VeriSign®

Technical Brief

Building an E-Commerce Trust Infrastructure

SSL Server Certificates and Online Payment Services

Contents

Executive Summary

Businesses that can manage and process e-commerce transactions can gain a competitive edge by reaching a worldwide audience, at very low cost. But the Web poses a unique set of trust issues, which businesses must address at the outset to minimize risk. Customers submit information and purchase goods or services via the Web only when they are confident that their personal information, such as credit card numbers and financial data, is secure.

The solution for businesses that are serious about e-commerce is to implement a complete e-commerce trust infrastructure. PKI cryptography and digital signature technology, applied via Secure Sockets Layer (SSL) digital certificates, provide the authentication, data integrity, and privacy necessary for e-commerce. Internet payment gateway systems provide online merchants with the ability to efficiently and securely accept and process a variety of online payments from customers.

VeriSign, Inc., offers the essential components of an Internet trust infrastructure to e-commerce businesses. By installing a VeriSign SSL Server ID on their Web servers, businesses can securely collect sensitive information online and increase business by giving their customers the confidence of knowing that payment transactions are safe. VeriSign Payment Services VeriSign Payflow Payment Services simplify e-commerce by providing payment connectivity over the Internet between buyers, sellers, and financial networks for transactions involving all major consumer credit card, debit card, electronic check, purchase card, and Automated ClearingHouse (ACH) transactions. VeriSign's Commerce Site solutions combine both SSL Server IDs and Payflow Pro payment services, along with additional value-added features, to form a complete e-commerce trust infrastructure solution.

I. The E-Commerce Opportunity

A secure e-commerce Web site can provide businesses with powerful competitive advantages, including increased online retail sales as well as streamlined application processes for products such as insurance, mortgages, or credit cards. E-commerce credit card sales can be especially lucrative: according to independent analysts, cash transactions on the Internet will reach $9 billion in 2000, and $30 billion in 2005.

By offering products and services on the Web, businesses can gain unique benefits:

- **New customers**: Anyone with an Internet connection is a potential customer: millions around the world are already using the Internet for business transactions. Web storefronts are open 24 hours a day, and require no investments in brick and mortar.
- **Cost-effective delivery channel**: Many products and services, such as software or information, can be distributed directly to customers via the Web, enhancing the customer experience and increasing profitability by eliminating the shipping and overhead costs associated with order fulfillment.
- **Streamlined enrollment**: Paper-based enrollment workflows are fraught with delays. Applications for insurance, a mortgage, or a credit card, for example, can be held up in the mail. And once received, application information must be entered into computer systems manually, a labor-intensive process that can introduce errors. By accepting applications via a secure Web site, businesses can speed application processing, reduce processing costs, and improve customer service.
- **Better marketing through better customer knowledge**: Establishing a storefront on the Web positions enterprises for one-to-one marketing—the ability to customize products and services to individual customers rather than large market segments. The Web facilitates one-to-one marketing by enabling businesses to capture information about demographics, personal buying habits, and preferences. By analyzing this information, enterprises can target merchandise and promotions for maximum impact, tailor Web pages to specific consumers, and conduct effective, tightly focused marketing campaigns.

No business can afford to ignore this opportunity. But businesses also can't ignore the potential pitfalls. Before entering the fiercely competitive e-commerce arena, businesses must carefully assess and address the accompanying risks.

A. The Risks and Challenges of E-Commerce Trust

To succeed in the fiercely competitive e-commerce marketplace, businesses must become fully aware of Internet security threats, take advantage of the technology that overcomes them, and win customers' trust. Eighty-five percent of Web users surveyed reported that a lack of security made them uncomfortable sending credit card numbers over the Internet. The merchants who can win the confidence of these customers will gain their loyalty—and an enormous opportunity for expanding market share.

In person-to-person transactions, security is based on physical cues. Consumers accept the risks of using credit cards in places like department stores because they can see and

touch the merchandise and make judgments about the store. On the Internet, without those physical cues, it is much more difficult to assess the safety of a business. Also, serious security threats have emerged. By becoming aware of the risks of Internet-based transactions, businesses can acquire technology solutions that overcome those risks:

- **Spoofing**—The low cost of Web site creation and the ease of copying existing pages makes it all too easy to create illegitimate sites that appear to be published by established organizations. In fact, con artists have illegally obtained credit card numbers by setting up professional-looking storefronts that mimic legitimate businesses.
- **Unauthorized disclosure**—When transaction information is transmitted "in the clear," hackers can intercept the transmissions to obtain customers' sensitive information.
- **Unauthorized action**—A competitor or disgruntled customer can alter a Web site so that it refuses service to potential clients or malfunctions.
- **Eavesdropping**—The private content of a transaction, if unprotected, can be intercepted en route over the Internet.
- **Data alteration**—The content of a transaction can be not only intercepted, but also altered en route, either maliciously or accidentally. User names, credit card numbers, and dollar amounts sent "in the clear" are all vulnerable to such alteration.

B. The Goals of Implementing an E-Commerce Trust Infrastructure

To take advantage of the opportunities of e-commerce and avoid the risks of communicating and transacting business online, every business must address practical problems and questions involving privacy, security, and overall confidence in the underlying features of the system. Such concerns include:

"How can I be certain that my customers' credit card information is not accessible to online eavesdroppers when they enter into a secure transaction on the Web?"

"How can I reassure customers who come to my site that they are doing business with me, not with a fake set up to steal their credit card numbers?"

"Once I've found a way to authoritatively identify my business to customers and protect private customer information on the Web, what's the best way to let customers know about it, so that they can confidently transact business with me?"

"When customers feel confident enough to buy something from me online, how can I enable them to pay me easily using their credit cards or other payment methods?"

" How can I verify that customer's credit card information is valid?"

"What do I do with payment information once customers send it to me?"

The process of addressing these general security questions determine the fundamental goals of establishing an e-commerce trust infrastructure:

Authentication: Customers must be able to assure themselves that they are in fact doing business and sending private information with a real entity—not a "spoof" site masquerading as a legitimate bank or e-store.

Confidentiality: Sensitive Internet communications and transactions, such as the transmission of credit card information, must be kept private.

Data integrity: Communications must be protected from undetectable alteration by third parties in transmission on the Internet.

Nonrepudiation: It should not be possible for a sender to reasonably claim that he or she did not send a secured communication or did not make an online purchase.

II. The Solution: How to Build an Infrastructure for Trusted E-Commerce

The solution for meeting each of the goals above includes two essential components:

- Digital certificates for Web servers, to provide authentication, privacy and data integrity through encryption
- A secure online payment management system, to allow e-commerce Web sites to securely and automatically accept, process, and manage payments online

Together, these technologies form the essential trust infrastructure for any business that wants to take full advantage of the Internet.

A. Overview: Public Key Cryptography & Digital Certificates

This section presents background technical information on cryptographic systems, including Public Key Cryptography, the system underlying Secure Sockets Layer (SSL)—the basis for every e-commerce trust infrastructure.

Encryption is the process of transforming information before communicating it to make it unintelligible to all but the intended recipient. Encryption employs mathematical formulas called cryptographic algorithms, or ciphers, and numbers called keys, to encrypt or decrypt information.

1. Symmetric Cryptography

Until recently, symmetric encryption techniques were used to secure information transmitted on public networks. Traditional symmetric cryptographic systems are based on the idea of a shared secret. In such a system, two parties that want to communicate securely first agree in

advance on a single "secret key" that allows each party to both encrypt and decrypt messages.

Symmetric cryptography has several drawbacks. Exchanging secret keys is unwieldy in large networks. Furthermore, the sharing of secret keys requires both senders and recipients to trust, and therefore be familiar with, every person they communicate with securely. Also, symmetric systems require a secure channel to distribute the "secret" keys in the first place. If there is indeed such a secure channel, why not use it to send the entire secret message?

In today's Web-based systems involving many participants and transitory interactions with strong cryptography requirements, such symmetric key-based systems are highly impractical as a means for agreeing upon the necessary secrets to begin communicating securely.

This problem, the key agreement, or key distribution problem, is part of a larger problem that is central to the modern understanding of cryptographic systems—the key management problem. The key management problem described more fully below. Together, they represent the fundamental challenge in designing effective cryptography systems for modern computing systems. Symmetric key encryption plays an important role in the SSL protocol, along with asymmetric public key encryption.

2. Public-Key Cryptography

Today's public key, or asymmetric cryptography systems are a considerable improvement over traditional symmetric cryptography systems in that they allow two parties to exchange data privately in the presence of possible eavesdroppers, without previously agreeing on a "shared secret." Such a system is a called "asymmetric" because it based on the idea of a matched cryptographic key pair in which a cryptographic key is no longer a simple "shared secret" but rather is split into two subkeys, the private key and public key.

Abstractly, a participant wishing to receive encrypted communications using an asymmetric cryptography system will first generate such a key pair, keeping the private-key portion as a secret and the "publishing" the public-key portion to all parties that would like to encrypt data for that participant. Because encrypting data requires only access to the public key, and decrypting data requires the private key, such a system in principle can sidestep the first layer of complexity in the key management problem since no shared secret need be exchanged.

3. Modern Cryptography Systems: A Hybrid Approach

In fact, a combination of both public-key and traditional symmetric cryptography is used in modern cryptographic systems. The reason for this is that public-key encryption schemes are computationally intensive versus their symmetric key counterparts. Because symmetric key cryptography is much faster for encrypting bulk data, modern cryptography systems typically use public-key cryptography to solve the key distribution problem first, then symmetric key cryptography is used to encrypt the bulk data.

Such a scheme is used by today's SSL protocol for securing Web transactions, as well as by secure e-mail schemes such as S/MIME that are built into such products as Netscape Communicator and the Microsoft Internet Explorer. See "IV. SSL Server Certificates" below for more on SSL.

