Digital Signature Guidelines

Legal Infrastructure for Certification Authorities and Secure Electronic Commerce

August 1, 1996

Information Security Committee

Electronic Commerce and Information Technology Division

Section of Science and Technology

American Bar Association

ISBN 1-57073-250-7
Printed in the United States of America

Contents

I. Introduction

The Information Security Committee

These Digital Signature Guidelines have been drafted by the Information Security Committee of the Electronic Commerce Division, Section of Science and Technology of the American Bar Association. The Committee explores legal and information security aspects of electronic commerce and other issues related to information technology. The Information Security Committee is comprised of lawyers, government policy and management professionals, information technology and security professionals, notaries from various legal systems, trade facilitation experts, and others.

Information about membership in and publications of the Section of Science and Technology and the American Bar Association is available from Manager, Section of Science and Technology, American Bar Association, 750 North Lake Shore Drive, Chicago, IL 60611 USA, (312) 988-5599, Fax (312) 988-5628, E-mail sciencetech@attmail.com.

The following have participated in the drafting of the Digital Signature Guidelines, a project which has spanned more than four years from 1992 to the current time:

Digital Signature Guidelines - Editorial Committee Members

Committee Chair	Michael Baum, Esq. - VeriSign, Inc.
CommitteeVice Chair	Ruven Schwartz, Esq. - West Publishing Company
Reporter for Guidelines	Alan Asay, Esq. - CertCo, formerly the State of Utah
Reporter for Guidelines	Charles Merrill, Esq. - McCarter & English
Reporter for Guidelines	Joseph Wackerman, Esq. - United States Postal Service
	Ted Barassi, Esq. - CertCo, formerly US Council for International Business
	Charles Miller, Esq - Attorney, San Francisco
	Randy Sabett - Spyrus, Inc.
	Frank Sudia - CertCo, formerly Banker's Trust Co.

Digital Signature Guidelines - Contributing Members

Maureen Adamache, Esq. - Canada Dept of Justice
Richard Ankney - Fischer International, Inc.
Christine Axsmith, Esq. - US Dept of State
Stewart Baker, Esq. - Steptoe & Johnson
Kenneth Bass, Esq. - Venable and Baetjer
Bill Bryant, Esq. - Katz Kutter
Hal Burman, Esq. - US Dept of State
Bartlett Cleland, Esq - Aide to Sen Ashcroft (MO)
Michel Cloutier - Govt of Quebec
Robert Daniels - US Social Security Admin
George Danielson - State of Utah
Harold Deal - NationsBank
John Doktor - Los Angeles County
Tony Dunford, Esq. - Notaries' Society (England)
Deborah Enix-Ross, Esq. - US Cncl for Internatl Bus
William Ensing, Esq - Attorney, Lake Forest, IL
Richard Field, Esq - Attorney, Cliffside Park, NJ
Warwick Ford - Consultant, formerly Nortel
Yair Frankel - Sandia National Laboratories
Gary Fresen, Esq. - Baker & McKenzie
Michael Froomkin, Esq. - Univ of Miami Law School
Lawrence Greene, Esq. - International Law Institute
The Hon. Peter Greenlee, Esq. - Social Security Adm
Daniel Greenwood, Esq. - Commonwealth of Mass.
Andrew Grosso, Esq - Attorney, Washington, DC
Michael Hale, Esq. - Georgia Secy of State's Office
Barbara Harriman-Pauls, Esq. - AT&T
Peter Harter, Esq. - Netscape Communications Corp.
Thomas Hermann, Esq. - Squire Sanders & Dempsey
Skip Hirsh, Esq. - Certicom
Thomas Hopcroft, Esq - Attorney, Boston MA
Rick Hornbeck - Computer Sciences Corp
Russell Housley - Spyrus, Inc.
Noel Humphreys, Esq. - Sills Cummis
Steven Jensen - Commonwealth of Mass
Robert Jueneman - Novell, formerly GTE
Dale Juffernbruch, Esq. - Household Bank
William Kennair, Esq. - Soc Public Notaries of London
Stephen Kent - BBN Communications
Stan Kurzban, Esq - Attorney, Chappaqua, NY
Susan Laniewski, Esq. - Unisys, formerly NCSC
David Levy, Esq. - International Law Institute
Kenneth Lobenstein, Esq. - Allegheny Co Court, PA
Ulrich Lohmann, Esq - Attorney, Munich
Patrice Lyons, Esq. - Attorney, WashingtonDC
Karen Lyter - Natl Automated Clearing House Assn
David Maher, Esq. -Sonnenschein Nath & Rosenthal
Angel Marrero, Esq. - McConnell Valdes (San Juan)
Mario Miccoli, Esq. - International Union of Latin Notaries (Italy)
Steven Mitchell - Manhattan Software
Sead Muftic - COST (Sweden)
Larry Nelson - AT&T
James Newel, Esq. - Freddie Mac
Dwight Olson - Data Securities International, Inc.
Serge Parisien, Esq. - Université de Montréal
Ira Parker, Esq. - Alston & Bird
Michel Peereman - Féd. Nationale des Chambres de Commerce et d'Industrie de Belgique
Claude Perreault, Esq. - Chambre des Notaires du Quebec
Al Piombino - Consultant, Portland Maine
John Porter, Esq. - Beneficial Mgmt Corp of America
Joe Robinson - US Postal Inspection Service
Peter Robinson - US Council for Internatl Business
Richard Rothwell - US Postal Service
Susan Sabett - National Security Agency
David Sanford - Mitretek Systems
John Seth, Esq. - Amer Society of Notaries Public
Lawrence Shomo - NASA
Mark Silvern - VeriSign, Inc.
Thomas Smedinghoff, Esq.- McBride Baker & Coles
Clint Smith, Esq. - Steptoe & Johnson
David Solo - BBN Communications
Kaushik Sriram, Esq, - Cons. Geophysicist, Houston
Deborah Thaw - National Notary Association
Milt Valera - National Notary Association
Mike Wims, Esq. - Utah Attorney General's Office
Chris Yukins, Esq. - Wiley Rein

Tutorial

In today's commercial environment, establishing a framework for the authentication[1] of computer-based information requires a familiarity with concepts and professional skills from both the legal and computer security fields. Combining these two disciplines is not an easy task. Concepts from the information security field often correspond only loosely to concepts from the legal field, even in situations where the terminology is similar. For example, from the information security point of view, "digital signature" means the result of applying to specific information certain specific technical processes described below. The historical legal concept of "signature" is broader. It recognizes any mark made with the intention of authenticating the marked document.[2] In a digital setting, today's broad legal concept of "signature" may well include markings as diverse as digitized images of paper signatures, typed notations such as "/s/ John Smith," or even addressing notations, such as electronic mail origination headers.

From an information security viewpoint, these simple "electronic signatures" are distinct from the "digital signatures" described in this tutorial and in the technical literature, although "digital signature" is sometimes used to mean any form of computer-based signature. These Guidelines use "digital signature" only as it is used in information security terminology, as meaning the result of applying the technical processes described in this tutorial.

---

[1] For purposes of these Guidelines, authentication is generally the process used to confirm the identity of a person or to prove the integrity of specific information. More specifically, in the case of a message, authentication involves determining its source and providing assurance that the message has not been modified or replaced in transit. *See* Guideline 28 (authentication).

[2] *See, e.g.,* U. C. C. § 1-201(39) (1992).

To explain the value of digital signatures in legal applications, this tutorial begins with an overview of the legal significance of signatures. It then sets forth the basics of digital signature technology, and examines how, with some legal and institutional infrastructure, digital signature technology can be applied as a robust computer-based alternative to traditional signatures.

Signatures and the Law

A signature is not part of the substance of a transaction, but rather of its representation or form. Signing writings serve the following general purposes:[3]

[3] This list is not exhaustive. For example, RESTATEMENT (SECOND) OF CONTRACTS notes another function, termed the "deterrent function," which seeks to "discourage transactions of doubtful utility." RESTATEMENT (SECOND) OF CONTRACTS § 72 comment c (1981). Professor Perillo notes earmarking of intent, clarification, managerial efficiency, publicity, education, as well as taxation and regulation as functions served by the statute of frauds. Joseph M. Perillo, *The Statute of Frauds in the Light of the Functions and Dysfunctions of Form*, 43 FORDHAM L. REV. 39, 48-64 (1974) (hereinafter "Perillo").

- **Evidence**: A signature authenticates a writing by identifying the signer with the signed document. When the signer makes a mark in a distinctive manner, the writing becomes attributable to the signer.[4]

- **Ceremony**: The act of signing a document calls to the signer's attention the legal significance of the signer's act, and thereby helps prevent "inconsiderate engagements."[5]

- **Approval**: In certain contexts defined by law or custom, a signature expresses the signer's approval or authorization of the writing, or the signer's intention that it have legal effect.[6]

- **Efficiency and logistics**: A signature on a written document often imparts a sense of clarity and finality to the transaction and may lessen the subsequent need to inquire beyond the face of a document.[7] Negotiable instruments, for example, rely

---

[4] *See* RESTATEMENT (SECOND) OF CONTRACTS, statutory note preceding § 110 (1982) (summarizing purpose of the statute of frauds, which includes a signature requirement); Lon L. Fuller, *Consideration and Form*, 41 COLUM. L. REV. 799, 800 (1941) (hereinafter "Fuller"); 6 JEREMY BENTHAM, THE WORKS OF JEREMY BENTHAM 508-85 (Bowring ed. 1962) (1839) (Bentham called forms serving evidentiary functions "preappointed [*i.e.*, made in advance] evidence"). A handwritten signature creates probative evidence in part because of the chemical properties of ink that make it adhere to paper, and because handwriting style is quite unique to the signer. Perillo, *supra* note 3, at 64-69. *See* U. C. C. § 1-201(39) ("'Signed' includes any symbol executed or adopted by a party with present intention to authenticate a writing.").

[5] 2 JOHN AUSTIN, LECTURES ON JURISPRUDENCE 939-44 (4th ed. 1873); RESTATEMENT (SECOND) OF CONTRACTS § 72 comment c (1982) and statutory note preceding § 110 (1982) (what is here termed a "ceremonial" function is termed a "cautionary" function in the Restatement); Perillo, *supra* note 3, at 53-56; Fuller, *supra* note 4, at 800; RUDOLF VON JHERING, GEIST DES RÖMISCHEN RECHTS § 45, at 494-98 (8th ed. 1883) (hereinafter "JHERING").

[6] *See Model Law on Electronic Commerce*, United Nations Commission on International Trade Law (UNCITRAL), 29th Sess., art. 7(1), at 3, U.N. Doc. A/CN.9/XXIX/CRP.1/Add.13 (1996) ("Where a law requires a signature of a person, that requirement is met in relation to a data message if: (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message...."); *Draft Model Law on Legal Aspects of Electronic Data Interchange (EDI) and Related Means of Data Communication,*United Nations Commission on International Trade Law (UNCITRAL), 28th Sess., art. 6, at 44, U.N. Doc. A/CN.9/406 (1994). For example, a signature on a written contract customarily indicates the signer's assent. A signature on the back of a check is customarily taken as an endorsement. *See* U.C.C. § 3-204 (1990).

[7] *See* Perillo, *supra* note 3, at 50-53; Fuller, *supra* note 4, at 801-802; JHERING, *supra* note 5, at 494-97 (analogizing

> upon formal requirements, including a signature, for their ability to change hands with ease, rapidity, and minimal interruption.[8]

The formal requirements for legal transactions, including the need for signatures, vary in different legal systems, and also vary with the passage of time. There is also variance in the legal consequences of failure to cast the transaction in a required form. The statute of frauds of the common law tradition, for example, does not render a transaction invalid for lack of a "writing signed by the party to be charged," but rather makes it unenforceable in court,[9] a distinction which has caused the practical application of the statute to be greatly limited in case law.

During this century, most legal systems have reduced formal requirements,[10] or at least have minimized the consequences of failure to satisfy formal requirements. Nevertheless, sound practice still calls for transactions to be formalized in a manner which assures the parties of their validity and enforceability.[11] In

---

the form of a legal transaction to minting of coins, which serves to make their metal content and weight apparent without further examination). The notion of clarity and finality provided by a form are largely predicated on the fact that the form provides good evidence. The basic premise of the efficiency and logistical function is that a signed, written document is such a good indicator of what the transaction is, that the transaction should be considered to be as the signed document says. The moment of signing the document thus becomes decisive.

[8] *See, e.g.*, U.C.C. § 3-401 (1990) (a person is not liable on an instrument unless the person signed it); *see generally* U.C.C. § 3-104 (1990) (requirements for negotiability).

[9] 2 ARTHUR L. CORBIN, CORBIN ON CONTRACTS § 279, at 20-23 (1950). In English law, the original 1677 statute of frauds was repealed in 1954 by the Law Reform (Enforcement of Contracts) Act, 2 & 3 Eliz. II, c. 34, except for its suretyship and real property provisions. However, it remains in force throughout the United States and in much of the British Commonwealth outside the United Kingdom.

[10] *See* Perillo *supra* note 3, at 41-42. In Anglo-American law, there are many examples of the trend away from formal requirements. For example, the common law seal has little remaining significance. *See* RESTATEMENT (SECOND) OF CONTRACTS, statutory note preceding § 95 (1982). Case law has greatly limited the effects of the statute of frauds through the part performance doctrine, promissory and equitable estoppel (*e.g.* Monarco v. Lo Greco, 35 Cal. 2d 621, 220 P.2d 737 (1950) (Traynor, J.)), leniency in determining what constitutes a sufficient memorandum, and by permitting restitution and reformation of a contract within the statute of frauds. For a classic examination of the advantages and disadvantages of formal requirements, *see* JHERING, *supra* note 5, at 470-504.

[11] Michael Braunstein, *Remedy, Reason, and the Statute of Frauds: A Critical Economic Analysis*, 1989 UTAH L. REV. 383, 423-26 (1989); JHERING, *supra*, note 5, at 474 (inattention to legally appropriate form for expressing intent exacts its own consequences ("rächt sich selber")).

current practice, formalization usually involves documenting the transaction on paper and signing or authenticating the paper. Traditional methods, however, are undergoing fundamental change. Documents continue to be written on paper, but sometimes merely to satisfy the need for a legally recognized form. In many instances, the information exchanged to effect a transaction never takes paper form. Computer-based information can also be utilized differently than its paper counterpart. For example, computers can "read" digital information and transform the information or take programmable actions based on the information. Information stored as bits rather than as atoms of ink and paper can travel near the speed of light, may be duplicated without limit and with insignificant cost.

Although the basic nature of transactions has not changed, the law has only begun to adapt to advances in technology. The legal and business communities must develop rules and practices which use new technology to achieve and surpass the effects historically expected from paper forms.

To achieve the basic purposes of signatures outlined above, a signature must have the following attributes:[12]

- **Signer authentication**: A signature should indicate who signed a document, message or record,[13] and should be difficult for another person to produce without authorization.

[12] *Cf.* The U.S. Comptroller General's rationale for accepting digital signatures as sufficient for government contracts under 31 U.S.C. 1501(a)(1): "The electronic symbol proposed for use by certifying officers . . . embodied all of the attributes of a valid, acceptable signature: it was unique to the certifying officer, capable of verification, and under his sole control such that one might presume from its use that the certifying officer, just as if he had written his name in his own hand, intended to be bound." *In re National Institute of Standards and Technology — Use of Electronic Data Interchange to Create Valid Obligations*, file B-245714 (Comptroller Gen'l, 1991).

[13] In U.C.C. ART. 2B (May 3, 1996 Draft), "Record" is defined by § 2B-102(30) as "information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.." *See also, Model Law on Electronic Commerce*, United Nations Commission on International Trade Law (UNCITRAL), 29th Sess., art. 7(1), at 3, U.N. Doc. A/CN.9/XXIX/CRP.1/Add.13 (1996) ("Where a law requires a signature of a person, that requirement is met in relation to a data message if: (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message...."). Throughout these Guidelines "message" means the digital representation of information (generally, computer-based information), "document" means information inscribed on a tangible medium (generally paper-based information), and "record" can be used to refer to a message or to a document, consistent with the definition of "record" in U.C.C. § 2B-102(30), *supra*, this footnote.

- **Document authentication**:[14] A signature should identify what is signed,[15] making it impracticable to falsify or alter either the signed matter or the signature without detection.

Signer authentication and document authentication are tools used to exclude impersonators and forgers and are essential ingredients of what is often called a "**nonrepudiation service**" in the terminology of the information security profession. A nonrepudiation service provides assurance of the origin or delivery of data in order to protect the sender against false denial by the recipient that the data has been received, or to protect the recipient against false denial by the sender that the data has been sent.[16] Thus, a nonrepudiation service provides evidence to prevent a person from unilaterally modifying or terminating legal obligations arising out of a transaction effected by computer-based means.[17]

- **Affirmative act**: The affixing of the signature should be an affirmative act which serves the ceremonial and approval functions of a signature and establishes the sense of having

---

[14]Document authentication is similar to the security service of message integrity which provides assurance that the information signed has not been altered. *See* Guideline 35 (authentication).

[15]A paper signature identifies the signed matter less than perfectly. Ordinarily, the signature appears below what is signed, and the physical dimensions of the paper and the regular layout of the text are relied upon to indicate alteration. However, those mechanisms are not enough to prevent difficult factual questions from arising. *See, e.g.,* Citizens Nat'l Bank of Downers Grove v. Morman, 78 Ill. App. 3d 1037, 398 N.E.2d 49 (1979); Newell v. Edwards, 7 N.C. App. 650, 173 S.E.2d 504 (1970); Zions First Nat'l Bank v. Rocky Mountain Irrigation, Inc., 795 P.2d 658, 660-63 (Utah 1990); Lembo v. Federici, 62 Wash. 2d 972, 385 P.2d 312 (1963).

[16]*Information Technology - Security Frameworks in Open Systems - Non-Repudiation Framework* (also *ITU-T Recommendation X.813*), ISO/IEC 10181-4 (1996); WARWICK FORD, COMPUTER COMMUNICATIONS SECURITY: PRINCIPLES, STANDARD PROTOCOLS & TECHNIQUES 29-30 (1994) (1994) (hereinafter "FORD"); MICHAEL S. BAUM, FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY: LAW AND POLICY OF CERTIFICATE-BASED PUBLIC KEY AND DIGITAL SIGNATURES 9 (National Institute of Standards and Technology 1994) (hereinafter "BAUM"). Sender and recipient have a mutual incentive to use an authentication service to exclude disruption from third party intrusion, but a nonrepudiation service is used by sender or recipient adversely against the other, when one wishes to deny having made or received a communication and the other has an incentive to prove that it was made or received. *See* Charles R. Merrill, *A Cryptographic Primer*, THE INTERNET AND BUSINESS: A LAWYER'S GUIDE TO THE EMERGING LEGAL ISSUES 14 (Joseph F. Ruh, Jr., ed., The Computer Law Association 1996).

[17]A nonrepudiation service provides only proof of facts to defend against an opponent's effort to avoid a transaction. *See* BAUM, *supra* note 16, at 6 (1994). *See* Guideline 1.20 (nonrepudiation), particularly Comment 1.20.1.

legally consummated a transaction.

- **Efficiency**: Optimally, a signature and its creation and verification processes should provide the greatest possible assurance of both signer authenticity and document authenticy, with the least possible expenditure of resources.

Digital signature technology generally surpasses paper technology in all these attributes.[18] To understand why, one must first understand how digital signature technology works.

How Digital Signature Technology Works

Digital signatures are created and verified by cryptography, the branch of applied mathematics that concerns itself with transforming messages into seemingly unintelligible forms and back again. Digital signatures use what is known as "**public key cryptography**," which employs an algorithm using two different but mathematically related "**keys**;" one for creating a digital signature or transforming data into a seemingly unintelligible form, and another key for verifying a digital signature or returning the message to its original form.[19] Computer equipment and software utilizing two such keys are often collectively termed an "**asymmetric cryptosystem**."

The complementary keys of an asymmetric cryptosystem for digital signatures are arbitrarily termed the **private key**, which is known only to the signer[20] and used to create the digital signature,

[18]For a more thorough examination of properties desirable in a digital signature, *see generally* BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS AND SOURCE CODE IN C §2.6, 33-40 (2d ed. 1996) (hereinafter "SCHNEIER"); MITCHELL, PIPER & WILD, DIGITAL SIGNATURES, IN CONTEMPORARY CRYPTOLOGY: THE SCIENCE OF INFORMATION INTEGRITY 325, 341-46 (Gustavas Simmons ed., 1991).

[19]In contrast with public key cryptography, "conventional," "single key," or "symmetric cryptography" uses the same single key to "encrypt" "plaintext" into "ciphertext," and to "decrypt" it from ciphertext back to plaintext.

[20]Of course, the holder of the private key may choose to divulge it, or may lose control of it (often called "compromise"), and thereby make forgery possible. The Guidelines seek to address this problem in two ways, (1) by requiring a subscriber, who holds the private key, to use a degree of care in its safekeeping, and (2) enabling the subscriber to disassociate himself from the key by temporarily suspending or permanently revoking his certificate and publishing these actions in a "certificate revocation list," or "CRL". A variety of methods are available for securing the private key.

and the **public key**, which is ordinarily more widely known and is used by a relying party to verify the digital signature. If many people need to verify the signer's digital signatures, the public key must be available or distributed to all of them, perhaps by publication in an on-line repository or directory where it is easily accessible. Although the keys[21] of the pair are mathematically related, if the asymmetric cryptosystem has been designed and implemented securely[22] it is "**computationally infeasible**"[23] to derive the private key from knowledge of the public key. Thus, although many people may know the public key of a given signer and use it to verify that signer's signatures, they cannot discover that signer's private key and use it to forge digital signatures. This is sometimes referred to as the principle of "**irreversibility**."

Another fundamental process, termed a "**hash function**," is used in both creating and verifying a digital signature. A hash function is an algorithm which creates a digital representation or "fingerprint" in the form of a "**hash value**" or "**hash result**" of a standard length which is usually much smaller than the message but nevertheless substantially unique to it.[24] Any change to the

---

The safer methods store the private key in a "cryptographic token" (one example is a "smart card") which executes the signature program within an internal microprocessing chip, so that the private key is never divulged outside the token and does not pass into the main memory or processor of the signer's computer. The signer must typically present to the token some authenticating information, such as a password, pass phrase, or personal identification number, for the token to run a process requiring access to the private key. In addition, this token must be physically produced, and biometric authentication such as fingerprints or retinal scan can assure the physical presence of the token's authorized holder. There are also software-based schemes for protecting the security of the private key, generally less secure than hardware schemes, but providing adequate security for many types of applications. *See generally* SCHNEIER, *supra* note 18, at § 2.7, 41-44.

[21]Many cryptographic systems will function securely only if the keys are lengthy and complex, too lengthy and complex for a person to easily remember or use.

