

An Attorney's Roadmap to the ABA Digital Signature Guidelines

Charles R. Merrill, Esq.

**Computer & High Tech Law
Practice Group of**

**McCarter & English
Newark, New Jersey**

Bob claims to have received the
following Internet E-Mail
Message:

From: alice@wonderland.com

To: bob@securities-r-us.com

Date: 1/31/97 8:30 PST

Buy 100 shs of Netscape for my account at the
market. /s/ Alice

The Price of Netscape Plummets.

Alice: I never sent it! **Bob:** You did so!

The Challenge of **Secure** Electronic Commerce on the Internet

- A Digital Message is **Bits Not Atoms**
- Closed vs **Open System**
- Anonymity "**They Can't Tell You're a Dog**"
- **Spoofing Alice's Identity and Messages**
- "**Why do you rob banks, Willie?**"

Some "Security Services" Which Electronic Commerce Must Deliver In Order to be Secure:

Confidentiality - Exclusive Knowledge

Authentication of Signer - WHO

Authentication of Message - WHAT

Time-Stamp - WHEN

Non-Repudiation - The Holy Grail

Conventional Crypto

A Single Key is used for:

Encryption of Plaintext --> Ciphertext

Decryption of Ciphertext --> Plaintext

Two Problems using Conventional Crypto on the Internet:

Single Key Must be Shared

Key Distribution Problem

"Public Key" Crypto

Instead of a Single Key, there is a **Key Pair**.

One of the Keys is kept Secret (**Private Key**)

The Other is Made Available (**Public Key**)

If One of the Keys Encrypts, **the Other** Decrypts

If One of the Keys Decrypts, **the Other** Encrypts

"Computationally Unfeasible" to Derive the
Private Key from Knowledge of the Public Key

Using Public Key Crypto

For Confidentiality, Sender Encrypts the Message with the **Public Key of the Recipient**. The Recipient Decrypts the Message with the **Private Key of the Recipient**.

For Authentication of Identity, the Sender Encrypts the Message with the **Secret Key of the Sender**. The Recipient Decrypts the Message with the **Public Key of the Sender**.

Crypto for Other Security Services

For Message Integrity, a "One-Way Hash" Algorithm Confirms that the Message has not been altered since it was hashed.

Time-Date Stamping needs Trusted Third Party System. Patented Technology is Digital Notary by Surety Technologies, Inc.

Non-Repudiation

"Nonrepudiation"

**Blocks the False Denial of the
SENDING of the Message**

Alice: "I never sent it!"

CONTENT of the Message

Alice: "I said you should sell, not buy!"

Technical vs Legal Nonrepudiation

Technical: Yes or No

Legal: Maybe. Prove It.

Guideline 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: As Determined by the Ultimate Dispute Resolution Authority

The Possible Theories Facing the Fact-Finder

- A Alice is lying and Bob is truthful.** Alice did send the message, and Bob did not falsify it.
- B Bob is lying and Alice is truthful.** Alice never sent the message, and Bob falsified it.
- C Alice and Bob are both truthful.** Alice did not send it and Bob did not falsify it. An imposter spoofed Alice's message without the knowledge of either Alice or Bob.

The Technology: Crypto Terms

Asymmetric Cryptosystem **G1.3**

Key Pair **G1.17** - Private Key **G1.24** -

Public Key **G1.25** - Private Key

Corresponding to the Public Key **G1.10**

Message **G1.18** - Hash Function **G1.12** -

Digital Signature **G1.11**

Certificate **G1.5** - Certification Auth **G1.6** -

Subscriber **G1.31** Relying Party **G1.27** Verify
a Digital Signature **G1.37**

The Ten-Step Roadmap to the Digital Signature Guidelines

Step 1 - Do we have a **digital signature**

Step 2 - The Crypto Software links the creation of the Digital Signature (and the freezing of Message Integrity) to the **use of the private key corresponding** to the available **public key**.

Dig Sig-->Priv Key-->Public Key

We still know nothing about who is the **signer**.

Step 3 - A **certificate** from a **trusted third party certification authority** binds the identity of **Alice** to **Alice's public key**.

Step 4 - **Verify the digital signature and message integrity** by determining that the **digital signature** was created by the **private key** corresponding to the **public key** listed in the **certificate**.

(Step 2) SW: Dig Sig-->Priv Key-->Pub Key

(Step 3) CA's Cert: Public Key-->Alice

(Step 4) Q.E.D: Digital Signature-->Alice

Here come the Legal Issues....

Legal Issues are in Blue:

Guideline 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.

Step 5

Guideline 5.6 Presumptions in Dispute Resolution

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, . . .

Rebutting the Presumption

Step 6 - Alice proves that the CA was wrong, that the **certificate contains the imposter's public key instead of Alice's public key**. Relying party looks to the CA under the terms of the CA's certification practice statement.

Step 7 - Or, Alice proves that her **private key was used by an imposter** without Alice's authority. Or possibility of rogue software substituting a doc.

Step 8 - If Alice succeeds with Step 8, there must be a determination of **whether Alice violated her duty to safeguard her private key**, Guideline 4.3.

Step 9 - If Alice discovers that her **private key** has been compromised, she must **notify the CA** that Alice's **certificate** should be **revoked**, so that CA can post it on a **certificate revocation list (CRL)**.

Step 10 - Limitations upon the right of a **recipient of a digital signature and a certificate** to rely upon them:

Guideline 5.3 Unreliable Digital Signatures

Guideline 5.4 Reasonable of Reliance

e.g., if the certificate has been revoked, and is listed in a CRL (certification revocation list) in a repository