

A Look at Electronic Signature Laws and Legal Standards: Issues and Options

Presentation at the Asia Foundation

August 18, 2000

Donna N. Lampert, Esq.

Background—Definitions

- ▶ Electronic Record
- ▶ Electronic Signature
- ▶ Digital Signature
- ▶ Certificate Authority/Trusted Third Party
- ▶ Keys (Private Key, Public Key, Key Escrow, Key Recovery)
- ▶ Authentication
- ▶ Revocation

Issue—Technological neutrality

How specific should the law be with respect to the type of digital signature technology?

- ▶ Public key infrastructure—use of “key pairs” to authenticate
- ▶ Biometrics (thumbprints, eye patterns, voice recognition, etc.)
- ▶ Dynamic Signature Analysis
- ▶ Other?

Trade-off: Consider today's technology and need for certainty versus tomorrow's technology and potential advances.

ISSUE—Forms of legislation: Prescriptive, two-tier, other?

- ▶ Some legislation addresses only “digital signatures,” i.e., using PKI.
- ▶ Others address range of electronic signatures, according more legal weight (and liability consequences, presumptions, etc.) to the extent the signatures is viewed as more “secure.”
- ▶ Still other laws take very broad approach and do not specify any technology and corresponding consequences.

Consider technological advances, involvement of government, pre-existing legal/regulatory regime.

Issue—How valid are electronic signatures?

Legal validity

- ▶ When is the electronic signature valid and will it be given the same weight as physical paper writings? (Should signature be uniquely linked to the signatory, capable of identifying the signatory, created by means under the signatory's sole control, and linked to data to which it relates so that subsequent alteration of the data is revealed?)

What is the impact on other laws?

- ▶ Usually there are thousands of laws that reference “written signatures”—what is the impact of electronic signature legislation?

Legal presumptions

- ▶ Are electronic signatures more reliable than written signatures and should they be given more weight? (They can indicate that the document has not been altered unlike a manual signature.)

What are standards? Should electronic signatures be mandatory? Who has burden?

Issue—Who is a “trusted third party” or “certificate authority?”

- ▶ Are they required to be licensed or otherwise register?
- ▶ If there are licensing requirements, what are they? Registration? Financial? Technical? Agreement to key escrow and third party key recovery?
- ▶ If there is a certification process, should it be self-certification? Government testing and certification?
- ▶ What about voluntary registration, certification, or accreditation?
- ▶ What services may be required (registration, certification, key generation, certificate revocation, time-stamping?)
- ▶ What criteria for certificates (identity of service provider, name of holder, attributes of the holder, valid period, certificate number, limitations on use, confidentiality information, etc.)?

Issue—Where does liability rest between the two/three parties (sender, recipient, certificate authorities)?

- ▶ Under what circumstances can the certificate authority limit liability if at all?
- ▶ Is liability limitation tied to registration, accreditation, or licensing?
- ▶ Do existing (non-electronic principles) of liability govern?
- ▶ Should there be some minimum liability?
- ▶ Should closed systems (when parties agree on terms, rights, and duties regarding electronic signatures) be subject to lesser requirements?
- ▶ Does allowing the limitation of liability help or hinder electronic commerce growth? Potential for creating legitimacy where business/practical realities might not justify risks; can create different levels of liability

Issue—What protections/measures will exist to protect the privacy of users of digital signatures?

- ▶ Who should have access to keys used in digital signatures and under what circumstances? Certificate Authority? Government? Law Enforcement?
- ▶ What measures will exist, if any, to safeguard information gathered through use of digital signatures? Should treatment differ for commercial use versus official use?
- ▶ Should individuals be permitted to consent to collection of information through an “opt in” process? What about an “opt out process?”

Issue—What are the impacts of national laws on international electronic commerce?

- ▶ Will substantive conflicts mean that international e-commerce is impractical unless there are international standards?
- ▶ Will certain requirements (e.g., licensing) impede the use of electronic signatures since they could require foreign certificate authorities to abide by domestic requirements?
- ▶ What about international initiatives (EU, UNCITRAL, OECD, APEC, International Chamber of Commerce)?