[22]*See generally* FORD, *supra* note 16, at 71-75; CHARLIE KAUFMAN, RADIA PERLMAN & MIKE SPECINER, NETWORK SECURITY: PRIVATE COMMUNICATION IN A PUBLIC WORLD 48-56 (1995) (hereinafter "KAUFMAN, ET AL., NETWORK SECURITY").

[23]"Computationally infeasible" is a relative concept based on the value of the data protected, the computing overhead required to protect it, the length of time it needs to be protected, and the cost and time required to attack the data, with such factors assessed both currently and in the light of future technological advance. *See generally*, SCHNEIER, *supra* note 18, at § 7.5, 166-67.

[24]*See generally* FORD, *supra* note 16, AT 75-84. COMPUTER COMMUNICATIONS SECURITY 75-84 (1994); KAUFMAN, ET AL., NETWORK SECURITY, *supra* note 22, at 101-27; Nechvatal, *Public Key Cryptography, in* COMTEMPORARY CRYPTOLOGY: THE SCIENCE OF INFORMATION INTEGRITY 179, 199-202 (Gustavas Simmons ed. 1991); SCHNEIER, *supra* note 18,

message invariably produces a different hash result when the same hash function is used. In the case of a secure hash function, sometimes termed a "**one-way hash function**," it is **computationally infeasible**[25] to derive the original message from knowledge of its hash value. Hash functions therefore enable the software for creating digital signatures to operate on smaller and predictable amounts of data, while still providing robust evidentiary correlation to the original message content, thereby efficiently providing assurance that there has been no modification of the message since it was digitally signed.

Thus, use of digital signatures usually involves two processes, one performed by the signer and the other by the receiver of the digital signature:

- **Digital signature creation** uses a hash result derived from and unique to both the signed message and a given private key. For the hash result to be secure, there must be only a negligible possibility that the same digital signature could be created by the combination of any other message or private key.

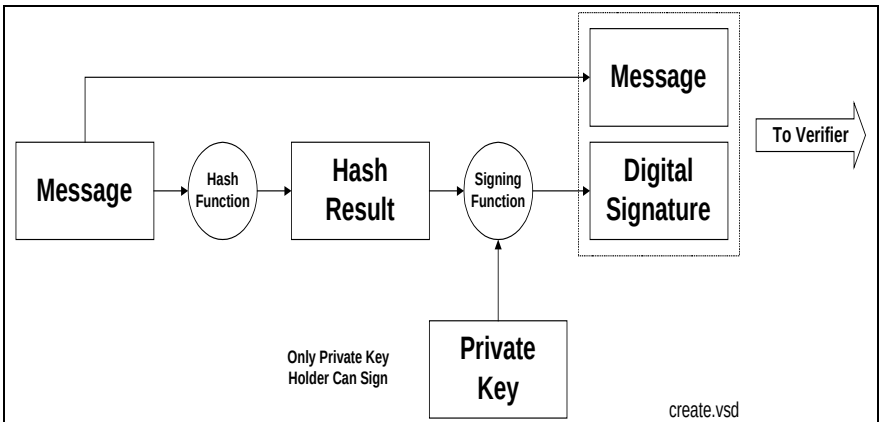
- **Digital signature verification** is the process of checking the digital signature by reference to the original message and a given public key, thereby determining whether the digital signature was created for that same message using the private key that corresponds to the referenced public key.

Figure 1 below describes the process of **digital signature creation**. To sign a document or any other item of information, the signer first delimits precisely the borders of what is to be signed. The delimited information to be signed is termed the "**message**" in these Guidelines. Then a hash function in the signer's software computes a hash result unique (for all practical purposes) to the

§§ 18.1-18.14, 429-459.

[25] "Because hash functions are typically many-to-one, we cannot use them to determine with certainty that the two [input] strings are equal, but we can use them to get a reasonable assurance of accuracy." SCHNEIER, *supra* note 18, at § 2.4, 30-31. It is extremely improbable that two messages will produce the same hash result. *See* KAUFMAN, ET AL., NETWORK SECURITY, *supra* note 22, at 102.

message. The signer's software then transforms the hash result into a digital signature using the signer's private key.[26] The resulting digital signature is thus unique to both the message and the private key used to create it.

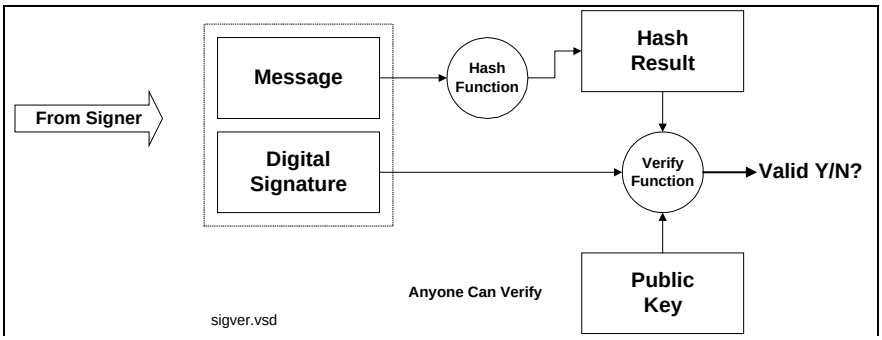


Typically, a digital signature (a digitally signed hash result of the message) is attached to its message and stored or transmitted with its message. However, it may also be sent or stored as a separate data element, so long as it maintains a reliable association with its message. Since a digital signature is unique to its message, it is useless if wholly disassociated from its message.

Verification of a digital signature, as illustrated in **Figure 2**, is accomplished by computing a new hash result of the original message by means of the same hash function used to create the digital signature. Then, using the public key and the new hash result, the verifier checks: (1) whether the digital signature was created using the corresponding private key; and (2) whether the newly computed hash result matches the original hash result which was transformed into the digital signature during the signing process. The verification software will confirm the digital signature as "**verified**" if: (1) the signer's private key was used to digitally sign the message, which is known to be the case if the signer's public key was used to verify the signature because the

[26] This transformation is sometimes described as "encryption," which is inaccurate terminology, because the message itself does not need to be confidential. Confidentiality can be provided as an optional feature of digital signature technologies, but the separate and distinct security service of confidentiality is not central to the security services of signer authentication and document authentication, and is thus outside the scope and focus of these guidelines.

signer's public key will verify only a digital signature created with the signer's private key;[27] and (2) the message was unaltered, which is known to be the case if the hash result computed by the verifier is identical to the hash result extracted from the digital



signature during the verification process.

Various asymmetric cryptosystems create and verify digital signatures using different algorithms and procedures, but share this overall operational pattern.

The processes of creating a digital signature and verifying it accomplish the essential effects desired of a signature for many legal purposes:

- **Signer authentication**: If a public and private key pair is associated with an identified signer, the digital signature attributes the message to the signer. The digital signature cannot be forged, unless the signer loses control of the private key (a "**compromise**" of the private key), such as by divulging it or losing the media or device in which it is contained.

- **Message authentication**: The digital signature also identifies the signed message, typically with far greater certainty and precision than paper signatures. Verification reveals any tampering, since the comparison of the hash results (one made at signing and the other made at verifying) shows whether the message is the same as when signed.

[27] Because of the mathematical relationship between the public and private keys which correspond to each other as a key pair. SCHNEIER, *supra* note 18, at § 2.6, 34-41.

- **Affirmative act**: Creating a digital signature requires the signer to use the signer's private key. This act can perform the "ceremonial" function of alerting the signer to the fact that the signer is consummating a transaction with legal consequences.[28]

- **Efficiency**: The processes of creating and verifying a digital signature provide a high level of assurance that the digital signature is genuinely the signer's. As with the case of modern electronic data interchange ("EDI") the creation and verification processes are capable of complete automation (sometimes referred to as "machinable"), with human interaction required on an exception basis only. Compared to paper methods such as checking specimen signature cards -- methods so tedious and labor-intensive that they are rarely actually used in practice -- digital signatures yield a high degree of assurance without adding greatly to the resources required for processing.

```
<Signed SigID=1>
          Promissory Note
I, Mary Smith, promise to pay to the
order of First Western Bank five
thousand dollars and no cents
($5,000) on or before June 10, 1998,
with interest at the rate of fifteen
per cent (15%) per annum.
                    Mary Smith, Maker
</Signed>
<Signature SigID=1 PsnID=smith082>
2AB3764578CC18946A29870F40198B240CD2
302B2349802DE002342B212990BA5330249C
1D20774C1622D39</Signature>
```

The processes used for digital signatures have undergone thorough technological peer review for over a decade. Digital signatures have been accepted in several national and international standards developed in cooperation with and accepted by many corporations, banks, and government agencies.[29] The likelihood of malfunction or a

[28] If the person "signing" the message is not a human being but a device under the control of a human being as permitted by these Guidelines, this ceremonial function may be undermined.

[29] As of this writing, the following jurisdictions have enacted or introduced some form of legislation dealing with digital signatures or electronic signatures:

security problem in a digital signature cryptosystem designed and implemented as prescribed in the industry standards is extremely remote,[30] and is far less than the risk of undetected forgery or alteration on paper or of using other less secure electronic signature techniques.

Public Key Certificates

To verify a digital signature, the verifier must have access to the signer's public key and have assurance that it corresponds to the signer's private key. However, a public and private key pair has no intrinsic association with any person; it is simply a pair of numbers. Some convincing strategy is necessary to reliably associate a particular person or entity to the key pair.

1996 Arizona House Bill 2444, amending ARIZ. REV. STAT. ANN. § 41-121 (1996) (enacted) (URL:http://www.azleg.state.az.us/legtext/42leg/2r/laws/0213.htm);
CAL. GOV'T CODE § 16.5 (West 1995) (enacted) (URL:http://www.sen.ca.gov);
CONN. GEN. STAT. § 19a-25a (1994) (enacted);
1996 FLA. Senate Bill 942 (enacted) (URL:http://www.scri.fsu.edu/fla-leg/senate-1996/sb0942er.html);
1995 GA. Senate Resolution 621 and House Resolution 1256 (pending); 1995 GA. Senate Bill 736 (died in committee);
1995 HAW. Senate Bill 2401(pending);
1995 ILL. House Bill 3394 (pending);
IOWA CODE § 48A.13 (1995) (enacted) (URL:http://www2.legis.state.ia.us/cgi-bin/IACODE/Code1995SUPPLEMENT.P1;
LA. REV. STAT. ANN § 40:2144 (West 1995) (enacted);
MICH. Senate Bill 939 (pending) (URL:http://www.coast.net/~misenate/dem/agenda/sig/sb939.html);
1995 N.Y. Senate Bill 7420 (pending) (URL:gopher.senate.state.ny.us);
1996 R.I. House Bill 8125 (pending);
UTAH CODE ANN. § 46:3 (1996) (URL:http://www.state.ut.us/ccjj/digsig/dsut-act.htm) ("Utah Digital Signature Act");
1996 VA. House Joint Resolution 129 (pending) (URL:http://www.state.va.us/dlas/ses19961/ful/hj129.htm);
1996 WASH. Senate Bill 6423 (URL:http://leginfo.leg.wa.gov/pub/billinfo/senate/);
1996 WYO. Senate File12 (URL:gopher://merlin.state.wy.us:70/00/wgov/lb/lb/session/BILLS/1995/Enrolled/Senate_Files/sf0012.frt).
Massachusetts is considering digital signature legislation. Telephone interview with Daniel Greenwood, Esq., Deputy General Counsel, Information Technology Division, Commonwealth of Massachusetts (July 19, 1996).
Germany and Chile are both considering digital signature legislation. *See generally*, on-line public discussion in E-Mail and Electronic Commerce Forum of Lexis Counsel Connect (Jan.-Mar. 1996).

[30] Although generally beyond the scope of these Guidelines, we note that current U.S. export restrictions, Department of State, "International Traffic in Arms Regulations (ITAR)," Office of Munitions Control, 22 C.F.R. §§ 120-130 (Nov. 1989), on software which possesses both confidentiality encryption and digital signature capability (or which can be converted into confidentiality encryption software) has caused software providers to intentionally emasculate ("dumb down") algorithms in some of their domestic as well as international products. This is considered by some to have cast doubt upon the "computational infeasibility" assumed by the standards, for digital signature as well as confidentiality encryption software. *See generally*, SCHNEIER, *supra* note 18, at § 25.14, 610-16.

In a transaction involving only two parties, each party can simply communicate (by a relatively secure "**out-of-band**" channel such as a courier or a secure voice telephone) the public key of the key pair each party will use. Such an identification strategy is no small task, especially when the parties are geographically distant from each other, normally conduct communication over a convenient but insecure channel such as the Internet, are not natural persons but rather corporations or similar artificial entities, and act through agents whose authority must be ascertained. As electronic commerce increasingly moves from a bilateral setting to the many-on-many architecture of the World Wide Web on the Internet, where significant transactions will occur among strangers who have no prior contractual relationship and will never deal with each other again, the problem of authentication/nonrepudiation becomes not merely one of efficiency, but also of reliability. An open system of communication such as the Internet needs a system of identity authentication to handle this scenario.

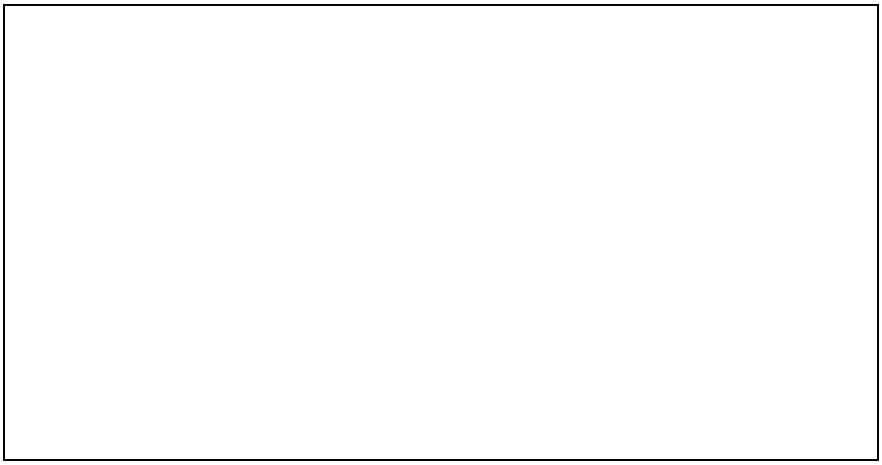
To that end, a prospective signer might issue a public statement, such as: "Signatures verifiable by the following public key are mine." However, others doing business with the signer may for good reason be unwilling to accept the statement, - especially where there is no prior contract establishing the legal effect of that published statement with certainty. A party relying upon such an unsupported published statement in an open system would run a great risk of trusting a phantom or an imposter, or of attempting to disprove a false denial of a digital signature ("**nonrepudiation**") if a transaction should turn out to prove disadvantageous for the purported signer.

The solution to these problems is the use of one or more **trusted third parties** to associate an identified signer with a specific public key.[31] That trusted third party is referred to as a "**certification authority**" in most technical standards and in these Guidelines.

To associate a key pair with a prospective signer, a certification authority issues a **certificate**, an electronic record which lists a public key as the "**subject**" of the certificate, and confirms that the prospective signer identified in the certificate holds the

[31] *See* SCHNEIER, *supra* note 18, at § 8.12, 185-7; BAUM, *supra* note 16, at 10-11; *See generally*, A. Michael Froomkin, *The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L. REV. 49 (1996).

corresponding private key. The prospective signer is termed the "**subscriber**."[32] A certificate's principal function is to bind a key pair with a particular subscriber. A "**recipient**" of the certificate desiring to rely upon a digital signature created by the subscriber named in the certificate (whereupon the recipient becomes a "**relying party**") can use the public key listed in the certificate to verify that the digital signature was created with the corresponding corresponding private key.[33] If such verification is successful, this chain of reasoning provides assurance that the corresponding private key is held by the subscriber named in the certificate, and



that the digital signature was created by that particular subscriber.

To assure both message and identity authenticity of the certificate, the certification authority digitally signs it. The issuing certification authority's digital signature on the certificate can be verified by using the public key of the certification authority listed in another certificate by another certificate authority (which may

[32]The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.

[33]The statement in the certificate of the beginning and ending date of the operational period of the certificate also allows a determination of whether or not a time-dated digital signature was created during the operational period of the certificate. A search of the certificate revocation list (CRL) also enables the verifier to determine the certificate has been revoked or suspended earlier than the end of the stated operational period of the certificate. *See* Guidelines 1.22 (operational period) and 1.37 (verify a digital signature).

but need not be on a higher level in a hierarchy)[34], and that other certificate can in turn be authenticated by the public key listed in yet another certificate, and so on, until the person relying on the digital signature is adequately assured of its genuineness. In each case, the issuing certification authority must digitally sign its own certificate during the operational period of the other certificate used to verify the certification authority's digital signature.

A digital signature, whether created by a subscriber to authenticate a message or by a certification authority to authenticate its certificate (in effect a specialized message) should be reliably time-stamped to allow the verifier to determine reliably whether the digital signature was created during the "**operational period**" stated in the certificate, which is a condition upon verifiability of a digital signature under these Guidelines.[35]

To make a public key and its identification with a specific subscriber readily available for use in verification, the certificate may be **published** in a **repository** or made available by other means. Repositories are on-line databases of certificates and other information available for retrieval and use in verifying digital signatures. Retrieval can be accomplished automatically by having the verification program directly inquire of the repository to obtain certificates as needed.

Once issued, a certificate may prove to be unreliable, such as in situations where the subscriber misrepresents his identity to the certification authority. In other situations, a certificate may be reliable enough when issued but come to be unreliable sometime thereafter. If the subscriber loses control of the private key ("compromise" of the private key), the certificate has become

[34] A number of models exist which implement different strategies for the certification of the public keys of certification authorities who issue certificates (sometimes referred to generically as "issuing authorities"). Some examples include (i) a multi-level hierarchical structure back to a single "root," where public keys of issuing authorities are certified by the next higher-level certification authority; (ii) a flatter hierarchical structure where a single "root" might directly certify the public keys of all issuing authorities below it; (iii) a single level of issuing authorities which "cross-certify" each others' public keys; or (iv) a "system in which each issuing authority's public key is certified in some reliable manner without reference to a second certification authority. In a hierarchical system, the public key of the "root" certification authority is, by definition, self-authenticating.

[35] A reliable time-stamp on the certificate also allows a determination as to whether it was created before or after the filing of a revocation or suspension of a certificate in a repository, which not only protects the subscriber who promptly revokes or suspends, but also provides increased assurance of nonrepudiatability by making it more difficult for a fraudulent subscriber to create a certificate and retroactively revoke it after reliance upon the certificate has occurred.

unreliable, and the certification authority (either with or without the subscriber's request depending on the circumstances) may **suspend** (temporarily invalidate) or **revoke** (permanently invalidate) the certificate. Immediately upon suspending or revoking a certificate, the certification authority must publish notice of the revocation or suspension or notify persons who inquire or who are known to have received a digital signature verifiable by reference to the unreliable certificate.

Challenges and Opportunities

The prospect of fully implementing digital signatures in general commerce presents both benefits and costs. The costs consist mainly of:

- **Institutional overhead**: The cost of establishing and utilizing certification authorities, repositories, and other important services, as well as assuring quality in the performance of their functions.

- **Subscriber and Relying Party Costs**: A digital signer will require software, and will probably have to pay a certification authority some price to issue a certificate. Hardware to secure the subscriber's private key may also be advisable. Persons relying on digital signatures will incur expenses for verification software and perhaps for access to certificates and certificate revocation lists (CRL) in a repository.

On the plus side, the principal advantage to be gained is more reliable authentication of messages. Digital signatures, if properly implemented and utilized offer promising solutions to the problems of:

- **Imposters**, by minimizing the risk of dealing with imposters or persons who attempt to escape responsibility by claiming to have been impersonated;

- **Message integrity**, by minimizing the risk of undetected message tampering and forgery, and of false claims that a message was altered after it was sent;

- **Formal legal requirements**, by strengthening the view that legal requirements of form, such as writing, signature, and an original document, are satisfied, since digital signatures are functionally on a par with, or superior to paper forms; and

- **Open systems**, by retaining a high degree of information security, even for information sent over open, insecure, but inexpensive and widely used channels.

II. Digital Signature Guidelines

Introduction to the Guidelines

The channels of commerce are rapidly being filled with computerized messages. Further, the channels themselves are being transformed. Inexpensive and accessible open networks are supplanting the formerly exclusive, expensive and limited-function communication channels. Since open networks are inherently less secure than the closed networks which they are replacing, secure electronic commerce increasingly depends upon securing the information itself, rather than relying upon the security of the channel.

Modern cryptography can make information safe from eavesdropping, tampering, or forgery, regardless of the security of a communication channel. With the legal and institutional infrastructure outlined in the foregoing tutorial, cryptographic technology can also authenticate a message by assuredly linking it to an identified person and guarding the message's integrity.

That legal and institutional infrastructure has been envisioned in a series of international standards. First, the International Consultative Committee on Telegraphy and Telephony (now International Telecommunication Union) laid in 1988 the technological foundation for authenticating computer-based information in its X.500 series of standards, particularly X.509. The Internet Architecture Board adopted similar standards for privacy-enhanced mail (PEM) in its RFC 1421-24 (1993). The National Institute of Standards and Technology has adopted Federal Information Processing Standard 186 (1994). The American Bankers Association is nearing completion of digital signature standards for adoption by the American National Standards Institute as American National Standards X9.30 and X9.31. For the electronic data interchange (EDI) community, a committee of the American National Standards Institute is drafting standard ANSI X12.58. For the medical community, the American Society of Testing and Materials Subcommittee on Electronic Authentication of Health Information has also drafted digital authentication guidelines known as ASTM E31.20. Further standards development efforts are underway or in the planning stage.

These Guidelines seek to establish a safe harbor - a secure, computer-based signature equivalent - which will (1) minimize the incidence of electronic forgeries, (2) enable and foster the reliable authentication of documents in computer form, (3)

facilitate commerce by means of computerized communications, and (4) give legal effect to the general import of the technical standards for authentication of computerized messages.

These Guidelines and the technical standards noted above all rely on certain legal and institutional support to enable an authentication strategy based upon digital signatures supported by certificates. As the foregoing tutorial explains, a trustworthy third party termed a "certification authority" must associate a key pair with the identity of a person who is to sign, termed a "subscriber." Once the certificate binds the identity of the subscriber to the key pair, the key pair plus a computer system to utilize the key pair, constitute the subscriber's digital signature capability. The subscriber must take care to retain control over that capability by safeguarding the private key against compromise. In large measure, the Guidelines are devoted to establishing the interrelated legal duties of certification authorities, subscribers, and persons relying on certificates and digital signatures which are verifiable with reference to those certificates.

