Glossary:
Electronic Recording Terms

Electronic recording sits at the intersection of several different industries and technologies. The language of electronic recording includes elements from general computer and Internet terminology, from the Public Key Infrastructure, from the science of cryptography, and from several other sources.

This glossary is intended to help you cut through the technical jargon, the alphabet of acronyms, to fully understand both the terms and the concepts related to electronic recording. In an effort to minimize the amount of jumping around, glossary entries themselves are encyclopedic in nature. However, ample links to related terms provide threads to interconnected ideas and related technologies. It is our hope that this glossary will serve as a useful resource for you as you acquaint yourself with this new field.

A note on some conventions is in order. Within this glossary, all headwords are printed in **blue**. Reference to terms covered elsewhere in the glossary are also printed in **boldface**. For the most part, reference to parts of speech (such as nouns and verbs) has been omitted, except in cases where this is needed for clarification. Pronunciation has likewise been omitted, except in cases of pronounceable acronyms.

acknowledgement: A legal process used to help guarantee the validity of a legal document. A document signer appears before a **notary public** and gives an acknowledgement that he or she is authorized to sign the document, and that neither coercion nor mental impairment is a factor in the signing. The notary verifies the signer's identity, witnesses the signature, and confirms the acknowledgement by notarizing it with an embossed seal. See also **digital notarization**.

Active Server Page (ASP): One of several web technologies that allows web pages to be dynamically generated from databases using ActiveX scripting. ASP is a Microsoft technology that runs on Microsoft's **Internet Information Server** (IIS). Active server pages carry the .asp filename extension and are usually generated using Visual Basic or Jscript code. ASP pages are similar to **common gateway interface** (CGI) scripts, but are created with different tools.

application service provider (ASP): A company that provides its customers software-based services and solutions across a **wide area network** (WAN) or over the **Internet**. Within the ASP model of software delivery, most software processes run from a central server, rather than from a user's own computer. This reduces the requirements of processing, memory, and hard disk space on **client** machines.

archive: *verb* The act of copying files to a long-term storage medium, such as floppy disk, recordable compact disc, or digital tape. Archiving "backs up" files for future or emergency use.

archive: *noun* Either the actual storage medium used to make a backup, or the file(s) held on the storage medium.

ASP: See **Active Server Page** or **application service provider**.

asymmetric encryption: See **asymmetric cryptography**.

asymmetric cryptography: A type of **cryptrography** that uses two keys: a

public key and a secret **private key**. Together, the keys constitute a **key pair**. Though the keys are mathematically related, it is not possible to deduce one from the other. The public key is published in a public repository and can be freely distributed. The private key remains secret, known only to the key holder.

Either key can be used to **encrypt** and **decrypt**. A message that is encrypted with a private key can only be decrypted by the corresponding public key, and vice-versa. This allows for two distinct encryption schemes:

- *Public to Private*: This method is used to exchange secret data without exchanging secret keys. Person A first obtains Person B's public key from an online repository and uses it to encrypt a message, which is then sent to Person B. Person B is the only individual who can read the message, because decrypting the message requires Person B's private key. This type of encryption is used to set up security for data that is transmitted across the Internet using **secure sockets layer** (SSL) technology.
- *Private to Public*: Person A can use his or her own private key to encrypt a message for Person B. The encrypted message is not secret, though, because the tool to decrypt it—Person A's public key—is freely available to anyone who wants it. However, Person B is assured that the document actually came from Person A, since only Person A's private key could have encrypted it. This type of encryption is used to create a **digital signature**.

Asymmetric cryptography is distinct from **symmetric cryptography**, a more common cryptographic strategy that uses a single key to both encrypt and decrypt a message. Also *public key cryptography*.

authentication: The act of tying an action or result to the person claiming to have performed the action. Authentication generally requires a password or encryption key to perform, and the process will "fail" if the password or key is incorrect.

For example, logging on to a computer system and withdrawing money from an automatic teller machine (ATM) both involve authentication, the first with a password and the second with a personal identification number (PIN). In the world of digital documents, **signature authentication** involves using a public key to verify a **digital signature**, ensuring document integrity and the correct identity of the signer.

back end: In the software industry, a program or part of a program not directly seen by the user, which performs important functions. Back end functions often involve complex computations and database access. For client-server applications, the back end is the **server** software that communicates with the **client** program. See also **application service provider**.

binary: A numbering system based on two digits: 0 and 1. Computers use the binary numbering system because a circuit's electrical nature allows for two states: on (1) and off (0).

The binary numbering system is distinct from the more familiar *decimal* system, which uses ten digits (0 through 9). All mathematical operations that are possible in the decimal system (addition, subtraction, multiplication, division, and so on) can also be performed in the binary system. See also **bit**.

bit: An abbreviation for ***bi****nary dig****it***, the smallest unit of information in the computer world, represented by either a 0 or a 1. A bit is represented in memory as a single switched circuit that is either on (1) or off (0). Bit-based data can also be stored on magnetic media (such as floppy disks and magnetic tape), or on compact disc media. See also **binary**.

browser: A software application that retrieves and displays web documents. The first widely used browser was called Mosaic; originally released in 1993, it was only capable of displaying text. Today's browsers give users access to a wealth of text, graphics, audio, video, and other data formats, with additional functionality provided by plug-in

applications such as Apple QuickTime, Adobe Acrobat, RealPlayer, and Macromedia Shockwave and Flash. Also *web browser*.

