Legal Aspects of Identity Management

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

Traditional approach to identity management

- Need to identify physical persons to establish trust, i.e., the reasonable expectation of future behaviour based on past practice
- Identification based on vital records
- Vital records were maintained by local communities
  - Relatively low mobility
- Expansion of commercial relations required new identity management tools

Traditional approach to identity management

- Different identity verification methods were established
  - Witnesses, signatures, seals
- Eventually, use of government-issued identity credentials (where available)
  - Typically, primarily designed for other purposes (e.g., travel)
- Government as an issuer does not accept liability for its credentials
- But users have no better option and, with practice, are in a position to assess risk

Verifying electronic transactions

- The ICT revolution dramatically increases the ability to process and re-use data
- This brings increased attention for data quality:
  - origin, integrity, etc.
- Initial focus on (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 development

- As the use of electronic signatures develops, some issues become clearer
  - Not all signatures are the same
    - Different levels of reliability based also on the use of different and/or multiple authentication factors
  - Steps for signing (in a system):
    - 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

- The multiplication of systems leads to an exponential increment in the number of credentials needed to access them
- Each IdM system requires costly maintenance and development
- The experience is not user-friendly
- The notion of federated IdM arises
  - Single sign-on

Models for assessment of reliability

1. Ex ante
    1. List of prequalified trusted methods – but who decides what qualifies?
2. Ex post
    1. Assessment of reliability of ID method is carried out only in case of need
3. Entirely left to parties
    1. Only commercial?

- Identity applies not only to physical and legal persons, but also to physical and digital objects
    - Autonomous identification does not mean autonomous liability
- Foundational IdM vs. transactional IdM

Foundational IdM

- Foundational IdM 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
- It has a human right component
  - Right to digital identity

Transactional IdM

- Transactional IdM 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

An IdM divide?

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

- Transactional to foundational:
  - Public trust frameworks may prefer identity-related information originating in public vital records
  - There may not be sufficient guarantee on the quality of transactional identity information

An IdM divide?

- Foundational to transactional:
  - Public bodies may not always be able to share their records for commercial purposes
  - Issue of liability of public bodies remains

- Need to define common rules for the interaction of the two types of identity
- Particularly challenging at the cross-border level
  - eIDAS sets a high standard for exchanges with non-EU public trust frameworks
  - Virginia IdM Act does not address the issue

IdM challenges

- Emergence of regional systems that are not interoperable and that are not open to mutual legal recognition
- Excessive reference to technical details may undermine technology neutrality and interoperability
- Limited appreciation for the principle of proportionality in IdM
- Difficulty in harmonising legislative and contractual provisions

The way forward

- Article 9(3) of the UN Electronic Communications Convention provides for multilateral legal recognition of electronic signatures:
  - Limited acceptance of that treaty prevents its broader use in commercial practice
- UNCITRAL Working Group IV is tasked with discussing legal aspects of IdM
- Several documents submitted to WG IV 55th session (New York, 24-28 April 2017)
- Desire to establish a comprehensive and inclusive process based on shared principles and terminology