4. The Key Management Problem

Underlying every cryptographic system is a set of practical problems and questions involving privacy, security, and overall confidence in the underlying confidentiality features of the system. In principle, the techniques of asymmetric and symmetric cryptography are sufficient to resolve the security questions and properties described above. For example, today's Web browsers use the public key of a Web site in order to send credit card numbers over the Web; similarly, one can protect access to files and data using a private symmetric key to scramble the information before saving it.

However, in practice, each of these problems requires a "certified" public key in order to operate correctly without third parties being able to interfere. This leads to a second set of questions; for example:

> "How can I be sure that the public key that my browser uses to send credit card information is in fact the right one for that Web site, and not a bogus one?"

> "How can I reliably communicate my public keys to my correspondents so that they can rely on it to send me encrypted communications?"

What's needed in order to address such concerns is the notion of a "secure binding" between a given entity that participates in a transaction and the public key that is used to bootstrap secure communication with that entity using asymmetric public key cryptography. The next section describes how a combination of digital signatures and X.509 digital certificates (which employ digital signatures), including SSL certificates, fulfills this role in e-commerce trust systems.

5. Digital Signatures

Digital signatures are based on a combination of the traditional idea of data hashing with public-key based encryption. Most hash functions are similar to encryption functions; in fact, some hash functions are just slightly modified encryption functions. Most operate by grabbing a block of data at a time and repeatedly using a simple scrambling algorithm to modify the bits. If this scrambling is done repeatedly, then there is no known practical way to predict the outcome—it is not in general practical for someone to modify the original data in any way while ensuring that the same output will emerge from the hash function. These hash-based signature algorithms use a cryptographically secure hash function such as Message Digest 5 (MD-5) or Secure Hash Algorithm (SHA) to produce a hash value from a given piece of data.

Because the digital signature process is central to the idea of a digital certificate—and in turn, the digital certificate is the primary tool to ensure e-commerce security—it's useful to look at a diagram of the process:

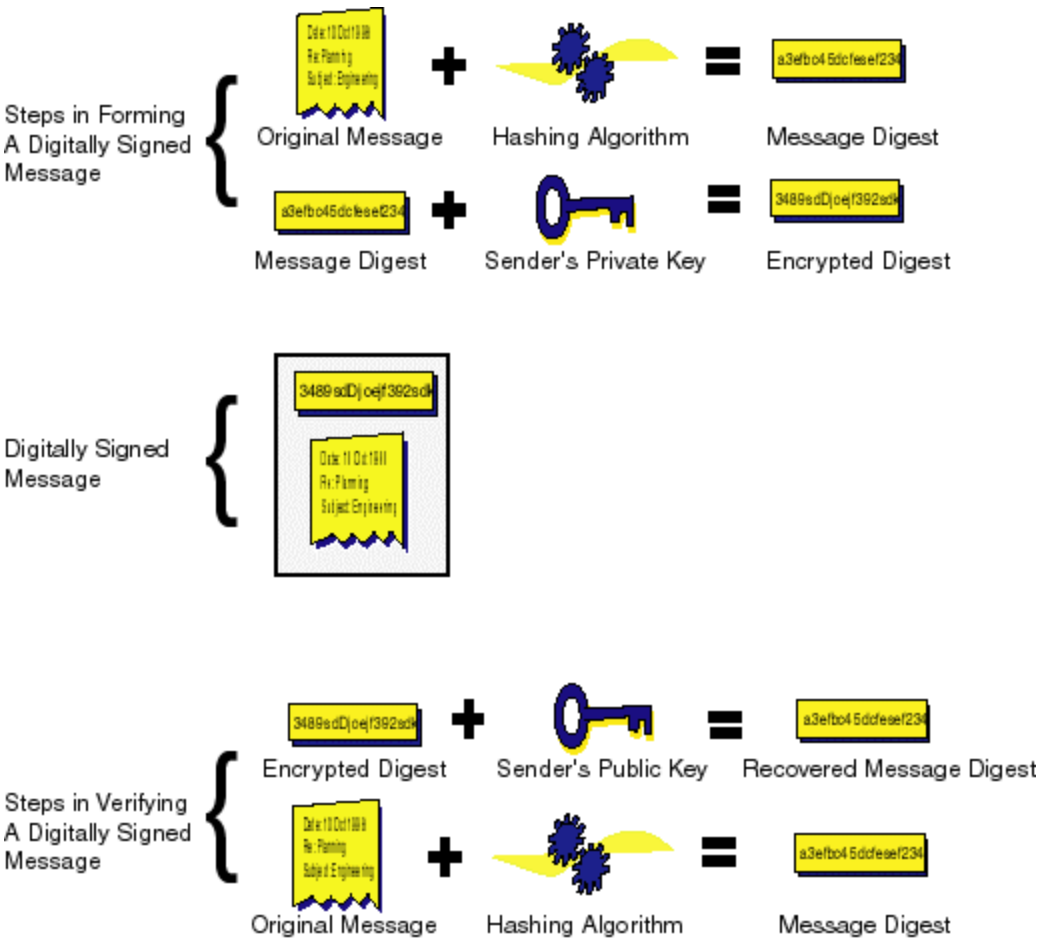


Figure 1: Steps in forming and verifying a digitally signed message

The figure illustrates the steps taken by a sender in forming a digitally signed message as well as the steps a recipient takes in verifying that the signed message is valid.

The first step is to take the original message and compute a "digest" of the outgoing message using a hashing algorithm. The result is a "message digest," which is typically is depicted as a long string of hexadecimal digits (and manipulated by software as binary data). In the next step, the sender uses his private key to encrypt the message digest.

The original message content, together with the encrypted digest, forms a digitally signed message, as depicted in the center of the figure. This digitally signed message is suitable for delivery to the recipient. On receipt, the receiver verifies the digital signature using an

inverse set of steps: first the encrypted digest is decrypted using the sender's public key. Next, this result is compared to an independent computation of the message digest value using the hashing algorithm. If the two values are the same, the message has been successfully verified.

Note that no actual encryption of the message content itself need take place. Only the digital signature itself is encrypted while the message is in transit (unless, of course there are privacy concerns, in which case the message content should be encrypted as well).

Why is a digital signature compelling evidence that only the intended signer could have created the message? For example, what if interlopers were to change the original message? It was not encrypted, after all, and could have been changed by a third party in transit. The answer is that if such a change had been made, then the decrypted, original message digest wouldn't have matched the recomputed one for the changed data in the message. Verification of the digital signature would fail. Similarly, the creation of a bogus signature is impractical because an interloper doesn't have the appropriate private key.

6. Digital Certificates

A digital certificate is an electronic file that uniquely identifies individuals and Web sites on the Internet and enables secure, confidential communications. It associates the name of an entity that participates in a secured transaction (for example, an e-mail address or a Web site address) with the public key that is used to sign communication with that entity in a cryptographic system.

Typically, the "signer" of a digital certificate is a "trusted third party" or "Certificate Authority" (CA), such as VeriSign, that all participants to the use of the such certificates agree is a point of secure storage and management of the associated private signing key. The CA issues, creates, and signs certificates as well as possibly playing a role in their distribution.

Using digital certificates simplifies the problem of trusting that a particular public key is in fact associated with a participating party, effectively reducing it to the problem of "trusting" the associated CA service. Digital certificates therefore can serve as a kind of digital passport or credential. This approach represents an advance in the key management problem because it reduces the problem of bootstrapping trust to the problem of setting up (or in today's marketplace, selecting as a vendor) the appropriate CA functionality. All parties that trust the CA can be confident that the public keys that appear in certificates are valid.

a. Example: Use of Signer Certificates in Netscape Communicator (v4.05 & later)

Digital certificates already play a fundamental role in Internet-based cryptography systems. For example, consider the case of a secure Web transaction that takes place when a user visits a Web storefront to make a credit card purchase. When the user's browser accesses a secure page, a public key from the Web store has already been

delivered to the client browser in the form of an X.509 digital certificate. All this happens transparently to the browser user at the time the secure connection is set up.

The browser trusts the certificate because it is signed, and the browser trusts the signature because the signature can be verified. And why can it be verified? Because the signer's public key is already embedded in the browser software itself. To see this in the particular case of Netscape Communicator, begin by clicking on the "Security" icon on the main toolbar.

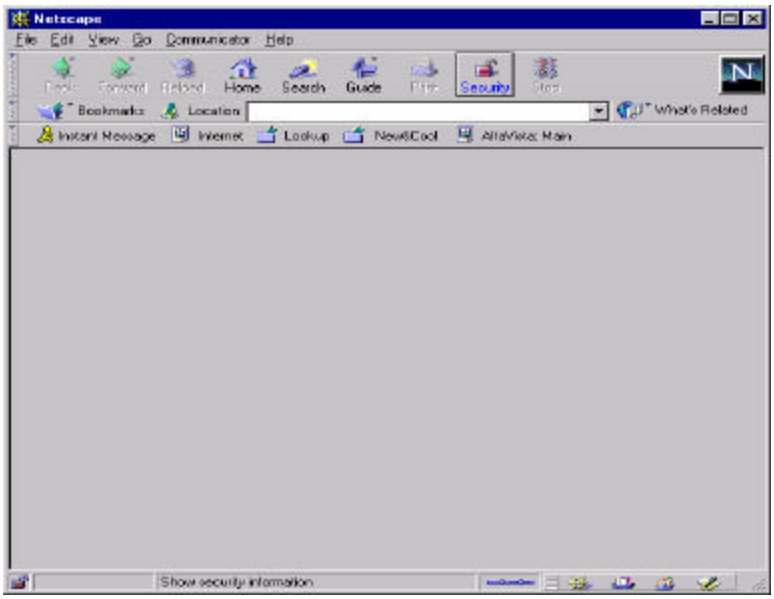


Figure 2: The "Security" Toolbar button in Netscape Communicator v4.0

Under "Certificates" choose "Signers," and scroll down the list. A window similar to the following should appear:

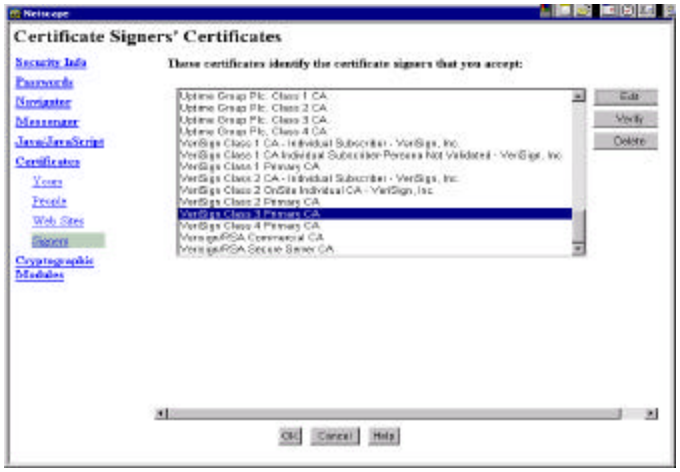


Figure 3: The list of certificate signers hard-coded to be trusted in Netscape Communicator

Next, select a particular certificate and click on the "Edit" button. A display similar to the following should appear:

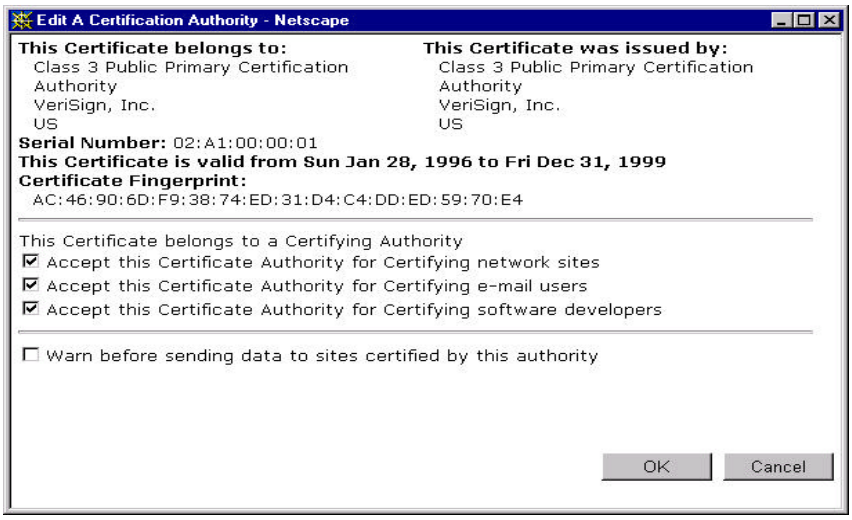


Figure 4: A VeriSign CA certificate embedded in Netscape Communicator

This is a representation of an X.509 digital certificate. Although X.509 certificates come in three different versions, version 3 certificates, such as the one displayed here, are the ones that are most commonly encountered in today's cryptography systems. Such a certificate consists of the following fields to identify the owner of the certificate as well as the trusted CA that issued the certificate:

version
serial number
signature algorithm ID
issuer name
validity period
subject (user) name
subject public-key information
issuer unique identifier (version 2 and 3 only)
subject unique identifier (version 2 and 3 only)
extensions (version 3 only)
digital signature for the above fields

Figure 5: The fields of a X.509 digital certificate

Although only a few of these fields are shown in Figure 4 (version, serial number, issuer name, and subject name) correspond to the display elements in Figure 4, these basic elements give an idea of what such a typical certificate contains.

A more detailed dump of raw certificate content looks like this:

```
Certificate:
  Data:
   Version: v3 (0x2)
   Serial Number: 8 (0x8)
   Signature Algorithm: PKCS #1 MD5 With RSA Encryption
   Issuer: CN=Root CA, OU=CIS, O=Structured Arts Computing Corporation, C=US
   Validity:
    Not Before: Fri Dec 5 18:39:01 1997
    Not After: Sat Dec 5 18:39:01 1998
   Subject: CN=Test User, OU=Test Org Unit, O=Test Organization, C=US
   Subject Public Key Info:
    Algorithm: PKCS #1 RSA Encryption
    Public Key:
     Modulus:
      00:c2:29:01:63:a1:fe:32:ae:0c:51:8d:e9:07:6b:02:fe:ec:
      6d:0e:cc:95:4b:dc:0a:4b:0b:31:a3:1a:e1:68:1f:d8:0b:b7:
      91:fb:f7:fd:bd:32:ba:76:01:45:e1:7f:8b:66:cd:7e:79:67:
      8d:48:30:2a:09:48:4c:9b:c7:98:d2:b3:1c:e9:54:2c:3c:0a:
      10:b0:76:ae:06:69:58:ac:e8:d8:4f:37:83:c3:f1:34:02:6d:
      9f:38:60:6f:5e:54:4f:71:c7:92:28:fb:0a:b3:44:f3:1a:a3:
      fe:99:f4:3f:d3:12:e2:f8:3b:03:65:33:88:9b:67:c7:de:88:
      23:90:2b
     Public Exponent: 65537 (0x10001)
   Extensions:
    Identifier: Certificate Type
     Critical: no
     Certified Usage:
      SSL Client
    Identifier: Authority Key Identifier
     Critical: no
     Key Identifier:
      a7:84:21:f4:50:0e:40:0f:53:f2:c5:d0:53:d5:47:56:b7:c5:
      5e:96
  Signature:
   Algorithm: PKCS #1 MD5 With RSA Encryption
   Signature:
    2d:76:3f:49:5b:53:3a:c5:02:06:a3:67:6d:d9:03:50:57:7f:de:a7:a9:
    cd:69:02:97:6f:66:6a:7f:95:ea:89:75:7a:fc:b0:26:81:fc:33:bb:60:
    e8:f7:73:77:37:f8:8a:04:3b:fc:c1:3e:42:40:3d:58:16:17:7e:47:35:
    1c:73:5a:ab:72:33:c3:f5:2b:c6:eb:b5:39:52:82:c6:3e:e1:38:c6:39:
    8b:ee:e3:9f:b3:b9:29:42:0d:11:a5:79:af:6d:3a:f8:a6:ba:d0:9c:55:
    48:0d:75:91:05:0b:47:67:98:32:f3:2d:2e:49:ed:22:ab:28:e8:d6:96:
    a1:9b
```

Figure 6: The fields of a X.509 digital certificate

In the next section, we describe how SSL digital certificates for Web servers apply cryptographic techniques to secure e-commerce Web sites.

IV. SSL Server Certificates

The practical means of implementing PKI and digital signatures are via Web server certificates that enable authentication and SSL encryption. SSL certificates form the basis of an Internet trust infrastructure by allowing Web sites to offer safe, secure information exchange to their customers. SSL server certificates satisfy the need for confidentiality, integrity, authentication, and nonrepudiation.

A. SSL Defined

Secure Sockets Layer (SSL), originally developed by Netscape Communications, is an information technology for securely transmitting information over the Internet. The SSL protocol has become the universal standard on the Web for authenticating Web sites to Web browser users, and for encrypting communications between browser users and Web servers.

Server certificates are available from Certificate Authorities (CAs) such as VeriSign—trustworthy, independent third parties that issue certificates to individuals, organizations, and Web sites. CAs use thorough verification methods to ensure that certificate users are who they claim to be before issuing them. CA's own self-signed SSL digital certificates are built into all major browsers and Web servers, including Netscape Communicator and Microsoft Internet Explorer, so that simply installing a digital certificate on a Web server enables SSL capabilities when communicating with Web browsers.

SSL server certificates fulfill two necessary functions to establish e-commerce trust:

- **SSL server authentication:** Server certificates allows users to confirm a Web server's identity. Web browsers automatically check that a server's certificate and public ID are valid and have been issued by a certificate authority (CA)—such as VeriSign— included in the list of trusted CAs built into browser software. SSL server authentication is vital for secure e-commerce transactions in which users, for example, are sending credit card numbers over the Web and first want to verify the receiving server's identity.

- **SSL encryption: SSL** server certificates establish a secure channel that enables all information sent between a user's Web browser and a Web server to be encrypted by the sending software and decrypted by the receiving software, protecting private information from interception over the Internet. In addition, all data sent over an encrypted SSL connection is protected with a mechanism for detecting tampering: that is, for automatically determining whether the data has been altered in transit. This means that users can confidently send private data, such as credit card numbers, to a Web site, trusting that SSL keeps it private and confidential.

B. How SSL Server Certificates Work

Server IDs take advantage of SSL to work seamlessly between Web sites and visitors' Web browsers. The SSL protocol uses a combination of asymmetric public key encryption and faster symmetric encryption.

