UNCITRAL United Nations Commission on International Trade Law

# Legal Aspects of Identity Management and Trust Services

**Anna Joubin-Bret**
**Secretary**
**UNCITRAL**

# What is Identity Management (IdM)?

- Fundamental issue for the use of electronic means
- Answers the basic questions:
  - Who or what is seeking to prove identity?
  - Reliability of proof of the identity?
- Relevance for Sustainable Development Goals:
  - Target 1.4: ensuring access of the poor to economic resources
  - Target 10c: reducing remittances costs
  - Target 16.5: reducing corruption
  - Target 16.9: providing legal identity for all

# What is Identity Management (IdM)?

- Need to identify in order to establish trust, i.e., the reasonable expectation of future behaviour based on past practice
- Applies to natural / legal persons and to physical / digital objects
- Performs several functions that may vary significantly in purpose and requirements
- Requires adjusting business practices and assessing risks
- Different types of IdM systems:
  - Commercial-driven vs. Government-driven;
  - Centralised vs. Decentralised.

# Traditional approach to IdM

- Different identity verification methods were established to respond to needs of identification
  - Witnesses, signatures, seals
- Expansion of commercial relations require new identity management tools
- Eventually, use of government-issued identity credentials became prevalent in trade
  - Based on civil registration and vital statistics registries (where available)
  - Designed for other purposes (e.g., travel)
- Possible involvement of trusted third parties (e.g., notaries) for high-value transactions
- Although governments as issuers of credentials do not accept liability, users have no better option and are able to assess risks based on practice

# Identification in an electronic environment

- The ICT revolution dramatically increases the ability to process and re-use data
- This brings increased attention for data quality:
  - origin, integrity, etc.
- In commercial transactions, reference to the functions of handwritten signatures seems obvious
  - Identify originator, clarify its intent with respect to the signed message
- However, electronic signatures go beyond handwritten ones
  - Trust services: presumption of integrity, time-stamping, etc.

# Electronic signatures’ features

- As the use of electronic signatures increases, some of its features become clearer
  - Not all signatures are the same:
    - reliability varies with the use of different methods and authentication factors.
  - Steps for signing:
    - Identification, authentication, authorisation
    - Identification (i.e. release of electronic credentials) is done against paper-based identifiers (for which the issuer typically accepts no liability)

# From electronic signatures to IdM

- Great legislative interest for electronic signatures
  - However, differences remain in policy, technical and legal choices
  - Challenges in cross-border recognition of electronic signatures
    - Article 9(3) of the UN Electronic Communications Convention enables multilateral legal recognition of electronic signatures.
- Each system requires costly maintenance and development
- The multiplication of systems led to an exponential increment in the number of credentials needed to access the system.
- For users, it is not user-friendly
- Hence the need for IdM system

# Electronic signatures and trust services

- “Trust service” means an electronic service normally provided for payments which consists of:
  - (a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
  - (b) the creation, verification and validation of certificates for website authentication; or
  - (c) the preservation of electronic signatures, seals or certificates related to those services.

Source: eIDAS, article 3(16).

- Most national laws deal with electronic signatures
- Other trust services receive piecemeal legal treatment
- eIDAS represents an early effort to frame e-signatures in the general trust services framework

# IdM policy implications

- IdM policy may pursue different goals:
  - E-Government / Commercial
  - E-Government only
  - Cybersecurity

  (See OECD report “Digital Identity Management: Enabling Innovation and Trust in the Internet Economy”)
- Success of IdM systems is proportional to the number of users and variety of applications
- Excessive reference to technical details and technology may hinder interoperability and mutual legal recognition
- Desire to harmonise legislative and contractual provisions
  - Need to define common rules for the interaction of the various types of identity and trust services
- Regional initiatives must be globally coordinated to avoid creating barriers to cross-border electronic exchanges

# Classification of Identities

| Primary or Foundational Identity | Secondary or Functional / Transactional Identity |
|---|---|
| It may be attributed only once to each entity | It may be multiple for each entity |
| It is an absolute quality that is normally unchangeable. For physical persons: parents, date of birth, biometrics, etc. | It may be built over time. For physical persons: creditworthiness, use of medical or educational facilities, etc. |
| It is difficult to replace if compromised: to be shared cautiously and selectively | It may be easier to replace in case of compromise |
| It has a human right component: the right to a digital identity (SDG 16.9) | It is the only possible if vital records are not available |

# Interaction of different types of identity

- In theory, foundational and transactional identities may be used interchangeably for commercial and non-commercial purposes.
- However, challenges may arise in practice:

| Primary or Foundational Identity | Secondary or Functional / Transactional Identity |
|---|---|
| Inability to share records originating in public vital records | Insufficient guarantee on the quality of transactional identity information |
| Limited liability of public providers | Liability determined commercially |

# Increasing trust in IdM: legal aspects

- Need to further increase trust in IdM in order to extend its use
- Trust is “the belief that something is reliable”
- Reliability is “the quality to perform consistently well”
  - It is the outcome of a process and not a product
  - Should be technology- and system-neutral
- IdM-specific laws need to address risk allocation and ensure it will be upheld in court:
  - Clarify parties’ obligations
  - Allocate liability, e.g., through:
    - Presumptions;
    - Exemptions and limitations of liability;
    - Mandatory insurance.

# IdM legal framework: current status

- IdM-relevant legal provisions may be found on three levels:
  - General laws (e.g. commercial and civil codes' provisions on identification, form requirements, liability, etc.)
  - Specific laws (eIDAS Regulation (2014); Virginia Electronic IdM Act (2015); Benin (2017))
  - Contractual agreements on legal and technical interoperability

- Limited guidance at the global cross-border level
  - eIDAS requires the conclusion of a treaty for recognition of non-EU IdM schemes
  - Virginia IdM Act and Loi 2017-20 of Benin do not address the issue

# Features of IdM-specific laws

- Assessment of reliability is based on compliance with pre-determined technical standards
- Legal consequences of reliability:
  - Cross-border recognition in participating States (eIDAS);
  - Exemption from liability (Va. E-IDM Act);
  - Authorisation to operate IdM scheme (Loi 2017-10 Benin).
- They may support agreements on mutual legal recognition and technical interoperability
- Is this approach sufficient for global recognition of IdM across borders?

# Elements of the UNCITRAL project

- Desire to establish a comprehensive and inclusive process based on shared principles and terminology
- Deal with all types of IdM systems (private/public), all roles, all entities (persons/objects), as well as with all trust services
- Respect general principles of uniform commercial and e-commerce law
- Address legal issues such as: rights and obligations of the parties; reliability; liability; effect of contractual agreements; cross-border aspects
- Exclude data protection and privacy?
- Clarify relationship between primary and secondary identity and/or IdM and trust services.

# Next steps

- WG IV 56th session (New York, 16-20 April 2018)
- Options:
  - Prepare a comprehensive legislative framework (e.g. in a model law defining rights and obligations of participants as well as functional equivalence requirements);
  - Focus on cross-border aspects
    - Possible to use common definitions of Levels of Assurance to facilitate cross-mapping identity schemes
    - Legal effects attributed by the scheme where recognition is sought