The interactive roles of a certification authority, subscriber, and relying party in these Guidelines are, for the most part, based on extensions of traditional legal doctrines relating to contract principles and tortious conduct, such as intentional or negligent misrepresentations of fact. The relationship between a certification authority and subscriber may be primarily contractual, whereby a subscriber and certification authority will agree to reinforce and enhance the subscriber's digital signature capability in exchange for a fee or other consideration. The duties of a certification authority to a third party relying on a certificate are rooted mainly in legal proscriptions against fraud and negligent misrepresentation. The duties of a subscriber to a person who relies upon the subscriber's certificate and digital signatures verified using that certificate, rest upon principles of both contract and tort.

Content and Style

The Guidelines contain two types of information, the Guidelines proper, and commentary on the Guidelines. The Guidelines proper are general statements of principle, intended as a common framework of unifying principles that may serve as a common basis for more precise rules in various legal systems.

The comments accompanying each of the Guidelines elaborate on the significance, scope and implications of the Guideline. They may explain the intent of a Guideline, put a Guideline in perspective, state limitations or cautionary notes, add information on implementation, or refer to external resources. Comments may also provide practical illustrations of the effect of a Guideline in practice. The comments assume knowledge of general law and of the technology explained in the introductory tutorial. They are not exhaustive, and the absence of commentary supporting a particular point of view should not be construed as disapproval of that view. Reference to additional resources, such as those listed in the bibliography, is strongly encouraged.

The following style conventions are used in this publication:

- **Text of a Guideline appears in this bold, Roman font, with defined terms underlined.**

  - Defined terms in the Guidelines are hypertext-linked to the full text of the definition in the electronic version of the Guidelines.

  - Commentary accompanying Guideline text appears on paper in this sans serif font.

Caveats

These Guidelines are distributed by the Information Security Committee of the Section of Science and Technology of the American Bar Association, Electronic Commerce and Information Tecnology Division. The Committee has prepared these Guidelines in an effort to facilitate discussion leading to the development of sound law and practice regarding digital signatures as a tool for conducting secure electronic commerce. These Guidelines are not intended as a substitute for legal counsel, and their proper interpretation will require both legal and technical expertise.

This publication, DIGITAL SIGNATURE GUIDELINES, has not been approved or endorsed by the House of Delegates or Board of Governors of the American Bar Association, the Council of the Section of Science and Technology, or its Electronic Commerce and Information Technology Division. Accordingly, no portion of these Guidelines is to be construed as representing the position of the American Bar Association or any of its subdivisions, other than the Information Security Commitee, whose members collectively authored this work.

These Guidelines are not intended for adoption as the text of a statute or regulation and are not suitable for that purpose. Legislation implementing a legal and institutional infrastructure for digital signatures will need to resolve and clarify issues left open in these Guidelines. These Guidelines are intended to assist in the drafting and interpretation of such legislation.

Text of Digital Signature Guidelines

1 Definitions

1.1 Accept a certificate

To demonstrate approval of a certificate while knowing or having notice of its contents.

Comment

1.1.1 As used in these Guidelines, acceptance of a certificate is always the act of a subscriber. In some systems, a "subscriber" is referred to as an "applicant" or "certificate applicant" prior to issuance of a certificate. *See* Guideline 1.16 (issue a certificate) and 1.31 (subscriber). In these Guidelines, reference to a subscriber includes reference to a subscriber before and/or after issuance, depending on the context.

1.1.2 Acceptance is the action by subscriber that triggers the subscriber's duties and potential liability. By accepting the certificate, the subscriber becomes bound to comply with Part 4 of the Guidelines (subscribers), which specify the duties of subscribers, and also becomes subject to potential liability to relying parties through potentially adverse rebuttable presumptions under the rules contained in Part 5 of the Guidelines (relying on certificates and digital signatures). It is this bundle of duties and presumptions which is the heart of the nonrepudiation features of these Guidelines. *See* the Tutorial, *supra* at 7, for an explanation of the security service of nonrepudiation ("A nonrepudiation service provides proof of the origin or delivery of data in order to protect the sender against false denial by the recipient that the data has been received, or to protect the recipient against false denial by the sender that the data has been sent."). *See also* Guideline 1.20 (nonrepudiation); *Information Technology - Security Frameworks in Open Systems - Non-repudiation Framework* (also *ITU-T Recommendation X.813*), ISO/IEC 10181-4 (1996).

1.1.3 A certificate is not "valid" under Guideline 1.36 (valid certificate) unless two conditions have been satisfied: (a) the certification authority must have "issued" the certificate within the meaning of Guideline 1.16 (issue a certificate), and (b) the subscriber must have "accepted" the certificate under this Guideline 1.1 (accept a certificate). If the certificate is not valid, then a digital signature of the subscriber is not capable of "verification" under Guideline 1.37 (verify a digital signature and message integrity). The digital signature of the subscriber which is not verified may still be proved to be the "signature" of the subscriber, enforceable against the subscriber under traditional principles. However, the subscriber's acceptance of the certificate tends to make it more difficult for the subscriber to repudiate his digital signatures, and easier for the relying party to enforce the subscriber's digital signatures against the subscriber.

1.1.4 Acceptance by the subscriber may be express or implied. Consideration of a number of potential scenarios is instructive as to the factual and legal issues involved in the determination of whether subscriber has impliedly accepted a certificate.

- The first scenario is a clear case of implied "acceptance" even in the absence of an express manifestation of approval by the subscriber. Under this first scenario, the subscriber first becomes an "applicant," for a certificate, requesting the certification authority to issue a certificate. The certification authority issues the certificate within the meaning of Guideline 1.16 (issue a certificate), which means that the subscriber is given a copy or is notified of the contents of the certificate. The subscriber, with notice that a copy of the certificate has been published or has otherwise been made available to potential relying parties within the meaning of Guideline 1.26 (publish), then proceeds to create at least one digital signature during the operational period of the certificate, using the private key corresponding to the public key listed in the certificate, under circumstances such that the subscriber might reasonably foresee reasonable reliance on the certificate by a recipient of the certificate. *See* Guidelines 2.3 (reliance on certicates foreseeable) and 4.2(3) (representations of subscriber to certification authority under such circumstances).

- At the opposite extreme is a second scenario, which illustrates a clear case for the absence of acceptance. The subscriber has a key pair which is used to create digital signatures. The public key may have been widely published, but the subscriber has not applied or made any request for a certificate to be issued. Without the subscriber's actual or implied consent, the certification authority "issues" a certificate within the meaning

of Guideline 1.16 (issue a certificate) by creating a certificate containing the subscriber's public key and sending a copy of the certificate to the subscriber. Subscriber continues to create digital signatures with his key pair as before, but does not expressly demonstrate approval of the certificate to the certification authority, and does not himself make the certificate available to anyone. Moreover, if the certification authority has published the certificate within the meaning of Guideline 1.26 (publish), the subscriber has no notice or knowledge that publication has occurred.

- Between these two extremes, key factors in evaluating whether subscriber has accepted a certificate include, (a) a request versus no request for issuance; (b) express approval versus silence following notice or knowledge of issuance; (c) knowledge versus absence of knowledge that the certificate is available to potential relying parties; (d) the reasonableness of reliance upon the certicate; and (e) the foreseeability of such reliance. The following general principles appear consistent with traditional jurisprudence and the policies behind these Guidelines: (1) express approval under (b) is a safe harbor for the conclusion that acceptance has occurred; (2) In the absence of express approval by the subscriber, approval may be inferred from silence or other indicia or circumstances of implicit approval, but *only if* there has been a request by the subscriber under (a), *or* the subscriber has knowledge of certificate availability to potential relying parties under (c).

1.1.5 In evaluating the existence of implicit approval by the subscriber, an objective test is more important than an attempt to determine the subjective mental state of the subscriber. By analogy to contractual acceptance, RESTATEMENT (SECOND) OF CONTRACTS §§ 18-20 (1981), the test is whether, in light of all relevant facts and any applicable trade usage or commercial practice, a reasonable person would conclude that the subscriber had demonstrated approval.

1.2Ancillary services

(1) A person offering or performing a

service, other than issuance of certificates, in support of digital signatures and other related areas of secure electronic commerce, or

(2) The service offered or performed by such person.

Comment

1.2.1 "Secure electronic commerce" as used throughout these Guidelines can be understood to mean the establishment of a system/infrastructure/method of communications such that transactions can be relied upon.

1.2.2 Ancillary services are not inherently core functions of certification authorities. Certification authorities, however, may provide such services in addition to the issuance of certificates.

1.2.3 The following are possible ancillary services, which should be established as trustworthy systems (*see* Guideline 1.35, trustworthy systems) and operated in accordance with generally accepted security principles. It is understood that these security principles, including practice statements for each such service, will be further developed as these services evolve. *See* Guideline 1.8 as an example of a practice statement, in that case relating to the core function of certificate issuance and management.

- **Archival service**: A person who keeps records for a certification authority, repository, or another person involved in electronic commerce. Archived records may be kept for commercial record-keeping purposes or to comply with law. They also may be needed in dispute resolution to support the certification authority's identification of the subscriber, other representations in the certificate, or revocation or suspension of the certificate. An archive service differs from a repository in that the archive need not be readily accessible on-line. Durability and future accessibility are primary concerns.

- **Confirmation service**: A person aiding a certification authority in performing its duty to confirm certain information (*see* Guidelines 3.7 - representations of certification authority in certificate, and 1.9 - confirm).

- **Directory service**: A person who locates and furnishes certificates and other information about persons, such as distinguished names, on-line addresses and identifying or descriptive information, either directly, or through links to third party directories of such information.

- **Technical due diligence services**: A person who reviews the technical compliance (with these Guidelines or the rules of any other applicable public key infrastructure) of a number of messages, time-stamps, digital signatures and certificates related to a particular transaction or series of transactions, and documents the results of such review to relying parties in electronic form suitable for deposit on-line in a repository and/or offline in an archival service. For example, a technical due diligence service might confirm that all material messages in the transaction contain digital signatures; that all certificates (including transactional certificates as defined by Guideline 1.34) are valid certificates (defined by Guideline 1.36); determine the time and date all digital signatures were created to determine whether they were created during the operational period (Guideline 1.22) of the certificate containing the corresponding public key; determine that no certificates have been revoked or suspended; verify the digital signatures of the certification authority and all higher certification authorities up to and including the root; and finally to "enclose" all messages pertinent to the transaction in an electronic envelope which is then digitally signed and time-stamped by the person performing the technical due diligence services.

- **Financial assurance service**: A person who aids a certification authority in satisfying the financial responsibility requirements of Guideline 3.3 (financial responsibility). Examples include a surety issuing a bond, a bank issuing a standby letter of credit, or a liability insurance carrier.

- **Key pair generation service**: A person who creates key pairs to be used by others. A key pair generation service does not include a person who generates his own key pair (see Guideline 4.1 - generating the key pair). To the extent a key

pair generation service is used to create a subscriber's key pair, it should utilize only trustworthy systems. In order to minimize the potential for compromise of the subscriber's private key, the key generation service should not normally hold the private key of the subscriber following its generation, unless authorized by a commercial key escrow service or a private key trust service as explained below.

- **Message corroboration service**: A person who creates a hash result (defined in Guideline 1.13) to fix the content of the message, and then associates a time-stamp (see Guideline 1.33) with the message and/or the hash result. Message corroboration provides assurance of message integrity and the time the message was created, but provides no authentication of the signer's identity. The reliability of a message corroboration service will depend upon whether or not it utilizes a trustworthy system (see Guideline 1.35).

- **Commercial key escrow service**: A person who holds the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of subscriber, an employer, or other party, upon provisions set forth in the agreement. The subscriber may have originally entered into the escrow agreement voluntarily, or the subscriber's entry into a binding contract may have been required as a condition upon the commencement or continuation of an employment relationship or vendor relationship with a customer, or other relationship with a third party. The purpose of the escrow arrangement may be to ensure the recovery (by the subscriber, employer, customer, or other third party) of the private key of the subscriber and other pertinent information, upon the death, disability, departure, or recalcitrance of a subscriber who is an employee. Where a key pair is used for digital signatures only (i.e., the same key pair is not also used for data encryption) there is unlikely to be any reason to recover a subscriber's key which becomes permanently unavailable. Rather, the appropriate remedy will likely be to revoke any certificates issued with respect to the public key (see Guideline 1.29 - revoke a certificate). To the extent the key pair could also be used for encryption of information, or to the extent a private key used for creating

digital signatures becomes only temporarily unavailable, the key escrow service should serve to complement key security (see Guideline 4.3 regarding duty of the subscriber to safeguard the security of the private key). A private key escrow service must use only trustworthy systems (see Guideline 1.35 - trustworthy systems), and the service must endeavor to minimize the potential compromise of the subscriber's private key, whether used for digital signature or for encryption purposes. Additional issues raised by laws requiring public agencies (rather than commercial private persons) to serve as escrow agents of private keys, session keys or message keys, in order to facilitate recovery of messages encrypted for confidentiality, are beyond the scope of these Guidelines.

- **Private key trust service**: A person who holds the private key of a subscriber pursuant to an express trust, letters testamentary, or similar legal arrangement which is voluntarily created by the subscriber. For example, a subscriber could establish a trust authorizing the trustee to hold the subscriber's private key temporarily, in order to facilitate recovery of the private key if it is destroyed or the subscriber forgets it or loses a token containing knowledge of the key. Alternatively, the terms of the trust might pass ownership of the private key to beneficiaries of the subscriber upon the subscriber's death, or allow another person to hold the subscriber's key upon the subscriber's disability. Or a subscriber might provide for passage of the subscriber's private key to beneficiaries in the subscriber's will. Where a key pair is used for digital signatures only (the same key pair is not also used for encryption of confidential messages) there will ordinarily be no reason to recover the subscriber's key which has been lost or destroyed, or upon the subscriber's death, and the persons succeeding to the ownership of the key will simply cease to use the private key and will revoke any certificate containing the corresponding public key (see Guideline 1.29 - revoke a certificate).

- **Time-stamping service**: A person time-stamping the digital signatures, messages, or records of others, pursuant to Guideline 1.33 (time-stamp), with reliability of such service determined by whether the service uses only trustworthy

systems under Guideline 1.35 (trustworthy system).

Other ancillary services could be envisioned and offered in addition to the examples enumerated above. These examples are illustrative only, and the exclusion of other ancillary services does not imply their prohibition.

1.2.4 For one view of services ancillary to the central roles of certification authority, subscriber, and relying party, *see generally,* MICHAEL S. BAUM & HENRY H. PERRITT, ELECTRONIC CONTRACTING, PUBLISHING, AND EDI LAW 227-305 (1991).

1.3Asymmetric cryptosystem

A system which generates and employs a secure key pair, consisting of a private key for creating a digital signature, and a public key to verify a digital signature.

Related Terms

"Public key cryptosystem" is a closely synonymous term.

Comment

1.3.1 Asymmetric cryptography is the core of digital signature technology. For introductory explanations and comparisons with other methods of security and cryptography, *see* WARWICK FORD, COMPUTER COMMUNICATIONS SECURITY: PRINCIPLES, STANDARD PROTOCOLS AND TECHNIQUES 71-75 (1994); BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C, §§ 2.1-2.8, 21-46 (2d ed. 1996).

1.3.2 A "secure key pair" is a key pair which is cryptographically strong and thereby capable of creating and verifying digital signatures in a highly reliable manner. In particular, a secure key pair "must have the property that, given knowledge of the public key, it is not feasible to determine the private key." WARWICK FORD, COMPUTER COMMUNICATIONS SECURITY: PRINCIPLES, STANDARD PROTOCOLS & TECHNIQUES 71-72

(1994). The security of a key pair may depend on restrictions specifying a minimum key size and other limitations. *See* Guideline 1.17 (key pair).

1.3.3 The asymmetric cryptosystem used for creating and verifying digital signatures may (but need not) include functions for encrypting or decrypting the message, in which case the public key of the key pair is used for encryption and the private key is used for decryption. These Guidelines principally support digital signatures, and deal to a far lesser extent with message encryption/decryption and message confidentiality.

1.3.4 This definition requires an asymmetric cryptosystem to provide a secure key pair as implemented in a trustworthy system. A trustworthy system is defined by Guideline 1.35 (trustworthy system) in light of the available and foreseeable technology. *See also* Guideline 1.12 (hash function), 1.17 (key pair), and the Tutorial, *supra* note 24.

1.4Authentication

A process used to ascertain the identity of a person or the integrity of specific information. For a message, authentication involves ascertaining its source and that it has not been modified or replaced in transit.

Comment

1.4.1 "Authentication" is not directly used in these Guidelines as an operative word to define the specific Guidelines strategy by which digital signatures are created and verified. The reason is that the Guidelines strategy is only one example of a variety of processes by which authentication of origin and integrity of

information are accomplished today, with varying levels of security and assurance, for records which are both documents and messages. *See* Guideline 1.18 (defining message, and defining document and record under "related terms" and in the commentary).

1.4.2 "Authentication" and its related forms "authenticate" and "authenticated" are nonetheless useful terms, and are frequently used throughout these Guidelines with the general meaning set forth in this Guideline to describe authentication processes which may but need not be implemented by the specific Guidelines strategy for the creation and verification of digital signatures. *See, e.g.,* Guideline 3.2(3) (allowing a certification authority to require either an authenticated message or a signed document as a condition precedent to the obligation of disclosure).

1.4.3 The term "authentication" is already used widely in various legal contexts, for example in U.C.C. § 1-201(39), U.C.C. § 2B-102(32), and in Federal Rules of Evidence 901(a):

- "'Signed' includes any symbol executed or adopted by a party with present intention to authenticate a writing." U.C.C. § 1-201(39) (1990).

- "'Signed' or 'signature" means a symbol, including a digital signature, encrypted identifier, or analogous symbol, or an act that encrypts a record in whole or in part, adopted by a party with present intent to authenticate a record or term." U.C.C. § 2B-102(32) (May 3, 1996 Draft)

- Rule 901. Requirement of Authentication or Identification

  (a) General provision. The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims.

  (b) Illustrations. By way of illustration only, and not by way of limitation, the following are examples of authentication or identification conforming with the requirements of this rule: . . . .

(9) Process or system. Evidence describing a process or system used to produce a result and showing that the process or system produces an accurate result.

FED. R. EVID. 901.

1.5 Certificate

A message which at least

(1) identifies the certification authority issuing it,

(2) names or identifies its subscriber,

(3) contains the subscriber's public key,

(4) identifies its operational period, and

(5) is digitally signed by the certification authority issuing it.

Comment

1.5.1 A person seeking to verify a digital signature needs, at a minimum, (1) the public key corresponding to the private key used to create the digital signature, and (2) reliable evidence that the public key (and thus the corresponding private key of the key pair) is identified with the signer. The basic purpose of the certificate is to serve both these needs in a reliable manner.

1.5.2 The certification authority's practices for identifying subscribers should be disclosed in a certification practice

statement (Guideline 1.8) which is incorporated by reference in the certificate in accordance with Guideline 1.15 (incorporate by reference). If a certification authority offers different types of certificates providing multiple assurance levels, each with different practices for identifying subscribers, the certification practice statement should disclose these differences and the certificate should identity what type of certificate it is.

1.5.3 A certificate will generally take the form of the binary records common in current electronic data interchange ("EDI"). A certificate will usually be in the form prescribed by International Telecommunications Union ("ITU") (formerly International Consultative Committee on Telephony and Telegraphy, "CCITT") Standard X.509 v3, but any certificate meeting the requirements of this Guideline 1.5 (certificate) is acceptable. The use of additional fields and extensions to provide additional attributes or information (e.g., authorization of the subscriber as an agent, or cross-reference to other databases providing information about the subscriber) is optional.

1.5.4 The certification authority issuing the certificate must digitally sign the certificate, with the twofold purpose of (a) protecting the message integrity of the certificate as a message, and also (b) to allow the digital signature of the certification authority to be verified.

1.5.5 The digital signature of the certification authority issuing the certificate should have a time-stamp for the same reasons that the digital signature of a subscriber should have a time-stamp, namely to facilitate proof that the digital signature (of the certification authority or of the subscriber as the case may be) was created during the operational period (Guideline 1.22) of a valid (Guideline 1.36) certificate (of the higher certification authority or of the certification authority as the case may be), so that such digital signature is capable of verification pursuant to Guideline 1.37 (verify a certificate). *See* Guideline 1.33 regarding time-stamping. An optional time-stamp on the internal auditable records of a certification authority (or perhaps even on the certificate itself) may also be useful to prove when a certificate was issued, or at least the earliest date and time when the certificate could have been issued. A further use might be the time-date stamping of historical versions of certification practice statements which have been incorporated by reference in the certificate, to determine which version was available to the subscriber and/or a relying party at pertinent times during the operational period of the

certificate. As set forth in Guideline 1.33 (time-stamp), the probative value of a time-date stamp is enhanced to the extent the time-stamp is provided by a trustworthy system (Guideline 1.35).

1.6Certification authority

A person who issues a certificate.

Related Terms

The terms "issuing authority" or "certificate issuer" are sometimes used to refer to what these Guidelines call a "certification authority". The two terms are closely synonymous. *See* Guideline 1.16 (issue a certificate).

Comment

1.6.1 Quality assurance should be a principal concern in selecting and utilizing certification authorities. Governmental regulation, professional accreditation, trade usage, auditing, and liability for negligent errors and omissions are examples of approaches toward assuring quality in certification authority practice.

1.6.2 Subject to applicable law, any person who undertakes the functions of a certification authority under these Guidelines may become a certification authority. The level of authority and reliance to be accorded to the certificates of the certification authority will be determined in part by the experience and reputation of the certification authority, and in part from the material presented in the certification practice statement. Those who seek a low level of responsibility to protect transactions of minor value or limited risk may accept a certificate of lower level assurance from a certification authority of unknown reputation. Those who seek the highest level of responsibility to protect transactions of high value and severe risk will obtain certificates providing the highest level of assurance, from certification authorities whose experience has earned them the highest respect.

1.6.3 A notaire or **CyberNotary**℠ may be a certification authority, and serving as a certification authority may well be a natural

extension of such a person's professional expertise, discipline, and practical experience. CyberNotaries℠ are attorneys at law admitted to practice in the United States and qualified to act as a CyberNotary℠ pursuant to specialization rules currently under development in the CyberNotary℠ Committee, Section of Science and Technology of the American Bar Association. A CyberNotary's℠ function mirrors that of a notaire, and is focused primarily on practice in international, computer-based transactions. Under the planned specialization rules, a Cyber-Notary℠ would possess technical expertise to facilitate computer-based transactions requiring a high level of certification, authentication, or other information security services. It is proposed that a CyberNotary℠ would be required to meet a level of qualification as a legal professional commensurate with that of a notaire, be a member in good standing of the bar of a state or territory of the United States, the District of Columbia, or Puerto Rico, be a member of the American Bar Association, and demonstrate technical competence in computer-based business transactions. For further information, contact the CyberNotary℠ Committee, Section of Science and Technology, of the American Bar Association.

