An Attorney's Roadmap to the *Digital Signature Guidelines*
Summary of Remarks at Financial Cryptography '97
Anguilla, BWI, February 27, 1997

By Charles R. Merrill[1]

Hypothetical Example:

Bob, a securities broker, has printed out the following document from a file on the hard drive of his PC, which he claims to be a true copy of an e-mail message he received via the Internet.

Alice has an active securities trading account with Bob, in which she maintains a credit balance of securities and cash. Alice has often used Internet e-mail to instruct Bob as to purchases and sales of securities in her account.

> To: Bob@securities-r-us.com
> From: Alice@restaurant.com
> Date: Feb 27, 1997 10:00
>
> Please buy 100 shs of Netscape common stock for my account immediately, at the prevailing market price. /s/ Alice

On Thursday, Feb 27, Bob did buy 100 shares of Netscape common stock for Alice's account. On Friday, Feb 28, the market price of Netscape plummeted, producing a substantial loss on this transaction. Upon receipt of routine written confirmation of purchase of 100 shares for her account, Alice claims, alternatively:

(1) Bob, I never sent any e-mail message! or
(2) Bob, I sent an e-mail message, but it said "sell 100 shs of Netscape"! or
(3) Bob, I sent that e-mail message, but not till Feb 28, after the price fell!

The Challenge of Conducting Secure Electronic Commerce on the Internet

The example illustrates the challenge of conducting secure electronic commerce on the Internet, where, as the famous *New Yorker* cartoon says, "They can't tell you're a dog." Although the Internet is increasingly attractive as a commercial channel, the dark side is that the Internet is notoriously insecure in its normal configuration as an "open system," where there are no trusted gatekeepers to authenticate identity of users entering the system. Sophisticated hackers are demonstrably able to send messages "spoofing" the identity and e-mail address of others, and to intrude in private communications between others - intercepting, reading, modifying and sending messages along again, without detection. Many believe that if electronic commerce continues to accelerate its volume without substantial improvements in security, commercial losses through such attacks will also grow in volume - motivated not only by mischief but by the "Willie Sutton" syndrome ("Willie, why do you rob banks?" "Because the money's there.")

On August 1, 1996, the Information Security Committee of the American Bar Association Section of Science and Technology published the *Digital Signature Guidelines*,[2] a four-year collaboration

---

[1] Mr. Merrill is a partner of the law firm of McCarter & English, Newark, N.J., where he chairs the firm's Computer and High-Tech Law Practice Group. He served as Co-Reporter of the *Digital Signature Guidelines*, published August 1, 1996 by the Information Security Committee of the American Bar Association Section of Science and Technology.

of more than 70 leading technologists and attorneys from all over the world.[3] The *Guidelines* seek to define a system of public key infrastructure which combines the powerful technological capabilities of an asymmetric cryptosystem with legal principles of commercial law.

Delivering Security Services – A Merger of Technological and Legal Viewpoints

Familiar terminology of the computer security profession defines a number of "security services" which must be delivered by a system of electronic communications if it is to be considered secure or trustworthy. The terminology is not generally familiar to attorneys because in this early stage in the transition from paper-based commerce to electronic commerce, it is not (yet) taught in law school or commonly encountered in general commercial practice.

Confidentiality	**Exclusive Knowledge**
Authentication of Sender	**WHO** sent the message?
Data Integrity	**WHAT** were the contents of the message?
Time-Stamp	**WHEN** was the message sent?
Non-Repudiation	**BLOCKS FALSE DENIAL** of (a) the **sending** of the message, and (b) the **contents** of the message.

The diverse composition of the Information Security Committee - half technologists and half attorneys - required a great deal of time and energy to be spent in the mutual learning of unfamiliar concepts and vocabulary. Attorneys needed to teach technologists principles of contract law; technologists such as computer security professionals needed to teach attorneys how cryptography works. Attorneys tend to be experienced with the concept of CONFIDENTIALITY, but tend to find concepts of WHO, WHAT, WHEN and NON-REPUDIATION to be less intuitive and more difficult to grasp in an alien digital environment devoid of paper-based and human-contact cues aiding authentication.

