Introduction to the law of electronic signatures

Luca Castellani

Head, Regional Centre for Asia and the Pacific

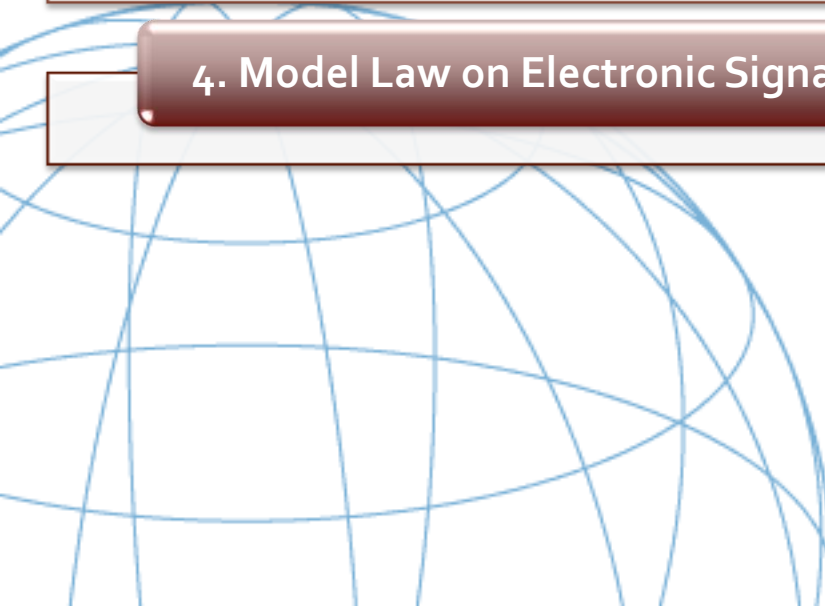UNCITRAL Secretariat

Incheon, Republic of Korea

Outline

1. Methods and technologies for electronic signatures

2. Policy approaches to electronic signatures

3. Certification service provider

4. Model Law on Electronic Signature

Methods and technologies for electronic signatures

Traditional hand-written signature

Notion of authentication and signature in the paper world

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

Basic Functions of hand-written signatures

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

Not all of these functions are intrinsic to the paper document. In particular, identification/trust may derive from other sources.

Electronic authentication technologies

E-mail addresses, URLs, scanned images

PIN codes, Smart Cards

Cryptography

Biometrics

Barriers to international use of electronic signatures

Absence of common standards

- o Different countries may adopt different methods

- o Same method may be applied with different technical standards in different countries
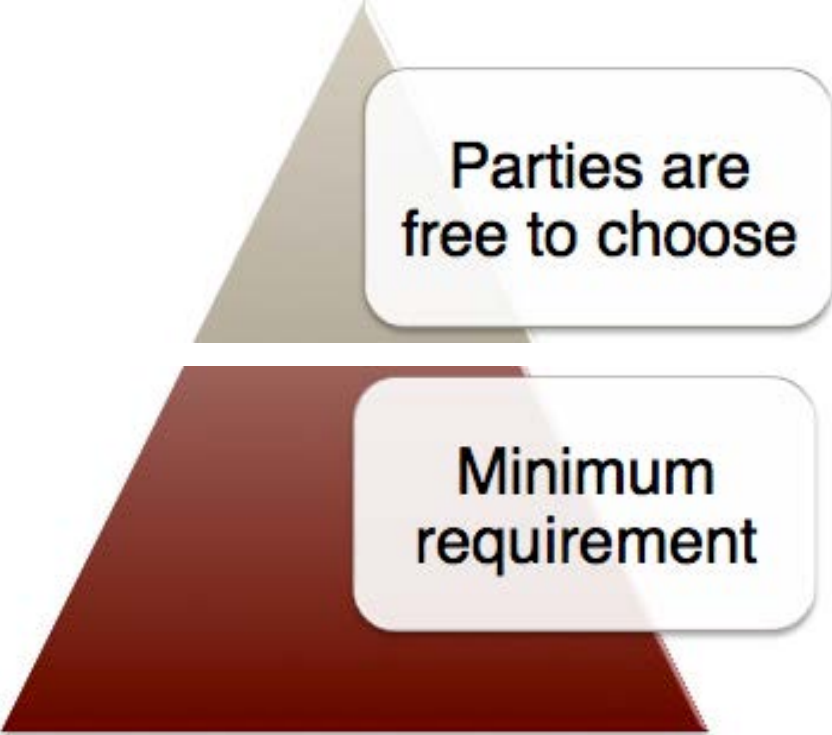
Variety of approaches and designs