CA: See **certificate authority**.

certificate: See **digital certificate**.

certificate authority (CA): A trusted third party that issues **digital certificates** to subscribers. A CA vouches for an individual's identity and effectively binds that person to a **key pair**, including the **public key** contained in a digital certificate. CAs will often issue different classes of digital certificates, each class offering a different degree of trust. See also **certificate practice statement**, **certificate revocation list**, **registration authority**.

certificate practice statement (CPS): A document that outlines the policies and procedural operations of a **certificate authority**. A CPS includes information ranging from how a subscriber is registered to the physical security used for the CA's system.

certificate revocation list (CRL): A published list of **digital certificates** that have been revoked or compromised. When a **signed digital document** goes through the process of **signature authentication**, the digital certificate used in the **digital signature** is checked against the CRL. If the document was signed after the time the certificate was put on the CRL, the signature and signed document are considered invalid.

CGI: See **common gateway interface**.

client: A software program that runs on a personal computer or workstation and connects to a network server to perform certain operations. Client applications are generally designed to require little memory and storage space, routing most of the data processing load to the server. A good example is the e-mail client, which allows a user to access the contents of an e-mail account hosted on a remote server. See also **application service provider**.

common gateway interface (CGI): A web standard that enables live interaction between computers and web servers, allowing web pages to be created dynamically to fit a particular user or context. Some standard functions provided by CGI scripts include searching, processing forms, and personalizing web pages. CGI scripts can be written in any programming language that conforms to the protocol's specification. Popular tools for CGI scripting include Perl, C, Java, and Visual Basic.

CPS: See **certificate practice statement**.

CRL: See **certificate revocation list**.

cryptoanalysis: The practice of systematically "attacking" an encrypted message, in an attempt to discover the encryption code and unlock the hidden data. Cryptoanalysis is similar to opening a combination lock by trying every combination, starting with 1-1-1 and working methodically—trying 2-1-1, then 3-1-1, and so on—until the lock opens. The theoretical amount of time it would take to "crack" an encrypted file is dependent on the complexity of the key used to encrypt it.

cryptography: The science of protecting information from unauthorized access through the use of numeric keys and special mathematical functions. An encrypted document looks like meaningless gibberish, and must be decrypted to be readable. Cryptography includes both **symmetric** and **asymmetric cryptography**.

data encryption: See **encrypt**.

decrypt: To apply a cryptographic key, such as the public key contained in a digital certificate, to encrypted information in order to make it readable. See also **encrypt**, **cryptoanalysis**.

digital certificate: An electronic file that is issued to a user by a **certificate authority** (CA). The primary purpose of a digital certificate is to link the certificate holder to a **public key**. Digital certificate information is commonly included along

with digital signatures. Digital certificates generally include the following information:

1. The name of the subscriber
2. The subscriber's public key
3. The name of the CA that issued the certificate
4. The issuing CA's public key
5. The digital signature of the CA
6. The expiration date of the certificate

A digital certificate is held by the user and the CA, and is published by the CA in a **public repository**. The public information included in a certificate is available to anyone who wants to view it. Though a digital certificate contains the certificate holder's public key, it does *not* contain the matching **private key**. The private key, which is generated with the public key by the certificate holder, is never divulged to anyone—not even the issuing CA.

digital identification (digital ID): Includes a person's **digital certificate**, **public key**, and secret **private key**. While the digital certificate (and the public key it contains) is public knowledge, the private key is known only to the ID holder, and is not even divulged to the holder's **certificate authority**.

digital notarization: The process by which a **notary public** signs an electronic document to endorse a signer's **acknowledgement**. The corollary in the paper world is the application of a notarial stamp to a document original. In the electronic world, the process is identical to that of creating a **digital signature**. The only difference is that the notary uses a special **digital certificate** issued only to notarial officials.

digital signature: A complex string of electronic data that is embedded in an **electronic document** for the purposes of verifying document integrity and signer identity. A mainstay of the **Public Key Infrastructure** (PKI), digital signatures are the most effective method for ensuring **nonrepudiation** for **digital documents**. The signing process involves three steps:

1. The electronic document is processed through an algorithm called a **hash function**. This results in a string of numbers called a **document fingerprint** (or *message digest*), which is unique to the document.
2. The document fingerprint is encrypted using the signer's **private key**, resulting in a digital signature.
3. The digital signature and the original document are combined into a single file, a **signed digital document**.

Once a document is signed, it can be validated using the signer's **public key**. The process, known as **signature authentication**, helps protect electronic transactions by providing a method for detecting tampering and forgeries.

Digital signatures are probably the most trusted kind of **electronic signature**. A digital signature is in no way related to a **digitized signature**, and has nothing to do with a signer's name or handwritten signature.

digitized signature: A representation of a person's handwritten signature, existing as a computerized image file. Digitized signatures are just one of several types of **electronic signature**, and have no relation to **digital signatures**, which are created using **asymmetric** (or *public key*) **cryptography**. See also **digital signature**.