Moreover, as a matter of culture and training, computer security professionals tend to be more comfortable when there is a binary, "yes or no" answer to the question of whether a particular security service is delivered by the system. Attorneys, on the other hand, are conditioned by their training to take a more analog, "yes and no or maybe" approach to an issue which will ultimately be decided by an imperfect system for resolving factual and legal disputes by decision of a judge and/or by vote of a layman jury. Although cultural differences caused communication difficulties in the beginning, in the end the diversity of the group was recognized as an asset in reaching a techno-legal consensus solution.

---

[2] Approximately one-third of this 99 page book, including a Tutorial, the Table of Contents, and List of Contributors, is available online at http://www.abanet.org/scitech/ec/isc/dsg-toc.html. A hardcopy version may be ordered from the ABA at http://www.abanet.org/scitech/ec/ for $34.95, with volume discounts at $20 and $15.

[3] This collaboration included extensive cooperation between the Information Security Committee and drafters of the pioneering Utah Digital Signature Law first enacted in 1995, as amended by Utah Code Ann. §46:3 (1996)(http://www.commerce.state.ut.us/web/commerce/digsig/dsmain.htm). Although there are many differences between the *Guidelines* and the Utah Digital Signature Act, the similar objectives, technology and scope of the *Guidelines* and the Utah Act cause both to be sometimes referred to as the "Utah Model". In 1997 the State of Washington enacted a digital signature law similar to the Utah Model, 1997 WA SB 6423, http://access.wa.net/sb6423_info/. For an up-to-date 50-state summary of legislation and pending legislation regarding digital signatures and electronic signatures, see http://www.state.ma.us/itd/legal/

In their quest for a secure electronic commerce in an open system, the *Guidelines* focus on the technology of "public key cryptography" (also known as an "asymmetric cryptosystem"), supported by a certificate-based "public key infrastructure" ("PKI") which builds rules for legal liability governing commercial parties and trusted third parties known as "certification authorities" ("CAs")

Although a number of leading public key cryptographic algorithms are capable of providing both encryption for confidentiality and digital signatures, the principal focus of the *Guidelines* is the security services provided by an asymmetric cryptosystem operated in digital signature mode only - the WHO, WHAT and NON-REPUDIATION security services. This technology is summarized in the next Section, below. Public key cryptography is not itself capable of providing the WHEN security service. But if a CA is supported by a trustworthy time-stamping service, its WHO, WHAT and NON-REPUDIATION services become more trustworthy, and the WHEN security service can be provided as well.[4]

NON-REPUDIATION deals with the same subject matter as WHO and WHAT security services, but from a different perspective, which has important significance for the legal rules of electronic commerce. In the case of the WHO and WHAT security services, both sender and recipient of a message are on the same side of the issue, seeking to defend and support the authenticity and integrity of the message against the efforts of an imposter to spoof and tamper with it. NON-REPUDIATION, however, contemplates that the sender and recipient are on opposite sides of a legal dispute. The recipient is attempting to defend and support the authenticity and integrity of the sender's legally binding message, and the sender is attempting to repudiate legal responsibility for the sending of the message or its contents by proving that the message could have been the work of an imposter.

The Technology of an Asymmetric Cryptosystem

For this particular audience, a very brief summary will suffice to explain the technological principles of an asymmetric cryptosystem applied by the *Digital Signature Guidelines.* (For those desiring more detail, see the Tutorial from the Guidelines at http://www.abanet.org/scitech/ec/isc/dsg-toc.html.) The references to "Guideline" or "GL" are references to numbered major headings in the *Digital Signature Guidelines*.