- o Conflicting conceptual outlay of electronic signature systems

- o Varying role of State
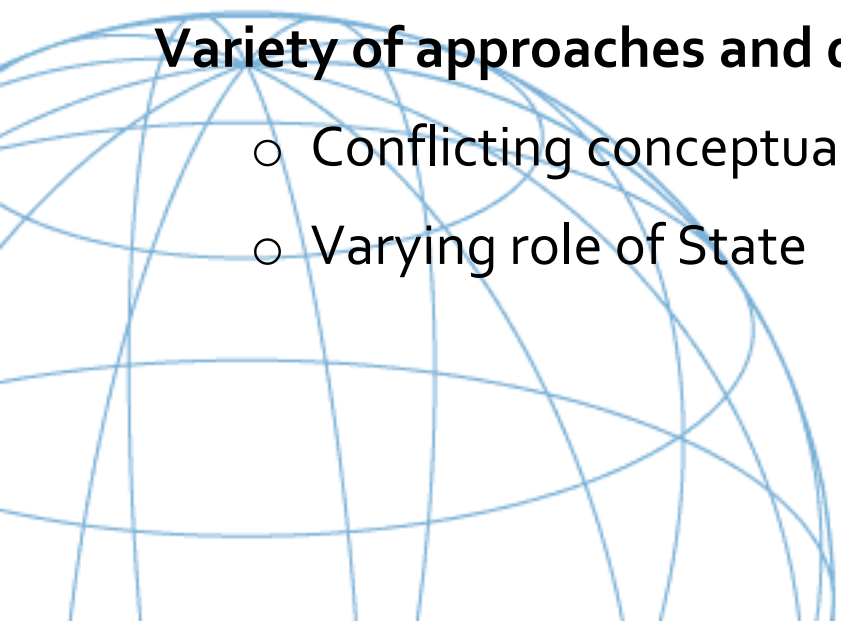
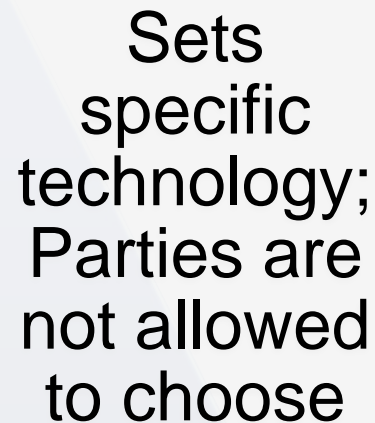# Policy approaches to electronic signatures

1. Minimalist approach

Parties are free to choose

Minimum requirement

- Law provides minimum requirements.

- Follows the principle of technological neutrality.

- Functional equivalence is confirmed provided that certain specified functions and requirements are met.

- Parties are free to choose any signature method they deem appropriate.

Min. Requirement & Choice of ID and Password

2. Technology-specific approach

Sets specific technology; Parties are not allowed to choose

- Prescribes the use of a specific technology.

- Not technology neutral – risks excluding superior technologies from entering and competing in the marketplace.

- Fixing requirements before a particular technology matures.

- Parties are not free to choose the signature method they deem appropriate.

Digital signature based on cryptography (PKI)

3. "Two-tier" legislation

Parties are free to choose method they deem appropriate

Advanced and secure signature
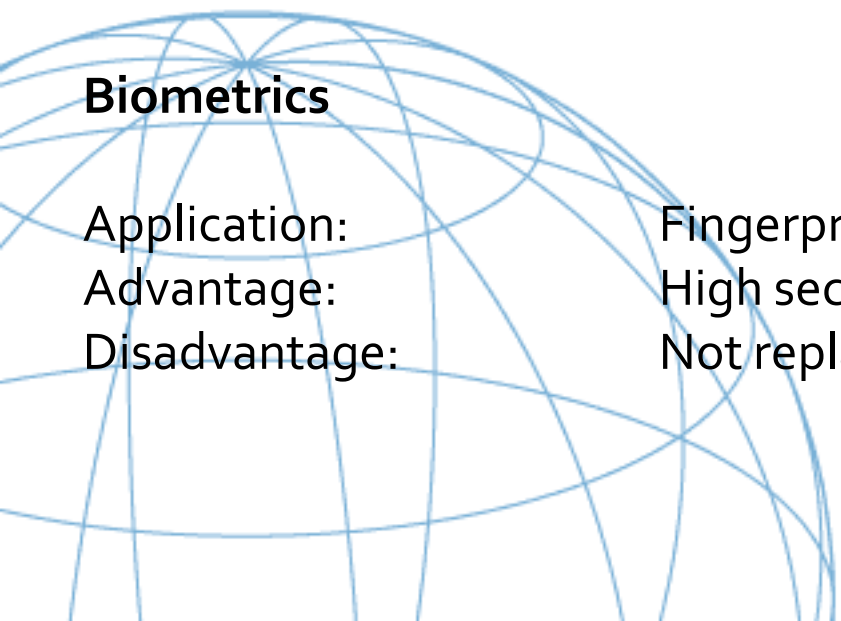
Any electronic signature

Advantages and disadvantages of electronic authentication and signature technologies

Cryptography

Application:	PKI (asymmetric cryptography)
Advantage:	High security level (encryption), speed
Disadvantage:	Costs; involvement of third party; unavailable in certain environments (mobile, objects); sometimes, not as secure as expected.

