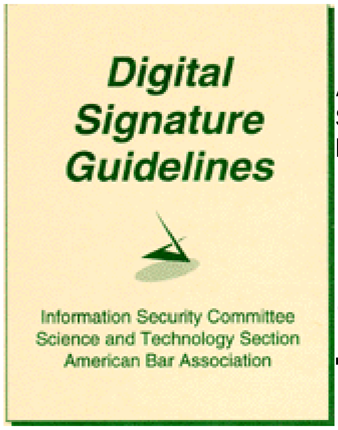

American Bar Association
Section of Science and Technology
Information Security Committee

Digital Signature Guidelines Tutorial

Digital Signature Guidelines Press Release

Tutorial

In today's commercial environment, establishing a framework for the authenticat of computer-based information requires a familiarity with concepts and professio skills from both the legal and computer security fields. Combining these two disc is not an easy task. Concepts from the information security field often correspon loosely to concepts from the legal field, even in situations where the terminology similar. For example, from the information security point of view, "digital signatur means the result of applying to specific information certain specific technical pro described below. The historical legal concept of "signature" is broader. It recogn any mark made with the intention of authenticating the marked document. <2> Ir digital setting, today's broad legal concept of "signature" may well include markir diverse as digitized images of paper signatures, typed notations such as "/s/ Joh Smith," or even addressing notations, such as electronic mail origination header

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

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

Signatures and the Law

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

- **Evidence:** A signature authenticates a writing by identifying the signer wi signed document. When the signer makes a mark in a distinctive manner, writing becomes attributable to the signer.<4>
- **Ceremony:** The act of signing a document calls to the signer's attention t legal significance of the signer's act, and thereby helps prevent "inconside engagements.<5>
- **Approval:** In certain contexts defined by law or custom, a signature expre the signer's approval or authorization of the writing, or the signer's intentic it have legal effect.<6>
- **Efficiency and logistics:** A signature on a written document often impart sense of clarity and finality to the transaction and may lessen the subsequ need to inquire beyond the face of a document.<7> Negotiable instrumen example, rely upon formal requirements, including a signature, for their ab change hands with ease, rapidity, and minimal interruption.<8>

The formal requirements for legal transactions, including the need for signatures 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 The statute of frauds of the common law tradition, for example, does not render transaction invalid for lack of a "writing signed by the party to be charged," but ra 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> least have minimized the consequences of failure to satisfy formal requirements. Nevertheless, sound practice still calls for transactions to be formalized in a mar which assures the parties of their validity and enforceability.<11> In current prac formalization usually involves documenting the transaction on paper and signing authenticating the paper. Traditional methods, however, are undergoing fundam change. Documents continue to be written on paper, but sometimes merely to sa the need for a legally recognized form. In many instances, the information excha to effect a transaction never takes paper form. Computer-based information can utilized differently than its paper counterpart. For example, computers can "read" information and transform the information or take programmable actions based o information. Information stored as bits rather than as atoms of ink and paper car near the speed of light, may be duplicated without limit and with insignificant cos

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

To achieve the basic purposes of signatures outlined above, a signature must ha following attributes:<12>

- **Signer authentication:** A signature should indicate who signed a docum message or record,<13> and should be difficult for another person to proc without authorization.
- **Document authentication:** <14> A signature should identify what is sign <15> making it impracticable to falsify or alter either the signed matter or 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 professior nonrepudiation service provides assurance of the origin or delivery of data in orc protect the sender against false denial by the recipient that the data has been re or to protect the recipient against false denial by the sender that the data has be sent. <16> Thus, a nonrepudiation service provides evidence to prevent a perso 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 serves the ceremonial and approval functions of a signature and establisl sense of having legally consummated a transaction.
- **Efficiency:** Optimally, a signature and its creation and verification proces should provide the greatest possible assurance of both signer authenticity document authenticity, 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 signa technology works.

How Digital Signature Technology Works

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

The complementary keys of an asymmetric cryptosystem for digital signatures a arbitrarily termed the private key, which is known only to the signer <20> and us create the digital signature, and the public key, which is ordinarily more widely kı and is used by a relying party to verify the digital signature. If many people need verify the signer's digital signatures, the public key must be available or distribut of them, perhaps by publication in an on-line repository or directory where it is ea accessible. Although the keys <21> of the pair are mathematically related, if the asymmetric cryptosystem has been designed and implemented securely <22> it "computationally infeasible <23> to derive the private key from knowledge of the key. Thus, although many people may know the public key of a given signer and to verify that signer's signatures, they cannot discover that signer's private key a 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 verifying a digital signature. A hash function is an algorithm which creates a digit 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 neverthele substantially unique to it. <24> Any change to the message invariably produces different hash result when the same hash function is used. In the case of a secu function, sometimes termed a "one-way hash function," it is computationally infe <25> to derive the original message from knowledge of its hash value. Hash fun therefore enable the software for creating digital signatures to operate on smalle predictable amounts of data, while still providing robust evidentiary correlation to original message content, thereby efficiently providing assurance that there has no modification of the message since it was digitally signed.

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

- **Digital signature creation** uses a hash result derived from and unique tc the signed message and a given private key. For the hash result to be se there must be only a negligible possibility that the same digital signature c be created by the combination of any other message or private key.
- **Digital signature verification** is the process of checking the digital signa reference to the original message and a given public key, thereby determ whether the digital signa ture was created for that same message using tl private key that corresponds to the referenced public key.

