Cross-border Legal Recognition and Technical Interoperability of Trust Services, Bangkok, 22 June 2023

Cross-border recognition of digital signatures – lessons learned from India

Tahseen Ahmad Khan

TABLE OF CONTENTS

- *Background: Why Mutual Recognition is important?*
- *Electronic Data and its inherent nature*
- *Scope of mutual recognition, need to go beyond trade related data*
- *Preliminary research and findings*
- *Experiences from India*
- *Conclusion*



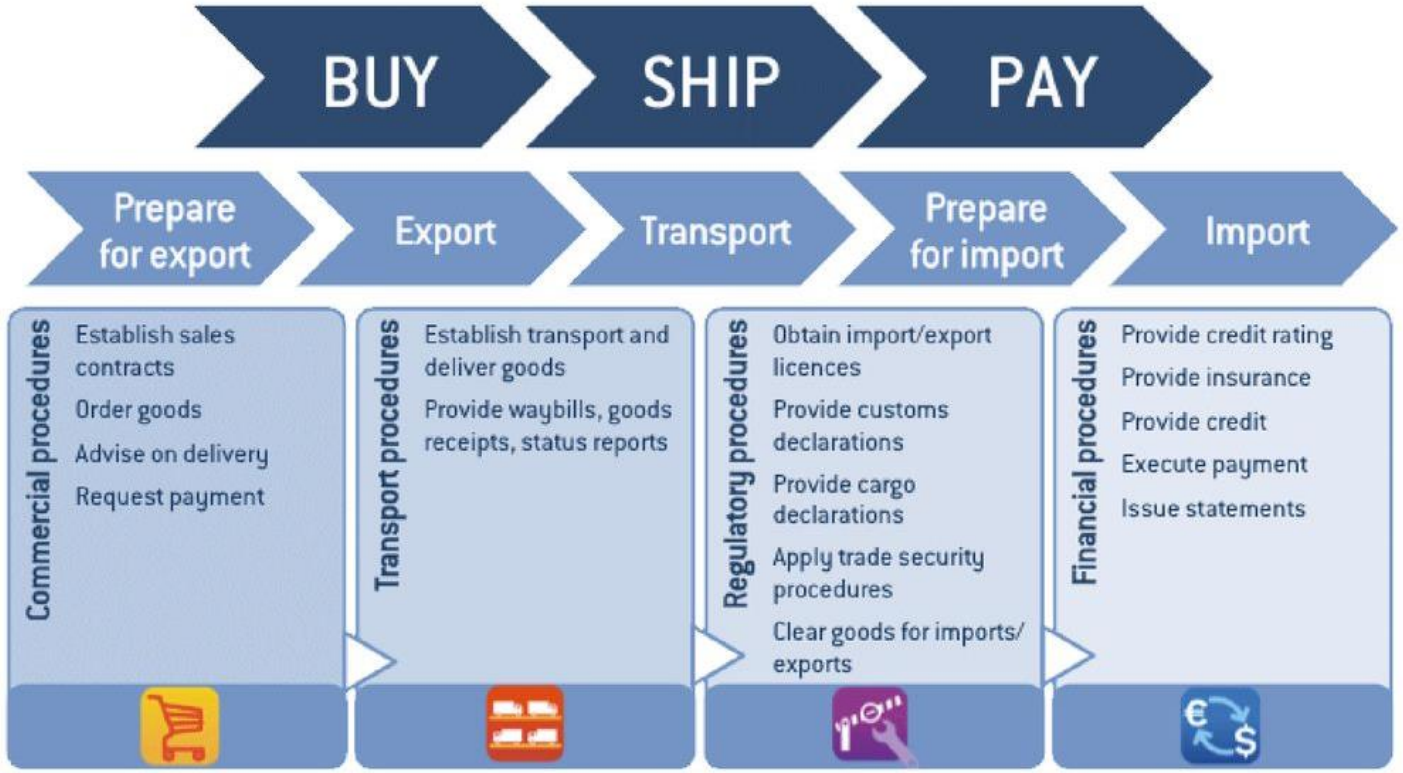
Background: Why Mutual Recognition is important?