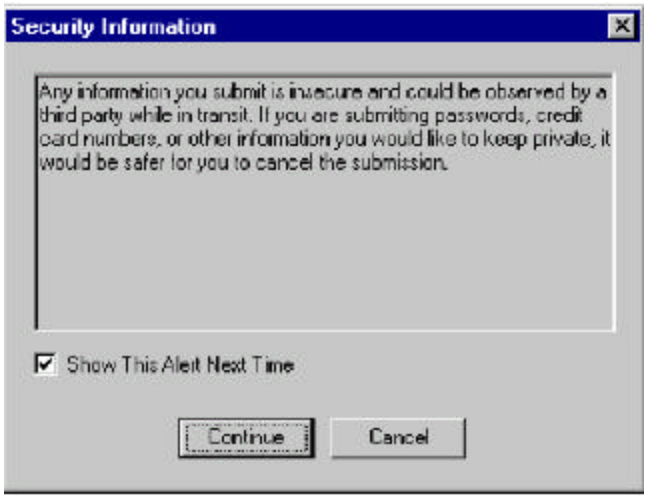
The process begins by establishing an SSL "handshake"—allowing the server to authenticate itself to the browser user, and then permitting the server and browser to cooperate in the creation of the symmetric keys used for encryption, decryption, and tamper detection:

1) A customer contacts a site and accesses a secured URL: a page secured by a Server ID (indicated by a URL that begins with "https:" instead of just "http:" or by a message from the browser). This might typically be an online order form collecting private information from the customer, such as address, phone number, and credit card number or other payment information.
2) The customer's browser automatically sends the server the browser's SSL version number, cipher settings, randomly generated data, and other information the server needs to communicate with the client using SSL.
3) The server responds, automatically sending the customer's browser the site's digital certificate, along with the server's SSL version number, cipher settings, etc.
4) The customer's browser examines the information contained in the server's certificate, and verifies that:
    a) The server certificate is valid and has a valid date.
    b) The CA that issued the server been signed by a trusted CA whose certificate is built into the browser
    c) The issuing CA's public key, built into the browser, validates the issuer's digital signature
    d) The domain name specified by the server certificate matches the server's actual domain name

    If the server cannot be authenticated, the user is warned that an encrypted, authenticated connection cannot be established.
5) If the server can be successfully authenticated, the customer's Web browser generates a unique "session key" to encrypt all communications with the site using asymmetric encryption.
6) The user's browser encrypts the session key itself with the site's public key so that only the site can read the session key, and sends it to the server.
7) The server decrypts the session key using its own private key.
8) The browser sends a message to the server informing it that future messages from the client will be encrypted with the session key.
9) The server then sends a message to the client informing it that future messages from the server will be encrypted with the session key.
10) An SSL-secured session is now established. SSL then uses symmetric encryption, (which is much faster than asymmetric PKI encryption) to encrypt and decrypt messages within the SSL-secured "pipeline."
11) Once the session is complete, the session key is eliminated.

It all takes only seconds and requires no action by the user.

The Netscape Navigator and the Microsoft Internet Explorer browsers have built-in security mechanisms to prevent users from unwittingly submitting their personal information over insecure channels. If a user tries to submit information to an unsecured site (a site without an SSL server certificate), the browsers will, by default, show a warning:



In contrast, if a user submits credit card or other information to a site with a valid server certificate and an SSL connection, the warning does not appear. The secure connection is seamless, but visitors can be sure that transactions with a site are secured by looking for the following cues:

- The URL in the browser window displays "https" at the beginning, instead of http.
- In Netscape Communicator, the padlock in the lower left corner of the Navigator window will be closed instead of open.
- In Internet Explorer, a padlock icon appears in the bar at the bottom of the IE window.

1. SSL Strengths: 40-bit and 128-bit SSL

SSL comes in two strengths, 40-bit and 128-bit, which refer to the length of the session key generated by every encrypted transaction. The longer the key, the more difficult it is to break the encryption code. 128-bit SSL encryption is the world's strongest: according to RSA Labs, it would take a trillion trillion years to crack using today's technology. 128-bit encryption is approximately 3×10^{26} stronger than 40-bit encryption.

Microsoft and Netscape offer two versions of their Web browsers, export and domestic, that enable different levels of encryption depending on the type of SSL server certificate with which the browser is communicating.

- **40-bit SSL server certificates** (such as VeriSign's Secure Server IDs) enable 40-bit SSL when communicating with export-version Netscape and Microsoft Internet Explorer browsers (used by most people in the U.S. and worldwide), and 128-bit SSL encryption when communicating with domestic-version Microsoft and Netscape browsers.
- **128-bit SSL server certificates** (such as VeriSign's Global Server IDs) enable 128-bit SSL encryption—the world's strongest—with both domestic and export versions of Microsoft® and Netscape® browsers.

In order to fully enable 128-bit encryption with a Global Server ID, it's important to generate the right kind of private key during the process of obtaining a Server ID. An important step in the process is generating a Certificate Signing Request within the Web server software. In generating a CSR, Web server administrators should be careful to select a 1024-bit private key, which enables the Global Server ID to establish 128-bit SSL encryption, rather than a 512-bit private key, which enables only 40-bit encryption.

Netscape users can follow these steps to see what level of encryption is protecting their transactions:

- Go to the secure Web page you want to check.
- Click the Security button in the Navigator's toolbar. The Security Info dialog box indicates whether the Web site uses encryption.
- If it does, click the Open Page Info button to display more information about the site's security features, including the type of encryption used.
- You can also check to see which level of SSL is activated on your Web server by following these steps:
- Using a 128-bit client, such as the domestic version of the Netscape Navigator, click on Options/Security Preferences.
- Under the enable SSL options, click on Configure for both SSL 2 and SSL 3. Make sure acceptance for the 40 and 56 bit encryption ciphers are turned off.
- Try to access the site. If it using less than 128 bit security, then you will receive an error in your browser window: "Netscape and this server cannot communicate securely because they have no common encryption methods."

IE users can find out a Web site's encryption level by following these steps:

- Go to the Web site you want to check.
- Right-click on the Web site's page and select Properties.
- Click the Certificates button.
- In the Fields box, select "Encryption type." The Details box shows you the level of encryption (40-bit or 128-bit. See the following section for more information about SSL encryption levels).

E-businesses may choose to simplify the process of certificate checking for site visitors by describing the security measures they have implemented in a Security and Privacy statement on their sites. Sites that use VeriSign Server IDs can also post the Secure Site Seal on their home page, security statement page, and purchase pages. The Seal is a widely recognized symbol of trust that enables site visitors to check certificates in real time from VeriSign with one click (see "VII. The VeriSign Advantage" below for more information about the Seal).

2. SGC and 128-bit Step-up

To ensure that strong 128-bit encryption protects e-commerce transactions for all users, businesses should install 128-bit IDs, such as VeriSign's Global Server IDs, on their servers. However, the export browsers that permit only 40-bit encryption with 40-bit SSL

server certificates will allow strong 128-bit encryption when interacting with 128-bit server certificates because these certificates are equipped with a special extension that enable "Server Gated Cryptography (SGC)" for Microsoft browsers and "International Step-Up" for Netscape browsers.

The extension enables 128-bit encryption with export-version browsers by prompting two "handshakes" when a user's browser accesses a page protected by a Global Server ID. When an export-version Netscape or Microsoft browser connects to the Web server, the browser initiates a connection with only a 40-bit cipher. When the server certificate is transferred, the browser verifies the certificate against its built-in list of approved CAs. Here, it recognized that the server certificate includes the SGC or International Step-Up extension, and then immediately renegotiates the SSL parameters for the connection to initiate an SSL session with a 128-bit cipher. In subsequent connections, the browser immediately uses the 128-bit cipher for full-strength encryption.

C. Securing Multiple Servers and Domains with SSL

As organizations and service providers enhance their Web sites and extranets with newer technology to reach larger audiences, server configurations have become increasingly complex. They must now accommodate:

- Redundant server backups that allow Web sites and extranets to maximize site performance by balancing traffic loads among multiple servers
- Organizations running multiple servers to support multiple site names
- Organizations running multiple servers to support a single site name
- Service providers using virtual and shared hosting configurations

But in complex, multiserver environments, SSL server certificates must be used carefully if they are to serve their purpose of reliably identifying sites and the businesses operating them to visitors and encrypt e-commerce transactions —establishing the trust that customers require before engaging in e-commerce.

When used properly in an e-commerce trust infrastructure equipped with multiple servers, SSL server certificates must still satisfy the three requirements of online trust:

1. Client applications, such as Web browsers, can verify that a site is protected by an SSL server certificate by matching the "common name" in a certificate to the domain name (such as www.verisign.com) that appears in the browser. (Certificates are easily accessible via Netscape and Microsoft browsers).
2. Users can also verify that the organization listed in the certificate has the right to use the domain name, and is the same as the entity with which the customer is communicating.
3. The private keys corresponding to the certificate, which enable the encryption of data sent via Web browsers, are protected from disclosure by the enterprise or ISP operating the server.

1. The Certificate Sharing Problem

VeriSign recommends that, to satisfy the requirements of Internet trust, one SSL server certificate be used to secure each domain name on every server in a multi-server environment, and that the corresponding private keys be generated from the hosting server.

Some enterprises or ISPs practice certificate sharing, or using a single SSL server certificate to secure multiple servers. Organizations use certificate sharing in order to secure back-up servers, ensure high-quality service on high-traffic sites by balancing traffic among several servers, or, in the case of ISPs and Web hosts, to provide inexpensive SSL protection to price-sensitive customers. However, as described in the following section, certificate-sharing configurations do not satisfy the fundamental requirements of Internet trust.

2. VeriSign Recommendations for Implementing SSL on Multiple Servers

Here are some common shared certificate configurations and VeriSign's recommendations for addressing them to most effectively reinforce an e-commerce trust infrastructure:

Fail-Safe Backup: Redundant servers, not used simultaneously
Certificate sharing is permissible. However, when the back-up server is not under the same control as the primary server, the private key cannot be adequately protected, and a separate certificate should be used for each server.

Load Balancing: Multiple sites with different common names on multiple servers
To prevent browsers from detecting that the URL of the site visited differs from the common name in the certificate, and to protect the security of private keys, a different certificate should be used for each server/domain name combination.

Load Balancing: Multiple sites with the same common name on multiple servers
Instead of jeopardizing private key functionality by copying the key for multiple servers, a different certificate should be used for each server. Each certificate may have the same common name and organizational name, but slightly different organizational unit values.

ISP Shared SSL: One certificate issued to an ISP's domain, used on multiple servers by multiple Web sites
This prevents site visitors from verifying that the site they are visiting is the same as the site protected by the certificate and listed in the certificate itself. Each site's server should have its own certificate. Or merchants must inform their customers that site encryption is provided by the ISP, not the merchant, and the ISP must guarantee the services of all the hosted companies whose sites use shared SSL.