- Conventional cryptography, sometimes referred to as a "symmetric cryptosystem," uses a single secret key to encrypt/transform data and to decrypt/restore it to its original form. This system requires knowledge of the secret key to be shared by others. This detracts from the security service of non-repudiation because if the single key becomes compromised, it is possible to claim that someone else compromised the key.
- Public key cryptography (sometimes called an asymmetric cryptosystem, Guideline 1.3) uses two separate but mathematically related keys known as a key pair (GL 1.17). If either key is used to encrypt/transform data, the other key is used to decrypt/restore it to its original form.
- One key is called the private key (GL 1.24) and is kept secret by its holder and shared with no one. The other key is called the public key (GL 1.25) and is made publicly available online. It is computationally unfeasible to derive the private key merely from knowledge of the public key. This arrangement strongly supports non-repudiation because the source of compromise of a private key must by definition be the only person authorized to hold or have knowledge of the private key.
- Using cryptographic software, the signer of a message (under GL 1.18, this means a digital, computer-based record, rather than a paper-based record) will use the sender's private key

[4] See Guidelines 1.33 and 1.35 and related comment. See http://www.surety.com for one example of a proprietary time-stamping service, known as the Digital Notary™ Service of Surety Technologies, Inc.

and a one-way hash function (GL 1.12) to transform the message into a digital signature (GL 1.11).

- A party receiving the digital signature in a position to rely upon it is called the relying party (GL 1.37).
- The relying party will use the sender's public key to verify (GL 1.37) that the digital signature was created by the private key corresponding (GL 1.10) to this public key. Because the message was transformed with a one-way hash at the time of signature, verification will also determine that the message was not altered since the time it was digitally signed.
- Although confidentiality of the message is not required for digital signature purposes, if the security service of confidentiality is desired, some public key algorithms may be reversed, to allow the sender to encrypt for confidentiality by using the recipient public key, whereupon the recipient may decrypt the message by using the recipient's corresponding private key.

The Certification Authority: Binding Public Key to Identity

It is important to note that the verification process itself merely determines that the private key corresponding to the public key available to the relying party was used to the sign the message. It does not yet say anything about who actually signed the message, let alone who is legally bound by the message.

To complete the chain of links, the critical step is to bind the purported sender's identity to the sender's public key, so that Bob, the relying party, has reason to believe that the public key used to verify Alice's digital signature is in fact the public key of Alice, and not the public key of an imposter which the imposter uses to spoof the public key of Alice.

Under the *Guidelines*, the job of binding the identity of Alice to Alice's public key is handled by a certification authority (GL 1.6), a trusted third party which issues a certificate (GL 1.5) to a subscriber (GL 1.31). The certification authority publishes a certification practice statement (GL 1.8), generally setting forth statements of its practices and procedures and the allocation of legal rights among the three pertinent parties - namely the certification authority and the subscriber (who contract directly with each other) and the relying party (who is not likely to be in direct contractual privity with the certification authority).

In accordance with the certification practice statement, the subscriber and the certification authority undertake a procedure of application, approval, issuance (GL 1.1) and acceptance (GL 1.16), pursuant to which the certification authority or its delegate validates through specified identification procedures that the applicant for Alice's certificate is in fact Alice. The certification authority then digitally signs the certificate with the verifiable (all the way to the top or trusted root of the certification authority) digital signature of the certification authority, so that the certificate cannot be spoofed. Once the certificate has been accepted (expressly or impliedly) by the subscriber, it is published in an online repository or otherwise made available to Alice and/or to potentially relying parties.

Remember Alice? A Summary of the Legal Issues

Our hypothetical example illustrates a classic case of where a robust system of non-repudiation is needed to block Alice's false denial that she sent the message produced by Bob. If in fact Alice did send that message, a plausible motive could be the intention to remain unfairly flexible at the expense of Bob, by waiting to see the future market price before confirming or denying that she sent the message. Such conduct (if unfair) is recognized and remediable under the equitable principle of "laches" in the Anglo-American legal system.