Biometrics

Application:	Fingerprints, iris scan, voice recognition…
Advantage:	High security level (unique data)
Disadvantage:	Not replaceable; privacy issues.

Advantages and disadvantages of electronic authentication and signature technologies

Sharing of codes and secrets

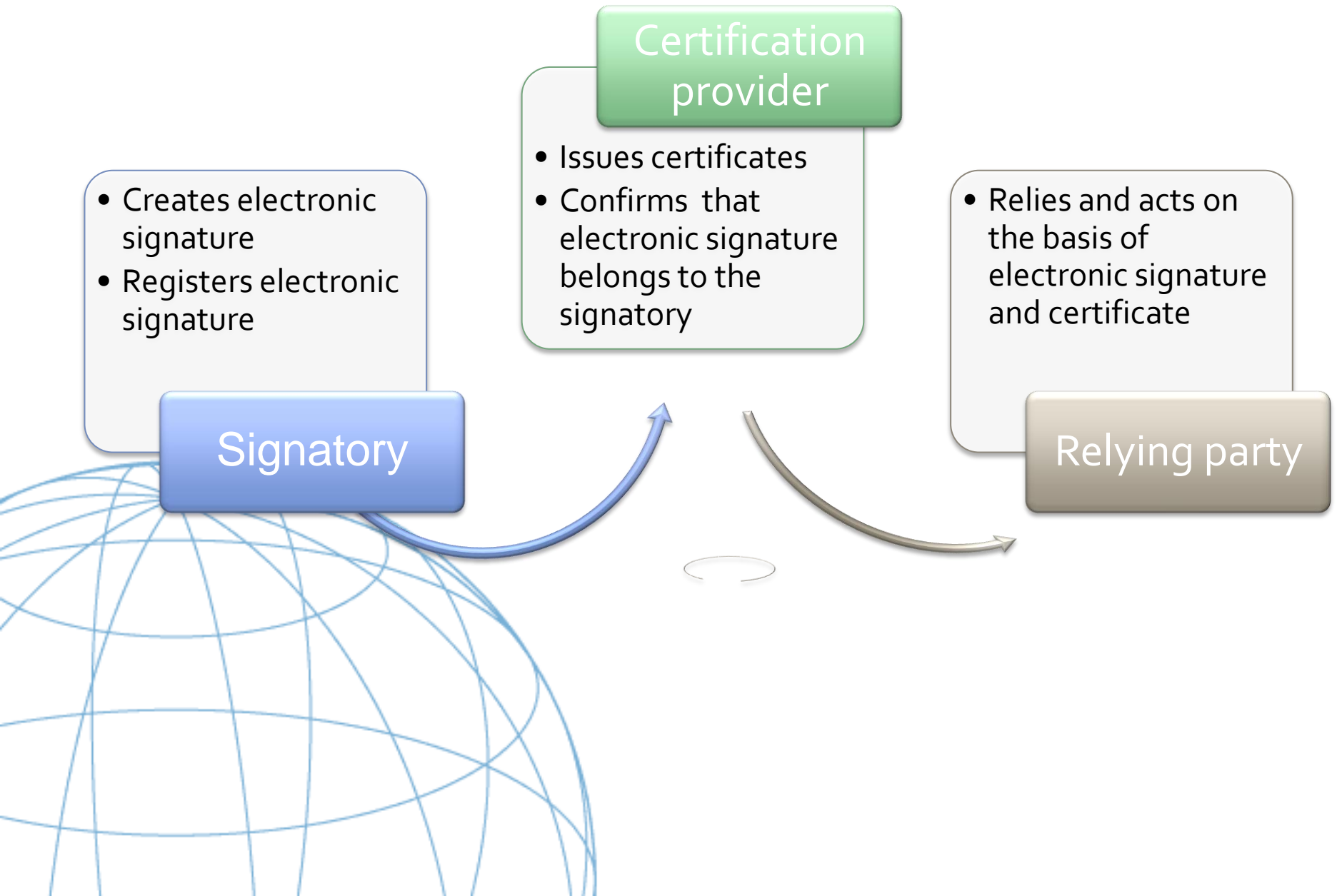|	
Application:	PINs, Smart Cards
Advantage:	Speed, no third party involved
Disadvantage:	Risk of compromise

Other methods

Application:	Scanned signatures, verification of e-mail address or IP addresses
Advantages:	Ease of use, speed, low cost
Disadvantage:	Low level of security

Certification service provider

Certification provider
- Issues certificates
- Confirms that electronic signature belongs to the signatory

Signatory
- Creates electronic signature
- Registers electronic signature

Relying party
- Relies and acts on the basis of electronic signature and certificate

Approaches to certification service providers

Free market approach
- Any entity may offer certification services without requiring prior authorization

Accreditation schemes
- Certification authorities encouraged to seek accreditation with a public body or with a private non-for profit business sector organization.