Name-Based Virtual Hosting: An ISP or Web Host provides each hosted customer with a unique domain name, such as customername.isp.com.

If the same certificate is used for each domain name, browsers will indicate that the site domain name does not match the common name in the certificate. To solve this problem, a "wildcard" certificate of the form *.isp.com is required to properly serve the multi-hostname configuration without creating browser mismatch error messages. (VeriSign offers wildcard certificates on a case-by-case basis, and they are subject to certain additional licensing terms and conditions. For more information, please contact shared-ssl@verisign.com.)

For a complete explanation of VeriSign's solutions for securing multiple Web server and domain configurations, please see our white paper at http://www.verisign.com/rsc/wp/certshare/index.html .

Next, we examine the second key component of an Internet trust infrastructure: secure online payment management.

V. Online Payment Services

Once businesses have built a Web site and implemented SSL certificates to authenticate themselves to customers and encrypt communications and transactions, they must address another crucial component of an e-commerce infrastructure: enabling customers to easily pay for products and services online, and processing and managing those payments in conjunction with a complex network of financial institutions.

Today's fragmented Internet payment systems often connect online merchants to banks via privately operated, point-to-point payment networks. In 1998, for example, over 5 billion electronic payment transactions—originating from approximately 2 million merchant locations and representing over $250 billion in merchant dollar volume—were passed over leased lines and non-Internet interfaces to a single transaction processor (First Data Corporation).

This situation is rapidly changing. Internet commerce is entering an accelerated growth phase. IDC estimates worldwide e-commerce revenues will increase to $218 billion in 2000. Behind each of these Internet purchases is a payment transaction. However, traditional payment systems have proven to be ill equipped to manage the costs and complexity of transitioning and enabling transactions over the Internet. As a result, only a fraction of today's potentially automated e-commerce transactions are currently enabled for Internet payment. The situation is particularly acute in the B2B payments arena—today, most B2B systems stop short of enabling actual payment execution on the Web.

Demand is therefore high for a simpler, "Internet payment gateway" approach that provides easier Internet connectivity between buyers, sellers, and the financial networks that move money between them. A truly flexible Internet payment gateway must support multiple payment instruments, connect to all relevant back-office payment processors, and be packaged for easy integration into front-office Web applications. Ideally, the gateway should also offer uniform interfaces to payment functionality, permitting e-

businesses to deploy payment applications that can be easily switched between alternative financial instruments, institutions, and payment processors. And to form part of a complete e-commerce trust infrastructure, the gateway must assure fail-safe security for payment data as it passes from customer to Web site and through the back-end processing system.

Some merchants may build an Internet payment gateway themselves, or purchase a software-based solution. However, according to the Gartner Group, most e-merchants have transaction volumes that do not justify the expense of bringing the process in-house, and are opting to outsourced, ASP solutions.

A. The Internet Payment Processing System

Understanding how best to address the need for Internet payment gateway services requires first briefly examining the participants in an Internet payment processing system.

Participants in a typical online payment transaction include:

- **The customer**: typically, a holder of a payment card—such as a credit card or debit card—from an issuer.
- **The issuer**: a financial institution, such as a bank, that provides the customer with a payment card. The issuer is responsible for the cardholder's debt payment.
- **The merchant**: the person or organization that sells goods or services to the cardholder via a Web site. The merchant that accepts payment cards must have an Internet Merchant Account with an acquirer.
- **The acquirer**: a financial institution that establishes an account with a merchant and processes payment card authorizations and payments. The acquirer provides authorization to the merchant that a given card account is active and that the proposed purchase does not exceed the customer's credit limit. The acquirer also provides electronic transfer of payments to the merchant's account, and is then reimbursed by the issuer via the transfer of electronic funds over a payment network.
- **The payment gateway**: This function, operated by a third-party provider, processes merchant payments by providing an interface between the merchant and the acquirer's financial processing system.
- **The processor**: a large data center that processes credit card transactions and settles funds to merchants, connected to the merchant on behalf of an acquirer via a payment gateway.

The basic steps of an online payment transaction include the following:

1. The customer places an order online by selecting items from the merchant's Web site and sending the merchant a list. The merchant often replies with an order summary of the items, their price, a total, and an order number.
2. The customer sends the order to the merchant, including payment data. The payment information is usually encrypted by an SSL pipeline set up between the customer's Web browser and the merchant's Web server SSL certificate.
3. The merchant requests payment authorization from the payment gateway, which routes the request to banks and payment processors. Authorization is a request to

charge a cardholder, and must be settled for the cardholder's account to be charged. This ensures that the payment is approved by the issuer, and guarantees that the merchant will be paid.

4. The merchant confirms the order and supplies the goods or services to the customer.
5. The merchant requests payment, sending the request to the payment gateway, which handles the payment processing with the processor.
6. Transactions are settled, or routed by the acquiring bank to the merchant's acquiring bank for deposit.

B. VeriSign Payflow Payment Services

VeriSign Payflow Payment Services offers the most effective way to streamline the flow of all kinds of payments through this complex system—quickly, efficiently, and above all, securely. Payflow simplifies e-commerce by providing payment connectivity over the Internet between buyers, sellers, and financial networks. VeriSign uses a client server architecture to process transactions: the client is installed on the merchant's site and integrated with the merchant's e-commerce application. The client software establishes a secure link with the VeriSign processing server using an SSL connection to transmit encrypted transaction requests. The VeriSign server transmits the request over a private network to the appropriate financial processing network. When the authorization response is received via the financial processing network, the server returns the response to the merchant's client, which then completes the transaction by sending an acknowledgment to the server. Typical transactions occur within 3 seconds.

By partnering with VeriSign, merchants gain the ability to free themselves from point-to-point and difficult-to-integrate payment solutions, reaping the benefits of an integrated payment platform designed specifically for the Internet. Payflow supports all major consumer credit card, debit card, electronic check, purchase card, and Automated ClearingHouse (ACH) transactions. (ACH is a nationwide, wholesale electronic payment and collection system that serves as a method of transferring funds between banks via the Federal Reserve System.)

Its robust and open architecture has been designed to support both business-to-consumer (B2C) and business-to-business (B2B) payment applications. It provides the industry's highest performance and reliability and is a highly scalable outsourced solution that can easily grow to hundreds of millions of transactions per month. VeriSign Payflow has proven to be considerably faster, more reliable and scalable than any other competing solution. Using VeriSign Payflow, a merchant can connect to most banks, transaction services, or forms of payment without worrying about the underlying technology. Customers can pay with a variety of financial instruments, including checking accounts, savings accounts, and credit cards, quickly and simply.

VeriSign Payflow hides the complexity of payment

Competitive design advantages of the VeriSign Payflow service include:

- Open connectivity with almost all bank processors and payment types through unified interfaces
- Pre-integration with the most popular e-commerce applications and forthcoming payment-enabled Internet appliances such as Personal Digital Assistants (PDAs)
- Continuous maintenance of a TCP/IP network connection throughout each transaction until it either successfully completes or times out. Unlike most competing solutions, VeriSign Payflow's payment connection both enables a faster response times (averaging 2.2 seconds) and—through confirmation of transaction completion—elimination of uncertainty of transaction status.
- High availability that exceeds 99.99 percent with dynamic load balancing and failover between all servers
- An XML integration layer both on the server side for ease of integration with additional services (such as fraud screening), and on the merchant side for ease of integration into back office applications
- A Software Development Kit (SDK) allowing for more advanced custom integration into e-commerce applications

On the merchant side, VeriSign's payment connectivity technology works with all major shopping carts and e-commerce systems. Merchants can select the shopping cart system and storefront system that best suits their needs and be confident that VeriSign can make the connections.

To the Internet merchant, VeriSign offers:

- **Lower connectivity cost**: Connecting to the payment networks over the Internet through VeriSign costs less to set up and maintain than leased lines or modem connections.

- **Better connection quality**: VeriSign manages high-bandwidth, fault-tolerant network connections to the processing networks.

- **More payment options**: Merchants can add new payment types without having to install new software.

- **Increased flexibility**: Merchants can switch banking relationships and continue to use the same installed software to process payments with the new bank.

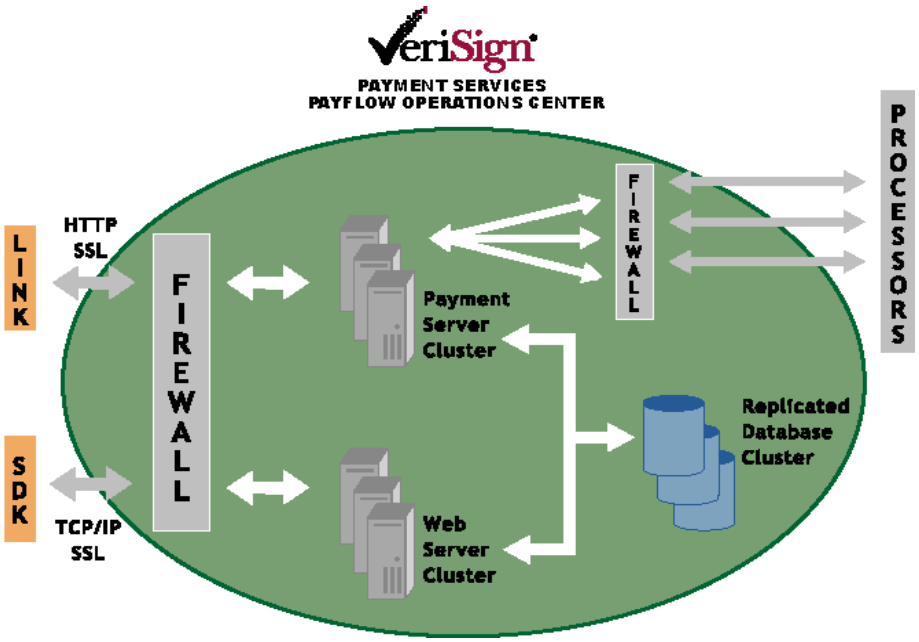
On the processor side, VeriSign works with all of the major processing and bank networks. Again, the merchant just selects an appropriate shopping cart, e-commerce package, or VeriSign-provided software development kit and knows that VeriSign will make the necessary connections to the transaction processing services.

