

# The Utah Digital Signature Act

---

Lee Hollaar

Professor of Computer Science

University of Utah

# Distinguished Visitor

---

Computer Science Department

Virginia Tech

1996 November 11

Reproduced with permission

# Why signatures?

---

- ◆ Authenticates who created a document
- ◆ Adds formality and finality
- ◆ In many cases, required by law or rule
  - Deeds and wills
  - Contracts over \$500 or for more than a year (Statute of Frauds)
  - Timesheets and reports
  - Homework

# Digital signatures

---

- ◆ Not simply a typed name or image of a handwritten signature
- ◆ Based on public-key encryption
- ◆ Associated with a digital document

# Public-key encryption

---

Based on use of a related pair of keys

- Unable to determine one key from the other
- Either key can decrypt material encrypted with the other key
- One is made public, the other kept private

How to obtain public keys

Issue of key escrow

# Digitally signing a document

---

- Indicate extent of signed document
- Compute checksum of signed document
- Encrypt checksum, time and date, and other information using private key
- Attach digital signature to end of document
- Optionally, encrypt signed document with receiver's public key

# Verification of document

---

- Decrypt signed document, if necessary, using private key
- Decrypt digital signature using public key
- Verify checksum for document
- Display the time and date of the document

# Trusted public keys

---

- ◆ Public key given on a certificate, issued by licensed certification authority
- ◆ Able to trace pedigree of certificate to government regulator
  - Utah Department of Commerce
- ◆ Certificate has not been revoked
  - Revocations listed in a repository

# Certificates

---

## Contents of certificate

- Identifies the subscriber
  - Verified by certification authority
- Contains subscriber's public key
- Identifies the certification authority
- Digitally signed by certification authority
- May include a reliance limit

Subscriber must accept certificate

# Effect of a digital signature

---

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, if:

- (1) that digital signature is verified by reference to the public key listed by a licensed certification authority;
- (2) that digital signature was affixed by the signer with the intention of signing the message; and
- (3) the recipient has no knowledge or notice that the signer either:
  - (a) breached a duty as a subscriber; or
  - (b) does not rightfully hold the private key used to affix the digital signature.

Utah Code 46-3-401

# Written document (New Definition)

---

A message is as valid, enforceable, and effective as if it had been written on paper, if it:

- (1) bears in its entirety a digital signature; and
- (2) that digital signature is verified by the public key listed in a certificate which:
  - (a) was issued by a licensed certification authority; and
  - (b) was valid at the time the digital signature was created.

Utah Code 46-3-403

# Status of the Act

---

- Passed by Utah legislature in 1995
- Revised in 1996
- Implementing regulations now been written
- Initial infrastructure providers have been selected
- First state applications to be electronic filing of court documents and UCC<sup>1</sup> forms

<sup>1</sup> Uniform Commercial Code

# Future developments

---

- ◆ State actions
  - Smart cards
  - Electronic notary seals
  - “Signature surrogates”
- ◆ Private sector actions
  - Cybernotaries
  - Electronic checks
  - Anonymous, verified transactions

# For More Information

---

WWW: <http://www.commerce.state.ut.us>

E-mail: [hollaar@cs.utah.edu](mailto:hollaar@cs.utah.edu)