- Electronic exchange of data across borders requires a **certain degree of trust**
- **Legislative frameworks exist within national jurisdictions** that recognize electronic data and their exchange
- In a cross border electronic data exchange
  - Establishing confidence and "**substantial equivalent level of reliability**" can be difficult because of differing local legislation
  - Electronic data **exchange, storage and retention standards may differ** and may have evolved based on local regulatons
  - Usage of technologies such as **cloud computing** results in **data residing in multiple jurisdictions**
  - **Emerging technologies** such as Blockchain, IoT are adding new dimensions resulting in increased types and source of data

To address these issues, a mutual recognition mechanism is required to create trusted trans-boundary electronic interaction and enable cross border exchange of electronic data

Electronic Data and its inherent nature

- **The Buy Ship Pay process developed by UN/CEFACT indicates that a number of documents and data are exchanged during a trade related process**



Electronic Data and its inherent nature

- As electronic systems have matured, over time, standards have also evolved which define how electronic data can be exchanged, for example: Electronic Data Interchange
- Reliable exchange and acceptance of electronic data needs to tackle a number **of issues**
  - **Data could be in structured or unstructured form**
  - **Interoperability and compatibility issues** arising out of different data standards, for example**: XML, PDF** etc and different technologies used
  - Ability to ascertain **integrity of data** where required
  - Need for **tackling** high volume and velocity of data as in the case of **big data** use cases such as IoT
  - Usage of legacy systems and need for migration of data
  - Differing language environments

Given this context, electronic data poses significant challenges in enabling digital trust in cross border exchange of trade related data and documents

Scope of Mutual Recognition

- The scope of mutual recognition mechanism should cover aspects and areas that allow establishment of “substantial equivalent level of reliability.
- This may have to **go beyond just trade related data** and take into account
  - Technical standards used in data exchange (for ex: ability to ascertain data integrity)
  - Entities owning, certifying and/or transmitting data,
  - **Establishment of level of confidence (identification, authentication methods) through a trusted environment**
  - Role that accreditation bodies could play in **monitoring the trusted environment**