1.6.4 Moreover, notaires and CyberNotaries℠ provide important adjunct services in addition to assuring the validity of a signature; for example, a notarial authentication in certain legal systems assures the validity and legal efficacy of the transaction itself, not merely its signatures. Notaires and CyberNotaries℠, therefore, may be well suited to serving as certification authorities, subject, of course, to satisfaction of the standards of training and practice required of all certification authorities by Guideline 3.1 ("A certification authority must utilize trustworthy systems in performing its services.") and Guideline 1.35 (the definition of computer hardware, software and procedures which meet the test of a "trustworthy system").

1.7 Certification authority certificate

A certificate which lists a certification authority as subscriber and contains a public key corresponding to a private key

used to digitally sign another certificate.

Related Terms

The term "issuing authority" is sometimes used in a hierarchical certificate-based system as a reference to all entities who issue certificates, reserving the term "certification authority" for those entities who issue certificates only to end-users for their own transactions. *See* Guideline 3.6 (availability of certification authority certificate).

Comment

1.7.1 A certificate (Guideline 1.5) is issued by a certification authority (Guideline 1.6) to a subscriber (Guideline 1.31). The definition of "subscriber" is broad enough to include those who also issue certificates (i.e., a certification authority) and those who do not (i.e., an end-user), and the definition of "certificate" is broad enough to include certificates which name both end user and certification authorities as subscribers of such certificates. "Certification authority certificate" under this Guideline 1.7 refers only to the subset of certificates which are *not* issued to end-users.

1.8Certification practice statement

A statement of the practices which a certification authority employs in issuing certificates.

Related Terms

Current terminology in the computer security industry often employs "policy statements" or similar words instead of "certification practice statement"; *see, e.g.,* Stephen Kent, RFC 1422: Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management (1993).

The term "certification practice statement" is used in the Guidelines to avoid ambiguity or confusion in the usage of the word "policy."

Comment

1.8.1 A certification practice statement may take the form of a declaration by the certification authority of the details of its trustworthy system and the practices it employs in its operations and in support of issuance of a certificate, or it may be a statute or regulation applicable to the certification authority and covering similar subject matter. It may also be part of the contract between the certification authority and the subscriber. A certification practice statement may also be comprised of multiple documents, a combination of public law, private contract, and/or declaration. A certification practice statement is useful in helping subscribers and relying parties distinguish which certification authorities provide more reliable representations in the certificates they issue. *See* Guideline 3.8 (certification authority's representations in certificate).

1.8.2 Certain forms for legally implementing certification practice statements lend themselves to particular relationships. For example, when the legal relationship between a certification authority and subscriber is consensual, a contract would ordinarily be the means of giving effect to a certification practice statement. The duties a certification authority owes to a relying person are generally based on the certification authority's representations, which may include a certification practice statement.

1.8.3 Whether a certification practice statement is binding on a relying person (who would not usually be a party to the certification practice statement) depends on whether the relying person has knowledge or notice of the certification practice statement. *See* Guideline 1.21 (notify). A relying person has knowledge or at least notice of the contents of the certificate used by the relying person to verify a digital signature, including documents incorporated into the certificate by reference (*see* Guideline 1.15 - incorporate by reference). Documents considered incorporated by reference should be available through the same channel or repository through which the incorporating document is accessible. It is therefore advisable to incorporate a certification practice statement into a certificate by reference.

1.8.4 As much as possible, a certification practice statement should indicate any of the widely recognized standards to

which the certification authority's practices conform. Reference to widely recognized standards may indicate concisely the suitability of the certification authority's practices for another person's purposes, as well as the potential technological compatibility of the certificates issued by the certification authority with repositories and other systems.

1.8.5 For more information on certification practice statements, including relevant technical standards, *see generally* MICHAEL BAUM, FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY: LAW AND POLICY OF CERTIFICATE-BASED PUBLIC KEY AND DIGITAL SIGNATURES 352-58 (1994).

1.9Confirm

To ascertain through appropriate inquiry and investigation.

Comment

1.9.1 This term is used in these Guidelines to denote the certification authority's duty to investigate the facts supporting a certificate which it issues, as required by Guideline 3.7 (certification authority's representations in certificate) for issuance of a certificate or by Guideline 3.10 (revocation of a certificate at the subscriber's request).

1.9.2 In determining the level of inquiry and investigation appropriate under the circumstances, the certification authority and any reviewing tribunal should take into account the probable use of the certificate based on the prospective subscriber's representations, the prospect of reliance on the certificate, and any effective limits on reliance.

1.9.3 This Guideline does not require the certification authority to guarantee or underwrite the factual accuracy or legal significance of the confirmed information. The level of investigation required will vary according to the circumstances for which a certificate is intended, and may be increased by a certification practice statement or contract. The certification authority may specify in a certification practice statement the detailed methods and practices it uses for confirming the

information in the certificate. *See* Guideline 3.7 (certification authority's representations in certificate), especially Comment 3.7.1.

1.10 Correspond

To belong to the same key pair.

Comment

1.10.1 An asymmetric cryptosystem may employ more than two keys, whereas "correspond" implies a pair. "Correspond" is said of any two keys which have the characteristic that one of them generates a digital signature and the other verifies a digital signature, regardless of how many related keys may perform the same or related functions.

1.11 Digital signature

A transformation of a message using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine

(1) whether the transformation was created using the private key that corresponds to the signer's public key, and

(2) whether the initial message has been altered since the transformation was made.

Related Terms

The term "electronic signature" is sometimes used,

generally with a meaning including all legally recognizable signatures under the currently prevalent, broad definitions of "signature." *See, e.g.,* U.C.C. § 1-201(39) (1990). An "electronic signature" thus includes digital signatures as defined by these Guidelines as well as digitized images of paper-based signatures, typed notations such as "s/James Jones", and perhaps addressing information such as the "From" headers in electronic mail.

Comment

1.11.1 Because it is very difficult to find two different messages which yield the same hash result (*see* Guideline 1.13 - hash result), a digital signature created out of a hash result of a message correlates the digital signature to the message sufficiently to satisfy the requirement of paragraph (2) of this Guideline. Since the digital signature is also created by the private key of the signer, it is also traceable to that private key, which must be uniquely under the control or authority of the proper signer. A digital signature is therefore unique both to each message and signer. Moreover, since a private key corresponds to a public key in an asymmetric cryptosystem, the fact that the digital signature was created using the private key can be verified without access to the private key. *See* Tutorial, *supra* note 20.

1.11.2 Any change in the message will cause the hash function (see Guideline 1.13 - hash result) to produce different results, and those different results will produce a different digital signature by application of the private key. The message must therefore be clearly delimited, and the delimitation used for digitally signing must be the same as that used for verifying.

1.11.3 Additional information must accompany a digital signature, including an indicator of the algorithm(s) used, an indicator of the signer's identity or of the public key to be used for verification, a time-stamp, a sequence number, identification of certification authority, and other data. The digital signature may be integral to, appended to, or kept apart from its message.

1.11.4 For technological background on digital signatures, *see generally* WARWICK FORD, COMPUTER COMMUNICATIONS SECURITY: PRINCIPLES, STANDARD PROTOCOLS AND TECHNIQUES 78-84 (1994); Mitchell, Piper & Wild, *Digital Signatures, in* CONTEMPORARY CRYPTOLOGY: THE SCIENCE OF INFORMATION INTEGRITY 325-356 (Gustavas Simmons ed.,

1991); Nechvatal, *Public Key Cryptography, in* CONTEMPORARY CRYPTOLOGY: THE SCIENCE OF INFORMATION INTEGRITY 195-99 (Gustavas Simmons ed., 1991); BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C §§ 2.6-2.7, 34-44 (2d ed. 1996).

1.12 Hash function

An algorithm mapping or translating one sequence of bits into another, generally smaller, set (the hash result) such that

(1) a message yields the same hash result every time the algorithm is executed using the same message as input,

(2) it is computationally infeasible that a message can be derived or reconstituted from the hash result produced by the algorithm, and

(3) it is computationally infeasible that two messages can be found that produce the same hash result using the algorithm.

Related Terms

What the Guidelines term a "hash function" is sometimes called a "one-way function" or "message digest algorithm" elsewhere. *See also* the related terms listed under Guideline 1.13 (hash result), and Guideline 1.2 (ancillary services) regarding the ancillary service therein described as a “message corroboration service.”

Comment

1.12.1 For technological background on hash functions, *see* WARWICK FORD, COMPUTER COMMUNICATIONS SECURITY:

PRINCIPLES, STANDARD PROTOCOLS AND TECHNIQUES 75-84 (1994); Mitchell, Piper & Wild, *Digital Signatures*, *in* CONTEMPORARY CRYPTOLOGY: THE SCIENCE OF INFORMATION INTEGRITY 325, 344-46 (Gustavas Simmons ed., 1991); Nechvatal, *Public Key Cryptography*, *in* CONTEMPORARY CRYPTOLOGY: THE SCIENCE OF INFORMATION INTEGRITY 179, 199-202 (Gustavas Simmons ed., 1991); BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C §§ 2.3-2.4, 29-31 (2d ed. 1996). *See also* the specification of the "secure hash function" in NIST, SECURITY REQUIREMENTS FOR CRYPTOGRAPHIC MODULES, FIPS PUB 180 (1994).

1.12.2 Although there exist hash functions which do not have all the properties specified by this Guideline 1.12, “hash function” as defined here is meant to imply a “secure hash function” which meets all three requirements set forth in this Guideline.

1.13 Hash result

The output produced by a hash function upon processing a message.

Related Terms

The output of a hash function is sometimes called a "message digest," "manipulation detection code," "integrity check value," “message authentication code,” “message integrity check,” or "cryptographic checksum" in other materials. *See also* the related terms under Guideline 1.12 (hash function) and Guideline 1.2 (ancillary services) for the ancillary service therein described as a “message corroboration service.”

Comment

1.13.1 All of the data generated in the course of running a hash function may not be significant in satisfying the requirements of

a hash function as defined in Guideline 1.12 (hash function). The publisher of a hash function should specify which part of the data generated by the hash function satisfies the requirements of the definition. That particular portion of the total product of the hash function is what "output" means in this definition.

1.14 Hold a private key

To use or be able to use a private key.

Comment

1.14.1 A private key is normally held by only one person, the subscriber who creates it or has been provided it for his use, absent specialized organizational considerations or arrangements such as a commercial key escrow service or a private key trust service described in Guideline 1.2 (ancillary services).

1.14.2 Absent such authorization for one person to hold the private key of another under specialized considerations or arrangements, it is very unlikely that two persons can hold the same private key without risk to the objective of nonrepudiation (see Guideline 1.20), or invasion of the rightful holder's interest, or both. If a private key held by one person is discovered to be held by another as well, any certificates containing the corresponding public key should first be revoked, then the other party should be notified, and then both should cease the creation of digital signatures using that private key (*see* Guideline 4.4 - initiating suspension or revocation).

1.14.3 Holding the private key is distinct from holding the medium or container in which the private key is recorded. The private key is a numerical quantity, regardless of the means by which it is stored. *See* Guidelines 4.3 (safeguarding the private key) and 4.4 (initiating suspension or revocation).

1.14.4 For additional analysis of digital forgery, *see* MICHAEL S. BAUM, FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY: LAW AND POLICY OF CERTIFICATE-BASED PUBLIC KEY AND DIGITAL SIGNATURES 147-59 (1994).

1.15 Incorporate by reference

To make one message a part of another message by

(1) identifying the message to be incorporated,

(2) providing information which enables the receiving party to access and obtain the incorporated message in its entirety, and

(3) expressing the intention that it be part of the incorporating message.

The incorporated message shall have the same effect as if it had been fully stated in the incorporating message, to the extent permitted by law.

Comment

1.15.1 When these Guidelines refer to information "in the certificate", the reference means all information within the actual limits of the certificate as well as all information incorporated into it by reference.

1.15.2 The incorporating message is generally a certificate in these Guidelines. Certificates in the form prescribed by ITU X.509 are database-type digital records with rigidly prescribed contents. Such a certificate, particularly under the recently amended X.509 v3, may incorporate other information by

reference, for example, a certification practice statement. *See* Guideline 1.8 (certification practice statement), especially 1.8.3.

1.15.3 If all requirements of this Guideline are satisfied, the incorporated message has the same legal significance and effect that it would have if set forth verbatim within the certificate. Upon receipt of a certificate under circumstances satisfying the Guideline, therefore, the recipient is notified of not only the certificate's actual contents but also the contents of all incorporated messages which the recipient is enabled to access and obtain in their entirety. An incorporation by reference into a certificate or other message is effective as notice when, among other things, it sufficiently identifies the message to be incorporated and expresses the intention to incorporate it, such that, according to applicable law, it is sufficiently likely under the circumstances to impart knowledge of the information in the incorporated message to the relying person. *See* Guideline 1.21 (notify). The extent to which there can be considered to be constructive notice of the incorporated message under applicable law, is a question which should be addressed in future legislation implementing these Guidelines. *Cf.* Guideline 1.28 (repository), particularly Comment 1.28.3; Guideline 1.26 (publish), particularly Comment 1.26.3.

1.15.4 An expression purporting to incorporate information in a difficult or obscure form may not be a commercially reasonable incorporation under Guideline 2.1, and may not effectively notify someone as described in Guideline 1.21. The general principle of commercial reasonableness (Guideline 2.1) requires that, to be incorporated into a message intended to serve in an efficient business setting, material information be readily locatable.

1.15.5 Guideline 1.18 defines a message as a "digital representation of information," which does not include a paper-based or other tangible record defined as a "document." *See* Comments 1.18.2 and 1.18.3. This Guideline is not intended to render invalid the incorporation by reference of documents by messages, messages by documents, or documents by documents, where permitted by law, and where the conditions of this Guideline and commercial reasonableness under Guideline 2.1 are otherwise satisfied.

1.15.6 Not every referenced message is incorporated. Whether a reference incorporates depends on the intent of its author and may be limited or conditional. For example, a certification

authority's incorporation may be conditioned on whether the certificate is used in a transaction within the sphere of application of the *United Nations Convention on Contracts for the International Sale of Goods,* Official Records 178-190, art. 1-6, at 1-2, U.N. Doc. A/Conf.97/19; Sales No. E.82.V.5 (1981), *reprinted in* 15 U.S.C.A. United Nations Conventions on Contracts for the International Sale of Goods (West Supp. 1996) (Sphere of Application).

1.15.7 The incorporated message should exist at the time the reference takes effect. If the message does not exist until after such effective time, or the information in the incorporated message is subsequently altered, such subsequently created or altered messages will not be considered incorporated by reference under this Guideline. In a case where incorporation by reference is intended to furnish notice of incorporated information at the time of reliance upon the information in the incorporating message, the effective time of the reference will not be considered to occur until the time of such reliance.

1.15.8 If the message to be incorporated has been lost, destroyed, modified, or otherwise not available after it was referenced, its content may be established from extrinsic evidence.

1.15.9 The establishment of registries or repositories of commonly incorporated information may facilitate finding and retrieving incorporated information, and, if the registry or repository is trustworthy, will help assure authenticity and control over document evolution processes. Trade or industry associations, governments, or similar institutions could provide registries. Standards institutions such as the American National Standards Institute already provide such registries pursuant to standard 9070 of the International Organization for Standardization (ISO) (1991).

1.16 Issue a certificate

The acts of a certification authority in creating a certificate and notifying the subscriber listed in the certificate of the contents of the certificate.

Comment

1.16.1 The creation of a certificate by a certification authority includes both generation of the certificate and the digital signature of the certificate. The certification authority must generate the certificate before it can be digitally signed. How and by whom it is generated depends on the specific practices of the certification authority for issuing the certificate. In some cases, the subscriber may apply for a certificate by generating an initial prototype of the certificate, inserting the public key and other information known to the subscriber, and submitting it to the certification authority for review. The certification authority may need to fill in additional information before issuing a certificate partially filled-in by the subscriber. In some cases the certification authority will need to perform investigations before issuing a final certificate, but may be willing to issue a temporary or provisional certificate, or the like, in accordance with rules set forth in its certification practice statement.

1.16.2 The certification authority may give notice of the creation and contents of the certificate by giving the subscriber a printed representation of the certificate, by allowing the subscriber to view the contents of the certificate on-line or on subscriber's computer, or by communicating the content of the certificate to the subscriber in any other reasonable way. The notification requirement may be accomplished by providing the subscriber with an electronic copy of the certificate, which has the further advantage of enabling the subscriber to further distribute the certificate to third parties in the position of relying on it to verify the subscriber's digital signature. *See also* Guideline 1.21 (defining "notify" as "to communicate information to another person as required by the substantive law applicable under the circumstances").

1.16.3 Issuance of a certificate does not include publication (defined in Guideline 1.26), and a certificate may be properly issued without also being published. *See* Guideline 4.2(2) (subscriber's representations regarding issued but unpublished certificates).

1.16.4 If issuance of a certificate occurs without an acceptance of the certificate by the subscriber, the certificate is not a valid certificate under Guideline 1.36 (valid certificate), and therefore is not capable of verifying digital signatures under Guideline 1.37 (verify a digital signature and message integrity), even if

the digital signatures are created during the operational period of the certificate under Guideline 1.22 (operational period). The operational period of the certificate begins upon issuance even though the certificate does not become valid until acceptance at a subsequent time.

1.16.5 Guideline 3.7(1) (certification authority's representations regarding issuance and acceptance of a certificate) provides that a certification authority represents to persons who rely on the certificate that the certification authority has "issued" it within the meaning of this definition. If the certification authority has also "published" it or otherwise made it available (see Guideline 1.26, publish), the certification authority also represents that the certificate has been "accepted" by the subscriber, with the resulting effect that the certificate is represented to be valid under Guideline 1.36 (valid certificate). If a certificate is not valid, a relying party will not be able to use it to verify the digital signature of the subscriber, and thus will have diminished ability to enforce the subscriber's digital signature against the subscriber. See Guideline 5.6(2) (presumption that a properly verified digital signature is the digital signature of the subscriber).

1.16.6 If the relying party has reasonably relied (see Guideline 5.4, reasonableness of reliance) upon an invalid certificate which the certification authority has *published*, then Guideline 3.7(1) provides the relying party a potential remedy against the certification authority. See also Guideline 1.1 (accept) regarding the circumstances under which the subscriber's acceptance of the certificate may be implied, and Guideline 4.2(3) (subscriber's obligations to certification authority regarding the obligation of the subscriber not to *use* a certificate unless it has been accepted). In this sense, the word "use" means that the subscriber is utilizing the certificate to facilitate the verification of digital signatures the subscriber creates, and thus enhancing their acceptability by relying parties.) See also Guideline 3.8 (prerequisites to disclosure of certificate), which obligates the certification authority not to publish or disclose a certificate known to be unaccepted by the subscriber).

1.17 Key pair

In an asymmetric cryptosystem, a private key and its mathematically related public key, having the property that the public key can verify a digital signature that the private key creates.

Comment

1.17.1 For a key pair to be secure or serve as a critical component of a trustworthy system, it must be computationally infeasible to discover the private key from the public key. What is computationally infeasible should be determined according to the present state of the art of computational technology and the state of the art foreseeable during a material time period, such as the validity period of a certificate or the anticipated period of reliance on certificates and digital signatures verifiable with reference to the public keys listed in the certificates. Computational infeasibility may be subject to conditions that may be satisfied by reasonable means. For example, a key pair may be secure only if its public key exceeds a certain minimum length, because, in the asymmetric cryptosystem in question, private keys cannot be derived from public keys if they exceed a specified minimum length. If in practice a public key used with such an asymmetric cryptosystem exceeds the specified minimum length, it would be secure as applied.

1.18 Message

A digital representation of information.

Related Terms

See Model Law on Electronic Commerce, United Nations Commission on International Trade Law (UNCITRAL), 29th Sess., art. 2(a), at 2, U.N. Doc. A/CN.9/XXIX/CRP.1/Add.13 (1996) ("'Data message' means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or

telecopy...."); U.C.C. § 2B-102(30) (May 3, 1996 Draft) ("'Record' means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.").

Comment

1.18.1 As used in these Guidelines, a "message" is any form of digital information. This includes without limitation, text, graphics, database-type data, video, sound, images or multimedia. Its internal structure depends on the computing standards and practices of computing for representing such information digitally.

1.18.2 As used in these Guidelines, a "document" is information that is inscribed on a tangible medium, the most familiar example being paper.

1.18.3 As used in these Guidelines, a "record" describes both a "message" or a "document," similar to the definition of "record" in proposed U.C.C. § 2B-102(30) cited above. An example of a message is an e-mail stored in electronic format. An example of a document is a paper contract with a pen and ink signature.

1.18.4 *See* Guideline 1.30 for the definition of "signer," which in the case of a message, means a person who creates a "digital signature."

1.19 Message integrity

The assurance of unaltered transmission and receipt of a message from the sender to the intended recipient.

Comment

1.19.1 The successful verification of a digital signature using the signer's public key provides authentication in the signature verification process, since only the signer's private key corresponding to that public key could have created the signature associated with the message.

1.19.2 The successful verification of a digital signature also

provides message integrity, since any alteration to the message would cause the computation of an incorrect hash result. This, in turn, would result in the failed verification of the digital signature.

1.19.3 Verification of digital signatures is explained in greater detail in the Tutorial.

1.20 Nonrepudiation

Strong and substantial evidence of the identity of the signer of a message and of message integrity, sufficient to prevent a party from successfully denying the origin, submission or delivery of the message and the integrity of its contents.

Comment

1.20.1 The ISO Nonrepudiation Framework treats nonrepudiation as a technical definition of a security service. The Guidelines define nonrepudiation not as an automatic result of technical mechanisms, but as a property which can ultimately only be determined after recourse to available dispute resolution mechanisms such as a court or arbitrator. The definition of nonrepudiation in this Guideline 1.20 is intended to express a legal conclusion or result which flows from the use of digital signatures verified by certificates in the manner provided in these Guidelines. Nonrepudiation as defined in this Guideline 1.20 is intended to express a legal conclusion something less than a final determination by a court of last resort, but something more than a naked rebuttable presumption as is now provided by simple e-mail.

1.20.2 Nonrepudiation includes not only the denial of a message by the signer, but also the prevention of successful denial of origin, submission and delivery, as well as integrity of content.

1.20.3 Nonrepudiation applies to both parties to a transaction - binding the sender as well as precluding the recipient from denying the message - upon receipt of secure acknowledgment message from the recipient.

1.21 Notify

To communicate or make available information to another person as required under the circumstances.