DNS: See **domain name server**.

document fingerprint: The result of processing an original **electronic document** through a **hash function**. Because the hash function is a one-way mathematical process, the original document cannot be reconstituted from the document fingerprint. Also *message digest* or *document thumbprint*.

document thumbprint: See **document fingerprint**.

document type definition (DTD): A document, created using the **Standard Generalized Markup Language** (SGML), that defines a unique markup language (such as **XHTML** or **ERML**). A DTD includes a list of tags, attributes, and rules of usage.

domain name: A word-based address that identifies a computer (or group of computers) connected to the Internet. A domain name is used in a **URL** to locate a web page. For example, the domain name *yahoo.com* would show up in a URL as *http://www.yahoo.com*.

Every domain name has a suffix indicating its top level domain. Common top level domains include *.com* (commercial), *.edu* (education), and *.gov* (government). There are also two-letter top-level domains that indicate a server's country of origin, such as *.ca* for Canada and *.uk* for Great Britain.

domain name server (DNS): An Internet service that converts a word-based **domain name** into a number-based **internet protocol** (IP) **address**. The DNS network is an interconnected system of computers that shares information about which domain names link to which IP addresses. For example, when a user types *http://www.google.com/* into a browser, the DNS is queried to find out which IP address matches *google.com*. Once the proper address is found, the request can be routed to the appropriate server. The DNS system allows system administrators to change the IP addresses assigned to a particular domain, if necessary. Also *domain name system*.

domain name system: See **domain name server**.

DTD: See **document type definition**.

dual key certificate: A special type of **digital identification**—introduced relatively recently—that includes two separate **key pairs**, a **signing pair** and an **encryption pair**. As with a standard **digital certificate**, the keys are generated by the user when the certificate is issued. The private keys are kept secret while the public keys are published

with the certificate. The signing pair is reserved exclusively for creating and authenticating digital signatures, and the encryption pair is used for encoding and decoding data.

e-commerce: See **electronic commerce**.

e-document: See **electronic document**.

E-SIGN: Pronounceable acronym: *EE-sign*. See **Electronic Signatures in Global and National Commerce Act**.

electronic commerce: Trade that occurs electronically—usually over the Internet. Electronic commerce often involves buying, selling, and sharing information, extending both new and traditional services to customers via electronic means. E-commerce allows businesses to take advantage of e-mail, the **World Wide Web**, and other online innovations to improve the business process and offer consumers more ways to access products, faster information transfer—and ultimately, decreasing costs. Also *e-commerce*.

electronic document: A document which exists as numbers in a computer-readable medium, not as words on a printed page. Since any electronic document is essentially just a collection of bits (ones and zeroes), mathematical processes can be used to **encrypt** and **decrypt** the document's contents. Also *e-document*.

Electronic Recording Markup Language (ERML): An XML language created and defined by Ingeo to facilitate the electronic recording of documents.

electronic signature: Any of several methods that links a person to a document or action using electronic data. According to electronic signature laws in the U.S. (including the federal **Electronic Signatures in Global and National Commerce Act**, E-SIGN, and the **Uniform Electronic Transactions Act**, UETA), any embedded electronic element can serve as a signature if a person embeds it with the *intent* to sign. Several methods are commonly used to create electronic signatures:

- **digitized signature**: A scanned image of a person's handwritten signature, which is captured using special digitizing hardware and stored as a computer file. Shipping services such as Federal Express and UPS often use digitized signatures to reduce paperwork and speed up the business process.
- **digital signature**: A complex string of electronic data that contains encoded information about a document and the person who signed it. Because they use powerful **asymmetric encryption** technology, digital signatures are the most "secure" type of electronic signature. A digital signature is the result of processing an **electronic document** through a special **hash function** to create a **document fingerprint**, then encrypting the document fingerprint using the signer's **private key**.
- **voice authorization**: A digital audio recording that serves an audio record of an agreement. In a voice authorization, a person indicates verbal approval of the terms of an agreement, often over the telephone. The person's voice is recorded and stored as proof of the agreement.
- **text-based signature**: A typed name at the bottom of an e-mail or in a word processing file. Since virtually any action can be considered a signature if it is intended as such, the difficulty with this type of signature lies in proving the signer's intent.
- **biometric signature**: An electronic signature that is the result of a computerized scan of a measurable body part, such as a fingerprint or retina.

Electronic Signatures in Global and National Commerce Act (E-SIGN): A U.S. federal law, passed in 2000 by both houses of Congress, which enables the use of **electronic documents** and **digital signatures** for interstate business, in international trade, and by the federal government. The legislation also sets standards for the kinds of documents that can be created and processed electronically. E-SIGN affirms that e-documents are valid and enforceable if both parties

have agreed to use them, but it does not *require* that e-documents be used in any case.

encrypt: To apply an **encryption** key to a message in order to make it unreadable, in an effort to prevent unintended use of the information.

encryption: The use of **cryptography** to make a message unreadable, to prevent unauthorized access. Also *data encryption*. See also **symmetric encryption**, **asymmetric encryption**.

encryption pair: A **digital identification**, consisting of a **digital certificate** (containing a **public key**) and a **private key**, reserved specifically for **encryption**. See also **signing pair**.

