VeriSign®
The Value of Trust℠

Digital ID

A Brief Overview

CONTENTS

What is a Digital ID?

A Digital ID, sometimes called a digital certificate, is a file on your computer that identifies who you are. Some software applications use this file to prove your identity to another person or computer. Here are two common examples:

- When you bank online, your bank must be sure that you are the correct person to get account information. Like a driver's license or passport, a Digitial ID confirms your identity to the online bank.
- When you send important e-mail to someone, your e-mail application can use your Digital ID to "digitally" sign the e-mail message. A digital signature does two things: it lets the recipient know the e-mail is from you, and it tells them the e-mail was not tampered with from the time you sent it to the time they received it.

A Digital ID typically contains the following information:

- Your public key (for more information see What is a Digital ID key pair?)
- Your name and e-mail address
- Expiration date of the public key
- Name of the company (the Certification Authority (CA)) who issued your Digital ID
- Serial number of the Digital ID
- .Digital signature of the CA

What can I do with a Digital ID?

Software applications, networks, and computers can use your Digital ID in several ways:

- *Encryption* (or data scrambling) is a way of protecting information before sending it from one computer to another. Typically e-mail applications use the Digital ID that belongs to the person receiving the encrypted e-mail message. For you to send someone encrypted messages, you need their public key. See the section on secure e-mail for more information.
- *Client authentication* is the term used to describe how you (the client) prove your identity to somone else or to a computer. For example, online banks need to make sure you are the correct customer for a given bank account. To prove your identity at the bank in person, you usually present your driver's license or passport. When online, your software application presents your Digital ID. Some Web sites might request that you present your ID before letting you view Web pages that are hidden from others, such as pages for people who subscribe to a particular service on the Web site.
- A *Digital signature,* like a hand-written signature, shows that a person created or otherwise agreed to the document containing the signature. A digital signature actually provides a greater degree of security than a handwritten signature because the digital signature verifies both that the message originated from a specific person and that the message has not been altered either intentionally or accidentally. Furthermore, if you sign a document, you cannot later disown it by claiming the signature was forged (this is called nonrepudiation).

How can I get a Digital ID?

You can aquire a Digital ID from a company called a Certification Authority (CA). Also, your company or organization might issue you a Digitial ID through the Digital ID Center in conjunction with a CA.

When your company issues you a Digital ID, they are providing you with a way to identify yourself to other people in the company, to your company's business partners, or to computers in your network.

If you are getting a Digital ID for personal reasons, you should seriously consider who you want to be your CA. When you need to prove your identity, you want a CA that others will trust. For example, most people and companies trust the validity of a driver's license or passport. This is because they trust the way the government issues these documents. However, a student ID is typically accepted as proof of your identity only to the school that issues the ID. The same holds true for Digital IDs. You want a Digital ID from a CA that is trusted by all major companies doing business on the Internet.

VeriSign continues to be the leading Certification Authority on the Internet.

What is a Digital ID key pair?

When you communicate with another person (or computer), you need a way to exchange information securely, so no one can intercept and read the information. Currently, the most advanced way to scramble (encrypt) data is through a system that uses key pairs. A key pair consists of a public and a private key. The keys are used similarly to keys in a lock, except the key pair requires one key to secure the lock and another to open the lock.

With key pairs, your software application uses one key to encrypt a document. The person who receives your encrypted document then must use the matching key to decrypt the message. The problem with this process is how do you give someone the "key" to decrypt your message without allowing anyone else to get the key?

The solution is in the way the keys are used. When you request a Digital ID, your Web browser creates both a private key, that can only be used with the Digital ID you requested, and a public key, that becomes part of the Digital ID. The Web browser might ask you for a password to use when accessing the private key. It is very important that you choose a password that only you will know (not your birthday or other number or phrase someone is likely to guess).

Once you received and installed a Digital ID, you distribute it to whoever needs it. The Digital ID that you send contains your public key. When someone needs to send you an encrypted message, they use your public key. Once the message is encrypted with your public key, you are the only person who can decrypt the message because only you have the matching private key.

Likewise, when you want to send someone an encrypted message, you must first get their public key. You do this either by looking up their Digital ID in a directory or you simply have them send you a signed e-mail message, which contains their Digital ID and public key. Then your e-mail application can automatically store the Digital ID until you need to use it.

Why do I need a Digital ID?

Virtual malls, electronic banking, and other electronic services are becoming more commonplace. However, your concerns about privacy and security might be preventing you from taking advantage of this new medium for your personal business. A Digital ID can help.