1. How Payment Processing Services Work

At the application level, VeriSign's payment processing services can be accessed in three ways:

- **Payflow-enabled e-commerce applications:** Many off-the-shelf e-commerce applications are pre-enabled to use VeriSign's Payflow payment processing, giving merchants a complete solution that can be used out-of-the-box. VeriSign's broad third-party support and superior payment connectivity enables merchants to independently choose the best e-commerce application and the best payment processor for their business needs.
- **Payflow Link:** A hosted order form service that makes payment processing as simple as adding Web links to a merchant's Web site. See "VI. VeriSign E-Commerce Trust Infrastructure Solutions" below for more on Payflow Link.
- **Payflow Pro SDK:** A software development kit that gives merchants direct access to VeriSign's Payflow payment processing API via a "thin client" network service. See "VI. VeriSign E-Commerce Trust Infrastructure Solutions" below for more on Payflow Pro and the Payflow Pro SDK.

Through VeriSign's acquiring bank partners, merchants are also able to apply for merchant bank accounts during the registration process. In all cases, online registration and account management enables merchants to be up and running in minutes.



A look inside the VeriSign Payflow payment processing operations center

C. Payment Processing Backbone

The VeriSign payment client is a Secure Sockets Layer (SSL)-enabled communications agent that uses routing parameter inputs to locate and establish communications with a VeriSign transaction server. After a secure communication channel has been established, transaction data is passed to the VeriSign payment infrastructure for processing. VeriSign transaction communications have been designed to minimize message-handling errors by ensuring an uninterrupted, TCP-level communication stream between the client and the server. The VeriSign architecture has the highest performance in the industry. The average transaction response time is 2.2 seconds.

The following sequence of messages illustrates the communication stream during a typical transaction from a VeriSign-enabled client to the VeriSign Payment Services operations center.

- The client opens an SSL connection to a server and sends all transaction data.
- The server processes the transaction, sends a response back to the client.
- The client sends an acknowledgment to the server indicating that the response was successfully received.
- The connection is closed.

VeriSign Payment Services incorporate the following features to reinforce an e-commerce trust infrastructure:

1. Connectivity

VeriSign provides connectivity to more payment processors and supports more payment types than any other online payment solution provider.

PROCESSOR	PAYMENT TYPES	AVAILABE
First Data Corporation 'Nashville'	Credit Cards Level II Purchase Cards	Now
Paymentech	Credit Cards Level II Purchase Cards	Now
TeleCheck	Electronic Check Verification and Guarantee	Now
Wells Fargo Norwest	ACH	Now
NOVA	Credit Cards Level II Purchase Cards	Now
VITAL	Credit Cards Level II Purchase Cards	Now
EDS Aurora	Credit Cards Level II Purchase Cards	Now
First Data Corporation 'South'	Credit Cards Level II & III Purchase Cards	Now

2. Scalability

VeriSign's transaction processing power can grow quickly, providing throughput and reliability as the transaction load grows from millions to hundreds of millions of transactions per month and beyond. VeriSign combines custom-developed, high-throughput server software with a load-balancing network architecture to deliver a solid payment Internet service explicitly intended for today's quickly growing e-commerce community.

3. Maximum Throughput

While many payment solutions have been implemented as "add-ons" to existing Web server platforms, VeriSign has built server software specifically designed for payment transactions. This provides significant advantages in three areas:

- **Internal Resources**: VeriSign server software incorporates a sophisticated threading model designed specifically to deliver maximum throughput for payment transactions. Signal and timer logic for handling payment transaction exceptions and errors is built into the server's kernel. File system access and logging are optimized for payment transactions.
- **Database Resources**: VeriSign uses state-of-the-art DBMS technology to store and log the transaction activity. It has kernel-level control of database logins and

resources, which provides a level of performance tuning and error recovery that is not available to payment systems that are based on Web servers.

- **Network Resources**: Because the VeriSign server is "payment-aware" at its core, it can manage the complex dynamics of communicating with card processing networks. Effective load balancing is achieved both in the local processes and in coordination with peer servers to implement an array-wide throughput optimization strategy—in other words, VeriSign servers perform load balancing both internally and in relation to other transaction servers in their cluster. As transaction loads grow for a cluster, this advantage becomes increasingly important.

4. Load Balancing and Linear Growth

Highly available payment processing requires that individual transaction servers be both extremely reliable and efficient. To provide true scalability, it must be practical to add new server capacity on demand. VeriSign services are delivered through clusters:

- **Payment Server Cluster**: These machines run the VeriSign Payment Server and manage the processing of inbound transaction requests to the processing networks.
- **Web Server Cluster**: These servers provide Web application functionality associated with the payment services. VeriSign's merchant reporting and virtual terminal systems are provided here.
- **Replicated Database Cluster**: These machines host the database servers. This cluster is broken up into write-biased, read-biased, and replicator machines. Write-biased servers are configured for maximum throughput for new transactions and are used by default by the transaction servers. Read-biased servers are configured for maximum speed on queries and reports and are used by default by the Web servers. Replication machines manage the synchronization of the data between all of the local database machines in the cluster as well as other cluster and backup/archive services.

VeriSign provides quality service for immense numbers of transactions by ensuring that it has provided adequate service clusters and has sufficient bandwidth on the front side (Internet) and back side (banking networks) to accommodate the load.

VeriSign's current production cluster supports a nominal load of two million transactions per day. In practice, capacity is added well before it is needed. As a general rule, when a cluster reaches a nominal load of 30% of capacity or when there are frequent spikes above 50% of capacity, either new capacity is added to the cluster or a new cluster is added to the service.

5. Reliability

In addition to load balancing, VeriSign's server clusters also provide failure protection. When a cluster suffers a server failure, the transaction load is seamlessly redistributed to the remaining servers in the cluster. Hardware redundancy is also provided within each server for every important subsystem.

6. Security

One of VeriSign's fundamental design considerations is, of course, security. The hardware, software, and physical plant developed and used by VeriSign services are carefully coordinated with an aggressive set of best practices to provide maximum protection and integrity at the transport, system, and physical levels.

Transport Security

Transport security provides protects transaction messages between the VeriSign client and server. Most transactions sent from the VeriSign client to VeriSign's payment servers are sent over the Internet—a public network. To ensure that the contents of transactions are private and that they cannot be altered or embellished in any way, VeriSign uses the Secure Sockets Layer (SSL) protocol for all communications between clients and servers. Similarly, Web access to every VeriSign Web site that provides sensitive data is available only under the HTTPS protocol, which is the same SSL protocol used by the client, running on top of HTTP.

VeriSign has licensed RSA Security, Inc.'s cryptographic tools. These tools are the de facto standard for highly secure communications over the Internet and are widely regarded as the best available platform on which to build a secure client/server system. This means that transaction data sent by the merchant to the VeriSign server can be read and used only by the VeriSign server.

Additionally, VeriSign offers merchants the opportunity to identify a set of IP addresses or subnets that constitute valid transaction sources for a given merchant. This means that in addition to the protection afforded by SSL message encryption, the merchant can specify a range of IP addresses using a string (for example, 192.32.4.18-20 or 192.4.22.*) This specifies the valid IP addresses for the VeriSign payment server. Transactions that originate from unregistered IP addresses are logged as suspicious behavior for VeriSign's network monitoring tools to investigate. This allows the merchant to further validate and protect the transaction stream to the VeriSign service.

System Security

VeriSign payment services are protected by firewall systems based on an extremely conservative access strategy: VeriSign's payment services are isolated from all other services. VeriSign permits communication with the VeriSign payment server or secured Web servers only through SSL (port 443.) This means there is no backdoor access for email, FTP, DNS, ICMP, and so on, which are all security risks. The only data that can enter is SSL traffic. All access requires user name and password, IP address validation, or X.509 client authentication.

The VeriSign service is also protected on the "back side"–its array of network connections to the processing networks–by firewall systems that ensure that only authorized traffic from authorized sources gets through to VeriSign's payment servers.

Inside the server array, a layering strategy further isolates repositories that contain sensitive information. Best-of-breed intruder detection systems and network monitoring

tools are manned on a 24x7 basis, providing instant notification of suspicious or unauthorized access, as well as automatic countermeasures and remedies.

Physical Security

VeriSign's measures for physically protecting its Payment Services include 24x7 card key customer access to data centers, 24x7 video surveillance and recording of the premises by security personnel, and 24x7 on-site security personnel

7. XML

In cooperation with selected e-commerce partners and industry standards bodies, VeriSign has built an XML integration and automation layer into its payment infrastructure. This layer provides uniform XML access to all payment-related services including payment execution, registration, and reporting.

XMLPay

XMLPay is a VeriSign Payment Services specification that defines a set of XML document types for payment transactions and XML digital receipts. Although XMLPay loosely follows level 3 purchase card data formats, it supports a variety of payment instruments beyond just purchase cards. XMLPay is compliant with the joint IETF/W3C working group specification for digitally signed XML.

XMLRegister

Turning on a business for VeriSign PayFlow is a moderately complex process that involves the manual intervention of several parties, including not only the merchant and VeriSign Payment Services itself but also the merchant's acquiring bank and a payment processor to move money between buyer and seller banks. Both resellers and emerging B2B marketplaces are increasingly demanding more automated access to the process of enabling online merchant payment accounts. In response, VeriSign is developing XMLRegister, a specification defining data formats and processing infrastructure supporting the automation of VeriSign Payment Services merchant registrations.