Related Terms

"Notice" is the result of notification.

Comment

1.21.1 For commercial transactions in the United States, "notice" is defined in U.C.C. § 1-201(25) through 1-201(27) (1991) ("a person has 'notice' of a fact when he has actual knowledge of it, he has received a notice or notification of it [as provided in § 1-201(26)], or from all the facts and circumstances known to him at the time in question he has reason to know that it exists"). In an international setting, the UNIDROIT Principles of International Commercial Contracts are informative:

> (1) Where notice is required it may be given by any means appropriate to the circumstances.
>
> (2) A notice is effective when it reaches the person to whom it is given.
>
> (3) For the purpose of paragraph (2) a notice "reaches" a person when given to that person orally or delivered at that person's place of business or mailing address.
>
> (4) For the purpose of this article "notice" includes a declaration, demand, request or any other communication of intention.

Principles of International Commercial Contracts, International Institute for the Unification of Private Law (Unidroit), art. 1.7(1) (1994). In defining "reach," Comment 4 in the same article states that notice reaches the addressee

> as soon as [it is] delivered...to [the addressee's] place of business or mailing address. The particular communication in question need not come into the hands of the addressee. It is sufficient that it be ... received by the addressee's fax, telex or computer.

See also United Nations Convention on Contracts for

the International Sale of Goods, Official Records 178-190, art. 8, at 2, U.N. Doc. A/Conf. 97/19; Sales No. E.82.V.5 (1981), *reprinted in* 15 U.S.C.A. United Nations Convention on Contracts for the International Sale of Goods (West Supp. 1996) ("[S]tatements made by and other conduct of a party are to be interpreted according to his intent where the other party knew or could not have been unaware what that intent was.").

1.21.2 In some circumstances actual notice may be required and in other instances constructive notice may be sufficient. This definition does not attempt to determine which form of notice is necessary in any given circumstance, nor does it attempt to conform the somewhat divergent concepts of notice in varying legal systems. Rather, the definition in this Guideline incorporates those concepts, divergence and all.

1.21.3 Publication is related to the concept of notification; indeed, notification is often the purpose of publication. *See* Guideline 1.26 (publish), especially Comment 1.26.2.

1.22 Operational period of a certificate

The operational period of a certificate begins on the date and time it is issued by a certification authority (or on a later date and time certain if stated in the certificate), and ends on the date and time it expires or is earlier revoked or suspended.

Comment

1.22.1 The operational period of a certificate begins on the date of issuance (or on a later date and time certain which is stated in the certificate) even though the certificate does not become valid unless and until acceptance by subscriber. This rule allows the certification authority to unambiguously fix the beginning of the operational period at time at time of issuance, without requiring reprocessing upon subsequent acceptance by the subscriber. *See* Guideline 1.5 (certificate).

1.22.2 The expiration of the certificate can be a date and time certain stated in the certificate, or the expiration can be stated as an offset from the beginning of the operational period, such as "12:01 a.m. GMT on the second anniversary of the issuance date set forth in Field #7." See Guidelines 1.29 and 1.32 regarding termination of the operational period earlier than the expiration of the certificate by "revocation" or "suspension" of the certificate.

1.22.3 Until the subscriber accepts the certificate (or if acceptance never occurs), the certificate is not valid under Guideline 1.36 (valid certificate), so that the digital signature and message integrity are not capable of verification under Guideline 1.37 (verify a digital signature). Although the relying party will not have the benefits of the rebuttable presumptions under Guideline 5.6(2) ("A digital signature verified by reference to the public key listed in a valid certificate is the digital signature of the subscriber listed in that certificate."), the relying party may nonetheless prove that the digital signature is in fact the signature of the subscriber.

1.23 Person

A human being or an organization (or a device under the control thereof which is capable of signing a message or verifying a digital signature).

Related Terms

The word "entity" is used in the same sense as the Guidelines use the word "person."

Comment

1.23.1 Some persons are not individuals, but are recognized at law as being able to perform legal acts; corporations are an example. Other persons, such as minors, may be able to sign as a factual matter, but the law may accord only limited significance to their signatures.

1.23.2 An act or forbearance by a device or automated process is

the act or forbearance of the person (human being or organization) who causes the device or process to perform the act or forbearance. Neither a human nor a device ceases to be a person during periods of temporary disability or technical difficulties.

1.24 Private key

The key of a key pair used to create a digital signature.

Comment

1.24.1 A subscriber holding a private key must keep it secure according to Guideline 4.3 (safeguarding the private key) to avoid compromise of the private key. A subscriber should therefore prevent access by all other persons. Depending upon the desired level of assurance, methods for securing the private key from compromise may include (a) access to the private key conditioned upon supplying a password, pass phrase or PIN number known only to the subscriber; (b) possession of a cryptographic token with cryptographic software and private key embedded in a chip; and (c) biometric techniques binding the physical presence of the subscriber to the use of the token.

1.24.2 Regarding one's legal rights and protections in holding the private key, *see* Guideline 1.14 (defining "hold a private key").

1.25 Public key

The key of a key pair used to verify a digital signature.

Related Terms

"Public key cryptology" or "public key cryptography" is often used to describe the branch of cryptology or cryptography dealing with asymmetric cryptosystems.

Sometimes what is termed in these Guidelines an "asymmetric cryptosystem" is called a "public key cryptosystem."

1.26 Publish

To record or file in one or more repositories.

Comment

1.26.1 The general objective of publication is to make certificates and related information (such as certificate revocation lists and information incorporated by reference) available for use in verifying digital signatures. Publication can be accomplished by filing or recording in any repository.

1.26.2 Whether publication notifies a person of the published information generally depends on whether it was reasonably likely to impart actual knowledge to the person. *See* Guideline 1.21 (notify). If access to a repository is subject to commercially reasonable conditions such as reasonable fees and compliance with reasonable security requirements, then filing in the repository should constitute notice, if, under the circumstances, it was reasonably likely to impart actual knowledge to the person notified. Filing in a repository may not constitute notice if the notifier knows in a specific instance that the person to be notified lacks computer-based information capabilities, or the repository in which the information is published is unreliable or obscure, or access to the repository is subject to onerous conditions precedent or severe restrictions.

1.26.3 *See* Guideline 1.21 (notify). The extent to which publication of information in a repository (or alternative methods of official or unofficial publication) can be considered to be constructive notice of the information, is a question of which should be addressed in the future. *Cf.* Guideline 1.15 (incorporate by reference), particularly Comment 1.15.4; Guideline 1.28 (repository), particularly Comment 1.28.3.

1.27 Relying party

A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.

Comment

1.27.1 A relying party as defined in this Guideline 1.27 can mean a person actually or potentially relying upon a particular certificate and/or a digital signature verifiable with reference to a public key listed in the certificate, depending upon the context. The purpose of Guideline is merely to identify one of the parties to the transaction (the other parties are the subscriber and the certification authority), without specifying the extent to which this party should or does in fact rely on the certificate or digital signature.

1.27.2 Guideline 1.37 (verify a digital signature) describes the conditions under which a *digital signature* created by a private key may be verified by the use of the corresponding public key listed in a particular certificate. The relying party relies upon the *certificate* to bind the public key to the identity of the subscriber. Therefore, if the *digital signature* is verified, reliance upon the *certificate* is anticipated to lead to reliance upon the digital signature as the digital signature of the subscriber identified in the certificate. *See* Guideline 5.6(2) (dispute resolution presumptions).

1.27.3 A "recipient" of a certificate is sometimes used in these Guidelines to refer to a relying party, where the context might cause the use of the term "relying party" to be awkward.

1.28 Repository

A trustworthy system for storing and retrieving certificates or other information relevant to certificates.

Comment

1.28.1 The basic contents of a repository generally consist of certificates which have been published in that repository. A repository may also contain certification practice statements, as well as further information about certification authorities (particularly those certification authorities who publish information in the repository), notices of suspension or revocation, subscribers, information processing and electronic commerce standards, and similar materials.

1.28.2 Ordinarily, a repository will make its information available on-line. A repository's information may be made available to a broad, generally defined group of users or to a limited group, and its availability may be subject to conditions such as payment of fees, reasonable and regular hours of operation, security measures such as identification of persons or systems having access, etc. If a repository limits access restrictively, however, publication in such a repository would not serve as notice to someone not a member of the defined group. *See* Guideline 1.26 (publish), especially Comment 1.26.2.

1.28.3 *See* Guideline 1.21 (notify). The extent to which publication of information in a repository (or alternative methods of official or unofficial publication) can be considered to be constructive notice of the information, is a question which should be addressed in the future. *Cf.* Guideline 1.15 (incorporate by reference), particularly Comment 1.15.4; Guideline 1.22 (publish), particularly Comment 1.26.3.

1.29 Revoke a certificate

To permanently end the operational period of a certificate from a specified time forward.

Comment

1.29.1 Revocation is effected by notification or publication of a list

of revoked certificates, often termed a certificate revocation list ("CRL"), or through any other reasonable means by which a certification authority notifies a relying party that a certificate is revoked. It does not imply that a revoked certificate is destroyed or made illegible.

1.29.2 Guidelines 3.10 and 3.11 prescribe a certification authority's duties in revoking a certificate.

1.29.3 Guideline 1.37 (verify a digital signature) provides that a digital signature is not verifiable unless it is created during the operational period of the certificate. Since a revocation of the certificate ends the operational period under this Guideline 1.29 and under Guideline 1.22 ("operational period"), a digital signature created after revocation of a certificate is not verifiable by a public key listed in that certificate. The effect is that reliance on such digital signature is not reasonable. *See* Guideline 5.4 (listing factors relating the reasonableness of reliance), in particular Comment 5.4.2.

1.29.4 *See* Guideline (Initiating suspension or revocation) and Guideline 1.32 (suspend a certificate).

1.30 Signer

A person who creates a digital signature for a message.

Related Terms

"Signatory" is perhaps a more common synonym, but "signer" was selected for use in these Guidelines to avoid ambiguity arising from the various meanings of "signatory." A "signer" may, but need not, also be a "subscriber" of a certificate under Guideline 1.31 (subscriber).

Comment

1.30.1 Signing and digitally signing may include an agency relationship. For example, a corporation president may sign, with proper authority, and this signature is tantamount to that of the corporation.

1.30.2 If an imposter uses the private key of another person, without authority, to create a digital signature, that person is a

"signer" under this Guideline, but on behalf of himself rather than for the account of the rightful holder of the private key. But under Guideline 5.6(2) (presumptions in dispute resolution) if the rightful holder of the private key is the subscriber of a valid certificate, and the digital signature can be verified by reference to a public key listed in the certificate, the imposter's digital signature is rebuttably presumed to be the digital signature of the subscriber. *See* Guideline 1.14 (hold a private key); Guideline 5.6(2) (presumptions in dispute resolution); Guideline 1.37 (verify a digital signature).

1.31 Subscriber

A person who

(1) is the subject named or identified in a certificate issued to such person, and

(2) holds a private key that corresponds to a public key listed in that certificate.

Related Terms

See Comment 1.31.4 for relationship with "signer" in Guideline 1.30. Prior to issuance of a certificate, a subscriber is referred to as an "applicant" in some systems which require an application procedure to precede issuance. "Subscriber" under this Guideline is intended to include a reference to "applicant" unless the context clearly requires otherwise.

Comment

1.31.1 A subscriber is assumed in these Guidelines to be a person distinct from the certification authority and the person relying on the subscriber's certificate. These Guidelines do not apply to a situation in which an organization issues a "certificate" listing an employee or other agent as a "subscriber" for use within the organization only.

1.31.2 Guideline 3.2 (disclosure) reflects the fact that a certification authority, subscriber, and relying party tend to

have different access to and awareness of different facts. For example, Comment 3.2.1 requires a certification authority to disclose any financial interest the certification authority may have in an entity which is subscriber to that certification authority.

1.31.3 Part 4 of these Guidelines sets forth the obligations and duties of a subscriber.

1.31.4 A subscriber and a signer may, but need not, be the same person. A digital signature can exist without an associated certificate, in which case there is a signer but no subscriber. A certificate can exist with no associated digital signatures, in which case there is a subscriber but no signer. If an imposter gains access to the private key of a subscriber under certain circumstances, the digital signature of the imposter signer can be rebuttably presumed to be the digital signature of the subscriber. *See* Guideline 1.30 (signer), especially Comment 1.30.2.

1.32 Suspend a certificate

To temporarily suspend the operational period of a certificate for a specified time period.

Comment

1.32.1 Suspension is effected by notification or publication in a list of suspended and/or revoked certificates, often termed a certificate revocation list ("CRL"), or through any other means by which a certificate authority notifies a relying party that a certificate is revoked. Suspension does not imply that the suspended certificate is destroyed or made illegible.

1.32.2 Guidelines 3.9(suspension of certificate at subscriber's request) and 3.11 (revocation or suspension without subscriber's consent) set forth a certification authority's duties in suspending a certificate.

1.32.3 See Guideline 1.36 (valid certificate), which bases validity upon issuance plus acceptance alone. Validity is unaffected by revocation or suspension, which terminates or suspends only the operational period of a certificate - the period during which digital signatures must be created in order to be

verifiable by a public key listed in that certificate. *See* Guideline 1.37 (verify a digital signature).

1.32.4 If a certificate is suspended under this Guideline 1.32 rather than revoked under Guideline 1.29 (revoke a certificate), then the operational period is considered to be terminated for the duration of the period of suspension, with the effect that digital signatures created during the period of suspension cannot be verified under Guideline 1.37 (verify a digital signature). A suspension may be converted into a revocation, in which case no digital signature created after the beginning of the suspension period will become verifiable by reference to that certificate. If the conditions which caused the suspension are satisfactorily resolved, it is possible to end the suspension period and re-start the operational period, so that digital signatures created during the newly-started operational period will be capable of verification, until the originally-stated expiration of the operational period, assuming no additional suspension or revocation. Alternatively, it may be considered preferable to simply revoke the certificate and issue a replacement, notwithstanding the resolution of the condition which caused the suspension.

1.32.5 See Guideline 3.9 (suspension of certificate at subscriber's request), particularly Comment 3.9.2, for a discussion of the implementation of the suspension procedure prior to the time that suspensions have become widely adopted in recognized technical standards.

1.33 Time-stamp

(1) To create a notation that indicates, at least, the correct date and time of an action, and the identity of the person that created the notation; or

(2) Such a notation appended, attached or referenced.

Comment

1.33.1 The time-stamped message may be a digital signature or a hash result, or any other electronic record or unit of data. A certificate may also be time-stamped, either directly or by a time-stamp on the digital signature of the certification authority when issuing the certificate. Time-stamping is also important under Guideline 1.15 (incorporate by reference) to establish which version of an extrinsic message is incorporated by reference, and as a tool for the performance of many of the ancillary services described in Guideline 1.2 (ancillary services).

1.33.2 The timing of a digital signature in relation to the operational period of a certificate (defined in Guideline 1.22) is critical to the verification of the digital signature and message integrity under Guideline 1.37 (verify a digital signature). For example, a digital signature created after a certificate has expired, been revoked or suspended, or before it has been issued, is not verifiable under the rules of Guideline 1.37 (verify a certificate) even if the certificate is or subsequently becomes valid under Guideline 1.36 (valid certificate). Similarly, the digital signature of a certification authority on a certificate issued by the certification authority must be created during the operational period of the "certification authority certificate" (*see* Guideline 1.7) issued by the issuing authority higher in the hierarchy. A time-stamp on the certification authority's digital signature (or on the certificate or on internal auditable records of the certification authority) is thus critical to the verification of the certification authority's digital signature, and will also be a factor in determining the time and date when the certificate is issued, the beginning point of the certificate's operational period.

1.33.3 In addition to its effect upon the verifiability of the digital signature and the message integrity under Guideline 1.37, the time and date when the digital signature was created may under the circumstances also be an indicator that the digital signature is unreliable under Guideline 5.2.8 (unreliable digital signatures) for purposes of determining whether reliance on a certificate and a digital signature verifiable with reference to a public key listed in the certificate, is unreasonable under Guideline 5.4 (reasonableness of reliance), in particular Comment 5.4.3.

1.33.4 A time-stamp should be expressed in a form that clearly

indicates its frame of reference so that time-stamps are universally comparable, notwithstanding different time zones and seasonal adjustments.

1.33.5 The probative value of a time-stamp will depend in part upon the extent to which the time-stamp is provided by a trustworthy system defined by Guideline 1.35 (trustworthy system).

1.34 Transactional certificate

A certificate for a specific transaction incorporating by reference one or more digital signatures.

Related Terms

"Certificate" without "transactional" in these Guidelines generally refers to a certificate which states a time-based operational period as defined in Guideline 1.5 (certificate), unless the context clearly indicates otherwise.

Comment

1.34.1 A transactional certificate is a certificate that is specific to one or more specific transactions, and the digital signatures in those transactions, and is intended for use only with those signatures. Such a certificate may be useful, for example, for a certification authority which has agreed to act for only one transaction, or set of transactions, in which either of the parties or the certification authority do not wish to accept the greater risk of a certificate applicable to an unlimited number of digital signatures created within the certificate's operational period.

1.34.2 A transactional certificate is valid only for the digital signature(s) incorporated into it by reference. *See* Guideline 1.36 (valid certificate). In all other respects the transactional certificate is governed by the rules of these Guidelines governing certificates.

1.34.3 To illustrate, suppose a lawyer officiates at the closing of a real estate transaction in which the lawyer's client is to execute and deliver a deed to a grantee, and the deed is to be

electronically recorded immediately after it is signed. The lawyer then prepares a transactional certificate incorporating the digital signature on the deed by reference and containing his client's public key. The lawyer, acting as a certification authority for his client, the subscriber in this transaction, attaches the transactional certificate to the deed and transmits it to a public official for recordation. (This illustration does not address questions of local law applicable to specific types of transactions which require particular formalities such as delivery, etc.)

1.34.4 The practice of issuing transactional certificates with respect to digitally signed messages by certification authorities is analogous to traditional certification processes undertaken by notaries with respect to documents executed with pen and ink. *See* Guideline 1.6 (certification authority), particularly Comment 1.6.4.

1.35 Trustworthy system

Computer hardware, software, and procedures that:

(1) are reasonably secure from intrusion and misuse;

(2) provide a reasonably reliable level of availability, reliability and correct operation;

(3) are reasonably suited to performing their intended functions; and

(4) adhere to generally accepted security principles.

Comment

1.35.1 The objectives of a trustworthy system are, in essence:

- **Confidentiality**: Ensuring that information is not disclosed or revealed to unauthorized persons.

- **Integrity**: Ensuring consistency of data; in particular, preventing unauthorized creation, alteration, or destruction of data.

- **Availability**: Ensuring that legitimate users are not unduly denied access to information and resources.

- **Legitimate use**: Ensuring that resources are used only by authorized persons in authorized ways.

> WARWICK FORD, COMPUTER COMMUNICATIONS SECURITY: PRINCIPLES, STANDARD PROTOCOLS AND TECHNIQUES 13 (1994); *see also* MICHAEL BOTHE & WOLFGANG KILIAN, RECHTSFRAGEN GRENZüBERSCHREITENDER DATENFLüSSE 565-83 (1992).

1.35.2 A thorough description of how to achieve a trustworthy system is a technical subject outside the scope of this work. By way of example, the design, implementation, and maintenance of a trustworthy system would include measures:

- to prevent unauthorized access to or use of the system, especially of its private key, and particularly a certification authority's private key used in issuing certificates;

- to arrange personnel duties, access restrictions, and internal auditing procedures such that the system's security and operation cannot be compromised through the efforts of any single person having an interest in the outcome of system operations, or in collusion with other persons having an interest in the outcome of system operations;

- to provide failsafes and processes designed to minimize consequences, should a primary security measure fail;

- to reduce the effects of natural disasters and other forces majeures, as well as the risk of financial difficulties, sabotage, employee infidelity, and other foreseeable events;

- to maintain an auditable record of its services separately and independent of from its operative system.

This is only a partial list. For more information, *see, e.g.* UNITED STATES POSTAL SERVICE, DRAFT SECURITY POLICY: A REPORT BY THE SECURITY POLICY TEAM (1994) (unpublished study, on file with the U.S. Postal Service, c/o Joseph Wackerman, Esq., Washington D.C.), and consult works by experts in computer security, such as WARWICK FORD, COMPUTER COMMUNICATIONS SECURITY: PRINCIPLES, STANDARD PROTOCOLS AND TECHNIQUES (1994).

1.35.3 Computer security is a matter of degree rather than an absolute. In most situations, a greater degree of security is often possible, but may not be prudent or worthwhile under the circumstances. The determination whether a particular system is "reasonably secure," should be based on the following considerations:

- whether more secure or reliable systems and practices are available and feasible, and

- If such systems and practices are feasible and available, the cost of providing a higher level of assurance balanced against the seriousness of the risk incurred by forgoing the higher level of assurance.

Guideline 5.4 (reasonableness of reliance), especially Comment 5.4.4, relate to the reasonableness of reliance in view of the range of trustworthiness technologically available and the cost-benefit analysis inherent in assessing the reasonableness of a level of trustworthiness.

1.35.4 The design and operation of other systems required to be trustworthy and serving comparable users may be informative in evaluating the trustworthiness of a system, but should not be considered determinative.

1.35.5 As between a certification authority, repository, trustworthy

time-stamping service, or a subscriber generating a key pair, on the one hand, and a person relying on a certificate and/or digital signature on the other, a certification practice statement provides the details of what is "reasonably secure from intrusion and misuse,... provides a reasonably reliable level of availability," or is designed to satisfy the other general requirements of this Guideline. Notice of the statement to the relying person may affect the reasonableness of the reliance as provided in Guideline 5.4. However, a statute, regulation, or other law or public policy may preclude a certification authority, repository, or key-generating subscriber from unreasonably limiting the trustworthiness required for its system.

1.35.6 As Guideline 2.2 notes generally, the parties in a contractual relationship, such as a subscriber and certification authority, may agree between themselves regarding the specifics of the implementation of a trustworthy system.

1.35.7 The design and implementation of a trustworthy system will differ depending on what the system is expected to do. For example, the trustworthy system required for a time-stamping service will differ in some respects from the trustworthy system required for a certification authority, since the services of time-stamping and of issuing certificates differ. For time-stamping, a trustworthy system would obviously need to include functionality for accurately determining the time and date, but might not require the key management functionality which is central to the operations of a certification authority.

1.35.8 Guideline 3.1 requires certification authorities to utilize only trustworthy systems. Guideline 4.1 requires a subscriber to generate a key pair using a trustworthy system. Guideline 5.6(4) (presumptions in dispute resolution) creates a factual presumption of timing based on a time-stamp by a trustworthy system.

