UNCITRAL United Nations Commission on International Trade Law

UNCITRAL legislative standards on electronic communications and electronic signatures: an introduction

Luca Castellani
Legal Officer
UNCITRAL secretariat

International harmonization of e-Commerce law

- UNCITRAL Model Law on Electronic Commerce (1996)

  text and list of enacting states available at
  www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html

- UNCITRAL Model Law on Electronic Signatures (2001)

  text and list of enacting states available at
  www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2001Model_signatures.html

- United Nations Convention on the Use of Electronic Communications in International Contracts (2005)

  text and list of signatory states available at
  http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/2005Convention.html

International harmonization of e-Commerce law

Sources of legal obstacles to electronic transactions

- **Legal concepts based on the existence of a tangible medium**

  "instrument", "document", "original", "signature"

- **Legal concepts based on geographic location:**

  "delivery", "receipt", "dispatch", "surrender"

Recognition and evidentiary value of electronic communications: basic questions

- **If there is no Law on electronic transactions:**
  - Do courts adopt a liberal interpretation to form requirements and evidentiary rules?
  - Or do they take a restrictive approach?

- **If there is a Law on electronic transactions:**
  - Does it limit the types of electronic records that are legally recognized?
  - Does it admit other types of electronic records as well?

Basic principles of e-commerce legislation

- **Non discrimination**
  - Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message (or it is incorporated by reference).
- **Functional equivalence**
  - To facilitate rather than regulate electronic commerce
  - To adapt existing legal requirements
  - To provide basic legal validity and raise legal certainty

Basic principles of e-commerce legislation

- **Media and technology neutrality**
  - Equal treatment of paper-based and electronic transactions
  - Equal treatment of different techniques (EDI, e-mail, Internet, telegram, telex, fax)
- **Party autonomy**
  - Primacy of party agreement on whether and how to use e-commerce techniques
  - Parties free to choose security level appropriate for their transactions

Functional equivalence of the written form

Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

(UNCITRAL Model Law on Electronic Commerce, article 6).

Functional equivalence of “original” messages

A data message can be regarded as an “original” document if:

- There exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and
- The information is capable of being displayed to the person to whom it is to be presented.

(UNCITRAL Model Law on Electronic Commerce, article 8)

Traditional authentication and signature methods

Notion of authentication and signature in the paper world

- "Authenticity" as a quality
- "Signature" as a method

Varying functions under areas of law and across legal systems

- Contract law and procedural law
- Common law and civil law distinctions

Traditional authentication and signature methods

Basic functions of hand-written signatures

- Identify a person
- Associate that person with the content of a document
- Attest to signatory's intent to
  - to be bound by the content of a signed contract
  - to endorse authorship of a text
- Prove the signatory's presence at a given place at a given time

Policy approaches to electronic signatures

- Prescriptive legislation
  - Imposes use of a specific technology (typically digital signature technology)
- “Two-tier” legislation
  - Creates legal presumptions in favour of one technology or method, but also admits other means of identification
- “Minimalist” legislation
  - Provides minimum requirements and leave the parties free to choose signature method they deem appropriate

Policy approaches to electronic signatures

Countries that enacted legislation to support digital signatures (exclusively or primarily):

- Americas: Argentina, Brazil (only for use within public administration), Chile, Colombia, Dominican Republic, Ecuador, Panama, Uruguay.
- Africa: Tunisia, South Africa.
- Asia and the Middle East: India, Malaysia, Israel, Japan.
- Europe: Belarus, Russian Federation.

Policy approaches to electronic signatures

- Examples of enactment of two-tier legislation in “old” EU:
  - Specific e-signature laws: Italy, Germany, Portugal (all had to amend existing legislation), Austria, Belgium, Denmark, Finland, Greece, Spain, Sweden, UK (new legislation)
  - Incorporated in broader framework: Ireland, Luxemburg (e-commerce specific); France, Netherlands (civil code)
- Other European countries:
  - Czech Republic, Estonia, Hungary, Lithuania, Poland, Slovenia (already prior to EU accession); Croatia, Norway, Romania, Switzerland
- Examples of two-tier legislation in other continents:
  - Mexico, Pakistan, Singapore, Thailand

Policy approaches to electronic signatures

Main examples of minimalist legislation

- Australia
- Canada
- New Zealand
- United States of America

Policy approaches to certification services

- Free market approach
  - Any entity may offer certification services without requiring prior authorization: United States
- Mandatory licensing schemes
  - Certification authorities need to obtain a license from a governmental body: Colombia, India, Singapore
- Accreditation schemes
  - Certification authorities encouraged to seek accreditation with a public body or with a private non-for profit business sector organization: European Union, Pakistan
- Monopoly schemes
  - Only public bodies or notaries authorized to issue certificates: typically applied to digital signatures used in governmental functions: Argentina, Chile

Electronic signatures under the UNCITRAL Model Law on Electronic Commerce

Legal signature requirements are met in relation to a data message if:

- a method is used to identify the signatory and to indicate his approval of the information contained in the data message; and
- that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated

(ex-post facto reliability of signature method: UNCITRAL Model Law, article 7)

The UNCITRAL policy: technology neutrality

Model Law on Electronic Signatures, article 3
(Equal treatment of signature technologies):

Nothing in the Law shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies its requirements or otherwise meets the requirements of applicable law.