ERML: Pronounceable acronym: *ER-muhl*. See **Electronic Recording Markup Language**.

Ethernet: One of the least expensive and most widely implemented networking schemes. Ethernet allows data to be transferred among several computers (or other devices) through a central hub. Ethernet was first developed in 1972 at Xerox's Palo Alto Research Center (PARC). The name *Ethernet* is a registered trademark of the Xerox Corporation.

Extensible Hypertext Markup Language (XHTML): A computer language used to create web page documents. XHTML is a reformulation of **Hypertext Markup Language** (HTML) as a module of **Extensible Markup Language** (XML), reproducing the familiar functionality of HTML with the power and expandability of XML. The **World Wide Web Consortium** (W3C), the main standards body of the web, now recommends XHTML over HTML as the standard for web development.

Extensible Markup Language (XML): A computer language used to create markup languages. XML allows developers to specify a **document type definition** (DTD)or **schema** in order to devise new markup languages for general or specific uses. Some examples of languages made with

XML include **Extensible Hypertext Markup Language** (XHTML), which reproduces the functionality of **Hypertext Markup Language** (HTML), and **Electronic Recording Markup Language** (ERML), which allows the creation of documents for use in electronic recording. XML, which shares some similarities with **Standard Generalized Markup Language** (SGML), was created by the **World Wide Web Consortium** (W3C) to facilitate information exchange.

Extensible Stylesheet Language (XSL): A computer language that can be used to translate between one **Extensible Markup Language** (XML) language to another. XSL is especially useful in electronic commerce applications to convert information from one format to another, facilitating the easy translation of document types for use with different software tools.

FAQ: Pronounceable acronym: *FACK*. See **frequently asked questions**.

file transfer protocol (FTP): A standard method used for sending and receiving files over the Internet. This protocol can be used within a **browser** or in a special FTP **client**.

frequently asked questions (FAQ): A list of questions and answers on a given topic. FAQs began as a standard in newsgroups, attempting to anticipate the needs of new members in an effort (sometimes vain) to reduce the numerous repetitive questions from less-informed users. FAQs are now a staple of web information, and it is possible to find FAQs on the web dealing with just about every topic imaginable.

front end: In the software industry, a program or part of a program that enables user interaction. With standard software applications, the front end is often a **graphical user interface** (GUI), or command-line interface. For client-server applications, the front end is a **client** program, and **back end** functions are provided by a **server**. See also **application service provider**.

FTP: See **file transfer protocol**.

graphical user interface (GUI): A visual platform that allows a computer user to activate and perform computer commands by manipulating virtual "tools" with a pointing device or keyboard. GUIs are distinct from command-line interfaces, which respond to text-based commands. Apple's Macintosh computer offered the first popular computer GUI, and set the standard for all user interfaces to come. Other popular GUIs include the interface for Microsoft's Windows operating systems and XWindows for Linux. GUIs commonly include a desktop, icons, windows, menus, and a pointer.

GUI: Pronounceable acronym: *GOO-ee*. See **graphical user interface**.

hash function: A mathematical algorithm that takes an **electronic document** and creates a **document fingerprint**, or *message digest*. The document fingerprint is much smaller than the original document, and does not allow the reconstitution of the original document from the fingerprint. A slightly different document, processed through the same hash function, would produce a very different document fingerprint. A hash function helps to secure data by providing a way to ensure that data is not tampered with. Also *one-way hash*.

HTML: See **Hypertext Markup Language**.

HTTP: See **hypertext transfer protocol**.

hypertext: A method of organizing information that allows the construction of **links** between related topics. The word *hypertext* belies its origins in text documents, where words and phrases would link to other words and passages in the same document or in other documents. For example, clicking on a word might bring up a definition, and clicking on a quotation would reveal the passage in the quoted original. On the **World Wide Web** today, hypertext provides a rich media experience, in which text, images, audio, and

video can all be interconnected. For example, clicking on a word can bring up an illustration, and clicking on a video clip of a movie preview can load a new page offering the video for sale.

Links in web-based hypertext documents are achieved using either **HTML** or **XHTML**.

Hypertext Markup Language (HTML): A computer language used to create web pages. HTML is composed of **tags**, special codes that help a web **browser** format the web page for display. The language is simple enough for grade schoolers to use, yet complex enough to describe very complex layouts and styles.

hypertext transfer protocol (HTTP): A system of messages and replies that allows computers to communicate on the Internet. The protocol defines the format and transmission methods for messages, specifying how browsers and servers should respond to the commands. HTTP is the predominant technology used to transport web pages from servers to **client** machines, to be displayed in **browsers**.

IIS: See **Internet Information Server**.

infinite loop: See **loop, infinite**.