1.36 Valid certificate

(1) A certificate which (a) a certification authority has issued, and which (b) the subscriber listed in it has accepted; or

(2) A transactional certificate which (a) a certification authority has issued, and which (b) the subscriber listed in it has accepted, but limited to the digital signatures created pursuant to the specific transaction to which the transactional certificate relates.

Comment

1.36.1 Guideline 1.16 governs the question of whether the certificate has been "issued", and Guideline 1.1 governs the question of whether the subscriber listed in the certificate has "accepted" the certificate. Both issuance and acceptance are required for a certificate to be "valid" under this Guideline.

1.36.2 Guideline 1.22 provides that the "operational period" of a certificate (for purposes of digital signature verification under Guideline 1.37) begins upon issuance of the certificate, whether or not acceptance of the certificate has also occurred. For this reason, if issuance but not acceptance has occurred, the certificate is not yet valid (although its operational period has begun), but becomes valid if acceptance subsequently occurs. Until such time as acceptance has occurred (or if it never occurs), the certificate remains invalid and thus incapable of verifying any digital signature under Guideline 1.37 (verify a certificate), regardless of when the digital signature is created.

1.36.3 There is no inherent reason why a certification practice statement or other applicable rule could not allow a certificate to become valid upon acceptance following issuance, even if such acceptance occurs after the operational period has ended. Such retroactive validation, if allowed, would retroactively allow verification of digital signatures created during the operational period of the certificate. The circumstances of the tardy acceptance, however, may cause reliance upon the certificate (or upon a digital signature verified by reference to a public key contained in the certificate) to be unreasonable under Guideline 5.4 (reasonableness of reliance) because the digital signature is unreliable under 5.2.8(2) (unreliable digital signatures).

1.36.4 It may be advisable to establish a "rule of repose," whereby

actions occurring after a certain deadline (which could coincide with or occur later than the end of the certificate's operational period) will be ineffective to change the rights and obligations of the parties as they existed prior to such deadline. *Cf.,* Guideline 3.12 (notice of suspension or revocation) , particularly Comment 3.12.4, discussing the possibility of a similar rule of repose beyond which certification authorities are not required to provide services as to certificate revocation lists (CRL) and certificate revocation databases. *See also,* Guideline 3.5 (records), particularly Comment 3.5.4.

1.37 Verify a digital signature and message integrity

In relation to a given digital signature, message, and public key, to determine accurately:

(1) that the digital signature was created during the operational period of a valid certificate by the private key corresponding to the public key listed in the certificate; and

(2) the message has not been altered since its digital signature was created.

Comment

1.37.1 The purpose and technological basis of verification of digital signatures and message integrity is explained in greater detail in the Tutorial.

1.37.2 This Guideline 1.37, governing verification, relies closely upon the definitions of "valid certificate" in Guideline 1.36 and "operational period" in Guideline 1.22.

1.37.3 See Guideline 3.12 (notice of suspension or revocation,

particularly Comment 3.12.4, regarding the optional extension under X.509 v3 to set forth the operational period. The "validity period" field provided in the basic X.509 certificate relates to the beginning and end of the obligation to support certificates with CRL services, which should be distinguished from the use of "valid certificate" in these Guidelines.

2 General Principles

2.1 Interpretation

(1) Unless otherwise provided, these Guidelines should be interpreted so as to be consistent with what is commercially reasonable under the circumstances.

(2) Questions not expressly settled in these Guidelines should be settled in conformity with the general principles on which these Guidelines are based.

Comment

2.1.1 The requirement of commercial reasonableness lends meaning to general terms applied in specific factual situations, in order to prevent unjust evasion of responsibility for a harm that could have been averted or inequitably harsh results, and to ensure that the parties act in good faith. *See* HERBERT L.A. HART, THE CONCEPT OF LAW 121-50 (1961); Wolfgang Friedmann, *Legal Philosophy and Judicial Lawmaking*, 61 COLUM. L. REV. 821, 826-34 (1961) (surveying civil and common law views of judicial interpretation of legal texts).

2.1.2 General terms such as "reasonable" in the Guidelines afford an interpreter greater latitude than the standard principle of commercial reasonableness. "Reasonable" and similar words invite an equitable balancing of conflicting interests in a potentially complex factual situation, especially in a situation that may be difficult to foresee from the *a priori* vantage point of these Guidelines.

2.1.3 Both commercial reasonableness and the broader reasonableness standards invite resort to traditional interpretive guides such as the course of dealing between the

parties and usage of trade.

2.1.4 Under existing law, the concept of "commercially reasonable" is central to an understanding of security procedures required for electronic funds transfers. *Model Law on International Credit Transfers*, United Nations Commission on International Trade Law (UNCITRAL),28th Sess., art. 5(2)-5(3), U.N. Doc. (1994) (a sender is bound if "authentication is in the circumstances a commercially reasonable method of security against unauthorized payment orders, and the receiving bank complied with the authentication"); U.C.C. § 4A-202(b) (1992).

2.1.5 The concept of commercial reasonableness relates in some respects to the concept of good faith or *bona fides*, and the well-developed case law and scholarly discussion elaborating good faith may inform the meaning of commercial reasonableness. *See* U.C.C. § 1-203 (1992); *Principles of International Commercial Contracts*, International Institute for the Unification of Private Law (Unidroit), art. 1.7(1) ("Each party must act in accordance with good faith and fair dealing in international trade.") and art. 1.8(2) ("The parties are bound by a usage that is widely known to and regularly observed in international trade by parties in the particular trade concerned except where the application of such a usage would be unreasonable.") (1994).

2.2 Variation by agreement

Persons whose duties are prescribed by these Guidelines may more precisely define those duties by agreement among themselves.

Comment

2.2.1 A certification authority and subscriber may well have a contractual relationship, and their contract will affect their rights as between themselves. However, their contract does not bind

a person not a party to that contract, who potentially relies on a certificate or on a digital signature verifiable by a public key listed in the certificate. Notice of a policy or practice employed pursuant to that contract may, however, have an indirect impact upon the rights and obligations of the relying third party by affecting the reasonableness of such person's reliance. S*ee* Guideline 5.4 (factors relating to reasonableness of reliance).

2.2.2 Public policy or legislation may reasonably limit the extent to which the certification authority and subscriber may create enforceable agreements that are inconsistent with the fundamental principles of these Guidelines. For example, to protect relying persons' interests and maintain a general, minimal level of quality in certificates, legislation could limit or preclude a certification authority from disclaiming its implied representations under Guideline 3.7 (certification authority's representations in certificate). As another example, a certification authority may well specify details of its trustworthy system in a contract with a subscriber and in a certificate, but the effect of that specification should not be to relieve the certification authority from responsibility to utilize a trustworthy system pursuant to Guideline 3.1 (certification authority must utilize trustworthy system).

2.2.3 The contract between a certification authority and subscriber may consist of a certification practice statement to which the certification authority and subscriber assent. *See* Guideline 1.8 (certification practice statement).

2.2.4 Similar provisions preserving "party autonomy" are common in international settings, *see, e.g., Model Law on Electronic Commerce*, United Nations Commission on International Trade Law (UNCITRAL), 29th Sess., art. 4(1), at 3, U.N. Doc. A/CN.9/XXIX/CRP.1/Add.13 (1996) ("As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided, the provisions of Chapter III [Communication of Data Messages] may be varied by agreement."); *United Nations Convention on Contracts for the International Sale of Goods*, Official Records 178-190, art. 6, at 2, U.N. Doc. A/Conf. 97/19; Sales No. E.82.V.5 (1981), *reprinted in* 15 U.S.C.A. United Nations Convention on Contracts for the International Sale of Goods (West Supp. 1996) ("The parties may exclude the application of this Convention or, subject to article 12, derogate from or vary the effect of any of its provisions.").

2.3 Reliance on certificates foreseeable

It is foreseeable that persons relying on a digital signature will also rely on a valid certificate containing the public key by which the digital signature can be verified.

Comment

2.3.1 As explained in the Tutorial and in Guideline 1.27 (relying parties), reliance upon a digital signature is a two-step process. First, the relying party relies upon the verification of the digital signature under Guideline 1.37 to provide assurance that the private key corresponding to the public key listed in the certificate was used by the signer. Second, the relying party relies upon the accuracy of the certification authority's representations under Guideline 3.7 (certification authority's representations in certificate), particularly Comment 3.7.3, to provide assurance that the signer who holds the private key corresponding to the public key listed in the certificate is in fact the subscriber identified in the certificate, and not an imposter.

2.3.2 This Guideline is to avoid any doubt that such reliance on certificates in verifying digital signatures, and the risk of loss arising from such reliance, is foreseeable when a certification authority issues a certificate, *cf.* Ultramares Corp. v. Touche, 255 N.Y. 170, 174 N.E. 441 (1931).

2.3.3 Reliance on a certificate for reasons other than the verification of a digital signature may, however, not be foreseeable.

2.3.4 A certification authority is charged with treating its subscribers and others with ordinary care, such as is typical for commercial transactions, a lesser standard than what Benjamin Cardozo describes (in characterizing fiduciary duties) as "not honesty alone, but the punctilio of an honor the most sensitive, is then the standard of behavior." Meinhard v. Salmon, 249 N.Y. 458, 464 (1920). *See* Guideline 2.4 (fiduciary relationship).

2.4 Fiduciary relationship

A certification authority is a fiduciary to a subscriber where a certification authority holds that subscriber's private key or where provided by contract. A certification authority is not otherwise a fiduciary to a subscriber and is not a fiduciary to any relying party, except where provided by contract or by law.

Comment

2.4.1 A certification authority typically provides services at arm's length and does not create a special trusted relationship with its subscribers or relying parties, such as a fiduciary relationship.

2.4.2 Certification authority services vary considerably and neither create nor inherently require a fiduciary relationship, except in a case where the certification authority holds the private key of a subscriber or where an agreement (such as a subscriber agreement or certification practice statement) expressly creates a fiduciary relationship.

2.4.3 The commercial marketplace and usage of trade will ultimately determine the extent of any demand for "fiduciary-like" certification services. *See* the discussion of ancillary services such as commercial key escrow and private key trust service under Guideline 1.2 (ancillary services).

3 Certification Authorities

3.1 Certification authority must use trustworthy systems

A certification authority must utilize trustworthy systems in performing its services.

Comment

3.1.1 Guideline 1.35 (trustworthy system), particularly Comment 1.35.3, notes that computer security is a matter of degree. The degree of security should be determined according to a reasonableness standard in light of the factors listed in Comment 1.35.3 to Guideline 1.35 (trustworthy system).

3.1.2 Because the requirement of this Guideline 3.1 is a *sine qua non* of the achievement of nonrepudiation under these Guidelines, any legislative or regulatory implementation of these Guidelines should therefore restrict any attempts by the certification authority to dilute its obligation to use trustworthy systems by certification practice statement under Guideline 1.8 (certification practice statement), contract under Guideline 2.2 (variation by agreement), or otherwise.

3.2 Disclosure

(1) A certification authority must disclose any material certification practice statement, as well as notice of the revocation or suspension of a certification authority certificate.

(2) A certification authority must use

reasonable efforts to notify any persons who are known to be or foreseeably will be affected by the revocation or suspension of its certification authority certificate.

(3) A certification authority may require an authenticated message or document from an identified person as a condition precedent to effecting a disclosure required in paragraph (1) above.

(4) In the event of an occurrence which materially and adversely affects a certification authority's trustworthy system or its certification authority certificate, the certification authority must use reasonable efforts to notify any persons who are known to be or foreseeably will be affected by that occurrence, or act in accordance with procedures specified in its certification practice statement.

Comment

3.2.1 The certification authority must comply with its duty to disclose information within a commercially reasonable time. *See* Guideline 2.1 (generally requiring commercial reasonableness in the interpretation of these Guidelines).

3.2.2 A certification authority may well disclose further information in order to reduce its risk of liability. Furthermore, additional disclosure may be required to serve regulatory objectives. For either risk management or regulatory purposes, a certification authority should disclose any known fact adversely and materially affecting reliance upon a certificate or a digital signature verifiable by reference to a public key listed in a certificate.

3.3 Financial responsibility

A certification authority must have sufficient financial resources

(1) to maintain its operations in conformity with its duties, and

(2) to be reasonably able to bear its risk of liability to subscribers and persons relying on certificates issued by the certification authority and digital signatures verifiable by reference to public keys listed in such certificates.

Comment

3.3.1 A certification authority's overall risk of liability will largely be a function of (1) its success in implementing a trustworthy system and utilizing the services of competent, conscientious personnel, (2) the number of certificates outstanding, and (3) the amounts at stake in transactions in which issued certificates are used (since those amounts tend to become damages if the certification authority is held liable), all evaluated in light of any applicable limits upon legal liability and cautionary notices of recommended reliance limits. The certification authority can control factors (1) and (2), but can do little to manage its risk in regard to factor (3), unless an applicable certification practice statement, or legislation, states that an issued certificate is not suitable for transactions in excess of a monetary amount specified either generally in the certification practice statement or specifically in regard to a particular certificate. *See, e.g.,* UTAH CODE ANN. §§ 46-3-103 and 46-3-309 (1996).

3.3.2 If a relying party has notice of such a recommended limit on reliance, reliance in excess of the specified amount may well be unreasonable under Guideline 5.4 (reasonableness of reliance), since a relying person would have notice that the

certificate was not considered suitable for transactions in excess of the specified amount. However, even with such a recommended reliance limitation, in an open system, the certification authority cannot control or even ascertain reliably its aggregate liability for a particular certificate (i.e., the recommended reliance multiplied by the number of times a particular certificate is used to verify digital signatures).

3.3.3 Financial responsibility may be assured through security arrangements such as surety bonds or standby letters of credit, or perhaps through liability insurance, when it becomes more widely available. For information on the insurability of certification authorities, *see generally* MICHAEL S. BAUM, FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY: LAW AND POLICY OF CERTIFICATE-BASED PUBLIC KEY AND DIGITAL SIGNATURES § 9(b), 337-347 (1994).

3.3.4 The adequacy of an issuing certification authority's financial responsibility is a factor to consider in assessing the reasonableness of one's reliance on a certificate and digital signatures verified with reference to a public key listed in that certificate. *See* Guideline 5.4 (reasonableness of reliance).

3.4 Employees and contractors

A certification authority must formulate and follow personnel practices which provide reasonable assurance that the trustworthy system of the certification authority is supported by the performance of duties of employees and contractors on behalf of the certification authority.

Comment

3.4.1 Although not every employee or contractor of a certification authority will need to meet rigorous security requirements, a certification authority should take care not to overlook any worker's potential to cause problems. As much as possible,

processes should be designed to prevent, correct, or reveal human error or tampering, and to minimize consequences of error or misconduct. Procedures for auditing and oversight of all certification-related personnel activities should be thorough and rigorous.

3.4.2 Because certain activities of a certification authority, such as suspensions and revocations of certificates, require a prompt response, it is imperative that staffing levels should suffice to provide all necessary services at the times specified in a certification practice statement and/or contracts with subscribers, or at reasonable times if a certification practice statement or contract does not specify times when services are to be available.

3.5 Records

A certification authority must

(1) document all facts material to the issuance, suspension, or revocation by it of a certificate, and

(2) retain that documentation for an appropriate period of time.

Comment

3.5.1 Records documenting issuance of a particular certificate could include, for example, a passport or driver's license, and records evidencing all other steps taken to confirm the identity of the subscriber and the other facts represented by the certification authority in issuing a certificate. If the subscriber is a corporation, the required records might include copies of a resolution of its board of directors, minutes and due notice of the meeting at which the resolution was adopted, and a certificate of good standing from the registry of corporations. *See* Guideline 3.7 (certification authority's representations in certificate).

3.5.2 A certification authority should specify what it considers to

be an appropriate record retention period in a certification practice statement or contract with a subscriber. See Guideline 3.2 (disclosure) for the certification authority's requirement to disclose certification practice statements.

3.5.3 The record retention period may depend upon various factors, including: contractual obligations to subscribers, statutory record retention requirements, and business needs. For example, digital signatures used in land transactions may be contestable for a period specified under local land registry laws, and must be accessible during such period. Subscribers to a certification authority involved in land transactions would therefore have a business need for record retention over that period.

3.5.4 The question of how long a certification authority must provide certification revocation list and data services after the end of a certificate's operational period is discussed in Guideline 1.36 (valid certificate), particularly in Comments 1.36.3 and 1.36.4, and in Guideline 3.12 (notice of suspension or revocation), particularly Comment 3.12.4.

3.6 Availability of the certification authority certificate

A certification authority must make a copy of its own certification authority certificate available to any person duly verifying a digital signature, if that digital signature is verifiable by reference to a public key listed in a certificate issued by the certification authority.

Related Terms

The term "issuing authority" is sometimes used in a hierarchical certificate-based system to refer generically to all entities who issue certificates to any person (including subscribers who are themselves certification authorities, as well as subscribers who intend to create digital signatures as end-users). In such a

system, the term "certification authority" is reserved for those entities who issue certificates to end-users only. In such a system, the certification authority (who issues certificates to end-users only) would be issued its own certification authority certificate by an "issuing authority." Extrapolating further up the hierarchical chain, that issuing authority (and all higher issuing authorities including the root) would be subscribers of "issuing authority certificates." *See* Guideline 1.7 (certification authority certificate).

Comment

3.6.1 Because a certification authority is in the business of enabling others to rely on its certificates and the digital signatures of its subscribers, the certification authority has a greater duty than an ordinary subscriber to make its certification authority certificate available. A certification authority certificate must be easily and conveniently available for reference in a trustworthy manner.

3.6.2 This Guideline 3.6 does not require publication or disclosure of any certificate other than the certification authority certificate.

3.7 Certification authority's representations in certificate

By issuing a certificate, a certification authority represents to any person who reasonably relies on a certificate or a digital signature verifiable by the public key listed in the certificate, that the certification authority, in accordance with any applicable certification practice statement of which the relying person has notice, has confirmed that

(1) the certification authority has complied with all applicable requirements of these Guidelines in issuing the certificate, and if the certification authority has published the certificate or otherwise made it available to such

reasonably relying person, that the subscriber listed in the certificate has accepted it,

(2) the subscriber identified in the certificate holds the private key corresponding to the public key is listed in the certificate,

(3) if the subscriber is acting through agents, that the agents have authority to accept the certificate for the subscriber,

(4) the subscriber's public key and private key constitute a functioning key pair, and

(5) all information in the certificate is accurate, unless the certification authority has stated in the certificate or incorporated by reference in the certificate that the accuracy of specified information is not confirmed.

Further, the certification authority represents that there are no known, material facts omitted from the certificate which would, if known, adversely affect the reliability of its representations under this Guideline.

Comment

3.7.1 The certification authority is required to "confirm" the information described in this Guideline. "Confirm" is defined by Guideline 1.9 as "ascertain through appropriate inquiry and investigation." This Guideline 3.7 does not require the

certification authority to guarantee or underwrite the factual accuracy or legal significance of the confirmed information. The level of investigation required will vary according to the circumstances for which a certificate is intended, and may be increased by a certification practice statement or contract. The certification authority may specify in a certification practice statement the detailed method and practices it uses for confirming the information in the certificate.

3.7.2 The certification authority's representations in the certificate as required by this Guideline may be express, or may be implied by law into the certificate through statute, regulation, contract, or an applicable certification practice statement.

3.7.3 The certification authority's representation under paragraph (2) implements the certification authority's confirmation of binding between the identity of the subscriber listed in the certificate, and the public key listed in the certificate. Binding between the identity of the subscriber and the subscriber's purported digital signature is accomplished indirectly through the process of verification of the digital signature under Guideline 1.37 (verify a digital signature). *See* Tutorial, *supra.* If the private key held by a subscriber is compromised, so that an imposter signer other than the subscriber uses subscriber's private key without authority, then the subscriber may be rebuttably presumed to be the signer under Guideline 5.6(2) (presumptions in dispute resolution), and even if the subscriber may rebut such presumption factually, the subscriber may nonetheless be liable to the relying party if the subscriber is in breach of its responsibility to safeguard its private key under Guideline 4.3 (safeguarding the private key).

3.7.4 Pursuant to paragraph (5) of this Guideline 3.7, if the accuracy of information in the certificate is not confirmed by the certification authority, the certification authority must clearly state or incorporate by reference which information in the certificate is not confirmed. *See generally,* ITT X.509 v3, which provides the capability to provide such notification to a party relying on the certificate and digital signatures verified with reference to a public key stated in the certificate.

3.7.5 *See* Guideline 4.2 (subscriber's representations) for related representations by the subscriber as to the accuracy of information furnished to the certification authority, including information contained in the certificate issued by the certification authority. Guideline 4.2(3) complements Guideline

3.7(1) by providing the certification authority a remedy against the subscriber in the event subscriber's failure to accept causes the certification authority to be liable to a relying party because of such party's reasonable reliance upon a published yet invalid certificate.

3.8 Prerequisites to disclosure of certificate

A certification authority must not publish a certificate or otherwise make it available to a person known by the certification authority to be in a position to rely on the certificate or on a digital signature which is verifiable with reference to a public key listed in the certificate, if the certification authority knows that

(1) the certification authority listed in the certificate has not issued it, or

(2) the subscriber listed in the certificate has not accepted it.

Comment

3.8.1 Guideline 4.5 (availability of the certificate) requires a subscriber to make a copy of the certificate available to a person relying on the subscriber's digital signature, a duty that may often be facilitated by publication of the certificate; *see* Guideline 1.26 (publish). In any event, a relying party needs a copy of the certificate in order to verify the digital signature, and repositories have an incentive to make certificates available for verification. This Guideline is intended to provide assurance that published (or otherwise available) certificates are suitable for disclosure, in order to protect:

- **The reliance interest of parties relying on digital signatures.** Publication or disclosure of the certificate places potentially relying parties in a position to rely on a certificate which has become valid because it has been both issued and accepted. See Guideline 1.36 (valid certificate).

- **A purported subscriber from claims** of a person who relied upon a certificate without the purported subscriber's acceptance under Guideline 1.1 (accept a certificate).

- **A purported subscriber's right to privacy** and right to be free from injurious falsehood. Publication of a certificate which has not been accepted by subscriber may disclose an identification, business relationship, or other fact which the purported subscriber wishes to keep confidential, and may have a right to keep confidential under applicable privacy law. *See, e.g.,* European Union Council and European Parliament, Directive on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data (1995); *see generally* IAN J. LLOYD & MOIRA SIMPSON, LAW ON THE ELECTRONIC FRONTIER 31-59 (1994) (policies and British legislation on data bank privacy); M. ETHAN KATSH, LAW IN A DIGITAL WORLD 227-36 (1994). Moreover, an unaccepted certificate may contain misrepresentations whose publication or disclosure injures the purported subscriber.