Mandatory licensing schemes
- Certification authorities need to obtain a license from a governmental body.

Monopoly schemes
- Only public bodies or notaries authorized to issue certificates: typically used for digital signatures used in governmental functions.

Additional issues

- **Duties of signatories and relying parties**
  - o Should users bear risk?
  - o Analogy to ATM cards and credit cards
- **Liability of certification authorities**
  - o Should there be statutory limitation of liability?
  - o Should there be statutory standards of care?
- **Cross-certification and foreign certificates**
  - o Should the law protect local market?
  - o On what basis should foreign certificates be recognized?
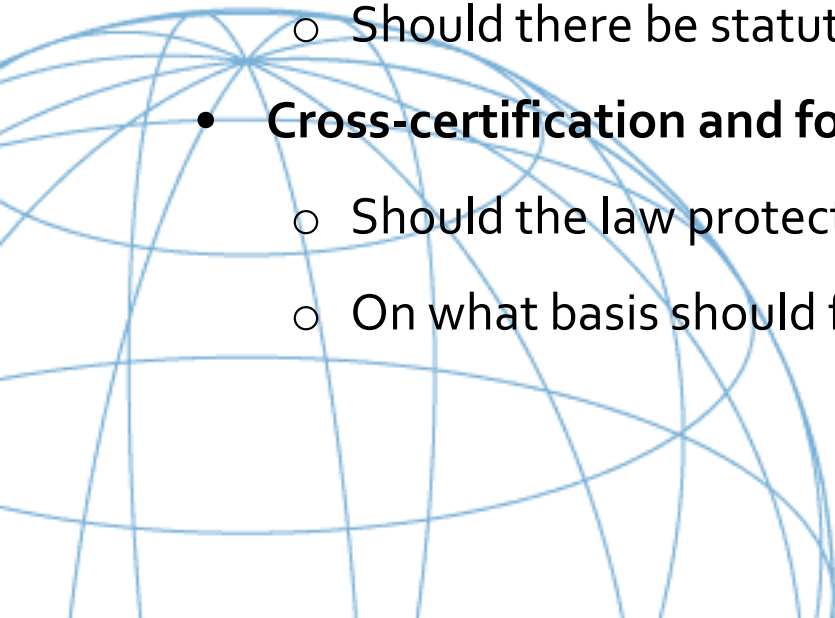
Public Key Infrastructure (PKI)
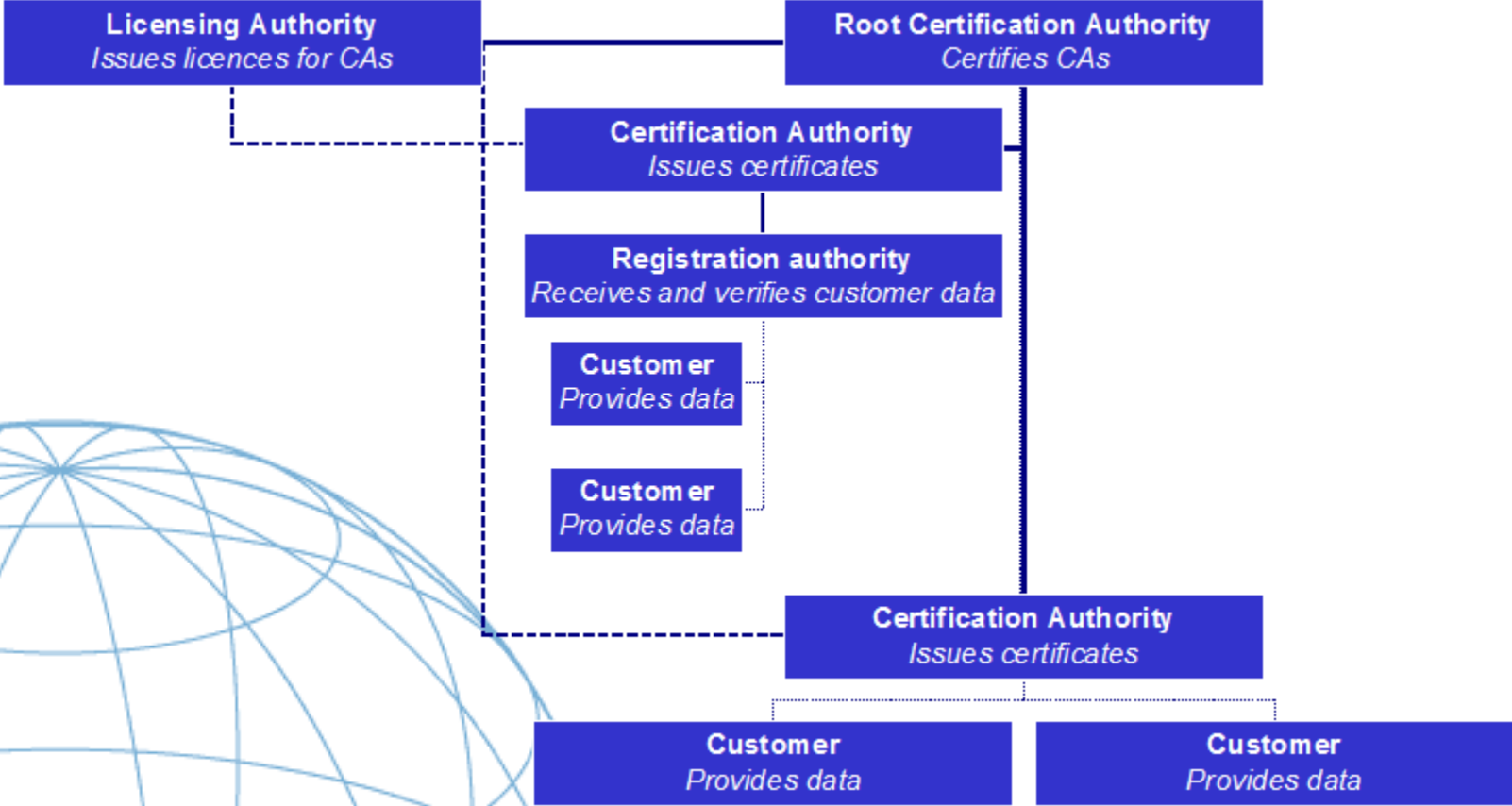
UNCITRAL
Model Law on Electronic Signature