Internet: The world's largest network of computers, consisting of interconnected **local area networks** (LANs), linked using **transmission control protocol/internet protocol** (TCP/IP) communication methods. The two biggest uses for the Internet include the **World Wide Web**, which is accessed using web **browsers**, and e-mail, which is accessed using e-mail **client** software. Some other uses of the Internet include newsgroups and the ability to download files and programs using the **file transfer protocol** (FTP).

The Internet actually began in the 1960s as a networking project of the Defense Advanced Research Projects Agency (DARPA) of the U.S. Department of Defense. The network, originally called ARPANet, grew steadily, with government agencies, universities, and

various companies making contributions. The project was officially decommissioned in 1990, and after five years of management by the National Science Foundation (NSF), became a public entity in 1995.

Internet Information Server (IIS): A Microsoft-branded web server designed to run on Windows NT. IIS's tight integration with the NT operating system makes it a relatively easy server platform to manage. Despite the widespread use of Windows on the desktop, the vast majority of Internet servers use a UNIX-based operating system. Because of this, IIS is relegated to second place (with about 20% of all Internet servers), behind the open-source Apache server (with about 60% of all Internet servers).

internet protocol (IP): A standard that defines how information is passed among different systems across the Internet. IP defines methods for creating *packets* (little chunks of data), and the addressing scheme for getting the packets from one place to another. The system is like a digital postal system. A message is broken into little pieces (*packetized*) and each packet is put into a separate "digital envelope," addressed, and sent on its way. As the packets are handled by Internet routers—the "postal agents" of the networking world—the addresses indicate where the information needs to be sent.

internet protocol address (IP address): A set of numbers that identifies a computer within a specific network environment. IP addresses are "stamped" onto data packets—the little chunks of data that are sent back and forth across the Internet—to tell servers and routers where to send them. The addresses themselves are represented as four numbers separated by periods, such as 192.168.1.12.

Internet service provider (ISP): A local or national organization that offers public access to the Internet, often as a fee-based service. The firms commonly provide a dial-up connection to the Internet, e-mail, and web page hosting. Some of the more popular ISPs include America Online, CompuServe, and EarthLink.

intranet: A private network, generally owned and controlled by a single company or other organization, that provides web-like access to proprietary information. The information hosted on an intranet is accessed using a web browser and can appear like a standard web page. Some of the technologies involved in intranets include **hypertext transfer protocol** (HTTP) and **transmission control protocol/internet protocol** (TCP/IP). Unlike the **World Wide Web**, intranet content is accessible only to authorized members, generally an organization's employees or other affiliates. Institutional intranets are growing in popularity because they are less expensive to build and manage than private networks.

IP: See **internet protocol**.

IP address: See **internet protocol address**.

ISP: See **Internet service provider**.

key pair: A set of keys, including a **private key** and a **public key**, used in **asymmetric cryptography**. Sometimes a key pair will be reserved for specific uses, such as creating digital signatures (**signing pair**) or encrypting secret information (**encryption pair**).

LAN: Pronounceable acronym: *LAN* (rhymes with *man*). See **local area network**.

link: "Hot spots" on a web page that allow a user to navigate to another section of the same document or to another document elsewhere on the Web. In text, links generally appear as underlined or colored words or phrases. Images can also serve as links, and often appear as buttons or tabs. Links can also be placed in other types of content, such as video clips and interactive documents created with Flash and Shockwave.

local area network (LAN): A computer network contained in a relatively small area. Most LANs are institutional, established within a company, school, or other physical location in a single

building or group of buildings. The different computers connected to a LAN are known as *nodes* or **clients**. Most LANs use **Ethernet** to connect all of the nodes.

loop, infinite: See **infinite loop**.

message digest: See **document fingerprint**.

modem: An electronic device that enables a local computer to communicate with other computers over telecommunication lines. A modem is the most common device used by home computers to connect to the Internet. *Dialup modems* plug into a phone jack, and can connect at speeds up to 56 kilobits per second. Faster *cable modems* are also available that connect to the Internet using larger connection lines. Note that the word modem is a shortened version of *mo*dulator/*dem*odulator.

National Conference of Commissioners on Uniform State Laws (NCCUSL): An organization of more than 300 attorneys, judges, and law professors, working together to draft proposals for uniform state legislation. The NCCUSL is a non-profit unincorporated association that can only propose laws; their proposals do not become state law until adopted by state legislatures.

NCCUSL: See **National Conference of Commissioners on Uniform State Laws**.

network: The wires, routers, and other hardware that connect two or more computers. Networks allow computer users to share files, programs, and other resources. See also **local area network**, **wide area network**, **Internet**, **intranet**.

nonrepudiation: Effectively implementing a process in such a way that the creator of a **digital signature** cannot deny having created it. Nonrepudiation involves supplying enough evidence about the identity of the signer and the integrity of a message so that the origin, submission, delivery, and integrity of the message cannot be denied. Protection of a user's **private key** is also a crucial factor in

ensuring nonrepudiation. The entire **Public Key Infrastructure** (PKI) industry exists to create and ensure the trust necessary for nonrepudiation.

notarization: See **acknowledgement**.

