communications safe? Industry leaders agree that the answer is the VeriSign Server ID. VeriSign has issued over 485,000 Server IDs. Companies using VeriSign's Server IDs include 90 of the Fortune 100 companies and all of the RelevantKnowledge, Inc. Top 20 Commerce Sites.

2.1. What Is a Digital ID?

A Digital ID, also known as a digital certificate, is the electronic equivalent to a passport or business license. It is a credential, issued by a trusted authority, that individuals or organizations can present electronically to prove their identity or their right to access information.

When a Certification Authority (CA) such as VeriSign issues Digital IDs, it verifies that the owner is not claiming a false identity. Just as when a government issues a passport it is officially vouching for the identity of the holder, when a CA gives your business a digital certificate it is putting its name behind your right to use your company name and Web address.

2.2 How Do Digital IDs Work?

The solution to problems of identification, authentication, and privacy in computer-based systems lies in the field of cryptography. Because of the non-physical nature of electronic communication, traditional methods of physically marking transactions with a seal or signature are useless. Rather, some mark must be coded into the information itself in order to identify the source and provide privacy against eavesdroppers.

One widely used tool for privacy protection is what cryptographers call a "secret key." Log-on passwords and cash card PINs are examples of secret keys. Consumers share these secret keys only with the parties they want to communicate with, such as an on-line subscription service or a bank. Private information is then encrypted with this password, and it can only be decrypted by one of the parties holding that same password.

Despite its widespread use, this secret-key system has some serious limitations. As network communications proliferate, it becomes very cumbersome for users to create and remember different passwords for each situation. Moreover, the sharing of a secret key involves inherent risks. In the process of transmitting a password, it can fall into the wrong hands. Or one of the sharing parties might use it maliciously and then deny all action.

Digital ID technology addresses these issues because it does not rely on the sharing of secret keys. Rather than using the same key to both encrypt and decrypt data, a Digital ID uses a matched pair of keys, which are unique complements to one another. In other words, what is done by one key can only be undone by the other key in the pair.

In this type of key-pair system, your "private key" gets installed on your server and can only be accessed by you. Your "public key" gets widely distributed as part of a Digital ID. Customers, partners or employees who want to communicate privately with your server can use the public key in your Digital ID to encrypt information, and you are then the only one who can decrypt that information. Since the public key alone does not provide access to communications, you do not need to worry about who gets hold of this key.

Your Digital ID tells customers and correspondents that your public key in fact belongs to you. Your Digital ID contains your name and identifying information, your public key, and VeriSign's own digital signature as certification.

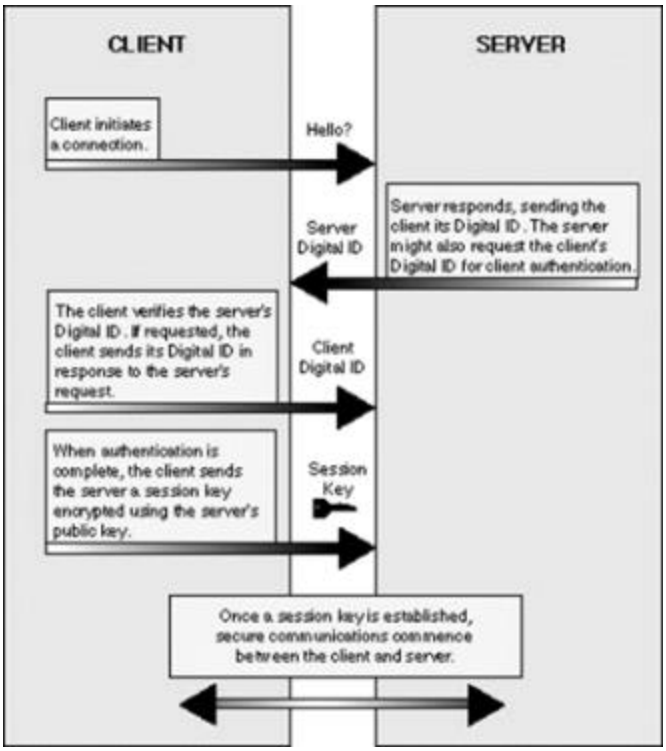
2.3 How Do Server IDs Work?