Or, your employer might have a new network that requires you to have a Digital ID for applications that you use on the job. Because you will use this technology on the job, you need to learn to use Digital IDs quickly.

Digital IDs are used by Web sites and network applications to scramble data passed between two computers. Encryption is a powerful tool, but encryption alone is not enough protection for your information.

Encryption cannot prove your identity or the identity of someone sending you encrypted information. For example, an online stock broker might have a site that encrypts data sent to you through its Web pages. The site might even require you to enter a username and password. However, these types of usernames and passwords are easily intercepted and cannot be trusted to prove your identity. Without additional safeguards, someone could impersonate you online and get access to your accounts or other valuable and private information.

Digital IDs address this problem, providing an electronic means of verifying your identity. Digital IDs provide a more complete security solution, assuring the identity of all parties involved in a transaction.

Because of the way Digital IDs work, they provide a function called nonrepudiation, which essentially prevents people from denying that they sent a message. For example, when you use a credit card, you have to sign a receipt authorizing payment. Because a signature is required on the receipt, you can prove someone stole or used your card by comparing your signature to theirs. With nonrepudiation, your "authorization" happens automatically when you send your Digital ID.

If someone manages to steal your Digital ID, they cannot use it unless they have the password and your private key. This is why it is critical that you do not tell anyone your password.

How do I use Digital IDs?

Once you receive a Digital ID from the Digital ID Center, you need to install it in the software applications that you use. Typically you install it in your Web browser or your e-mail application. (See the How To section on the online help for complete instructions.) Once set up correctly, the applications do most of the work for you, which makes using Digital IDs fairly easy.

How you use the Digital ID depends on why you need it:

- If you use Web sites or network applications that require your Digital ID, you need to enter the password for your private key to confirm that you want the application to send your Digital ID. The application or Web browser takes care of sending your ID to the Web site or network application. (Of course, this process varies depending on what application you are using.)
- When sending encrypted (secure) e-mail, you need to retrieve Digital IDs from the people you communicate with, and then you can configure your e-mail application to encrypt your messages to those people. Once configured, all e-mail messages to them are sent encrypted. Some e-mail applications make you select an option each time you want to encrypt a message. This functionality varies depending on which e-mail product you use.
- When digitally signing messages, your e-mail application attaches your own Digital ID to the e-mail message.).

How safe are Digital IDs?

Digital IDs are very safe provided you keep your private key and password to yourself. Think of your password as a key to a safe. If you are the only person with the key, the safe's contents are secure. However, if you share the key with others, you lessen the security of the safe contents.

If anyone gets your Digital ID, they cannot use it unless they have the matching private key and the password to the private key. Before your Web browser sends your Digital ID, the browser prompts you for your password. You must enter the password before your Digital ID is used.

Digital IDs also come in various strengths. The lowest strength is called "40-bit," which refers to the size of the key for the ID. The highest strength is called "128-bit." If a 40-bit key can be deciphered in 4 hours, it would take longer than the age of the universe to crack a 128-bit key.

How do I protect my Digital ID?

There are several things you can do to protect your Digital ID:

- Remember your passwords and do not share them with others.
- Protect your computer from unauthorized access by keeping it physically secure. For example, lock it in an office. When you leave your desk, use a screen saver with a password or shut down your computer.
- Use access control products or operating system protection features (such as a system password or password-enabled screen saver).
- Take measures to protect your computer from viruses, because a virus may be able to attack a private key.

Your private key is protected in two ways:

- When you enroll for a Digital ID, your Web browser creates a private key that is then stored on your computer's hard drive so you can control access to it. When you generate your private key, the software you use (such as your browser) will probably ask you for a password. This password protects access to your private key. For Microsoft Internet Explorer users, your private key is protected by your Windows password.
- A third party can access your private key only by having access to the file your key is stored in and by knowing your private-key password. Some software lets you choose to not have a password to protect your private key. If you use this option, then you are trusting that no one, presently or in the future, will have unauthorized access to your computer.

In general, it is far easier to use a password then to completely safeguard your computer physically. Not using a password is like pre-signing all of the checks in your checkbook and then leaving it open on your desk.

It is your responsibility to protect your private key. Anyone who obtains your private key can forge your digital signature and take actions in your name!

How does encryption work?

Encryption is the process of scrambling data. There are many different (and complicated) ways to scramble and unscramble information. This section provides a brief description of encryption without going into too much technical detail.