notary public: A public official with the authority to acknowledge a **signature** on a document. The **acknowledgement** takes the form of an embossed seal (for paper documents) or a special **digital signature** (for **electronic documents**), and certifies that the signer was identified and was acting voluntarily, without coersion. Depending on state law, notaries public might also take depositions, issue subpoenas, and administer oaths. Though notaries are government functionaries, most work in private industry. Also *notary*.

offline: Not connected to a computer network, or more specifically, not connected to the Internet. A computer that has been disconnected, or even turned off, is considered offline. Likewise, a person who is physically or metaphorically disconnected is also offline. *Offline* is also sometimes used metaphorically to indicate a discussion to be held outside of the immediate context.

one-way hash: See **hash function**.

online: Connected to a computer network, or more specifically, connected to the Internet. A computer configured to access the Internet is considered online. Likewise, a person using an online computer—or a person who habitually uses Internet applications—is also considered online.

operating system (OS): A program that coordinates the basic resources of a computer. Operating systems manage the workings of internal devices like memory, hard drives and processors, as well as external devices such as keyboards, monitors, and pointing devices. Some of the more popular operating systems for personal computers include Mac OS,

Microsoft Windows, LINUS, and DOS. Some others include UNIX (of which there are several varieties), OS/2, and Palm OS (used for handheld computers). Most computerized devices—including cell phones, camcorders and even automobiles—have some sort of operating system.

OS: See **operating system**.

PKI: See **Public Key Infrastructure**.

private key: A large, randomly generated prime number used in **asymmetric encryption**. The private key is used to encrypt a **document fingerprint** (the result of processing an **electronic document** through a **hash function**) to create a **digital signature**. A private key is generated by its holder at the same time a related **public key** is created. While the public half of a **key pair** is made available to anyone who wants it, the private key is only known by its owner, who must keep it absolutely secret to maintain its integrity.

protocol: Within the computer industry, rules of communication that must be followed in order for machines and programs to successfully communicate with each other. A protocol is a communication standard, and can be either open or proprietary.

public key: A large, randomly generated prime number that is used to **decrypt** an **electronic document** that has been encrypted with a **private key**. A public key is generated by its holder at the same time a related private key is created. Within the Public Key Infrastructure (PKI), public keys are used to verify **digital signatures**. Public keys are contained in **digital certificates**, published and otherwise distributed by the issuing **certificate authority** (CA).

public key cryptography: See **asymmetric cryptography**.

Public Key Infrastructure (PKI): The framework of different entities working together to create trust in electronic transactions. The PKI industry facilitates signed transactions by using

asymmetric cryptography to ensure security and verifiable authenticity. The PKI includes all parties, policies, agreements, and technologies involved in the following:

1. Identifying a person based on that person's **private** and **public keys** (**key pair**)
2. Binding public key information to a **digital certificate**
3. Issuing, disseminating, validating, and administering digital certificates
4. Ensuring the security of private keys
5. Promoting the integrity, manageability, and cost-effectiveness of the infrastructure

This sophisticated infrastructure allows all concerned parties to trust electronic transactions created within the standards set by the PKI industry.

public repository: An online library, maintained by a **certificate authority** (CA), that allows public access to its subscribers' **digital certificates**. To perform authentication on a **digital signature**, it is necessary to retrieve the signer's digital certificate (which contains his or her **public key**) from the repository. See also **signature authentication**.

RA: See **registration authority**.

registration authority (RA): A company or individual delegated by a **certificate authority** (CA) to verify the identity of **digital certificate** applicants. The RA looks at different forms of personal identification, and can use other methods—such as personal knowledge and credible references—to perform its responsibility. Once the applicant has been adequately identified, the RA makes a recommendation to the CA regarding whether or not to issue a certificate.

relying party: A person or entity who receives an electronic transaction containing a **digital signature** and **digital certificate**, and relies on the signer's **public key** to verify it.

root CA certificate: See **root certificate authority**.

root certificate authority certificate (root CA certificate): The top level of trust for **certificate authorities** (CA). When a person creates a document with a **digital signature**—created with a key linked to a **digital certificate**—people put trust in the certificate because the certificate itself contains the signature of the person or entity that issued and endorsed it. This chain of signatures and certificates goes up to a root CA certificate, which is signed by the person or company that created it. The root CA certificate functions as a sort of "charter of trust," enabling the certificate authority to lend that trust to its subscribers by issuing certificates. It is then up to the CA to live up to that trust by setting and following sound business practices.

schema: A method for specifying the structure and content of specific types of electronic documents which use **Extensible Markup Language** (XML). Schemas and **document type definitions** (DTDs) share some similarities, but have some important differences. A schema is created in XML, while a DTD uses **Standard Generalized Markup Language** (SGML). In addition, schemas provide much stronger "data typing," allowing the developer to be very specific in the types of data that can fill the fields in a defined document.

secure sockets layer (SSL): A security technology that uses both **asymmetric** and **symmetric cryptography** to protect data transmitted over the Internet. Here is what happens when a user connects to an SSL **server**:

1. Upon recognizing the SSL protocol, the user's browser generates a random **session key**, which will be used on both ends to protect the transmission.
2. The browser downloads the server's **digital certificate**, from which it retrieves the **public key**. This key is used to encrypt a copy of the session key.
3. The encrypted session key is sent to the SSL server, which uses its **private key** to decrypt the session key.