VeriSign Secure Server Digital IDs allow any server to implement the Secure Sockets Layer (SSL) protocol, which is the standard technology for secure Web-based communications. SSL capability is built into server hardware, but it requires a Digital ID in order to be functional.

With the latest SSL and a Secure Server Digital ID, your Web site will support the following functions:

- *Mutual Authentication*. The identity of both the server and the customer can be verified so that all parties know exactly who is on the other end of the transaction.
- *Message Privacy*. All traffic between the server and the customer is encrypted using a unique "session key." Each session key is only used with one customer during one connection, and that key is itself encrypted with the server's public key. These layers of privacy protection guarantee that information cannot be intercepted or viewed by unauthorized parties.
- *Message Integrity*. The contents of all communications between the server and the customer are protected from being altered en route. All those involved in the transaction know that what they're seeing is exactly what was sent out from the other side.

The diagram below illustrates the process that guarantees protected communications between a server and a client. All exchanges of Digital IDs happen within a matter of seconds and appear seamless to the client.

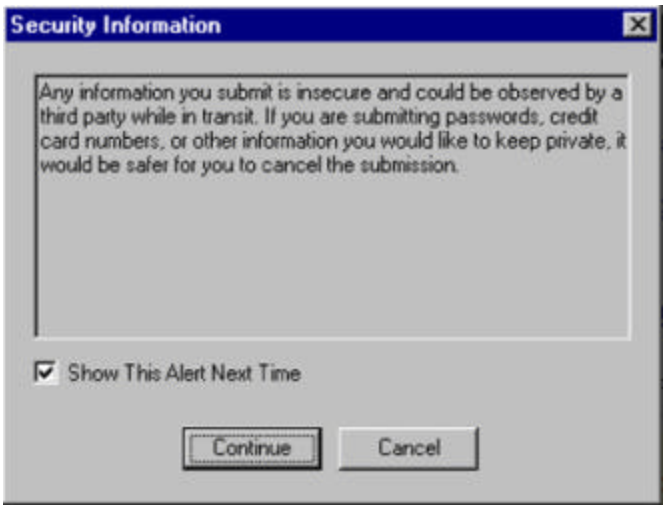


All of this technology translates to online communications that are safe for you and your customers. End users know exactly who they are dealing with and feel comfortable that the information they send is not falling into unknown hands. You know that your server is receiving accurate transmissions that have not been tampered with or viewed en route.

2.4 What Do End-Users See?

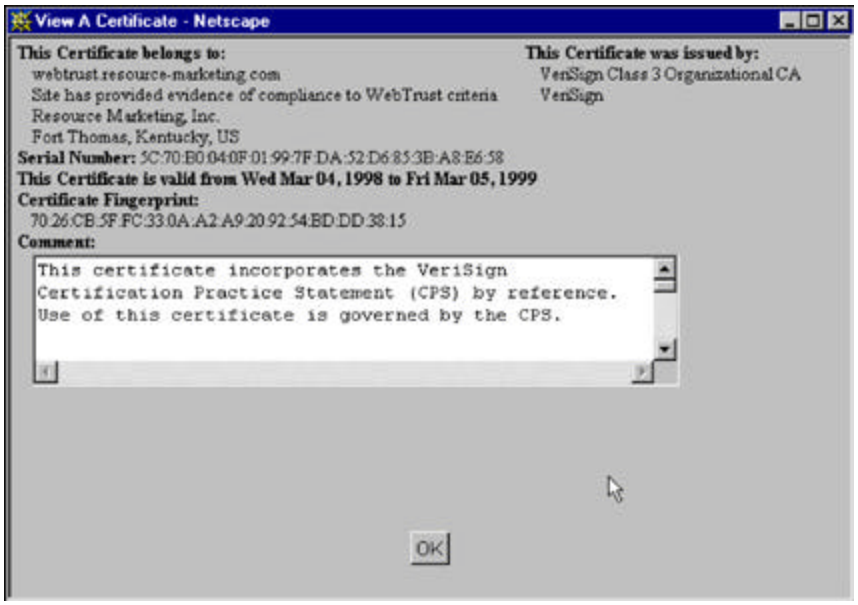
Both the Netscape Navigator and the Microsoft Internet Explorer browsers have built-in security mechanisms to prevent users from unwittingly submitting sensitive information over insecure channels.