The problem, of course, and the central dilemma for electronic commerce in an open system, is that in a digital environment based on bits rather than atoms, the jury and the opposing counsel will be deprived of cues or clues which would normally be available for the resolution of disputes in a paper-based and human-contact-based world. Here are the three possible factual theories which face the dispute resolution authority (judge, jury, arbitrator, mediator or the like):

(A) Alice is lying and Bob is truthful. Alice did send the message, and Bob did not falsify it. Alice intended to buy the stock, but after the market dropped, she is repudiating the transaction in order to avoid the loss, committing laches at Bob's expense. (Or she sent "buy" and wants to substitute "sell". Or she sent the message Feb 27 and now claims she sent it Feb 28, after the price dropped.)

(B) Bob is lying and Alice is truthful. Bob has falsified the message and the printout, and Alice never sent it. Bob bought the stock for his own account or for another customer, and after the market dropped, he tried to put the loss on Alice. (Or she did send "buy" and Bob has substituted "sell". Or she did sent the message Feb 28 and Bob has caused his PC to substitute Feb 27.)

(C) Alice and Bob are Both Telling the Truth!! Alice did not send the message, but Bob did receive it on Feb 27. An unknown imposter (for mischievous or other unknown motives) has either:

- Spoofed Alice and sent the message, or
- Intercepted Alice's message and changed "buy" to "sell"

The fact finder could rationally decide (A) or (B) on the basis of the relative credibility of the testimony of Alice or Bob - a process with which the legal system is comfortable and familiar. The most troublesome possibility for a system of jurisprudence is Case (C), where the fact finder decides that both Alice and Bob are truthful, innocent and victimized, yet must then decide which innocent victim should bear the damage caused by an imposter who is usually unknown, judgment-proof, and/or beyond the court's jurisdiction.

Under the facts of the hypothetical example, the e-mail message is "naked" of any cryptographic authentication of any kind. What would happen if the e-mail were digitally signed, and the case were decided in a jurisdiction (e.g., the States of Utah or Washington) where rules similar to the *Digital Signature Guidelines* are in force?

Deciding the Case Under the Digital Signature Guidelines

Step 1. Is there a digital signature on the message? GL 1.11 defines digital signature as the following:

> 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.

If there is a digital signature on the message, the *Guidelines* apply, and we proceed to Step 2. This is an "opt-in" system, where the use of digital signatures is entirely optional on the part of users. If the user has not digitally signed the message, the *Guidelines* do not apply, and existing law does.

Step 2. If a relying party has a message signed with a digital signature and also has a public key available, the crypto software allows the relying party to determine whether the digital signature was created by someone who used the private key corresponding to that public key. The effect is to link the digital signature to that public key. We still know nothing about who signed the document.

Step 3. Do we have a digital certificate issued by a trusted third party certification authority (CA)? The certificate follows the ITU x.509 standard, and (among other information) contains the distinguished name of the subscriber, and the subscriber's public key. Depending upon the rigor of the identification procedures required for the particular class of certificates, the certificate binds the identity of the subscriber to the subscriber's public key, during the typical one-year operational period of the certificate.

Step 4. The next step is to verify the digital signature and message integrity under GL 1.37, which defines that process as:

> 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.

From Step 2, the software has already told the relying party that the digital signature is linked to the public key available to the relying party. From Step 3, the CA linked the public key of Alice to Alice's identity. Step 4 requires that the digital signature be created during the operational period of a valid certificate (i.e., not before its issue date and not after it has expired or it has been revoked), and if this requirement is satisfied, the digital signature has been "verified". Combining Step 2, Step 3 and Step 4, the digital signature has now been linked with Alice.