Technology neutrality applied to electronic signatures: reliability standards

Model Law on Electronic Signatures, article 6(1)
(Compliance with a requirement for a signature):

Legal signature requirements are met in relation to a data message if an electronic signature is used which is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

Technology neutrality applied to electronic signatures: reliability standards

Model Law on Electronic Signatures, article 6(3)
(Compliance with requirement for signature):

(a) signature creation data must be linked to the signatory and to no other person;

(b) signature creation data must be under the control of the signatory at the time of signing;

(c) alterations to the electronic signature made after the time of signing must be detectable;

(d) where legal signature requirement aims at assuring integrity of the information, any alteration to the information must be detectable.

Technology neutrality applied to electronic signatures: reliability standards

When is a signature method “as reliable as appropriate”?

Model Law allows parties to decide taking into account:

- Sophistication of equipment used
- Nature of trade activity
- Frequency of commercial transactions between the parties
- Kind and size of the transaction
- Legal function of signature

Technology neutrality applied to electronic signatures: reliability standards: determining reliability in advance

Model Law on Electronic Signatures, article 7 (Satisfaction of article 6)

Enacting States may determine which electronic signatures satisfy the provisions of article 6, provided that any such determination must be consistent with recognized international standards.

Policy approaches to electronic signatures: additional issues

- **Duties of signatories and relying parties**
  - Should users bear risk?
  - Analogy to ATM cards and credit cards
- **Liability of certification authorities**
  - Should there be statutory limitation of liability?
  - Should there be statutory standards of care?
- **Cross-certification and foreign certificates**
  - Should the law protect local market?
  - On what basis should foreign certificates be recognized?

The UNCITRAL approach: basic good faith obligations for signatories

Article 8 (Conduct of the signatory)

The signatory has a duty to:

- exercise reasonable care to avoid unauthorized use of its signature creation data;
- without undue delay, notify interested parties if signature creation data have been compromised or may have been compromised;
- exercise reasonable care to ensure the accuracy and completeness of all material representations made which are relevant to the certificate throughout its life-cycle, or which are to be included in the certificate.

The UNCITRAL approach: market structure left for domestic policy, with basic standards of conduct for certification services providers

Article 9 (Conduct of the certification service provider)

The certification service provider has a duty to:

- Comply with representations on policies and practices;
- Ensure accuracy and completeness of all material representations relevant to the certificate;

Certification services provider must also provide reasonably accessible means for a relying party to ascertain from the certificate:

(i) the identity of certification service provider;

(ii) that signatory had control of signature creation data at the time when certificate was issued;

(iii) that signature creation data were valid at or before that time;

The UNCITRAL approach: market structure left for domestic policy, with basic standards of conduct for certification services providers

Article 9 (Continued)

Certification services provider must also provide reasonably accessible means for a relying party to ascertain:

(i) how signatory was identified;

(ii) limitations on the purpose or value of signature creation data or certificate;

(iii) that signature creation data are valid and have not been compromised;

(iv) limitations on the scope or extent of liability of certification service provider;

(v) availability of notice and revocation facilities.

The UNCITRAL approach: market structure left for domestic policy, with basic standards of conduct for certification services providers

Article 9 (Continued)

- Certification services provider must always utilize trustworthy systems, procedures and human resources in performing its services.
- Trustworthiness needs to be assessed on the basis of factors such as

  (a) financial and human resources

  (b) quality of hardware and software systems;

  (c) procedures for processing certificates and applications;

  (d) availability of information to signatories and potential relying parties;

  (e) regularity and extent of audits;

  (f) official certification of compliance.

The UNCITRAL approach: basic good faith obligations for relying parties

Article 11. Conduct of the relying party

Relying parties reminded of their duty to:

(a) take reasonable steps to verify the reliability of an electronic signature; or

(b) take reasonable steps to:

(i) verify the validity, suspension or revocation of the certificate; and

(ii) observe any limitation with respect to the certificate.

Barriers to international use of electronic signatures

- Absence of common standards:
  - Different countries accept different methods
  - Same method applying different technical standards in different countries
- Variety of approaches and designs:
  - Conflicting conceptual outlay of electronic signature systems
  - Varying role of State
- Recent UNCITRAL study: “Promoting confidence in electronic commerce: legal issues on international use of electronic authentication and signature methods”
  - Available at http://www.uncitral.org/pdf/english/texts/electcom/08-55698_Ebook.pdf

UNCITRAL policy on cross-border use of electronic signatures: no discrimination and substantive equivalence

Article 12. Recognition of foreign certificates and electronic signatures

In determining legal effectiveness of certificates or electronic signatures States should not take into account:

(a) place where the certificate is issued or the electronic signature created or used; or

(b) the place of business of the issuer or signatory.

Foreign certificates and electronic signatures created or used abroad should have the same legal effect in the country if they offer a substantially equivalent level of reliability as domestic ones in the light of recognized international standards and other relevant factors.

Contact information

For further information on the work of UNCITRAL on electronic commerce and electronic signatures, please visit: www.uncitral.org

You may reach me at luca.castellani@uncitral.org

Thank you for your attention!