If a user tries to submit information to an unsecured site, the browsers will, by default, show a warning such as the following:



By contrast, if a user attempts to submit information to a site with a valid Digital ID and an SSL connection, no such warning is sent. Furthermore, both the Microsoft and Netscape browsers provide users with a positive visual clue that they are at a secure site. In Netscape Navigator 3.0 and earlier, the key icon in the lower left hand corner of the browser, which is normally broken, is made whole. In Netscape Navigator 4.0 and later, as well as in Microsoft Internet Explorer, the normally open padlock icon becomes shut, as shown below:

For more information, users may visually inspect the site's Digital ID by double clicking on the security icon. They will then see a display like the following:

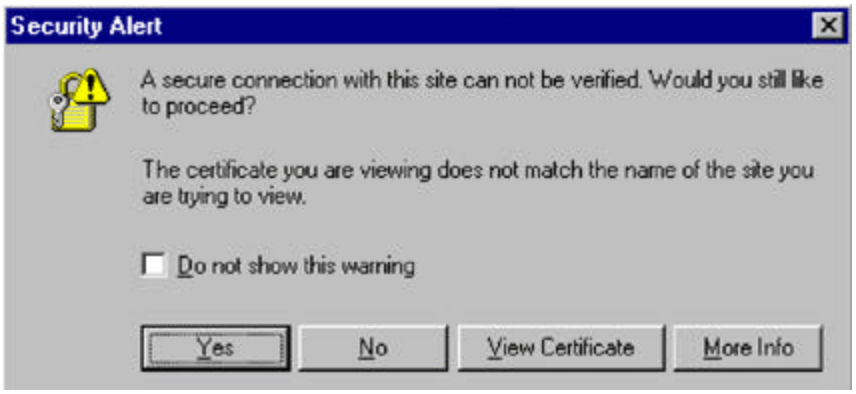


This Digital ID display establishes that the site (webtrust.resource-marketing.com) really does belong to Resource Marketing, Inc. of Fort Thomas, Kentucky. It also establishes that VeriSign issued the Digital ID and is vouching for the site's validity.

These positive visual cues only occur if the site has a valid digital certificate, issued by a Certificate Authority that is trusted by the browser. Technically, this means the CA's public key must be listed in the browser's directory of trusted roots. VeriSign's public keys are bundled with 98 percent of all of the browsers in use today.

By contrast, if a site has a certificate issued by an untrusted authority, the browser will display a warning such as the following:

Similarly, if a site is falsifying its claim to a certificate (e.g. if www.hacker.com tries to use a certificate for www.bookstore.com), the user will also receive a warning, such as the following:



When you install a VeriSign Digital ID on your server and enable SSL, your customers and partners see clearly that they are operating in a secure environment.

3. The Needs of Your Organization

Once you have decided to invest in the peace of mind that comes with VeriSign Server IDs, you will need to decide whether one-by-one purchasing or OnSite for Server IDs meets the needs of your organization. Following are several factors you should consider.

3.1 The Size of Your Network

If your company will be hosting 5 or more servers within the next year, you are a good candidate for OnSite for Server IDs. You can begin with 5 Server IDs and the administrator's kit. This should meet your current needs plus your renewals for later in the year. You will save money through a bulk discount, while increasing efficiency significantly by eliminating the need to enroll and pay separately for each Server ID.

3.2 Change Within Your Network

If you want the ability to expand, reduce, or restructure your network with no hassle, OnSite for Server IDs is the answer. With one-by-one purchasing, each addition, renewal, or cancellation of a secure server must go through VeriSign's service center. Each Server ID requires 3-5 business days to be issued and must be paid for with a separate credit card processing or purchase order. When you purchase in bulk through OnSite for Server IDs, your OnSite administrator can issue and cancel Server IDs instantly, giving you superior control of your operations, especially in critical times.

3.3 Cross-Departmental Coordination

If several groups within your organization are likely to work with secure servers, OnSite for Server IDs will simplify and enhance your information system management.

When server hosts from each department apply separately for Server IDs from VeriSign, the result can be disorganization, compromising both the efficiency and integrity of your network's security. A department might "reinvent the wheel" that has already been invented within the company, or alternatively a group might assume that a given security issue is being handled elsewhere and thus fail to address it. With one administrator distributing Server IDs as the need arises, you reduce the possibility for overlap or lapse in the security of your electronic communications.

