Trends in Digital Identity Verification for Secure Cross-Border Paperless Trade

Bangkok, 8 August 2024

The UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services

Luca Castellani
UNCITRAL Secretariat

The views expressed are those of the author and do not necessarily reflect the views of the United Nations and of UNCITRAL.
UNCITRAL texts on electronic commerce

- UNCITRAL Model Law on Electronic Commerce, 1996
  - Enacted in about 90 States.
- UNCITRAL Model Law on Electronic Signatures, 2001
  - Enacted in about 40 States
- United Nations Convention on the Use of Electronic Communications in International Contracts, 2005
  - 18 signatories, 18 States parties
  - 20+ States have enacted domestically its provisions
- UNCITRAL Model Law on Electronic Transferable Records, 2017
  - Enacted in 10 jurisdictions
- UNCITRAL Model Law on the Use and Cross-border Recognition of Identity Management and Trust Services, 2022
- UNCITRAL Model Law on Automated Contracting, 2024
Enabling data flows is essential for digital trade
- This goal calls for adoption of an adequate legal environment
- Enabling legal texts should balance regulation

UNCITRAL texts have been adopted in more than 100 States
- Many of them are developing and least developed countries
- Often referenced in RTAs and DEAs
The UNCITRAL Model Law on the Use and Cross Border Recognition of Identity Management and Trust Services (MLIT)

- Adopted in July 2022
- Text available on UNCITRAL website in all official languages
- Builds on prior UNCITRAL texts and eIDAS regulation
- Provides rules for reliable online identification and assurance of data quality
The MLIT: scope and general principles

- Refers to use in commercial activities and trade-related services
  - May also be used in non-commercial contexts
- Use of identity management (IdM) and trust services is voluntary
  - Does not introduce new requirements to identify or to use a particular IdM or trust service
- Does not affect any other law
  - Including data privacy and data protection law
The MLIT: Identity Management (IdM)

- Objective: legal recognition of the result of electronic identification

- **Identity** is “a set of attributes that uniquely distinguishes a person in a particular context”
  - A person is a physical or legal person

- **Identity management** is made of identity proofing and electronic identification
The MLIT: Identity Management (IdM)

• **Identity proofing** is “the process of collecting, verifying, and validating sufficient attributes to define and confirm the identity of a person within a particular context”
  – in technical terms, “onboarding”

• **Electronic identification** is “a process used to achieve sufficient assurance in the binding between a person and an identity”
  – in technical terms, “authentication”
The MLIT: reliability in IdM methods

- The *method* used for electronic identification must be *reliable*

- Two-tier approach to determine reliability:
  - Ex ante (before use)
    - *Designation* of reliable IdM services
  - Ex post (after use):
    - *Determination* of reliability based on an open-ended list of relevant circumstances
The MLIT: obligations and liability of IdM service providers

• List of obligations of IdM service providers
  – covering the IdM lifecycle
  – in case of data breach
  – Applies to private and public IdM systems and schemes

• Liability of IdM service providers
  – Breach of obligations set in the model law gives rise to liability
  – All other sources of liability remain applicable
  – Limitation of liability may be possible
The MLIT: trust services

- A trust service is an electronic service that provides assurance of certain qualities of a data message
  - “who, what, when, where, and why of data”
  - List of trust services is open-ended
  - Named trust services are similar to eIDAS
- Provision on legal recognition (non-discrimination) of the result of the use of trust services
- Certain trust services (electronic signatures, electronic seals) have an identity component
The MLIT: trust services (continued)

- Each trust service (except website authentication) has a dedicated provision drafted as a functional equivalence rule referring to the paper-based function
- Same “two tier” approach as for IdM
  - Ex-ante designation + ex-post assessment
- List of obligations of trust service providers
- Liability of trust service providers
The MLIT: cross-border aspects

- Geographic-neutral rules on the assessment of reliability of the method used and on the designation of reliable services
  - Apply to both IdM and trust services

- Dedicated provisions on cross-border recognition and on international cooperation
  - Compatible with a centrally-managed mutual recognition mechanism
  - May be used as a template for bilateral and plurilateral agreements