Technology neutrality

Article 3. Equal treatment of signature technologies

Nothing in the Law, except article 5, shall be applied so as to exclude, restrict or deprive of legal effect any method of creating an electronic signature that satisfies its requirements referred to in article 6, paragraph 1, or otherwise meets the requirements of applicable law.

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**

Article 5. Variation by agreement

The provisions of this Law may be derogated from or their effect may be varied by agreement, unless that agreement would not be valid or effective under applicable law.
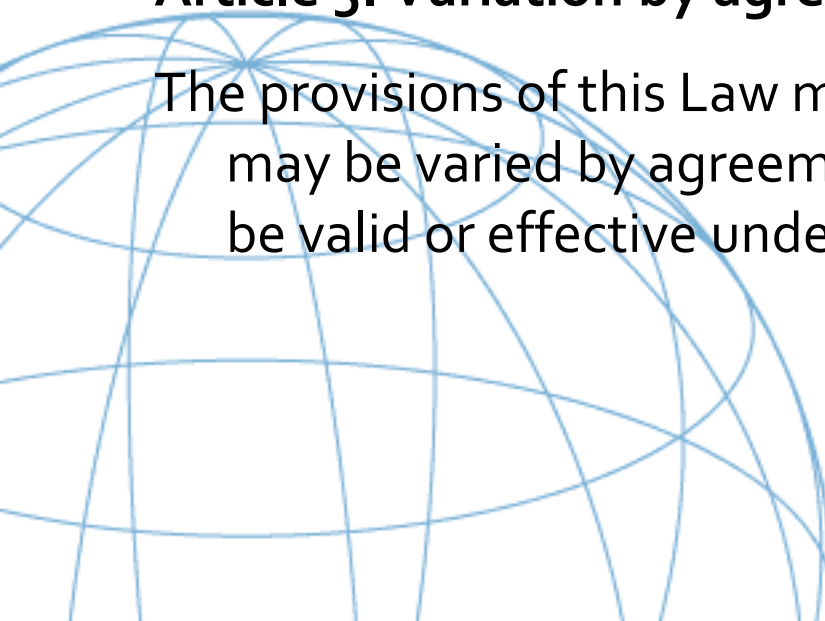
Functional equivalence of signature methods