On the Internet, there are two main uses for encryption. One occurs when you visit a "secure" Web site, such as an online store or shopping mall. This is called server-side encryption because it uses the Digital ID given to the server (computer) that runs the Web site. The other use occurs when you send or receive encrypted e-mail. In both cases, the encryption process involves exchanging public keys.

When encrypting information, the encryption process is done with either a public or a private key and then decrypted with the matching public or private key. Think of it as a lock that requires one key to close the lock and another key to open the lock. For example, when you visit a secure Web site, your computers receives the Web site's public key. When your computer sends information to the Web site, your computer encrypts it using the Web site's public key. The only way to decrypt the information you are sending is with the Web site's private key.

The same process is needed for secure e-mail. Before you can send someone an encrypted message, you need their Digital ID, which contains their public key. Your e-mail application uses their public key to encrypt the message. From that point on, only the recipient's private key can decrypt the message. So, you can distribute your Digital ID (and its public key) to as many people as you would like without harming the integrity of your Digital ID. However, you must guard your private key, since it is used to decrypt any messages sent to you.

There is one more topic of interest: trust. Many different companies (CAs) can create Digital IDs. Your applications are configured to trust Digital IDs that come from a few highly reputable companies. So, if someone sends you their Digital ID (either via e-mail or from a Web site you visit) and it is from a CA that your application does not trust, you will get an alert message asking if you want to trust the new CA.

For more information on trust, see What is public key infrastructure (PKI)? and What applications use Digital IDs?.

What is public key infrastructure (PKI)?

PKI describes a system that uses public keys and Digital IDs to ensure security of the system and to confirm the identity of its users. For example, a company might use PKI to control who accesses the company's computer network. In the future, companies might use PKI to control access to everything from entrance into buildings to procurement of goods.

PKI lets people and companies conduct business in private. Employees can securely send e-mail over the Internet, without worrying that a competitor could intercept the e-mail. Companies can build private Web sites, sending information only to known customers.

PKI is based on a system of trust, where two parties (these can be people or computers) mutually trust a CA to check and confirm the identity of both parties. For example, most people and companies trust the validity of a driver's license or passport. This is because they trust the way the government issues these documents. However, a student ID is typically accepted as proof of your identity only to the school that issues the ID. The same holds true for Digital IDs.

With PKI, both parties in a transaction (be it an online bank and its customers or an employer and its employees) agree to trust a CA who issues their Digital IDs. Typically, the software application that uses your Digital ID has some mechanism for trusting CAs. For example, a Web browser contains a list of CAs that it trusts. When the Web browser is presented a Digital ID (say from an online mall doing secure commerce), the browser looks up the CA who issued the Digital ID. If the CA is in the list of trusted CAs, the browser accepts the identity of the Web site and displays the web page for you. However, if the CA is not in the list of trusted CAs, the browser displays a warning message that asks you if you want to trust the new CA. Usually your browser gives you options for permanantly or temporarily trusting the CA or not trusting it at all. As a user, you have control over which CAs you want to trust, but the trust management is done by the software application (in this example, it is by the Web browser).

How does client authentication work?

Client authentication describes the process of a computer confirming your identity. The following example illustrates how a Web site might use client authentication. Client authentication is not limited to Web sites. Other applications, such as network applications, can use client authentication, but the process is generally the same.

When you access a Web site that requires a Digital ID, your Web browser presents your Digital ID to the Web site. The Web site then views information in your ID to determine what you have permission to do. (Digital IDs used for client authentication are sometimes called client certificates by Web browsers.)

Depending on your Web browser, you might have to confirm that you want to present your Digital ID to the Web site. Usually, you will see a dialog box asking for the certificate password (this is the password for your private key). After you enter the correct password, the Web browser sends your Digital ID to the Web site. This is why it is important to guard your password. If someone knows the password for your Digital ID and has access to your computer, they could easily access your private information or impersonate you online.

Once a Web site views your Digital ID, the site checks the validity of your ID. For example, the site checks to make sure the ID has not expired. The site might also consider who issued the Digital ID. If the Web site does not trust the CA who issued you the ID, then you might be denied access to the site. This is why it is important to use a reputable CA.

The Web site can use any information in the Digital ID when determining what permissions you have. Your Digital ID might contain some or all of the following information about you:

- Your public key (see What is a Digital ID key?)
- Your name
- Expiration date of the public key
- Name of the company (the CA) who issued your Digital ID
- Serial number of the Digital ID
- Digital signature of the CA
- Various information required by the CA

Once the Web site confirms your identity, it gives you access to the site.