3.4 The Needs of Your End Users

Would your end users benefit from a Web and e-mail interface that is designed for their specific use? With OnSite for Server IDs, you have the option of customizing the enrollment forms and support pages your users see. With one-by-one management, each person hosting a secure server interacts with the VeriSign system for enrollment, renewal and cancellation. This interface, while straightforward and user-friendly, is designed for general use with any server.

If you purchase your Server IDs through OnSite, your package includes VeriSign's enrollment and support screens, but you also have the option of customizing or creating your own pages. You can provide instructions specific to your server software, your organizational structure, or other company specifics. You can design the look and feel to match the interface your users are comfortable with, and even integrate it with your personal Digital ID interface if you use OnSite to issue digital certificates to individuals.

When your users need technical support, they can immediately access the OnSite administrator within your organization. If the problem cannot be addressed locally, the OnSite administrator can always contact a member of the support team at VeriSign.

4. The OnSite for Server IDs System

OnSite for Server IDs is designed to be easily installed and administered. The following features provide the backbone of your network security system.

4.1 The OnSite for Server IDs Administrator

When you use OnSite for Server IDs to manage your secure network, an administrator within your organization oversees a local control center to issue Server IDs.

This OnSite Administrator, using a standard PC with the Netscape Navigator browser, purchases OnSite for Server IDs from VeriSign and receives the Administrator's Kit. Before issuing the Administrator's Kit, VeriSign conducts the necessary background checks to ensure that your organization is legitimate and has the right to use the domain names being secured.

The Administrator's Kit includes all of the software necessary to establish the OnSite Control Center on the administrator's PC. It also includes an optional smart card reader and an
OnSite Administrator ID stored on a smart card.

Once the administrator's kit is installed and the Control Center is up and running, you are ready to start issuing Server IDs.

4.2. Instant Enrollment for Server IDs

The local Control Center allows users within your network to receive Secure Server IDs without any manual intervention from VeriSign. Since VeriSign has already verified your company and domain names, the only approval necessary is from the OnSite Administrator at your organization. The enrollment process goes as follows:

1. A user within your network generates a Certificate Signing Request (CSR) on the server being secured.

2. The user submits the CSR, along with the necessary enrollment forms, to the VeriSign Digital ID Center.

3. VeriSign instantly and automatically sends a pending request to the OnSite Control Center at your organization.

4. The OnSite Administrator within your organization validates the user's enrollment request.

5. VeriSign generates a Server ID and sends it to the user's e-mail address.

6. The user downloads the Server ID and installs it on the server.

All communications with VeriSign occur in protected SSL sessions and are thus safe for your company.

5. For More Information

For the strongest, most reliable protection of your client-browser communications, VeriSign Server IDs are widely recognized as the industry standard. Server IDs allow your Internet site or corporate network to enable SSL encryption, which authenticates your server and guarantees against alteration and interception of data.

For Server ID protection on multi-server networks, OnSite for Server IDs makes managing your Server IDs cheaper and more efficient, and enhances coordination within your organization. OnSite for Server IDs provides the options of customized end-user support, private label certification, and OnSite for issuing digital certificates to individuals integration, making it the security system that fits the unique needs of your company.

To learn more about OnSite for Server IDs, contact a VeriSign Sales Representative at 1-650-429-5115. Visit VeriSign on the Web at www.verisign.com.

6. Other VeriSign Solutions

VeriSign OnSite allows an organization to issue digital certificates to individuals within its network. These Digital IDs can replace password log-on to a company network and allow your Web site to control who accesses its content. Personal Digital IDs also make it possible to send digitally signed and encrypted e-mail, using the S/MIME (Secure Multipurpose Internet Mail Extension) protocol.

If your company already uses OnSite to issue digital certificates to individuals within its network, or if you are interested in doing so, you can integrate this system with your OnSite for Server ID management. The OnSite Administrator's Kit gives you the option of controlling all IDs from one Control Center.

VERISIGN, INC.
1350 CHARLESTON ROAD
MOUNTAIN VIEW, CALIFORNIA 94043
WWW.VERISIGN.COM