4. Since the session key is now known on both ends, all subsequent communication is protected with symmetrical encryption, using the session key as the password.

Essentially an "invisible" technology, SSL is involved in most online transactions involving credit card numbers and other protected information. The secure nature of the connection is indicated in a URL with the prefix *https*.

server: A computer that is used to control software resources and deliver data and services to other computers on the network. The name comes from the fact that they "serve up" information when requested. A server is generally an advanced computer that is designed to be less prone to mechanical failure or downtime, often featuring multiple power supplies, drives, and processors.

session key: A "disposable" password that is randomly generated and used to encrypt information transferred between a **client** computer and a **server** during a single communication session using **secure sockets layer** (SSL) technology.

SGML: See **Standard Generalized Markup Language**.

signature: A mark or sign that identifies a person as part of a transaction. In the paper world, a signature is generally a person's handwritten name. So-called **wet signatures**—created with pen and ink—are often highly stylized, ostensibly to help prevent forgery. In the digital world, a **digital signature** is the result of encrypting a **document fingerprint** (or *message digest*) using a person's **private key**.

signature authentication: The process by which a **digital signature** is used to confirm a signer's identity and a document's validity. Authenticating a **signed digital document** involves four steps:

1. The signer's **digital certificate** is obtained from his or her **certificate authority**'s (CA's) **online repository**. The certificate itself is **authenticated** to ensure that the certificate has not expired and has not been revoked.
2. The signer's **public key** is obtained from the retrieved digital certificate.
3. This public key is used to decrypt the digital signature, unlocking the **document fingerprint** hidden inside. The document fingerprint validates the signer's identity, since the message must have been encrypted with the matching public key.
4. A **hash function**—the same one used to create the first document fingerprint—is applied to the original document. The result is a second document fingerprint.
5. The two document fingerprints are compared. If they match, the document is considered valid because it is identical to the one used in signing.

See also **asymmetric cryptography**.

signed digital document: An **electronic document** that includes an embedded **digital signature**. The digital signature contains an encrypted **document fingerprint** (or *message digest*), which allows anyone receiving the document to verify its validity using the process of **signature authentication**.

signing function: A mathematical algorithm that uses a signer's private key to encrypt a **document fingerprint** (or *message digest*). The result is a **digital signature**. See also **hash function**.

signing pair: A **digital identification**, consisting of a **digital certificate** (containing a **public key**) and a **private key**, reserved specifically for creating **digital signatures**. See also **encryption pair**.

site: See **website**.

smart card: A small plastic card (the size and shape of a credit card) with an embedded token that holds digital data. Smart cards are

employed in a number of different security technologies. In **Public Key Infrastructure** (PKI) applications, smart cards are used to store private keys and digital certificates. These cards require a card reader to retrieve the stored key, which is usually also protected by a secret password.

SSL: See **secure sockets layer**.

Standard Generalized Markup Language (SGML): One of the first tagging language environments. SGML was created to fill the publishing industry's need for a uniform way to define electronic printing specifications (such as font, type size, and special formatting). SGML contains specifications, tools, and language syntax. SGML is used to create **document type definitions** (DTDs), which include lists of tags and tag attributes. Each document type definition describes a unique markup language, such as **Hypertext Markup Language** (HTML).

symmetric cryptography: A method for protecting sensitive information through the use of a single key to encrypt and decrypt. Symmetric cryptography requires a "shared secret" to work—the encryption key must be somehow given to the person who will decrypt the data. An example of symmetric cryptography is the password protection used on a word processor document. Though symmetric cryptography works well in a two-party system, it is not less secure when a great number of people are involved. The more the secret key is distributed, the greater the likelihood that security will be compromised. See also **asymmetric cryptography**.

symmetric encryption: See **symmetric cryptography**.

tag: A code used to mark a specific section of a hypertext document. A tag can mark an entire document, or a specific block, paragraph, phrase, or word. Tags are enclosed in angle brackets (< and >), and generally occur in pairs. For example, the tags and are used in **Hypertext Markup Language** (HTML) to indicate boldface type.

tagged information file format (TIFF): An image file format commonly used for photos, scanned documents, or other graphics. TIFF images are *raster* graphics rather than *vector* graphics, meaning that they are made up of individual dots or pixels. TIFF graphics can be created in any resolution; they can be color, grey-scaled, or black and white. Files in the TIFF format are distinguished by a .tif filename extension.

TCP/IP: see **transmission control protocol/internet protocol**.

template: A document that contains boilerplate text, formatting, and fill-in-the-blank fields. A good example of a paper-based template would be any of the do-it-yourself legal forms available at office supply stores. Online document templates are often interactive, requesting the required information and then returning a completed document.

three-letter acronym (TLA): A standard for abbreviation within the computer industry. While there are some notable exceptions (TIFF, IP), most computer acronyms include the three initials of a three-word term. Some are pronounced as individual letters (ASP, ISP, SSL, TCP) while others eventually become pronounceable as words (FAQ, GUI, LAN, WAN).