Some Web sites or network applications use the information in your Digital ID to customize the information you see. This customization is sometimes called access control, but do not confuse access control for client authenitcation. Client authentication is simply proving your identity.

How does a digital signature work?

When you use an application to digitally sign a message, you are basically attaching the public part of your Digital ID to the message along with other information that ensures the integrity of your e-mail message.

Before the e-mail message and Digital ID are sent, the message goes through an encoding process, called a *hash algorithm,* whereby the message you are sending is used to mathematically generate a set of characters (letters and numbers) that could only be created by your exact message. This set of characters is called a *message digest*.

It is important to know that the hash algorithm works quickly in one direction and is very difficult to work in reverse. That is, your e-mail application can take your e-mail message, run it through the hash algorithm, and quickly create a unique message digest. However, if given just the message digest, it would take years to decipher the e-mail message.

Once the e-mail application creates the message digest, it uses your private key to encrypt the message digest. This is critical. If you were to send the e-mail and the message digest, someone could easily change your message text, recreate the message digest, and then send that along as if it came from you.

Your e-mail application sends the e-mail with the Digital ID and encrypted message digest as attachments. Note that none of the e-mail message text is sent encrypted. So if someone wanted to, they could still read the contents of your message.

When someone receives your e-mail message, their application uses your Digital ID (the public key) to decrypt the message digest. Then the application runs your e-mail text through the same hash algorithm that your application used. It then compares the results (the message digests). If the message digests that it created matches the one attached to your e-mail, then the message text was not tampered with during the transfer from your computer to theirs.

For more information, see the section on public and private keys.

How does secure e-mail work?

You can use secure e-mail to do the following:

- Digitally sign a message so that the recipient can verify the message came from you and not an impostor. Signing a message also ensures the integrity of the message. That is, it ensures that no one tampered with the message.
- Encrypt a message so that no one can read it while it travels from your computer to another.

You can set up most e-mail applications to automatically sign or encrypt your messages or you can manually choose to do it on a case-by-case basis.

For more information, see the Tasks section of the online help.

What applications use Digital IDs?

Digital IDs are supported by Netscape Navigator 3.0 and higher (on Win 95, NT, Sun Solaris 2.5x, 2.6, SGI Irix 6.x and HP-UX 10.20) and by Microsoft Internet Explorer 3.02 with authenticode 2.0 update and higher (on Win95 and Win NT 3.5.x or later on x86 platform.)

For signing and encrypting e-mail, Digital IDs are supported by Netscape Messenger, Microsoft Outlook and Outlook Express, and by any other S/MIME (Secure Multipurpose Internet Mail Extensions) enabled e-mail application such as Deming, Frontier, Pre-mail, Opensoft, Connectsoft, and Eudora.

The latest Web browser packages (specifically Netscape Communicator and Microsoft Internet Explorer), have e-mail applications included (Netscape Messenger and Microsoft Outlook Express), so Digital IDs obtained through these packages can be used for both e-mail and the Web. If you are using an e-mail application other than Netscape Messenger or Microsoft Outlook Express, you should obtain your Digital ID through the e-mail vendor.

How are the keys for a Digital ID managed?

Users must be able to securely obtain your Digital ID so they can send you encrypted e-mail. Likewise, you need a way to look up their Digital IDs. You can send a digitally signed e-mail message to the people you want to send you encrypted messages. And you can have them send you signed messages so you can get their Digital IDs. You can also look up Digital IDs in various directories.

The Digital ID Center contains a search feature that lets you find Digital IDs that belong to you and to other people in your organization.

What happens when a key expires?

In order to guard against a brute-force attack, every key must have an expiration date after which it is no longer valid.

The expiration date is stored in the public key of a Digital ID. Every Web browser or e-mail application checks the validity of a Digital ID by making sure the date you receive the Digital ID (and the information it is protecting) is within the valid dates. This means that when your own key expires, everything you signed with it will no longer be valid.

After expiration, the you need to renew your Digital ID using the Digital ID Center.

What is a hash algorithm?

A hash function is a math equation that uses text (such as an e-mail message) to create a code called a message digest. Examples of well-known hash functions are MD4, MD5, and SHS.