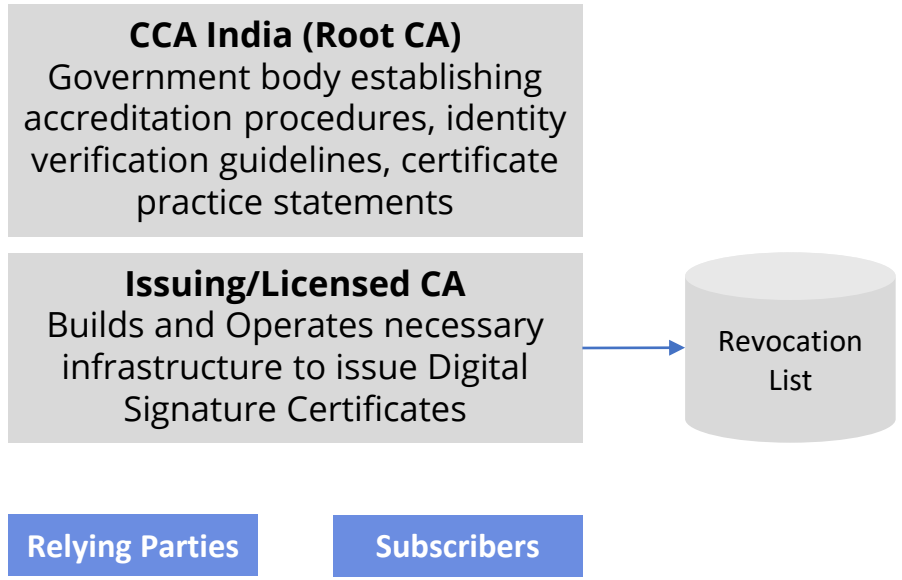
Preliminary Research and Findings

- **A number of bi-lateral and multi-lateral institutional and inter-governmental arrangements exist for cross-border mutual recognition**
- A closer analysis helps us make the following general observations
  - The concept of trusted trans-boundary legally significant electronic interactions is still fairly new
  - While most countries have put in place national legislation recognizing electronic documents or signatures, the scope is domestic or regional or limited to highly integrated union of states
  - Instruments are generic and not legally binding from the perspective of cross-border trade
  - **Awareness levels are generally low** across multiple sectors and their regulators making cross-sectoral adoption challenging
  - There is no concrete action at an implementation level to facilitate paperless cross-border electronic trade
  - **Initiatives at the level of Association of Southeast Asian Nations(ASEAN), Eurasian Economic Union(EEU), European Union (EU),UN/ESCAP and UN/CEFACT are worth mentioning**.

Experiences from India

- In India, the journey started 18 years back
- Key milestones achieved
  - 2000 – IT Act was passed based on UNCITRAL model law with following provisions introduced
    - Legal recognition to electronic records
    - Authentication of electronic records
    - Manner in which authentication can be satisfied (for ex: through the use of electronic signatures)
    - Procedures for licensing Certifying Authorities that can issue digital certificates
    - References with Indian Penal Code, Indian Evidence Act, 1872, Bankers Book Evidence Act, 1891, Reserve Bank of India Act, 1934
  - 2008 – Key amendments made including distinction between **electronic signature and digital signature**

PKI Hierarchy



Experiences from India

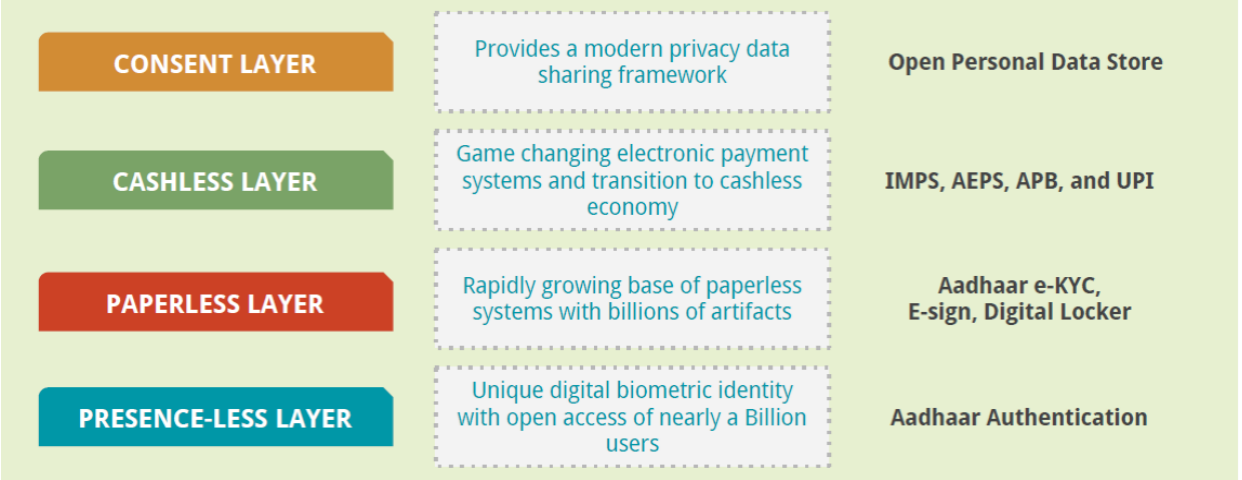
- Key milestones achieved (contd..)
  - 2012 – **Powers given to Controller of Certifying Authorities, Ministry of Information Technology to sign mutual recognition agreements with other countries**
  - 2013 – **First such mutual recognition agreement signed with South Korea**
  - 2014 – Central Bank (Reserve Bank of India) and published a comprehensive report outlining need for enhancing cyber security measures in Banking
    - **Electronic signature** was recommended to be **provided as an option** to customers for securely logging into internet banking or for fund transfers
    - Other cyber security measures include use of **Two Factor Authentication**
  - 2014 – **Tax Administration** and others adopted similar approach