Step 5. At this point, the analysis becomes primarily legal, diverging from the yes/no binary approach favored by computer security professionals, into the fuzzy, analog world of the dispute resolution process which determines who wins and loses in a commercial dispute. Guideline 5.6 provides the following **rebuttable**[5] presumption:

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

Under traditional paper-based law, it is often the case that the person relying on a signed document has the burden of proof (both the burden of going forward with evidence and persuading the fact finder with the preponderance of the evidence) that the document was signed by the person to whom it is attributed. Similarly, under Federal Reserve Regulations Reg E and Reg Z governing ATM devices and credit cards, the liability of even a negligent cardholder is generally limited to $50 regardless of how much loss is caused the cardholder's bank. Reflecting the robust security capabilities of asymmetric cryptosystem technology, the *Digital Signature Guidelines* intentionally reverse that presumption where a digital signature is properly verifiable. If the e-mail message in our hypothetical example was digitally signed and verified by reference to Alice's valid certificate as per the preceding four steps, then Alice is liable to Bob, unless she successfully rebuts the presumption that the e-mail message produced by Bob is signed by Alice and not modified since the time she signed it. There are two major ways Alice may rebut that presumption and avoid liability.

Step 6. The first and most obvious way Alice may rebut the presumption that she signed the message is to carry the burden of proof that the certification authority made a mistake in identifying Alice as the subscriber of the certificate which contains the public key. One factual theory available to Alice is that an imposter spoofed Alice's identity in applying for a certificate in the name of Alice, but bound to the imposter's public key. If Alice succeeds with this theory and the relying party has been damaged by

---

[5] The significant word "rebuttable" is sometimes inadvertently omitted by those who characterize the Utah Model as unduly burdensome to consumers who compromise their private keys. See the analysis below.

reliance upon the incorrect certificate, then the relying party could seek redress against the CA for damages caused by the CA's error. Under a so-called "closed PKI model" (in contrast with the "open PKI model" which the *Guidelines* represent) it may be that no one other than the CA itself (or a government or other entity controlling the CA or outsourcing duties to the CA) is entitled to rely upon the CA's certificate.

Step 7. The second way Alice may rebut the presumption that she signed the message is to carry the burden of proof that, although Alice's private key was used to sign the message, the use of Alice's private key was unauthorized by Alice. To do this, Alice would need to overcome the non-repudiation security service provided by the dual-key asymmetric cryptosystem, and carry the burden of proving that she compromised or lost control of her private key, and that the private key was used by another to sign the message, without her authority.

Step 8. Under GL 4.3, Alice has the affirmative duty to safeguard her private key from compromise. If Alice was successful under Step 7 in showing that her private key was used by another to sign the message without her authority, then the inquiry will proceed to the issue of whether Alice's compromise of her private key was negligent. If Alice violated her duty to safeguard her key from compromise, then as between the two innocent parties - Bob the relying party and Alice the subscriber - Alice would bear the loss if reimbursement is not possible against the unauthorized user of Alice's private key. It is not clear under the Guidelines whether Alice would have the burden of proving Alice's due care or whether Bob would have the burden of proving Alice's negligence. Either rule would be a rational approach by a State or other jurisdiction which wished to tilt the playing field more in favor of one of the two parties. The required standard of care is likely to be affected by the extent to which the digital signature software comes to be embedded in smart cards and other hardware devices with the triple compromise protection of (a) tangible token required, (b) secret PIN required, and (c) biometric proof of physical presence.

Step 9. If Alice discovers that her private key has been compromised, she can perhaps cut off her liability to relying parties (at least as to future reliance) by revoking her certificate, so that the certificate becomes listed on a certificate revocation list which cuts off the operational period of the certificate so that no digital signatures created thereafter are verifiable. See GL 5.4, regarding reasonable of reliance. An important issue is the extent to which relying parties have constructive notice of certificate revocation lists maintained online and elsewhere CAs, whether or not the relying party has actual notice of the certificate's revocation.

Step 10. Finally, even if Alice for some reason fails to revoke her certificate in time to warn relying parties, under the particular circumstances there may be factual arguments available to her under GL 5.3, regarding unreliable digital signatures, as to why Bob should be required to confirm the transaction with Alice "out-of-band" (e.g., by picking up the telephone) before proceeding to rely.