A hash function used for digital authentication must have certain properties that make it secure enough for cryptographic use. Specifically, it must be infeasible to find:

- Text that hashes to a given value. That is, if you know the message digest, you should not be able to figure out the message.
- Two distinct messages that hash to the same value

The ability to find a message that hashes to a given value would enable an attacker to substitute a fake message for a real message that was signed. It would also enable someone to falsely disown a message by claiming that he or she actually signed a different message hashing to the same value, thus violating the non-repudiation property of digital signatures.

The ability to find two distinct messages that hash to the same value could enable an attack whereby someone is tricked into signing a message that hashes to the same value as another message with a quite different meaning.

What is a message digest?

A message digest is the results you get when you run text (such as an e-mail message) through a hash algorithm. A message digest concisely represents a longer message or document. You can think of a message digest as the "digital fingerprint" of a larger document. A message digest is used to create a digital signature that's unique to a particular document.

A message digest does not reveal the contents of a document. That is, if you can view the message digest, you cannot figure out what the original message was.

MD2, MD4 and MD5 (MD stands for Message Digest) are widely used hash functions designed specifically for cryptographic use. They produce 128-bit digests and there is no known attack faster than exhaustive search.

Glossary

CERT.DB FILE
: This file contains your Digital ID for Netscape Navigator or Communicator.

CERTIFICATE (PUBLIC KEY CERTIFICATE)
: Certificate is another word for Digital ID. Some software applications and Web browsers use this term.

CHALLENGE PHRASE
: A set of numbers and/or letters chosen by a Digital ID applicant, and used to authenticate the subscriber for various actions such as the Digital ID revocation, replacement, and renewal.

CRYPTOGRAPHY (Cf.,PUBLIC KEY CRYPTOGRAPHY)
: The mathematical science used to secure the confidentiality and authentication of data by transforming data in order to hide its information content, prevent undetected modification, and/or prevent unauthorized use.

DIGITAL ID EXPIRATION
: A time and date specified in the Digital ID when the operational period ends.

DIGITAL ID HIERARCHY
: A structure of Digital IDs which allows individuals to verify the validity of a Digital ID's issuer. Digital IDs are issued and signed by Digital IDs which reside higher in the Digital ID hierarchy. The validity of a given Digital ID is determined by the corresponding validity of the Digital ID which signed it.

DIGITAL ID SERIAL NUMBER
: A value that unambiguously identifies a Digital ID issued by a Certification Authority.

DIGITAL SIGNATURE
: A method to validate that a specific message was not altered during transmission. This process involves creating a message, encrypting it, and sending both the original message and the encrypted message together. Once received, the recipient compares the contents of the original message against the contents of the encrypted message to make sure the information has not been changed.

DISTINGUISHED NAME
: The set of data used to identify an individual Digital ID holder. Within a Class 1 Digital ID this would be information such as your Name and your e-mail address, and the issuer of the Digital ID (VeriSign, Inc.).

DOMESTIC RELEASE BROWSER
: Available to US and Canadian browser customers only. This browser supports "strong" encryption at the 128-bit level. You can only download this type of browser if you live in the United States or Canada.

ENCRYPTION
: The process of scrambling information so that only the intended recipient can unscramble and read the information.

ENROLLMENT
: The process of applying for a Digital ID.

EXPORT

The process of backing up a Digital ID to avoid loss. Digital IDs contain information you cannot recover in the event of a hard drive crash or browser re-installation, so you should make a copy and store it in a secure place.

GENERATE A KEY PAIR

The process of creating a private key during Digital ID application whose corresponding public key is submitted to VeriSign for validation. (See also PUBLIC KEY CRYPTOGRAPHY; PUBLIC KEY and PRIVATE KEY)

INTERNATIONAL RELEASE BROWSER

Available worldwide, supporting maximum key sizes of 512 bits and 40 bit session keys. Higher encryption available to US and Canadian citizens by filing a eligibility declaration on the browser vendor's web site and downloading the application.

KEY GENERATION

The process of creating a private key during Digital ID enrollment whose corresponding public key is submitted to the Digital ID Center for validation.

KEY PAIR

A key pair consists of a private key and a corresponding public key. The private key, typically protected by a password and stored on your computer, is known only to you and is not sent to anyone. The public key is shared with other people and computers or web sites.

LIGHTWIEIGHT DIRECTORY ACCESS PROTOCOL (LDAP)

The Lightweight Directory Access Protocol (LDAP) is a protocol for accessing online directory services that might contain other user's Digital IDs.