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 in the light of all the circumstances, including any relevant agreement.
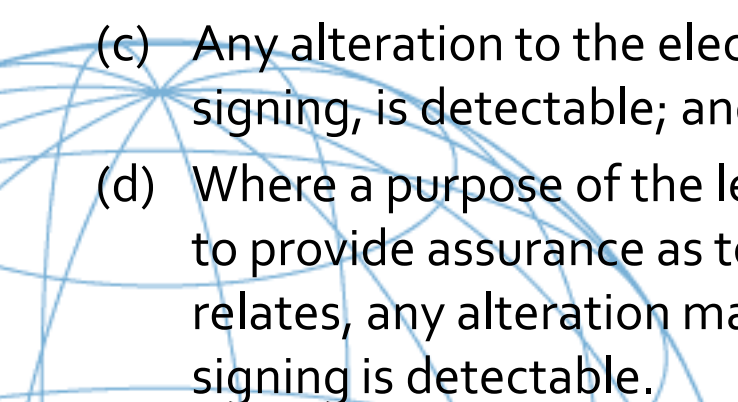
Ex-post facto reliability of signature method:

- UNCITRAL Model Law on Electronic Commerce, article 7;

- UNCITRAL Model Law on Electronic Signatures, article 6; and

- UN Convention on the Use of Electronic Communications in International Contracts, article 9(3).

Presumption of reliability "advanced electronic signatures"

Article 6. Compliance with a requirement for a signature

3. An electronic signature is considered to be reliable […] if:

   (a) The signature creation data are […] linked to the signatory and to no other person;

   (b) The signature creation data were, at the time of signing, under the control of the signatory and of no other person;

   (c) Any alteration to the electronic signature, made after the time of signing, is detectable; and

   (d) Where a purpose of the legal signature requirement for a signature is to provide assurance as to the integrity of the information to which it relates, any alteration made to that information after the time of signing is detectable.
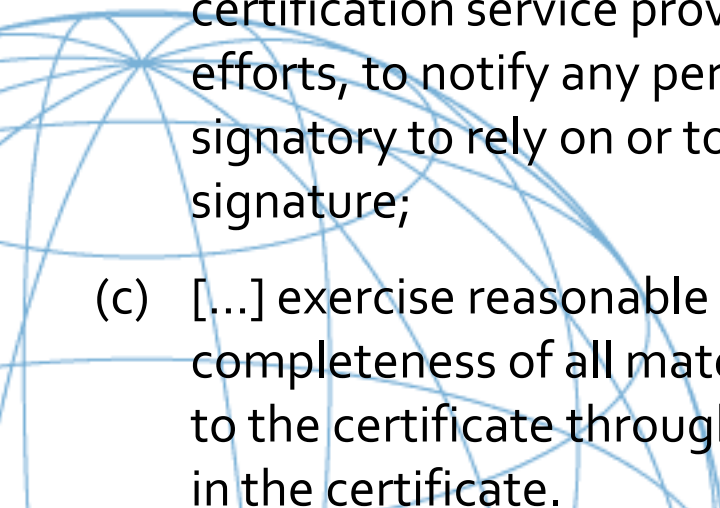
Reliability standards

- **When is a signature method "as reliable as appropriate"?**
- **Model Law allows to decide taking into account:**

    o Sophistication of equipment used

    o Business nature

    o Frequency of commercial transactions between the parties

    o Kind and size of the transaction

    o Legal function of signature

Signatory

Article 8. Conduct of the signatory

1. Where signature creation data can be used to create a signature that has legal effect, each signatory shall:

   (a) Exercise reasonable care to avoid unauthorized use of its signature creation data;

   (b) Without undue delay, utilize means made available by the certification service provider [...], or otherwise use reasonable efforts, to notify any person that may reasonably be expected by the signatory to rely on or to provide services in support of the electronic signature;

   (c) [...] exercise reasonable care to ensure the accuracy and completeness of all material representations made that are relevant to the certificate throughout its life-cycle, or that are to be included in the certificate.
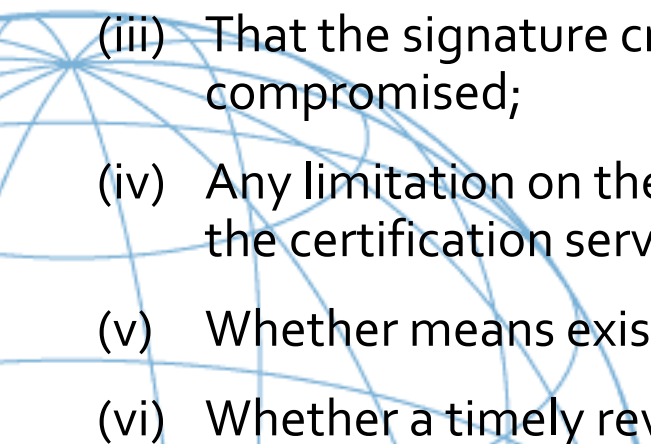
Certification service provider

Article 9. Conduct of the certification service provider.