Experiences from India

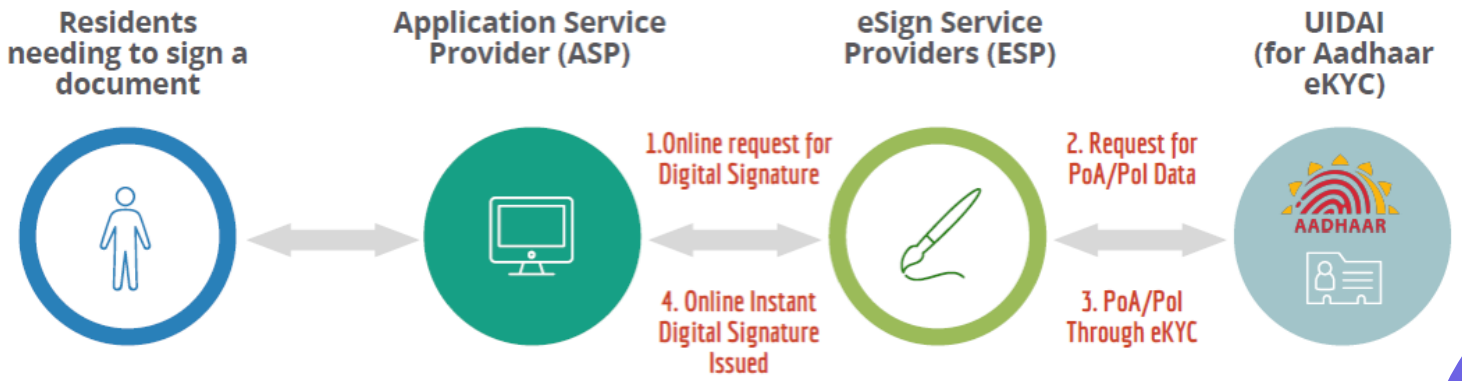
- Key milestones achieved (contd..)
  - 2015 **– Launch of AADHAAR enabled electronic Signatures**
    - AADHAAR is India's Digital ID now rolled out to **1.3bn residents**
    - Electronic signatures use OTP/Biometric authentication and leverage KYC data available with Govt of India to create **dynamic one time signatures that are legally valid**
    - Helped bring cost of adoption to **USD 10 cents** per transaction and create large scale adoption
    - Use cases include Account Opening in Banks, Insurance, Capital Markets, availing eGovernance services, employee onboarding etc

Experiences from India

- Creation of India Stack – a technology stack based on Open API's and Layered Innovation to enable electronic KYC, Signatures and Payments based on user consent



- **AADHAAR eSign – Digital Id based electronic signatures**



Experiences from India

- Key milestones achieved (contd..)
  - **2019 – Huge success of Digital India program**
    - **Over 3bn electronic KYC's**
    - **Over 40mn electronic signatures**
    - **Over 600mn electronic payments**

Conclusion

- The following will need to be considered in enabling mutual recognition
  - **Creation of a strategy which can help arrive at a legal, technical and operational umbrella framework. This need to be progressively created at national, sub-regional, regional and global levels.**
  - **Domain and country specific legislation, conforming to international standards, supporting cross border paperless trade.**
  - **Use of interoperable open standards in technology frameworks for Identity, Authentication etc**
  - **Capacity building for implementation**

Thank You

Tahseen Ahmad Khan
takhan@meity.gov.in