OPERATIONAL PERIOD

The period starting with the date and time a Digital ID is issued and ending with the date and time on which the Digital ID expires or is earlier suspended or revoked.

PASSWORD

Confidential authentication information, usually composed of a string of characters used to provide access to the private key of your Digital ID.

PIN NUMBER

The PIN number is used only once--during Digital ID retrieval. It consists of 32 characters using the letters A-F and the numbers 0-9. There are no spaces before, after or in the PIN number.

PKCS #12

A standard that specifies a portable format for storing or transporting a user's private keys and Digital IDs.

PRIVATE KEY

A mathematical key (kept secret by the holder) used to create digital signatures and, depending upon the algorithm, to decrypt messages or files encrypted (for confidentiality) with the corresponding public key.

PUBLIC KEY

A mathematical key that can be shared safely so that others can send you encrypted information that only your private key can unscramble. The public key can also verify signatures created with its corresponding private key. Depending on the algorithm, public keys are also used to encrypt messages or files that can then be decrypted with the corresponding private key.

PUBLIC KEY CRYPTOGRAPHY

A type of cryptography that uses a key pair of mathematically related cryptographic keys. The public key can be made available to anyone who wishes to use it and can encrypt information or verify a digital signature; the private key is kept secret by its holder and can decrypt information or generate a digital signature.

.P12 FILE

The file extension assigned to all Digital IDs exported from Netscape Communicator using the PKCS #12 standard.

.PFX FILE

The file extension assigned to all Digital IDs exported from Microsoft Internet Explorer using the PKCS #12 standard.

RECIPIENT (of a DIGITAL SIGNATURE)

A person who receives a digital signature and who is in a position to rely on it, whether or not such reliance occurs.

RELYING PARTY

A recipient who accepts a Digital ID and digital signature, such as an online bank or e-commerce company.

RENEW A DIGITAL ID

The process of obtaining a new Digital ID once an existing Digital ID has expired.

REPLACE A DIGITAL ID

The process of obtaining a replacement Digital ID once an existing Digital ID has been revoked.

RETRIEVE A DIGITAL ID

The process of picking up a pending Digital ID after the enrollment form is completed. When the Digital ID is picked up, it is considered issued.

REVOKE A DIGITAL ID

The process of permanently ending the valid period of a Digital ID. Someone must use the Digital ID Center to determine if a Digital ID has been revoked.

RSA

A public key cryptographic system invented by Rivest, Shamir & Adelman. For more information visit their Web site: www.rsa.com

SECURE CHANNEL

This refers to information sent encrypted over the network. For example, you purchase items from a web site using a secure (encrypted) channel.

SESSION KEY

The key size assigned for a secured communication between a client and server using SSL (Secure Sockets Layer). Depending on the use of International or Domestic browsing software the session will be assigned an 40 or 128 bit encryption session.

SIGNER

A person who creates a digital signature for a message or a signature for a document.

S/MIME

A specification for secure e-mail that uses a cryptographic message syntax in an Internet MIME (multipurpose internet message exchange) environment.

SUBSCRIBER

A person who has been issued a Digital ID and is capable of using the private key that corresponds to the public key listed in the Digital ID.

SUBSCRIBER AGREEMENT

The agreement executed between a subscriber and VeriSign for the provision of designated public certification services in accordance with the CPS.

SUBSCRIBER INFORMATION

Information supplied to a certification authority as part of a Digital ID application.

TRUSTED THIRD PARTY

In general, an independent, unbiased third party that contributes to the ultimate security and trustworthiness of computer-based information transfers, such as VeriSign.

UNIFORM RESOURCE LOCATOR (URL)

A standardized device for identifying and locating certain records and other resources located on the World Wide Web. Most URLs appear in the familiar form of Web site addresses such as <http://www.verisign.com>.

VALIDATE A DIGITAL ID

The process performed by a recipient or relying party to confirm that an end-user Digital ID is valid and was operational at the date and time a pertinent digital signature was created.

VERIFY (A DIGITAL SIGNATURE)

The process of determining accurately that a digital signature was created during the operational period of a valid Digital ID and the associated message was not altered since the digital signature was created.

WORLD WIDE WEB (WWW)

A hypertext-based, distributed information system in which users may create, edit, or browse hypertext documents. A graphical document publishing and retrieval medium; a collection of linked documents that reside on the Internet.

X.509

The ITU-T (International Telecommunications Union-T) standard for Digital IDs. X.509 v3 refers to Digital IDs containing or capable of containing extensions.