3.8.2 A finder of fact should apply an objective test in determining whether a certification authority knows that a person is in a position to rely upon the certificate or a digital signature verifiable by reference to a public key listed in the certificate. In other words, a certification authority should be deemed to know a fact if the certification authority could not reasonably be unaware of it. This standard is different from the standard applicable when a certification authority confirms information under these Guidelines pursuant to Guideline 1.9 (confirm).

3.8.3 If a certification authority discloses a certificate that is not valid under Guideline 1.36 (valid certificate) because it has not been both issued to, and accepted by, a person who has or receives the subscriber's digital signature (and thus is a relying party within the meaning of Guideline 1.27), the certification authority has breached its duty under this Guideline,

regardless of whether the certification authority knew that the person was a relying party.

3.8.4 Since the purpose of a certificate is to enable parties other than the issuing certification authority and accepting subscriber to rely on it, creation of a certificate should ordinarily occur with the expectation of issuance and acceptance. A prudent certification authority will create a certificate only for a subscriber expressing a desire to obtain a certificate or a willingness to accept one. In the absence of evidence of express acceptance, acceptance may be implied under Guideline 1.1 (accept a certificate), particularly Comment 1.1.3, especially in cases where the subscriber has applied to have the certificate issued.

3.9 Suspension of certificate at subscriber's request

Unless a contract between the certification authority and the subscriber provides otherwise, a certification authority must suspend a certificate as soon as possible after a request by a person whom the certification authority reasonably believes to be

(1) the subscriber listed in the certificate,

(2) a person duly authorized to act for that subscriber, or

(3) a person acting on behalf of that subscriber, who is unavailable.

Comment

3.9.1 Certification authorities may receive requests to invalidate certificates in situations where it is impossible to confirm the identity of the person making the request. In such situations, the request may in fact be a subscriber or another person such as someone attending an injured subscriber seeking to avoid the consequences of a compromise of the private key, or the request may be a prank or attack designed to hinder or disadvantage the subscriber. Since the certification authority lacks time under the circumstances to confirm the fact of request and the identity of the requester, any action it takes may be the result of a mere guess. If the subscriber uses digital signatures extensively or is a certification authority that has issued many outstanding certificates, the consequences of a revocation (which is permanent and irreversible) would be catastrophic. Suspension of the certificate, which is temporary and reversible by request, is a less drastic intermediate remedy permitting a certification authority additional time to confirm the material facts. While suspensions may still cause losses, those losses will be far smaller and easier to absorb than losses due to revocation.

3.9.2 The ability to suspend a certificate is an important part of the means by which the subscriber can manage the risk incurred by holding a private key, which may be subject to compromise. Many technical standards fail to provide for suspension of certificates, so that some actual implementations of these Guidelines may not provide for suspension of certificates. Technical research in this area continues. However, the certification authority should not fail to provide a means of suspending certificates without clearly apprising the subscriber of the unavailability of a means of interrupting the subscriber's digital signature capability short of revoking the certificate.

3.9.3 Since suspension is likely to occur in emergency situations, such as when a subscriber has just lost a key, a certification authority should provide a means of quickly executing requests to suspend. The meaning of "as soon as possible" in a particular set of circumstances is a question of fact informed by usage of trade.

3.9.4 Since suspensions must generally be effectuated with haste, the certification authority is not required to confirm any fact before suspending. However, the certification authority should ascertain through simple inquiry (but not necessarily with confirmation) that the person requesting suspension is or at least claims to be the subscriber or one acting on behalf of

an unavailable subscriber.

3.9.5 A suspension should specify when it takes effect and ends. If no effective date is specified, one may refer to available extraneous evidence and presume that a suspension was to take effect immediately upon request, or as determined in light of usage of trade.

3.9.6 *See* Guideline 1.32 (suspend a certificate), particularly Comment 1.32.4, regarding the effect upon the operational period when a suspension is converted to a revocation.

3.9.7 The availability of suspension may be varied by contract between the certification authority and subscriber. Because confirmed authentication is not required for suspension under this Guideline, a subscriber may have an interest in altering this rule by agreement with the certification authority, by specifying a particular method of authenticating a subscriber's request to suspend.

3.10 Revocation of certificate at subscriber's request

The certification authority which issued a certificate must revoke it at the request of the subscriber listed in it, if the certification authority has confirmed

(1) that the person requesting revocation is the subscriber listed in the certificate to be revoked, or

(2) if the requester is acting as an agent, that the requester has sufficient authority to effect revocation.

Comment

3.10.1 A revocation should specify the date and time when it takes effect. If no effective date is specified, one may refer to available extraneous evidence and presume that a revocation is to take effect immediately upon request, or as determined in light of usage of trade.

3.10.2 Pursuant to Guideline 1.22 (operational period of a certificate) the operational period, and thus the period during which digital signatures must be created in order to be verifiable under Guideline 1.37 (verify a digital signature), is terminated prematurely by a revocation. *See* Guideline 3.12 (notice of suspension or revocation), for the requirement of prompt publication and notice of the revocation.

3.10.3 The time for effecting a revocation may be critical. If a suspension of the certificate is already in effect, the certification authority should, whenever possible, avoid a gap between suspension and revocation by effecting the revocation before the expiration of the suspension period. *See* Guideline 1.32, particularly Comment 1.32.4, for the treatment of the conversion of a suspension into a revocation.

3.11 Revocation or suspension without the subscriber's consent

A certification authority must suspend or revoke a certificate, regardless of whether the subscriber listed in the certificate consents, if the certification authority confirms that

(1) a material fact represented in the certificate is false,

(2) a material prerequisite to issuance of the certificate was not satisfied, or

(3) the certification authority's private key or trustworthy system was compromised in a manner materially affecting the certificate's reliability.

Upon effecting such a suspension or revocation, the certification authority must promptly notify the subscriber listed in the suspended or revoked certificate.

Comment

3.11.1 This power to revoke or suspend unilaterally should be exercised pursuant to applicable certification practice statements and security policies, or incorporated into the contract between the certification authority and the subscriber. If the power is not based on statute or other widely known or ascertainable law, the certification authority should apprise the subscriber before issuing the certificate that it may be revoked or suspended without the subscriber's consent.

3.11.2 Paragraph (1) does not impose an obligation on the certification authority to monitor the accuracy of the information in the certificate over time. However, if the certification authority confirms that a material fact represented in the certificate is false, the certification authority must suspend or revoke the certificate to prevent prospective harm to persons potentially relying on digital signatures verifiable by reference to the certificate.

3.11.3 A certification authority revoking a certificate without a subscriber's consent may severely disrupt the subscriber's business, and should give the best and earliest notice of the revocation possible under the circumstances.

3.11.4 Although this Guideline is worded in the singular, some of the problems that could require revocation regardless of consent could affect multiple certificates. For such problems, the certification authority will need to determine quickly the extent of the damage, to revoke all unreliable certificates, but

leave unaffected ones intact.

3.11.5 A certification authority may incur liability for revoking a certificate without the subscriber's consent, if the certification authority was at fault. The certification authority could mitigate its liability by promptly replacing the revoked certificate. The certification practice statement (or contract between certification authority and subscriber) should provide the extent of damages recoverable by the subscriber (e.g., restitution of the price paid for the certificate), subject to any limitation of damages (e.g., disclaimer of consequential damages or a cap upon damages) set forth in such certification practice statement or contract.

3.11.6 *See* Guidelines 3.12 (notice of suspension or revocation) and 1.32 (suspend a certificate), regarding notice to the potential relying parties of a revocation or suspension, and the effect of reliance upon a certificate during a period of suspension or after an operational period which has been truncated due to revocation, prior to receipt of notice of the revocation or suspension.

3.12 Notice of suspension or revocation

Promptly upon suspending or revoking a certificate, a certification authority must publish notice of the suspension or revocation if the certificate was published, and otherwise must disclose the fact of suspension or revocation on inquiry by a relying party.

Comment

3.12.1 "Promptly" means that the certification authority must act with appropriate dispatch. The certification authority should consider the need to act promptly in revoking, suspending, publishing notice and responding to inquiry, when planning staffing levels (*see* Guideline 3.4, employees and contractors) and designing the trustworthy system (*see* Guideline 3.1, certification authority must utilize trustworthy system) and

Guideline 1.35 (trustworthy system).

3.12.2 For a suspension or revocation of a certificate to be effective in relation to a party in a position to rely upon the certificate and digital signatures verifiable with reference to a public key listed in the certificate, such relying party must be notified of revocation before reliance occurs. Relying on a revoked certificate despite notice of revocation is very likely to be considered unreasonable reliance upon the certificate and the digital signatures verifiable with reference to the public key listed in the certificate, under Guideline 5.4 (reasonableness of reliance).

3.12.3 It is important to realize that the end of the "operational period" of a certificate under Guideline 1.22 (operational period) does not terminate the "validity" of a certificate under Guideline 1.36 (valid certificate), even if the operational period ends by reason of revocation or suspension. Thus, if a digital signature has been created during the operational period of a certificate, that digital signature may be verified by a certificate long after the operational period ends by reason of expiration, revocation or suspension.

3.12.4 It may be desirable to create a "rule of repose" which expires the obligation of the certification authority to continue to publish notice of revocation, maintain a CRL and provide related certificate revocation database services, and/or to respond to inquiries, with respect to a particular certificate. Such expiration would occur after the passage of some stated period of time subsequent to the stated expiration date of a certificate's operational period. Such a strategy would avoid the overhead of perpetual maintenance of data with little adverse impact upon relying parties. Although it is possible for a digital signature to be created during an operational period of a certificate which expired long ago (which causes it to be verifiable by the certificate), fresh reliance upon such a stale certificate is factually unlikely and therefore unlikely to be considered reasonable reliance under Guideline 5.4 (reasonableness of reliance). *Cf.,* ITT X.509 v3, under which "operational period" is now an optional extension under X.509 v3, and the field for "validity period" in the basic certificate has been clarified to have a beginning and end date related to the obligation to support certificates with CRL services. *Information Technology - Security Frameworks in Open Systems - Non-repudiation Framework* (also *ITU-T Recommendation X.813*), ISO/IEC 10181-4 (1996), and

Authentication Framework, as modified by Technical Corrigendum 1 (1995) and *Amendment 1 on Certificate Extensions* (1996).

3.13 Termination of business with minimal disruption

A certification authority may discontinue providing certification authority services only

(1) after notifying subscribers listed in valid certificates issued by the certification authority,

(2) in a manner that will cause minimal disruption to the subscribers of valid certificates and to relying parties, and

(3) after making reasonable arrangements for preservation of the certification authority's records.

Comment

3.13.1 When a certification authority stops or curtails operations without adequate provision for an orderly transfer of its business to a reliable successor, all of the certification authority's outstanding certificates, other than transactional certificates, will generally be revoked. The revocation truncates the certificates' operational periods pursuant to Guideline 1.22, but has no effect on the continuing validity of the certificates for purposes of verification of digital signatures created prior to the end of the operational period. See Guideline 1.37 (verify a digital signature). *But see* Guidelines 1.36, (valid certificate) particularly Comment 1.36.4, and

Comment 3.12.4 (discussion of a possible rule of repose terminating certification authority's duty to provide certificate revocation list support for certificates subsequent to a date long after the termination of the certificate's operational period.)

3.13.2 The concept of "minimal disruption" should be interpreted in light of commercial reasonableness as required by Guideline 2.1(1). Thus, a withdrawing certification authority is not required to do everything possible to avoid disruption to subscribers, but rather, should make commercially reasonable efforts to minimize such disruption.

3.14 Liability of complying certification authority

A certification authority that complies with these Guidelines and any applicable law or contract is not liable for any loss which

(1) is incurred by the subscriber of a certificate issued by that certification authority, or any other person, or

(2) is caused by reliance upon a certificate issued by the certification authority, upon a digital signature verifiable with reference to a public key listed in a certificate, or upon information represented in such a certificate or repository.

Comment

3.14.1 The effect of this Guideline is to preclude liability for breach of a duty not included in these Guidelines. The role of a

certification authority is developing, and few will enter this uncharted area of business without first having the basic rules established with sufficient clarity to enable an evaluation of the legal risks of the new business. The Guidelines contain basic rules for certification authorities, and this Guideline seeks to limit the legal risk to those described in these Guidelines.

3.14.2 A certification practice statement or other contract or representation of the certification authority may include additional duties not inconsistent with these Guidelines.

4 Subscribers

4.1 Generating the key pair

If the subscriber generates the key pair whose public key is to be listed in a certificate issued by a certification authority and accepted by the subscriber, the subscriber must generate that key pair using a trustworthy system.

Comment

4.1.1 A trustworthy system includes a requirement that the asymmetric cryptosystem used to generate the key pair be used according to the asymmetric cryptosystem's specifications. *See* Guideline 1.3 (asymmetric cryptosystem).

4.1.2 A certification authority's certification practice statement should identify which particular asymmetric cryptosystems (including the algorithms for generating the key pair and creating and verifying the digital signature) are supported by the certification authority, all of which must be trustworthy systems pursuant to Guideline 3.1 (certification authority must utilize trustworthy systems).

4.2 Subscriber's obligations

(1) All material representations made by the subscriber to a certification authority, including all information known to the subscriber and represented in the certificate, must

be accurate to the best of the subscriber's knowledge and belief, regardless of whether such representations are confirmed by the certification authority.

(2) A subscriber who provides an otherwise unpublished certificate to a relying party must disclose that fact to the certification authority.

(3) If the foreseeable effect would be to induce or allow reliance upon a certificate which is invalid because the subscriber has not accepted it, the subscriber must not knowingly create digital signatures using a private key corresponding to any public key listed in such certificate.

Comment.

4.2.1 This Guideline requires the subscriber to correct affirmative misrepresentations, ambiguities, vagueness resulting in error, and omissions that are misleading to a certification authority issuing a certificate to the subscriber. Further, a subscriber who receives notice of a certificate has a duty to notify the certification authority if any information is incorrect. The "information known to the subscriber and represented in the certificate" includes all information in the certificate originating with the subscriber and all information of whose factual accuracy the subscriber could not be unaware.

4.2.2 The subscriber owes the duty prescribed by this Guideline to both the certification authority and any person relying on a digital signature verifiable by the public key listed in the certificate.

4.2.3 A subscriber may not eliminate by contract or disclaim its duty to accurately represent the known, material facts to the certification authority; however, the subscriber and the certification authority may agree concerning details of that duty and appropriate remedies as between themselves. Such contracts are unlikely to bind relying parties who are not parties to such contracts, especially in the absence of notice. S*ee* Guideline 2.2 (variation by agreement), especially Comment 2.2.1.

4.2.4 Liability for misrepresentation by the subscriber to the certification authority attaches as of the time the subscriber accepts the certificate. In other words, by accepting a certificate from a certification authority, a subscriber in effect affirms that all material information presented to the certification authority is true.

4.2.5 Guideline 3.7 (certification authority's representations in certificate) provides complementary requirements for certification authorities. It requires an issuing certification authority to confirm the accuracy of certain representations in the certificate. Taken together, this Guideline and Guideline 3.7 (certification authority's representations in certificate) require that all information in the certificate either be confirmed by the certification authority or be accurate according to the subscriber's duty in this Guideline. Some information, notably the subscriber's identification, is both confirmed by the certification authority and subject to this Guideline's requirement that the subscriber make accurate representations.

4.2.6 Guideline 4.2(3) (representations of subscriber) complements Guideline 3.7(1) (representations of certification authority regarding validity of published certificate). If the certification authority is liable to a relying party who reasonably relies upon a published certificate which was invalid because of the failure of the subscriber to accept it, this guideline 4.2(3) provides the certification authority a remedy against the subscriber who failed to accept the certificate, yet used the certificate under circumstances where reliance was foreseeable. See Guideline 1.1 (accept) for circumstances under which the acceptance of the subscriber may be implied in order to cause the certificate to be valid. See also the more detailed explanation of the liability among the parties in connection with issuance and acceptance.

4.3 Safeguarding the private key

During the operational period of a valid certificate, the subscriber shall not compromise the private key corresponding to a public key listed in such certificate, and must also avoid compromise during any period of suspension.

Comment

4.3.1 To safeguard the private key, access to it should require entry of a personal identification code, or the presentation of some other fact uniquely within the knowledge or control of the subscriber rightfully holding the private key. Some of the methods for securing private keys are described in WARWICK FORD, COMPUTER COMMUNICATIONS SECURITY: PRINCIPLES, STANDARD PROTOCOLS & TECHNIQUES 249-260 (1994). This area of technology is developing rapidly.

4.3.2 This Guideline is intentionally silent about the precise standard of care applicable to a subscriber's duty not to divulge the private key. The intention of this Guideline 4.3, however, is generally to impose a stronger duty of care on the subscriber than is currently imposed on a holder of an ATM card or a credit card. 12 C.F.R. part 205 (1994) (Federal Reserve Reg. E). The election of a precise standard of care presents a difficult question of public policy that could be resolved in implementing legislation; *see, e.g.,* UTAH CODE ANN. § 46:3-305 (1996) (Utah Digital Signature Act) (noting alternative standards of care for control of one's private key).

4.3.3 Examples of involuntary loss of control over the private key include: disclosure of the private key to a person not authorized to sign on the subscriber's behalf, loss of the medium on which the private key is recorded, and eavesdropping on use of the private key in insecure circumstances.

4.3.4 The loss of control over the private key proscribed by this Guideline may also occur through intentional disclosure. Persons who intentionally discloses their private keys, with or without fraudulent intent, should be held to a higher standard than an involuntary discloser. For example, if a person publicly posts a private key in an effort to make it difficult to prove liability for a fraudulent act, Guideline 5.6 (certification authority's representations in certificate) should be invoked to place the burden of disproving the authenticity of the digital signature on the person who publicly posted the private key and then repudiated a document signed with that key.

4.3.5 If a private key is compromised, and a certificate has been issued listing the corresponding public key, the appropriate corrective action is to revoke the certificate, or to suspend the certificate without delay until revocation can be effected. *See* Guideline 4.4 (initiating suspension or revocation); *see also* Guidelines 3.10 (revocation of certificate at subscriber's request) and 3.9 (suspension of certificate at subscriber's request). Once the certificate is suspended or revoked, reliance on a digital signature verifiable by reference to that certificate is ordinarily unreasonable. *See* Guideline 5.4 (reasonableness of reliance), especially Comment 5.4.2. By suspending or revoking, the subscriber has thus mitigated the consequences of compromising the private key.

4.3.6 A private key, as defined in these Guidelines, is not intended to be an "access device" within the meaning of 12 C.F.R. § 205.2(a)(1) (1994) (Regulation E of the Board of Governors of the Federal Reserve System), but rather a device for creating a digital signature which satisfies a requirement of a signature as provided in Guideline 5.2 (satisfaction of signature requirements). Therefore, loss of a private key is not intended to be governed by the provisions of Regulation E concerning loss of an access device, *see* 12 C.F.R. § 205.6 (1994).

4.4 Initiating suspension or revocation

A subscriber who has accepted a certificate must request the issuing certification authority to suspend or revoke the certificate if the private key corresponding to the public key listed in the certificate has been compromised.

Comment

4.4.1 Suspension (Guideline 3.9) and revocation (Guideline 3.10) of the certificate are remedial actions for a compromise of the security of a private key, which must be uniquely within the control of the subscriber. *See* Guideline 4.3 (safeguarding the private key).

4.4.2 Pursuant to Guidelines 1.29 (revociation of certificate) and 1.32 (suspension of certificate), suspension or revocation of the certificate has the effect of suspending or terminating the certificate's operational period as defined by Guideline 1.22 (operational period). Although the end of the operational period means that no subsequently created digital signatures may be verified by the certificate under Guideline 1.37 (verify a certificate), the end of the operational period does not affect the validity of the certificate under Guideline 1.36 (valid certificate) for purposes of verifying digital signatures which were created before the operational period was terminated by the suspension or revocation.

4.4.3 Because an issued certificate has been digitally signed by the certification authority, message integrity of the certificate is implied by Guideline 1.19 (message integrity). Therefore, the only acceptable method of amending the contents of the certificate is for the certification authority to revoke the certificate pursuant to the subscriber's request under Guideline 3.10 (revocation of certificate at subscriber's request) or

without the subscriber's consent under Guideline 3.11 (revocation of certificate without subscriber's consent), and then issue another certificate.

4.4.4 Suspension or revocation of a certificate (which truncates the operational period under Guideline 1.22 (operational period of a certificate) may be accomplished under this Guideline once a certificate has been issued by the certification authority under Guideline 1.16 (issue), whether or not the certificate has also been accepted by the subscriber under Guideline 1.1 (accept a certificate) to become a "valid" certificate under Guideline 1.36 (valid certificate).

4.4.5 Guideline 3.8 (prerequisites to disclosure of certificate) provides that if a certificate has not yet been accepted (and is therefore not yet valid), it may not be published or disclosed to a relying party by a certification authority. If the certificate has not theretofore been accepted by the subscriber, there will normally be no need for publication of notice of suspension or revocation under Guideline 3.12 (notice of suspension or revocation) unless there has been a breach of the duty of the certification authority not to publish an unaccepted certificate under Guideline 3.8 (prerequisites to disclosure of certificate).

5 Relying on certificates and digital signatures

5.1 Digitally signed message is written

A message bearing a digital signature verified by the public key listed in a valid certificate is as valid, effective, and enforceable as if the message had been written on paper.

Comment

5.1.1 The assurance of message integrity (see Guideline 1.19, message integrity) provided by a verified digital signature (including hash result)

generally equals or surpasses the comparable assurance provided by writing on paper, because any alteration of the message since it was digitally signed is immediately apparent.

5.1.2 This Guideline assures that a digitally signed message which is verified in accordance with Guideline 1.37 (verify a digital signature) satisfies an applicable statute of frauds or other requirement of a writing, regardless of whether the message ever assumes paper form.

5.1.3 Almost since its enactment the statute of frauds has been continually eroded. The United Kingdom has repealed the original act, and in the United States a similar trend is apparent. For example in 1981 the RESTATEMENT (SECOND) OF CONTRACTS § 139 (1981) provided for enforcement through promissory estoppel notwithstanding the statute of frauds). In the sale-of-goods context, the virtual repeal of the statute of frauds was apparent in the formerly proposed (but now superseded) §2-201(a) of U.C.C. REVISED ARTICLE 2, TRANSFERS OF PERSONAL PROPERTY, PROTOTYPE "HUB AND SPOKE" DRAFT (February 10, 1995 Draft) ("A contract or modification thereof is enforceable, whether or not there is a record signed by a party against whom enforcement is sought, even if the contract or modification is not capable of performance within one year after its making."). *See also*, proposed § 2B-201(a), Option 1, of U.C.C. ART. 2B (May 3, 1996 Draft). For international contracts for sales of goods, writing is expressly not required; *see United Nations Convention on Contracts for the International Sale of Goods,* Official Records 178-190, art. 11, at 3, U.N. Doc. A/Conf. 97/19; Sales No. E.82.V.5 (1981), *reprinted in* 15 U.S.C.A. United Nations Convention on Contracts for the International Sale of Goods (West Supp. 1996) ("A contract of sale need not be concluded in or evidenced by writing and is not subject to any other requirement as to form. It may proved by any means, including witnesses.") *See also Model Law on Electronic Commerce*, United Nations Commission on International Trade Law (UNCITRAL), 29th Sess., art. 6(1), at 3 ("Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.") and art. 5, at 3 ("Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message."), U.N. Doc. A/CN.9/XXIX/CRP.1/Add.13 (1996). However, notwithstanding the general erosion in both statutory and decisional law, the statute of frauds is still with us in many legal systems, and it is intended that the statute of frauds will be inapplicable if the requirements of this Guideline 5.1 are satisfied.