Without XMLRegister, merchants typically must register one at a time for VeriSign Payment Services. With XMLRegister, formatted XML documents may be submitted programmatically over a secure transport to a registration server. The registration server supports methods for a single or group merchant registration. Each registration element may be for a new registration or update of an existing account. Because business rules and the information needed to complete a registration vary among processors and acquirers, an XMLRegister document does not attempt to enforce business rules related to a registration. It merely transports data across the wire for processing by the registration server whose job is to enforce such rules and report non-compliance.

XMLReport

XMLReport specifies data used in payment transaction reports. Resellers or merchants submit XMLReport document when they need reports on their transactions.
In summary, today's widespread adoption of XML is leading to three significant developments in the payments industry:

- **Extensibility**: XML enables easy update and extension of existing services to quickly add altogether new services to existing applications.
- **Automation**: Currently, merchants can download a set of preset reports from the VeriSign Payflow Manager Web site, but have limited flexibility in what can be queried, or how the results are returned. XMLReport provides an automation language for merchant reporting. Complex queries and result formatting instructions can be communicated to the VeriSign service in a straightforward manner.
- **Interoperability**: XML is quickly gaining momentum as the *lingua franca* of system interchange. Via its three XML specifications, VeriSign Payment Services will publish an XML-based vocabulary for its services. By collaborating with partners, this vocabulary will be consistent with emerging industry-standard vocabularies, as well as those of the partners.

The VeriSign Payflow client continues to provide a high-level API for developers who don't want to switch to XML. The XML layer is therefore strictly optional, and is independently accessible when it is used to communicate requests and responses from VeriSign Payflow servers.

VI. VeriSign E-Commerce Trust Infrastructure Solutions

VeriSign offers a complete range of products and services to help businesses implement an end-to-end trust infrastructure for e-commerce. VeriSign's server certificates, or Server IDs, are available in both 40-bit and 128-bit SSL as part of Secure Site services. VeriSign Payflow Link and Payflow Pro online payment services enable businesses to easily accept, manage, and process payments electronically. VeriSign's Commerce Site services combine SSL Server IDs, Payflow services, and other value-added features to form a complete e-commerce infrastructure. And for large enterprises operating multiple servers, OnSite for Server IDs simplifies the process of issuing managing large numbers of Server IDs.

A. VeriSign Commerce Site and Secure Site Solutions

VeriSign provides SSL Server IDs in two encryption strengths:

- **VeriSign's 128-bit SSL (Global Server) IDs** enable the world's strongest SSL encryption with both domestic and export versions of Microsoft® and Netscape® browsers. 128-bit SSL Global Server IDs are the standard for large-scale online merchants, banks, brokerages, health care organizations, and insurance companies worldwide. U.S. Government regulations determine who can implement the powerful encryption of 128-bit SSL, though 128-bit IDs are now available to nearly every company worldwide (see www.verisign.com/server/rsc/faq.html#qualify2 for details).
- **40-bit SSL (Secure Server) IDs** are ideal for security-sensitive intranets, extranets, and Web sites.

VeriSign 128-bit SSL and 40-bit SSL Server IDs are available as part of VeriSign's site trust solutions.

- **Commerce Site Services**, exclusively from VeriSign, are complete, integrated solutions that are ideal for e-merchants and online stores.
  - **Commerce Site** includes a 40-bit SSL (Secure Server) ID and VeriSign Payflow Pro online payment management service (see below for more information), plus an array of additional value-added services.
  - **Commerce Site Pro** includes a 128-bit SSL (Global Server) ID, VeriSign Payflow Pro, and value-added services.

- **Secure Site Services** are best for intranets, extranets, and Web sites that require the leading SSL certificates and Web site services.
  - **Secure Site** includes a 40-bit SSL (Secure Server) ID, plus additional value added services.
  - **Secure Site Pro** includes a 128-bit SSL (Global Server) ID and value–added services.

The value-added services included with Secure Site and Commerce Site Services include the VeriSign Secure Site Seal.

The Seal is designed for display on Web sites as a symbol of security and trust, encouraging customers to confidently provide credit card numbers and other sensitive information. The Secure Site Seal is sent automatically to the technical contact businesses provide as part of the Secure Site or Commerce Site enrollment and purchasing process, 24 hours after the Server ID is issued.

When the Seal is posted on a Web site's home page, security/privacy policy page, or transaction pages, businesses can connect it to their Server ID. When visitors click on the Seal, they instantly link to a dynamic pop-up screen of information about the Server ID, assuring them that transactions with the site are encrypted by SSL, and allowing them to verify the site's identity and check the ID status in real time.

Secure Site and Commerce Site solutions also include up to $250,000 of NetSure protection, an extended warranty program that protects e-businesses against economic loss resulting from the theft, corruption, impersonation, or loss of use of a server certificate.

For a complete description of the additional features included with Secure Site and Commerce Site solutions, see http://www.verisign.com/site/index.html.

1. How to Enroll for Commerce Site and Secure Site Solutions

Businesses can try VeriSign's 40-bit SSL Secure Server ID for free. The trial Server ID can be applied for at http://www.verisign.com/server/trial/index.html now.

Businesses can purchase a one-year full-service Secure Server ID as part of VeriSign's Secure Site or Commerce Site Services by visiting http://www.verisign.com/server. The application process takes about 15 minutes. In one to three days, after VeriSign has verified credentials, it delivers your Secure Server ID via e-mail.

The U.S. Department of Commerce requires that companies qualify before buying the 128-bit SSL encryption power of Global Server IDs, included with Secure Site Pro and Commerce Site Pro Services. All companies within the United States are eligible for Global Server IDs. The U.S. Government determines the categories of companies that can implement 128-bit SSL encryption technology outside the U.S. and across U.S. borders. New regulations make Global Server IDs available to a wider group of customers than ever before: any company or organization around the world may purchase a Global Server ID, with the following exceptions: persons listed on the U.S. Government's Denied Person's List, and customers located in the following countries: Afghanistan (Taliban-controlled areas), Cuba, Iran, Iraq, Libya, North Korea, Serbia, Sudan, and Syria.

Before beginning VeriSign's online enrollment, businesses should check to make sure they are ready to proceed by following these steps:

- **Install server software**—Nearly all brands support VeriSign Secure Server IDs. The server on which the 128-bit Global Server ID can run server software from any non-U.S. software vendor, or software from a U.S. software vendor properly classified by the U.S. Department of Commerce, including:
    - Apache-SSL
    - BEA WebLogic
    - C2Net Apache Stronghold<
    - Compaq/Tandem iTP Webserver
    - Covalent Raven
    - Hewlett Packard Virtual Vault (with Netscape Enterprise)
    - IBM http Server/Webphone 1.3.3.1 and 1.3.6
    - Lotus Domino 4.6.2 and later
    - Microsoft IIS 3.0 and later
    - Mod-SSL
    - Nanoteq Netseq server
    - Netscape Suite Spot servers, 3.0 or later, including Netscape
    - Enterprise 3.0+ and Netscape Proxy Server 3.0 or later, 2.0
    - O'Reilly WebSite Pro v.2.5 and up

- Red Hat Professional 6.1

- Register domain name—If you haven't already, register your URL at http://www.networksolutions.com.
- Confirm firewall configuration —Secure Server ID enrollment requires that you can make both HTTP and HTTPS connections to VeriSign's Web site.
- Prepare payment—You can pay with a purchase order, check, wire transfer, or an American Express, Visa, Mastercard, or Discover card.
- Review legal agreement —In the process of enrolling, you will need to sign the VeriSign Secure Server Subscriber Agreement. To review it in advance, see http://www.verisign.com/repository/SUBAGR.html
- Gather proof of right documents —Before issuing your Secure Server ID, VeriSign must confirm that your company is legitimate and is registered with the proper government authorities. If you have a Dun & Bradstreet DUNS number, simply supply your number. International DUNS numbers must be in the Dun & Bradstreet database for at least two months before VeriSign can verify the information. If you do not have a DUNS number, either go to http://www.dnb.com and apply for one, or submit a hard copy of at least one of the following filed documents for your company: articles of incorporation, partnership papers, business license, or fictitious business license. All documents must be in English.

To complete your Server ID enrollment, please visit http://www.verisign.com/server. There you will be instructed to complete the following steps.

1. Generate Certificate Signing Request

Follow the instructions in your server software manual, or online at http://digitalid.verisign.com/server/enrollStep3.htm, to create a Certificate Signing Request (CSR) and a key pair. After the server software creates the two files, make backup copies of them on a floppy disk, and store the disk in a secure location. This is important: If your private key is lost, VeriSign will not be able to recover it for you.

2. Submit the Certificate Signing Request (CSR) to VeriSign

Open the CSR file in a text editor, such as WordPad, NotePad, or Textpad. Do not use a word processing application such as Microsoft Word or Adobe FrameMaker.
Select the text in the CSR, beginning with and including:

—-BEGIN NEW CERTIFICATE REQUEST—-
and ending with
—-END NEW CERTIFICATE REQUEST—-

Copy and paste the CSR into the VeriSign online enrollment form for the trial or the one-year subscription. Click the Submit button.

3. Complete application

Fill out the online application form with information about your company and contacts. The technical contact must be authorized to run and maintain your secure Web server and

must be employed by your organization. If you access the Web through an Internet Service Provider (ISP), the ISP may complete the CSR for you and serve as the technical contact, and you can then enroll. If your ISP does not offer VeriSign IDs, refer it to www.verisign.com/isp/index.html for information about VeriSign's Secure Site ISP Program. The organizational contact must be authorized to make binding agreements, such as the Secure Server Service Agreement, and must be employed by your organization. It is best to select a different person from the technical contact. The billing contact will receive invoices. This can be the same person as the technical or organizational contact.