1. Where a certification service provider provides services to support an electronic signature that may be used for legal effect as a signature, that certification service provider shall:

    (a) Act in accordance with representations made by it with respect to its policies and practices;

    (b) Exercise reasonable care to ensure the accuracy and completeness of all material representations made by it […];

    (c) Provide reasonably accessible means that enable a replying party to ascertain from the certificate:

        (i)   The identity of certification service provider;

        (ii) That the 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 when the certificate was issued;

# Certification service provider

Article 9. (Continued)

(d) Provide reasonably accessible means that enable a replying party to ascertain [...] from the certificate or otherwise:

    (i)   The method used to identity the signatory;

    (ii)   Any limitation on the purpose or value for which the signature creation data or the certificate may be used;

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

    (iv)   Any limitation on the scope or extent of liability stipulated by the certification service provider;

    (v)   Whether means exist for the signatory to give notice [...];

    (vi)   Whether a timely revocation service is offered;

Relying party

Article 11. Conduct of the relying party

A relying party shall bear the legal consequences of its failure:

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

    (b)   Where an electronic signature is supported by a certificate, to take reasonable steps:

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

        (ii)   To observe any limitation with respect to the certificate.
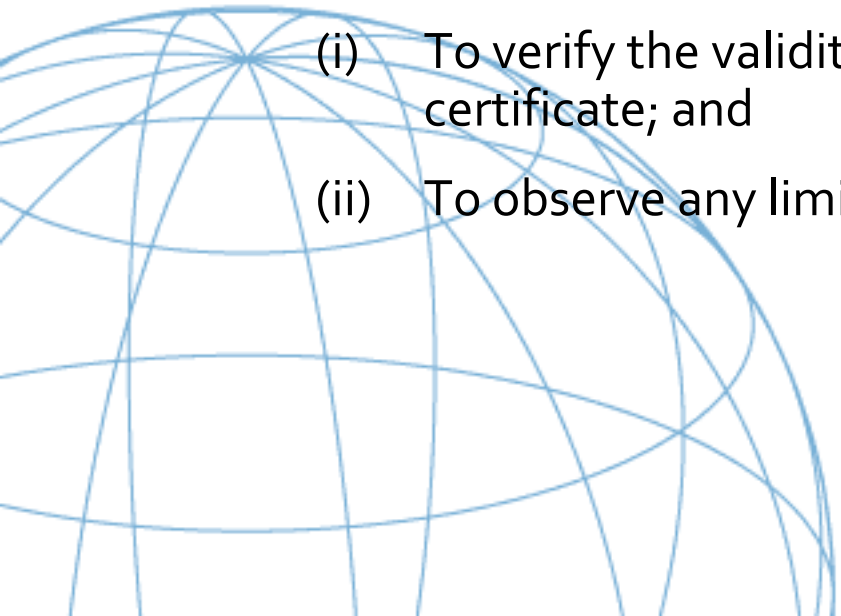
Cross-border use of electronic signatures

Article 12. Recognition of the foreign certifications and electronic signatures

1.   In determining whether, or to what extent, a certificate or an electronic signature is legally effective, no regard shall be had:

(a) To the geographic location where the certificate is issued or the electronic signature created or used; or

(b) To the geographic location of the place of business of the issuer or signatory.

- **No geographic discrimination and substantive equivalence**

  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.

Cross-border use of electronic signatures

- **Cross recognition** is an interoperability arrangement in which the relying party in the area of a PKI can use authority information in the area of another PKI to authenticate a subject in the area of the other PKI.

- **Cross certification** refers to the practice of recognizing another certification services provider's public key to an agreed level of confidence, normally by virtue of a contract. It essentially results in two PKI domains being merged (in whole or in part) into a larger domain. To the users of one certification services provider, the users of the other certification services provider are simply signatories within the extended PKI.

Cross-border use of electronic signatures

Contractual example: PAA

Based on the international standard and best practice, PAA has developed a CA Mutual Recognition Scheme. The scheme composes of a legal and a technical framework to enable electronic trading and logistic activities within the Alliance. Under these frameworks, PAA has established a certificate policy authority – the Pan Asian Certificate Policy Authority ("PAA Policy Authority") - to govern and oversee the usage of digital certificate for all electronic transactions among the PAA members.

The PAA Certificate Policy Authority establishes and maintains a certificate policy – the Pan Asian Certificate Policy Authority Certificate Policy ("PAA Certificate Policy"), which specifies standards and procedures to be adopted by certification authorities ("CA") which seeks recognition from the PAA Policy Authority. The PAA Policy Authority takes into account the ability of a CA to comply with the PAA Certificate Policy in determining whether such CA is suitable for recognition as a recognized CA under PAA Mutual Recognition Scheme.