5.2 Satisfaction of signature requirements

Where a rule of law requires a signature, or provides for certain consequences in the absence of a signature, that rule is satisfied by a digital signature which is

(1) affixed by the signer with the intention of signing the message, and

(2) verified by reference to the public key listed in a valid certificate.

Comment

5.2.1 This Guideline provides that a digital signature suffices to satisfy formal requirements of a signature. Under existing legal definitions of a "signature", a mark upon the message made "with the present intention to authenticate the [message]" constitutes a signature, *see* U.C.C. § 1-201(39) (1992); *compare* Barber & Ross Co. v. Lifetime Doors, Inc., 810 F.2d 1276, 1280-81 (4th Cir. 1987), *cert. denied*, 484 U.S. 823 (1987) (A trademark is sufficient to satisfy the signature requirement for the Statute of Frauds.); Hillstrom v. Gosnay, 614 P.2d 466 (Mont. 1980) (telegraphed name sufficed as signature where evidence indicated that the signer had dictated the message to the telegraph sender); and RESTATEMENT (SECOND) OF CONTRACTS § 134 (1981) (signature "may be any symbol made or adopted with an intention, actual or apparent, to authenticate the writing as that of the signer"); *with* MacKnight v. Pansey, 412 A.2d 236 (R.I. 1980) (signer, who intended to authenticate a listing agreement, not a contract for sale, had not signed a contract for sale); Durham v. Harbin, 530 So.2d 208, 210 (Ala. 1988) (typewritten and printed names were not signatures where the would-be signer did not know of the document, let alone intend to authenticate it); *see also Model Law on Electronic Commerce*, United Nations Commission on International Trade Law (UNCITRAL), 29th Sess., art. 7, at 3, U.N. Doc. A/CN.9/XXIX/CRP.1/Add.13 (1996) (from which much of the phrasing of this Guideline is drawn). It should be noted that this Guideline does not serve to waive any requirements in addition to a signature, such as a requirement for a seal or an attestation.

5.2.2 A digital signature, like a paper signature, is principally an authentication mechanism. It generally accomplishes the purposes of a paper signature described in the preceding Tutorial (evidence of ceremony, approval, efficiency and logistics). However, there are important distinctions between digital signatures and paper signatures, especially the techniques used to create and evaluate them. Paper and digital signatures accomplish authentication by different methods.

5.2.3 Electronic signature marks other than verified digital signatures may also satisfy signature requirements. For example, this Guideline assumes that an unverified or unverifiable digital signature may also satisfy signature requirements under applicable law such as U.C.C. § 1-201(39) (1990), or case law definitions applied to statutory signature requirements, *see e.g.* RESTATEMENT (SECOND) OF CONTRACTS § 134 (1981) ("signature" for purposes of the statute of frauds).

5.2.4 The significance of a message's authentication depends heavily on what the signer intended that authentication to signify. Prior to the application of a digital signature, the signer should be afforded the opportunity to review the entire message. Further, it should not be possible for the signer to sign a document without having been informed that the signer's signature is being applied. Optimally, the signer's intent should be expressed *as part of the message* using a forensically reliable and readily available medium, such as the signed message or the certificate containing the public key used to verify the digital signature.

5.2.5 Facts and circumstances surrounding the transaction are relevant in determining the significance of authentication; however, clear, authenticated expressions by the signer of the intended significance should control over vague or less reliable evidence of intent. The significance of an authentication, whether by a paper or digital signature, presents a question of fact, Vess Beverage Inc. v. Paddington Corp., 886 F.2d 208, 213 (8th Cir. 1989), to be determined from all relevant facts and circumstances. *See* Kohlmeyer & Co. v. Bowen, 126 Ga. App. 700, 192 S.E.2d 400, 404 (1972). Questions may arise, as in paper-based transactions, concerning whether an authenticated message constitutes simply a statement of position, as in negotiations, or a binding contract.

5.2.6 Paper messages have a physical geography that allows a reader to attach certain significance to a handwritten name when it appears on "the bottom line". A digital signature, however, might not appear in a position closely resembling a bottom line. For example, a digital signature serving as an endorsement will not appear on the back of an electronic message because it has no back. Cases have sometimes relied on the geography inherent in paper to determine the significance of a paper mark, *see, e.g.,* In re Sport Shack, 383 F. Supp. 37 (N.D. Cal. 1974) ("signature [on the

bottom line] sufficiently indicates the necessary intent"); Littky & Mallon v. Michigan Nat'l Bank of Detroit, 94 Mich. App. 29, 287 N.W.2d 359 (1979) (a printed name was not intended to authenticate where a forged signature appeared on the bottom line); Pollin v. Mindy Mfg. Co., 211 Pa. Super. 87, 236 A.2d 542, 545 (1967) (a printed name was not a signature where the bottom line apparently intended for a handwritten signature was left blank). New indicators for meaning appropriate for digital signatures will be needed for digital signatures.

5.2.7 This Guideline does not suggest that communication over a medium that uses authentication processes for information security purposes, such as a secure communication channel providing low-level authentication services, necessarily indicates an intention to affix a legally binding signature to a message. Use of a secure communications channel could be a material fact in determining whether the signer intended to authenticate the message, but it will rarely be the only such fact.

5.2.8 Often, in commercial practice, a mark that looks like a handwritten signature in the regular course of business is presumed to be a valid signature. This practice is codified in the United States for negotiable instruments in U.C.C. § 3-308(a) (1990), which has been applied by analogy to messages which are not negotiable, *see, e.g.,* Bradford Trust Co. of Boston v. Merrill, Lynch, Pierce, Fenner & Smith, 622 F. Supp. 208, 211 (S.D.N.Y. 1985), *aff'd* 805 F.2d 49 (2d Cir. 1986) (applying a presumption of signature genuineness to stock powers). Similar pragmatic presumptions are appropriate for a digital signature, especially if it is verified by reference to the public key listed in a valid certificate. Accordingly, Guideline 5.6(2) (presumptions in dispute resolution) provides a presumption for verified digital signatures.

5.3 Unreliable digital signatures

(1) Unless otherwise provided by law or contract, Guideline 5.2 (satisfaction of signature requirements) does not apply to a digital signature if a relying party knows or has notice that the signer breached a duty prescribed in Part 4 Of these Guidelines (subscribers) with respect to the digital signature.

(2) Unless otherwise provided by law or contract, a relying party assumes the risk that a digital signature is invalid as a signature or authentication of the signed message, if reliance on the digital signature is not reasonable under the circumstances in accordance with the factors listed in Guideline 5.4 (reasonableness of reliance).

Comment

5.3.1 Underlying this Guideline and the closely related Guideline 5.4 are several principles that are not entirely in harmony with each other. They include:

- **Certainty**: Automation works more efficiently and with more reliable results if decisions can be based on clear and machine-processable criteria.

- **Flexibility**: A variety of factors need to be weighed in making a decision regarding the reliability of a digital signature. Some of the more important factors may not be capable of specification in precise language. Accordingly, it may not be advisable to be more specific than the traditional reasonable-person analysis of tort law.

- **Avoidance of further consequences**: When errors occur, their consequences should be mitigated rather than exacerbated, if possible.

This Guideline and Guideline 5.4 (reasonableness of reliance) attempt to strike a balance between these conflicting considerations.

5.3.2 This Guideline is worded permissively. A relying party may choose to rely on a questionable digital signature, but probably assumes a greater risk that the digital signature is forged or unattributable to an ascertainable signer.

5.3.3 Whenever deciding whether to rely on a questionable digital signature, the relying party may (but need not) seek additional information or assurances from the subscriber or

certification authority to resolve the question of the digital signature's reliability, or to authenticate the message through means other than its digital signature.

5.3.4 Unverifiability of a digital signature, error by the signer, or fault in the use of a digital signature system may be cured by the signer's timely ratification of the digital signature or by other corrective measures in particular circumstances.

5.3.5 A certificate is itself a message digitally signed by the certification authority issuing it; *see* Guideline 1.5 (certificate). In some trust systems, to determine whether a certificate is reliable, the digital signature of the issuing certification authority would need to be verified by reference to another certificate, and that certificate would in turn need to be verified, and so on up a chain of certificates to a certification authority in the relevant hierarchy whose certificate is reasonably believed to be reliable without further verification. Whether and how far a relying person should ascend a chain of certificates is a question of what is reasonable under the circumstances according to the factors described in Guideline 5.4 (reasonableness of reliance) and in Guideline 1.20 (nonrepudiation).

5.3.6 Equitable principles such as unclean hands, set-off, or estoppel in United States law operate to preclude a signer from asserting its own breach of duty to attack its own apparent signature. For example, if a signer disavows its own apparent digital signature by claiming a failure to properly secure the private key against compromise, the signer should not be allowed to benefit from such behavior. See Guideline 4.3 (safeguarding the private key).

5.4 Reasonableness of reliance

The following factors, among others, are significant in evaluating the reasonableness of a recipient's reliance upon a certificate, and upon digital signatures verifiable with reference to the public key listed in the certificate:

(1) facts which the relying party knows or of which the relying party has notice, including all facts listed in the certificate or incorporated in it by reference,

(2) the value or importance of the digitally signed message, if known,

(3) the course of dealing between the relying person and subscriber and the available indicia of reliability or unreliability apart from the digital signature,

(4) usage of trade, particularly trade conducted by trustworthy systems or other computer-based means.

Comment

5.4.1 The facts described in factor (1) may include not only personal interactions between the parties but also all other facts and circumstances bearing on the validity and reliability of a material certificate.

5.4.2 If a certificate is not within its operational period (see Guideline 1.22, operational period) at the time the digital signature was created, the digital signature is not verifiable, and reliance upon the certificate or upon a digital signature (even if created with the private key corresponding to the public key listed in the certificate) becomes less reasonable. Suspension and revocation of the certificate causes its operational period to terminate prior to its stated expiration date, so that reliance upon a revoked or suspended certificate is most unlikely to be considered reasonable. Reliance on a certificate which is not valid because it has not been issued (*see* Guideline 1.16, issue a certificate) or because it has not been accepted by the subscriber (*see* Guideline 1.1, accept a certificate) would not be likely to be reasonable by a relying

party with knowledge or notice of such facts under factor (1) of this Guideline 5.4.

5.4.3 Under the first factor, a relying party is deemed to have notice of the contents of the certificate by which the digital signature may be verified, provided that the certificate has been made available by the subscriber as required by Guideline 4.5 (availability of the certificate). Notice of the contents of the certificate includes notice of all messages incorporated into the certificate by reference. *See* Guideline 1.15 (defining "incorporation by reference"), especially Comment 1.15.4.

5.4.4 Factor (2) above is introduced in relation to digital signatures in light of the fact that the security of information is generally a matter of degree: It is almost always possible to secure the information more or less extensively, and the degree of security that the law should require should be commensurate with the risk. *See* Guideline 1.35 (trustworthy system), especially Comment 1.35.3. Factor (2) thus recognizes that the degree of information security is determined according to a reasonableness test, and that evaluating the reasonableness of reliance on a digital signature is often the point at which the test is applied.

5.4.5 Reasonableness of reliance is evaluated by the relying party at the time the digital signature has been received and verified under Guideline 1.37 (verify a digital signature). Facts not known to the relying party, of which the relying party is without notice, or not accomplished or assured of being accomplished at the time of receiving and verifying the material digital signature, are not material.

5.5 Digitally signed originals and copies

A copy of a digitally signed message is as effective, valid, and enforceable as the original of the message.

Comment

5.5.1 This Guideline provides that a digitally signed document satisfies requirements or preferences for original documents. Typified by the "best evidence rule" of the common law

tradition, such requirements are found in many jurisdictions. *See, e.g.,* FED. R. EVID. 1002; 4 JOHN H. WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW §§ 1173-75 (Chadbourn rev. ed. 1972); *see also* Wolfgang Kilian, *Möglichkeiten und zivilrechtliche Probleme eines rechtswirksamen elektronischen Datenaustauschs (EDI)*, DATENSCHUTZ UND DATENSICHERUNG: RECHT UND SICHERHEIT DER INFORMATIONS- UND KOMMUNIKATIONSSYSTEME 608-609 (Nov. 1993) (German evidence rules); Chris Reed, *Authenticating Electronic Mail Messages - Some Evidential Problems*, 52 MOD. L. REV. 649, 652-53 (1989) (British evidence rules); JAMES V. VERGARI & VIRGINIA V. SHUE, FUNDAMENTALS OF COMPUTER-HIGH TECHNOLOGY LAW § 8.03(b)(1) (1991); *Model Law on Electronic Commerce*, United Nations Commission on International Trade Law (UNCITRAL), 29th Sess., art. 8, at 4 (requirement of "original") and art. 9, at 4 ("admissibility and evidential weight of data messages"), U.N. Doc. A/CN.9/XXIX/CRP.1/Add.13 (1996).

5.5.2 This Guideline's equal treatment of digital originals and copies for purposes of the best evidence rule is founded on the practicality that copies of a digital message, like the original, are composed of bits rather than atoms, and are therefore undistinguishable from the original. A method for distinguishing between a digital original and copy might be based on a system for tracking their processing history, but such a system would share none of the traditional rationale for the best evidence rule, namely the differing evidential quality of originals and copies of paper documents. *See* 4 JOHN H. WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW §§ 1173-75 (Chadbourn rev. ed. 1972).

5.5.3 The legal significance of copies is important in view of the fact that computer technology relies heavily on copying as a means of preserving and transmitting information. Indeed, in an electronic setting, a message generally exists only in the form of a copy, since it is likely that the digitally signed original was in volatile memory when signed, and has been preserved only by copying the contents of that volatile memory to another medium. Hence, as a matter of technical fact, it is unlikely in current technology that an original of a message ever survives after the signing process terminates.

5.5.4 A message, however authentic or genuine, is not treated as a negotiable instrument in banking and business practice unless it is also an original. Possession of the original

instrument is crucial in determining whether the instrument was issued. *See* U. C. C. § 3-105(a) (1990) (requiring delivery (transferring possession) of the instrument for issuance). If the instrument is payable to bearer, possession of the original is tantamount to the right to be paid. If the instrument is payable to order, the original of the instrument is controlling in determining to whose order the instrument is currently payable. *See* U.C.C. § 3-201(b) (1990) (order instruments are negotiated by endorsement and transfer of possession; bearer instruments by transfer of possession alone). If multiple copies of an instrument are equivalent to the original, identifying the single rightful holder of the instrument becomes difficult, if not impossible, and the risk of multiple payment may be unacceptable.

5.5.5 One possible strategy to reduce the risk of multiple payment of digital instruments is a central registry of the original paper instrument under depository control of a trusted third party, with digital endorsements, presentation and other transactions relating to the original document requiring the digital signature of the trusted third party who retains possession of the original instrument. Another is so-called "digital cash," namely emulated currency which keeps track of processing history events such as decrements or increments to a credit balance, either by reference to a central registry, or by a self-contained registry in a tamper-proof smart card or other token. *See generally*, Henry H. Perritt, Jr., *Legal and Technological Infrastructures for Electronic Payment Systems*, 22 RUTGERS COMPUTER & TECH. L.J. 1 (1996).

5.5.6 Where monetary value is digitized, as with digital cash, double-spending is disallowed not by attempting to distinguish between the original and copies of the digitized values, but rather by systematically referring to a register (either central or self-contained) which keeps track of processing history and validates only the first registered use of a digitized monetary transfer. Optional anonymity for digital cash is under development.

5.5.7 While the matter is still under consideration, at the present time these issues are outside the scope of these Guidelines: (a) whether any special treatment should be accorded originals, should it become technologically feasible to distinguish them from copies; (b) whether any special treatment should be accorded digital documents which are "negotiable"; and (c) whether anonymity in digital cash transactions can or should be protected as a legitimate

"security service."

5.6 Presumptions in dispute resolution

In resolving a dispute involving a digital signature, it is rebuttably presumed that

(1) the information listed in a valid certificate is correct, except for nonverified subscriber information,

(2) a digital signature verified by reference to the public key listed in a valid certificate is the digital signature of the subscriber listed in that certificate,

(3) the message associated with a verified digital signature has not been altered from its original form,

(4) a certificate of a certification authority, which is either published or made available to the subscriber listed in it, is issued by that certification authority, and

(5) a digital signature was created before it was time-stamped by a trustworthy system.

Comment

5.6.1 The effect of the presumptions listed in this Guideline is to

allocate the burden of going forward with evidence to the party challenging a digital signature, certificate, or a time-stamp created by a trustworthy system. In other words, a party taking the position that a verified digital signature, certificate, or trustworthy time-stamp is invalid or unreliable must take the initiative in a proceeding, must assert its position rather than remain silent, and must present evidence establishing the facts material to its position before its opponent is required to do likewise.

5.6.2 The presumptions provided in this Guideline are based on the premise that certificates issued by certification authorities and time-stamps provided by a trustworthy system are likely to be reliable; therefore, presuming their correctness will conserve resources by not requiring routine proof of what is generally true. Moreover, a person relying on a digital signature generally has less access to evidence of the authenticity of the signature than the subscriber; hence, the initial burden of marshaling available evidence should fall on the subscriber, who, in a case of forgery, for example, will generally be the party attacking the ostensible signature. Implementing legislation may require reasonable measures to assure that certification authorities and time-stamping services are sufficiently trustworthy to warrant such presumptions. The tribunal may be a court, arbitrator, mediator, or any other legally recognized forum for the resolution of disputes.

5.6.3 The presumptions of this Guideline may be rebutted by demonstrating material noncompliance with the Guidelines, a material misrepresentation or error, or any other fact indicating that the presumption is not well-founded.

5.6.4 In determining the admissibility of evidence in court proceedings, a digital signature verified by reference to a valid certificate should be presumed to be the genuine digital signature of the subscriber in the certificate listing the public key by which the digital signature is verified, pursuant to paragraph (2) of this Guideline. A court should thereupon hold the digitally signed evidence to have been *prima facie* authenticated and admissible, unless evidence is introduced rebutting the presumption of a verified digital signature.

5.6.5 The presumption that a verified digital signature is the subscriber's is analogous to the presumption that a paper signature is genuine. *See, e.g.,* U.C.C. § 3-308 (1990), formerly § 3-307 (1962); Bradford Trust Co. of Boston v. Merrill, Lynch, Pierce, Fenner & Smith, 622 F. Supp. 208, 211

(S.D.N.Y. 1985), aff'd 805 F.2d 49 (2d Cir. 1986); Bates & Springer, Inc. v. Stallworth, 56 Ohio App. 2d 223, 382 N.E.2d 1179 (1978); Virginia Nat'l Bank v. Holt, 216 Va. 500, 219 S.E.2d 881, 882 (1975); FRED H. MILLER & ALVIN C. HARRELL, THE LAW OF MODERN PAYMENT SYSTEMS AND NOTES ¶ 2.02[c] at 2-17 (1992).

IV. Bibliography

AMERICAN BANKERS ASSOCIATION & AMERICAN NATIONAL STANDARDS INSTITUTE, AMERICAN NATIONAL STANDARD X9.30-199X: PUBLIC KEY CRYPTOGRAPHY USING IRREVERSIBLE ALGORITHMS FOR THE FINANCIAL SERVICES INDUSTRY (1995).

AMERICAN BANKERS ASSOCIATION & AMERICAN NATIONAL STANDARDS INSTITUTE, AMERICAN NATIONAL STANDARD X9.31-199X: PUBLIC KEY CRYPTOGRAPHY USING REVERSIBLE ALGORITHMS FOR THE FINANCIAL SERVICES INDUSTRY (1995).

MICHAEL S. BAUM & H.H. PERRITT, ELECTRONIC CONTRACTING, PUBLISHING, AND EDI LAW (1991). John Wiley & Sons. ISBN 0-471-53135-9.

MICHAEL S. BAUM, FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY - LAW AND POLICY OF CERTIFICATE-BASED PUBLIC KEY AND DIGITAL SIGNATURES. U.S. Department of Commerce/NIST Publication No. NIST-GCR-94-654; National Technical Information Service Publication No. PB94-191-202 (1-800-553-6847).

MICHAEL BOTHE & WOLFGANG KILIAN, RECHTSFRAGEN GRENZüBERSCHREITENDER DATENFLüSSE (1992). Verlag Schmidt, KG. ISBN 3 504 56030 4.

WARWICK FORD, COMPUTER COMMUNICATION SECURITY: PRINCIPLES, STANDARD PROTOCOLS AND TECHNIQUES (1994). Prentice Hall. ISBN 0-13-799453-2.

INTERNATIONAL TELECOMMUNICATION UNION (formerly Consultative Committee on International Telephony and Telegraphy), DATA COMMUNICATION NETWORKS DIRECTORY, RECOMMENDATIONS X.500-X.521 (1988) (see especially recommendation X.509).

Internet Activities Board, Requests for Comment numbers 1421 through 1424 (1993).

C. KAUFMAN, R. PERLMAN & M. SPECINER, NETWORK SECURITY: PRIVATE COMMUNICATION IN A PUBLIC WORLD (1995). Prentice Hall. ISBN 0-13-0614466-1.

CHARLIE KAUFMAN, RADIA PERLMAN & MIKE SPECINER, NETWORK SECURITY: PRIVATE COMMUNICATION IN A PUBLIC WORLD (1995). Prentice Hall. ISBN 0-13-061466-1.

BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY: PROTOCOLS, ALGORITHMS, AND SOURCE CODE IN C (2d ed. 1996). New York: John Wiley & Sons, Inc. ISBN 0-471-11709-9.

GUSTAVAS SIMMONS, ED., CONTEMPORARY CRYPTOLOGY: THE SCIENCE OF INFORMATION INTEGRITY (1992). Piscataway, New Jersey: IEEE Press. ISBN 0-87942-277-7.

PIERRE TRUDEL, GUY LEFEBVRE & SERGE PARISIEN, LA PREUVE ET LA SIGNATURE (1993). Québec: Ministère des Communications. ISBN 2-551-15837-0.

V. Index