Forum on Trade Digitalization for Sustainable Regional Integration: Legal Aspects of Identity Management

Luca Castellani
Secretary, UNCITRAL Working Group IV (Electronic Commerce)

Traditional approach to identity management (IdM)

- Identification of physical persons helps to establish trust
- Originally, identification is based on communities registries
- Eventually, government-issued identity credentials are used
  - Designed for specific purposes (e.g., travel)
  - Used in other contexts (e.g. open a bank account)
- Government does not accept liability for the credentials it issues
  - Practice allows risk assessment

Identification in electronic transactions: electronic signatures

- ICT increases the ability to exchange information remotely and to analyse and re-use data
- How to identify the author of an electronic message or the source of data?
- Reference to handwritten signatures seems obvious
  - Functions of signature are identifying the signatory and clarifying its intent with respect to the signed message
- However, electronic signatures go further
  - Different levels of reliability based on the use of different technologies and methods
  - Trust services serve additional functions such as integrity, time-stamping, etc.

Approaches for assessment of e-signature reliability

1. Ex ante
   - List of prequalified trusted methods
     - May work nationally, but internationally who decides what qualifies?
2. Ex post
   - Assessment of reliability of ID method is carried out only if and when required (e.g. in case of dispute)
3. Entirely left to parties (contractual agreement)
   - May fit commercial uses
   - What about regulatory requirements?

Electronic signatures development

- Signing a document:
  - Acknowledging authorship
- Signing into a system:
  - Getting access to a IT system through a three steps process (identification, authentication, authorisation)
  - Actions, including messages, are attributed to the entity that has signed in
  - Identification for enrolment purposes (i.e. release of electronic credentials) is done against paper-based identifiers

From electronic signatures to IdM

- Multiplication of IT systems
  - Each requires own credentials for access
    - costly maintenance
    - the experience is not user-friendly
  - Federated IdM (single sign-on)
- Identity applies not only to physical and legal persons, but also to physical and digital objects
  - E.g., need to identify source of big data in the Internet of things
    - Autonomous identification does not mean autonomous legal status, e.g. for liability purposes

Foundational Identity

- Foundational Identity is attributed only once to each entity
- It is an absolute quality that is normally unchangeable
  - For physical persons: parents, date of birth, biometrics, etc.
- It may be difficult to replace once compromised
  - Need to share sensitive attributes cautiously and selectively
- Right to digital identity (SDG 16.9)
  - It has a human right component
    - E.g. art 7 Convention on the Rights of the Child

Transactional Identity

- Transactional Identity may be multiple for each entity and may be built over time
  - For physical persons: creditworthiness, use of medical or educational facilities, etc.
- It may be easier to replace in case of compromise
- The only one possible if vital records are not available

Legal aspects of IdM and trust services

- IdM is fundamental to the use of electronic communications
- Trust services enable transactional use of digital identity
- National / regional laws (eIDAS, Virginia IdM Act)
- What about global mutual legal recognition?
  - So far, only limited cross-border recognition of electronic signatures
- Need to establish a mutual recognition mechanism for IdM and trust services able to:
  - Generate trust in all participants
  - Preserve technology neutrality

UNCITRAL Working Group IV

- UNCITRAL Working Group IV is discussing legal aspects of IdM and trust services
  - Next meeting: New York, 8-12 April 2019
- Draft Provisions on the Cross-border Recognition of IdM and Trust Services and Explanatory Remarks
  - IdM legal recognition mechanism approach: ex ante / ex post
  - Mapping against levels of assurance
  - Use of certification / supervision
  - Obligations of involved parties, including liability
  - Trust services: difference with IdM, identification of each service, obligations, etc.
- Documents available on UNCITRAL website

IdM and trust services and trade facilitation

- Need to set common IdM standards across borders
- Need to accept identity-related information generated and exchanged automatically, including by physical and digital object
- In case of data pipeline implementation (e.g. blockchain-based), there may be a single source of all trade-related information
  - That source will be reliably identified by all concerned business partners and regulatory authorities
  - The liability of the declarant is not affected but there may be enforcement issues due to localisation outside the relevant jurisdiction