TIFF: See **tagged information file format**.

TLA: See **three-letter acronym**.

transmission control protocol/internet protocol (TCP/IP): A group of communication standards (TCP and IP) used to send and receive information across a computer network. TCP/IP is the main enabling technology used on the Internet. IP deals with the way information is *packetized* (broken up into small chunks of data) and *addressed* (marked for forwarding to a specific destination). TCP enables connections between two computers, and provides methods to make sure that packetized data gets from one to the other intact, and in the correct order.

UETA: Pronounceable acronym: *yoo-EE-tuh*. See **Uniform Electronic Transactions Act**.

Uniform Electronic Transactions Act (UETA): A body of recommended legislation drafted in 1999 by the **National Conference of Commissioners on Uniform State Laws** (NCCUSL) for adoption by state legislatures. UETA allows electronic documents and digital signatures to stand as equals with their paper counterparts. As of May 2001, 30 states had adopted UETA in some form, and the legislation was in consideration in 16 more states, the District of Columbia, and the US Virgin Islands.

uniform resource locator (URL): An Internet address system that allows **browser** or other Internet software to locate and retrieve specific web sites and web pages. A typical URL format is: http://www.domainname.com/location/page.html. See also **domain name**.

universal serial bus (USB): A standard for connecting external peripheral devices (hard drives, keyboards, pointing devices, and so on) to computers. A *bus* is simply a collection of wires through which information is transmitted from one part of a computer to another. A USB-equipped computer will generally have one or two *ports*, or *sockets*, that allow devices to be plugged in.

USB facilitates data transfer at a rate of up to 12 million bits per second. One bus can handle up to 127 peripheral devices. Originally developed by Intel, USB entered the commercial computer world in 1996, gaining general acceptance by 1998. Almost every desktop computer manufactured today offers USB connectivity as standard equipment.

URL: See **uniform resource locators**.

USB: See **universal serial bus**.

USB token: A device—about the size of a house key—that connects to a computer's USB port. Based on **smart card** technology, a USB token contains a microchip capable of storing confidential information, such as a person's **private key**. As with

smart cards, information on USB tokens is often protected with a secret password.

user ID: A unique alphanumeric text string used to identify one's self on a computer. A user ID is often used to log on to a computer system or network. A user ID is sometimes simply a person's name. Alternately, some systems use the text that comes before the @ in an email address (for example, *jsmith* in *jsmith@somecompany.com*).

username or **user name:** See **user ID**.

validation: A process by which a digitally signed document is **authenticated** and then checked for validity based on specific external requirements. During **signature authentication**, the embedded **digital signature** is decrypted using the signer's **public key**, to verify the signer's identity and the document's integrity. The second part of the process involves making sure that the document follows a specific set of conventions. For example, the document must have the required elements, and all information must be in the correct format.

W3C: See **World Wide Web Consortium**.

WAN: Pronounceable acronym: *WAN* (rhymes with *man*). See **wide area network**.

web: See **World Wide Web**.

web browser: See **browser**.

website: A page or collection of pages—usually thematically related or contained on the same server—available on the **World Wide Web**. The main page on a website is often called a *home page*. Also *site*.

wet signature: An original representation of person's name, written by hand with pen and ink, applied to a legal document. This type of signature is referred to as *wet* to distinguish it from other kinds of signatures: photocopies or facsimiles of handwritten signatures, **digital signatures**, **digitized signatures**, and so on. Wet signatures are

often highly stylized, sometimes bearing little resemblance to the name they are supposed to represent. The importance of handwritten signatures is that they are relatively difficult to forge, and thus a useful tool for **nonrepudiation**.

wide area network (WAN): A computer **network**—connected by telecommunication lines, radio waves, or satellite systems—occupying a relatively large geographical area. Generally a WAN will contain two or more **local area networks** (LANs). The **Internet** is the most extensive WAN in existence.

World Wide Web (WWW): A network of computers that uses the **hypertext transfer protocol** (HTTP) to enable access to a vast library of media content. Users view web pages using a web **browser**, a special software application that retrieves data and uses **HTML tags** to format it for display. Originally designed for text, the web now contains rich media such as video, audio, and special content like Flash and Shockwave. The World Wide Web's name derives from its intricate system of links, **URLs** embedded in **hypertext**, that allow pages to connect to each other. Credit for creating the World Wide Web is given to Tim Berners-Lee, who conceived it in 1989 while working at the European Laboratory for Particle Physics. Also *web*.

World Wide Web Consortium (W3C): The main controlling standards body of the web, founded by Tim Berners-Lee (who instigated the creation of the web) at the Massachusetts Institute of Technology in October 1994. The W3C is committed to creating and promoting compatible technologies (specifications, guidelines, software, and tools) to lead the Web to its full potential as a forum for information, commerce, communication, and collective understanding.

WWW: See **World Wide Web**.

XHTML: See **Extensible Hypertext Markup Language**.

XML: See **Extensible Markup Language**.

XSL: See **Extensible Stylesheet Language**.