4. Authentication takes 1-3 days

Within a few hours of receiving your application, VeriSign will send a confirming e-mail to your technical and organizational contacts. The e-mail will include a URL where you can check the status of your application, as well as a Personal Identification Number (PIN) you will need to view the status. If the information you submitted is complete, your technical contact and organizational contact will receive your Server ID by e-mail in 1–3 working days.

5. Install your Server ID

When you receive your Server ID, make a backup copy of it and store it on a labeled floppy disk, noting the date you received it. Store the floppy disk in a secure place. To install your Server ID, follow the instructions in your server software documentation for digital certificates.

6. Enable SSL on your server

Consult your server software manual to enable SSL. The process should take approximately five minutes.

7. Post the Secure Site Seal on all your secure pages

You should receive a file of the Seal, complete with instructions on how to install it, via e-mail shortly after completing the enrollment process. You can also find downloadable Seal files and instructions at http://www.verisign.com/server/prg/seal/install.html NOTE: SSL imposes some performance overhead. Therefore, most server software applications allow you to apply SSL selectively to Web pages that require encryption, such as payment pages. There is no benefit from applying SSL to product information pages, for example.

B. Payflow Link and Payflow Pro

VeriSign offers two Payment Services that let e-commerce businesses securely accept and process credit card, debit card, purchase card, and electronic check payments on the Internet:

1. VeriSign Payflow Link

Payflow Link provides a fast, easy-to-use solution that enables merchants to connect their customers via SSL-secured HTTP to a secure VeriSign-hosted order form to automate order acceptance, authorization, processing, and transaction management.

Payflow Link allows merchants to connect to VeriSign using simple Web links

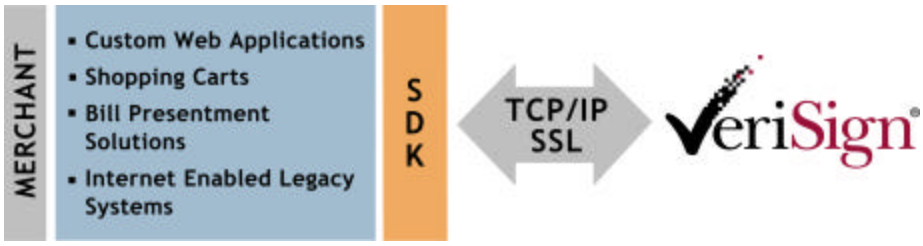
To use Payflow Link, merchants simply add a Web link to the appropriate Web pages at their site. When the customer clicks this link, he or she is brought to a secure order form that is hosted by VeriSign. Transaction details that are encoded in the link are used to initialize the form. This includes SKU data, order amount, tax amount, and other order-specific parameters. At the Payflow Link order form, the consumer enters the required payment information and submits the form to execute the order. When orders are submitted, the merchant is notified via email. Merchants fetch the specifics of new orders from the VeriSign Payflow Manager merchant Web site (see more information on Payflow Manager below).

Targeting the business-to-consumer marketplace, Payflow Link provides an inexpensive payment solution for any merchant needing the ability to quickly and efficiently process a variety of payment types. Payflow Link is intended for use by merchants who process up to 1,000 transactions per month. It is especially easy to implement and affordable, with a low setup cost and flat-fee billing. There is no long-term obligation.

2. Payflow Pro

VeriSign Payflow Pro is the most robust, versatile solution for online payment processing—ideal for large-scale e-commerce merchants that require peak performance and complete customizability. Payflow Pro is included with Commerce Site and Commerce Site Pro e-commerce solutions and is available separately as a downloadable Software Development Kit (SDK). It also comes pre-integrated with most shopping carts and e-commerce platforms.

Targeting the business-to-business market and enterprise environments requiring discrete control over payment functionality, Payflow Pro gives merchants direct access to the Payflow payment processing API via a “thin client” network service. The Payflow Pro SDK client software, which is installed on the merchant’s system, is a small (400k footprint) messaging agent that uses SSL and X.509 digital certificate technology to securely communicate with VeriSign’s payment servers.



Payflow Pro SDK gives merchants more control via a direct TCP/IP connection to the payment gateway and a flexible Software Development Kit (SDK)

To use Payflow Pro SDK, merchants pass payment transaction data to the client through a set name/value pairs. Here is an example of encoded payment transaction data:

TRXTYPE=S&TENDER=C&USER=userid&PWD=password&
ACCT=5499740000000016&EXPDATE=1299&AMT=1.00

The Payflow client's only job is to securely pass the payment transaction data to VeriSign's payment servers for processing. The Payflow client does not contain any payment-specific logic. This means that VeriSign is able to introduce new services or transaction types at any time, without upgrading the Payflow client software. Merchants can take advantage of a new service by simply adding the new parameter values it requires to their transaction requests.

Payflow Pro SDK provides support through a single client interface for the following payment types:

- Credit cards
- AmEx purchase card
- Purchase cards, Level II & III
- ACH transfer
- Electronic Check Verification and Guarantee

As with the Payflow Link service, Payflow Pro enables merchants to cost-effectively process high volumes of transactions under a flat-fee pricing schedule. Payflow Pro SDK is intended for merchants who process more than 1,000 transactions per month. It is robust and scalable up to hundreds of millions of transactions.

3. How to Purchase Payflow Link and Payflow Pro

At http://www.verisign.com/payment/seetrybuy.html, companies can register and obtain a username and password that will enable them to use and test VeriSign's Payflow and/or download Payflow Pro.

Business can purchase and download Payflow Link or Payflow Pro from http://www.verisign.com/payment/buyit.html; and can then begin using the service after

opening an activating an Internet Merchant Account from an acquiring bank or financial institution.

C. OnSite for Server IDs

Because managing the lifecycles of Server IDs can be challenging for companies with multiple servers spread across multiple divisions and locations, many businesses need an easy way to control the issuing, renewing, and revoking of IDs, and managing the access privileges associated with each ID.

VeriSign OnSite for Server IDs is ideal for companies that need to deploy Server IDs for 10 or more servers—for intranets, extranets, or up to four of a company's domain names ("www.verisign.com," for example). OnSite makes organizations their own "Certificate Authority (CA)," allowing enterprises to issue Server IDs in minutes to dozens or even hundreds of servers with fast, easy-to-use, Web-based tools for issuing server certificates– without the need for extra hardware, software, or dedicated personnel. Businesses can appoint one or more individuals to serve as OnSite administrators, with full authority to approve, renew, reject, and administer certificates, while VeriSign handles all the back-end services necessary to maintain and scale the CA to meet Internet trust needs.

OnSite for Server IDs offer e-businesses the following benefits:

- **Convenient, one-step purchasing:** OnSite for Server IDs lets enterprises take advantage of a single, unified enrollment process, plus volume discounts based on the number of Server IDs needed. Businesses need to complete only one purchase order a year for all its Server IDs.
- **Easy to set up and configure:** Enterprises can issue Server IDs quickly and manage them easily via the intuitive, Web-based OnSite interface. VeriSign supplies the cryptographic hardware, configuration wizards, enrollment Web templates, and installation guides.
- **Cost-effective:** OnSite eliminates the need to invest in the expensive hardware, software, or overhead necessary to build and maintain a server certificate system from the ground up.
- **Fast and simple to use:** OnSite administrators can issue certificates within minutes of receiving a request. VeriSign maintains the back-end infrastructure, including high-speed servers, telecommunications lines, data storage and back-up, disaster recovery, and 24X7 customer service.
- **Efficient, centralized ID management:** Enterprises can secure and manage multiple servers throughout their organization's domain, and easily renew IDs or buy additional IDs.
- **Flexible ID bundles:** Server IDs are available via OnSite in bundles of 10, 25, 50, 100, or more, based on businesses' needs.

1. How to Purchase OnSite for Server IDs

To talk to a VeriSign Sales Representative about purchasing VeriSign OnSite for Server IDs, businesses should call 1-650-429-5115. Businesses can also obtain more information by completing the form at http://www.verisign.com/onsite/server/form.html .

VII. The VeriSign Advantage

VeriSign's Server IDs and e-commerce trust services have earned the trust of businesses worldwide, including virtually all of the Fortune 500 companies on the Web and all of the top 40 e-commerce sites. To date, VeriSign, the world's leading CA, has issued more than 400,000 Server IDs.

A Server ID from VeriSign provides the ultimate in credibility for online businesses. VeriSign's rigorous authentication practices set the industry standard: VeriSign documents its carefully crafted and time-proven practices and procedures in a Certificate Practices Statement. And VeriSign annually undergoes an extensive SAS 70 Type II audit by KPMG. (The Statement of Auditing Standard 70, SAS 70, was established by the American Institute of Certified Public Accountants to certify trusted practices.) Employees responsible for dealing with certificates undergo complete background checks and thorough training.

VeriSign has achieved its unsurpassed reputation as a trusted third party by paying as careful attention to physical security as electronic security. For example, the company's 22,000-square-foot plant where keys are issued has five tiers of security, the last three requiring fingerprint identification.

VeriSign's rigorous authentication practices, leading-edge cryptographic techniques, and ultra-secure facilities are designed to maximize confidence in our services. These practices, technology, and infrastructure are the foundation for its e-commerce infrastructure services.

VIII. For More Information

- More about VeriSign's e-commerce trust infrastructure services is available on the VeriSign Web site at http://www.verisign.com/.
- A library of white papers, case studies, and other materials can be found at http://www.verisign.com/enterprise/library/index.html.
- For a free trial 40-bit Secure Server ID, go to http://www.verisign.com/server/trial/index.html.
- To purchase a VeriSign Commerce Site or Secure Site service, go to http://www.verisign.com/site/index.html, or contact a VeriSign Sales Representative at 650-429-5112.
- For more information about the OnSite for Server IDs service, see http://www.verisign.com/server/prd/m/index.html, or contact a VeriSign Sales Representative at 1-650-429-5115.
- Learn more about VeriSign Payment Service at https://www.verisign.com/payment/index.html.

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