(Source: http://www.paa.net/PaaPortal/PaaContent/PAACARecognition.htm)

Cross-border use of electronic signatures

Legislative example: EU e-signature directive

Member States shall ensure that certificates which are issued as qualified certificates to the public by a certification-service-provider established in a third country are recognised as legally equivalent to certificates issued by a certification-service-provider established within the Community if:
(a) the certification-service-provider fulfils the requirements laid down in this Directive and has been accredited under a voluntary accreditation scheme established in a Member State; or
(b) a certification-service-provider established within the Community which fulfils the requirements laid down in this Directive guarantees the certificate; or
(c) the certificate or the certification-service-provider is recognised under a bilateral or multilateral agreement between the Community and third countries or international organisations.

Source: Article 7 (1) of the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (under review).

Cross-border use of electronic signatures

Treaty solution:

Where the law requires that a communication or a contract should be signed by a party, or provides consequences for the absence of a signature, that requirement is met in relation to an electronic communication if:
(a) A method is used to identify the party and to indicate that party's intention in respect of the information contained in the electronic communication;
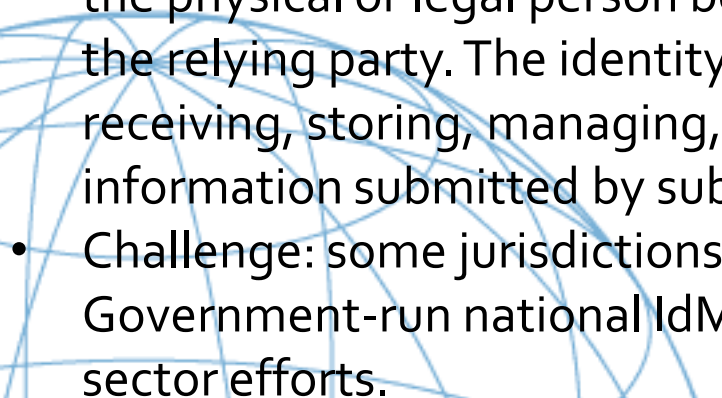and
(b) The method used is either:
(i) As reliable as appropriate for the purpose for which the electronic communication was generated or communicated, in the light of all the circumstances, including any relevant agreement; or
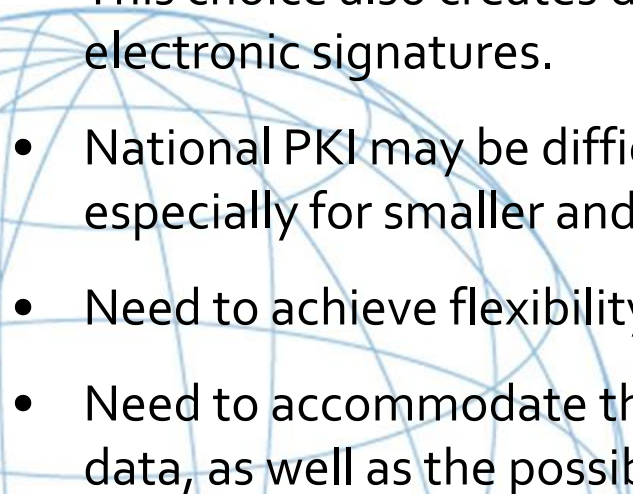(ii) Proven in fact to have fulfilled the functions described in subparagraph
(a) above, by itself or together with further evidence.

Source: Article 9(3) of the United Nations Convention on the Use of Electronic Communications in International Contracts, 2005.

Future of electronic signatures: identity management?

- Identity management (IdM) systems aim at enabling identity portability across different applications by facilitating the secure exchange of identity credentials and eliminating redundant operations.
- They may perform the identification, authentication and authorization of the user by a selective use of shared identity attributes, thus potentially reducing the proliferation of electronic identities.
- In their simplest form, IdM systems feature three actors: the subject (i.e., the physical or legal person being identified), the identity provider, and the relying party. The identity provider may act as a trusted third party, receiving, storing, managing, redistributing and possibly aggregating the information submitted by subjects and relying parties.
- Challenge: some jurisdictions are developing IdM systems based on Government-run national IdM schemes, others are relying on private sector efforts.

Electronic signatures and single window facilities

- Technical specifications for national single window facilities usually rely on PKI systems due to security concerns.

- This choice may hinder exchange of documents with the private sector, which is useful to improve data quality.

- This choice also creates difficulties in cross-border recognition of electronic signatures.

- National PKI may be difficult and expensive to design and maintain, especially for smaller and developing countries.

- Need to achieve flexibility without missing on security.

- Need to accommodate the use of mobile devices for submission of data, as well as the possibility for objects to authenticate themselves.

For more information, please visit
http://www.uncitral.org

Thank You!