To sign a document or any other item of information, the signer first delimits pre the borders of what is to be signed. The delimited information to be signed is ter 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 message. The s software then transforms the hash result into a digital signature using the signer' private key. <26> The resulting digital signature is thus unique to both the messa the private key used to create it.

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

Verification of a digital signature is accomplished by computing a new hash resu 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 check whether the digital signature was created using the corresponding private key; a whether the newly computed hash result matches the original hash result which 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 k used to digitally sign the message, which is known to be the case if the signer's key was used to verify the signature because the signer's public key will verify o digital signature created with the signer's private key; <27> and (2) the message unaltered, which is known to be the case if the hash result computed by the veri identical to the hash result extracted from the digital signature during the verifica process.

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

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

- **Signer authentication:** If a public and private key pair is associated with identified signer, the digital signature attributes the message to the signer digital signature cannot be forged, unless the signer loses control of the p key (a "compromise" of the private key), such as by divulging it or losing t 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 sig Verification reveals any tampering, since the comparison of the hash resu (one made at signing and the other made at verifying) shows whether the message is the same as when signed.
- **Affirmative act:** Creating a digital signature requires the signer to use th signer's private key. This act can perform the "ceremonial" function of ale the signer to the fact that the signer is consummating a transaction with le consequences. <28>
- **Efficiency:** The processes of creating and verifying a digital signature pr high level of assurance that the digital signature is genuinely the signer's

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

The processes used for digital signatures have undergone thorough technologic review for over a decade. Digital signatures have been accepted in several natic international standards developed in cooperation with and accepted by many corporations, banks, and government agencies. <29> The likelihood of malfunct security problem in a digital signature cryptosystem designed and implemented a prescribed in the industry standards is extremely remote, <30> and is far less tha risk of undetected forgery or alteration on paper or of using other less secure ele signature techniques.

Public Key Certificates

To verify a digital signature, the verifier must have access to the signer's public k have assurance that it corresponds to the signer's private key. However, a public 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 particula person or entity to the key pair.

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

To that end, a prospective signer might issue a public statement, such as: "Signa verifiable by the following public key are mine." However, others doing business the signer may for good reason be unwilling to accept the statement, especially w there is no prior contract establishing the legal effect of that published statement certainty. A party relying upon such an unsupported published statement in an o system would run a great risk of trusting a phantom or an imposter, or of attempt disprove a false denial of a digital signature ("nonrepudiation") if a transaction sh 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 p 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 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 hc corresponding private key. The prospective signer is termed the "subscriber. <3 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 th subscriber named in the certificate (whereupon the recipient becomes a "relying can use the public key listed in the certificate to verify that the digital signature w created with the corresponding corresponding private key. <33> If such verificati successful, this chain of reasoning provides assurance that the corresponding p key is held by the subscriber named in the certificate, and that the digital signatu created by that particular subscriber.

To assure both message and identity authenticity of the certificate, the certificati authority digitally signs it. The issuing certification authority's digital signature on certificate can be verified by using the public key of the certification authority list another certificate by another certificate authority (which may but need not be or higher level in a hierarchy) <34>, and that other certificate can in turn be authen by the public key listed in yet another certificate, and so on, until the person relyi the digital signature is adequately assured of its genuineness. In each case, the certification authority must digitally sign its own certificate during the operational 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 c certification authority to authenticate its certificate (in effect a specialized messa should be reliably time-stamped to allow the verifier to determine reliably whethe digital signature was created during the "operational period" stated in the certific which is a condition upon verifiability of a digital signature under these Guideline

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

Once issued, a certificate may prove to be unreliable, such as in situations wher subscriber misrepresents his identity to the certification authority. In other situati certificate may be reliable enough when issued but come to be unreliable somet thereafter. If the subscriber loses control of the private key ("compromise" of the key), the certificate has become unreliable, and the certification authority (either without the subscriber's request depending on the circumstances) may suspend (temporarily invalidate) or revoke (permanently invalidate) the certificate. Immed upon suspending or revoking a certificate, the certification authority must publish of the revocation or suspension or notify persons who inquire or who are known received a digital signature verifiable by reference to the unreliable certificate.

Challenges and Opportunities

The prospect of fully implementing digital signatures in general commerce prese 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 in the performance of their functions.
- **Subscriber and Relying Party Costs:** A digital signer will require softwa 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 authentic messages. Digital signatures, if properly implemented and utilized offer promisin

messages. Digital signatures, if properly implemented and utilized offer promisin
solutions to the problems of:

- **Imposters**, by minimizing the risk of dealing with imposters or persons wl attempt to escape responsibility by claiming to have been impersonated;
- **Message integrity**, by minimizing the risk of undetected message tampe and forgery, and of false claims that a message was altered after it was s
- **Formal legal requirements**, by strengthening the view that legal requirer of form, such as writing, signature, and an original document, are satisfiec digital signatures are functionally on a par with, or superior to paper forms
- **Open systems**, by retaining a high degree of information security, even f information sent over open, insecure, but inexpensive and widely used ch

ABA Copyright Statement ABA Privacy Statement

This document was created with Win2PDF available at http://www.daneprairie.com.
The unregistered version of Win2PDF is for evaluation or non-commercial use only.