Security and legal aspects of Cross-border paperless trade

Trust in the Electronic Environment

WCO-UNESCAP
5th UNNExT Masterclass: Facilitating Cross-border Paperless Trade using emerging technologies

Tahseen Ahmad Khan
takhan@meity.gov.in

Outline

- FA & other international initiatives
- National initiatives (Indian)
- UN/CEFACT initiatives

Securing electronic transactions

- AUTHENTICATION : Reliable identification of sender/recipient of data
- CONFIDENTIALITY : Protection of data from undesired disclosure.
- INTEGRITY : Prevention of undesired creation, modification or deletion of data
- NON-REPUDIATION: Committed transactions cannot be denied

I. FA & other international initiatives

A. Electronic transactions and signatures law

1. Electronic transactions legal issues, including:

1 (a) Legal recognition of electronic communications

- What are the conditions for the recognition of the legal validity of electronic communications?
- Do laws establish requirements for functional equivalence between paper-based documents and electronic communications? Do they recognize electronic communications as directly meeting requirements for documents, writing, signature, etc.?

1 (b) Legal issues related to identity management and trust services, including electronic signatures

- Are there laws that inhibit technological neutrality by mandating or favouring the use of specific technologies or business solutions for e-communications to be given legal effect?
- Do laws address how identification, authorization and authentication are carried out in an electronic environment?

A. Electronic transactions and signatures law

- For all the questions above, are those laws applicable to all electronic communications or transactions or only to some business sectors or categories of documents or users?
- In particular, are there special rules for specific types of electronic documents such as bills of lading, manifests, certificates of origin, invoices, phytosanitary certificates, etc.?

2. Regulatory/legal requirements for data retention and electronic archiving

- Are there laws requiring preservation of stored information?
- Do they prescribe a minimum data retention period or a maximum retention period?
- Do they clearly apply to electronically stored data? If so, are there rules to ensure its integrity while stored and its accessibility to anyone with sufficient cause to inspect it?

3. The admissibility of electronic evidence, for example in judicial and enforcement proceedings

- Is electronic evidence admissible in judicial and administrative/regulatory proceedings?
- If so, are there special rules for collecting or producing electronic evidence or for ordering the disclosure of electronic evidence?

A. Electronic transactions and signatures law

- Is a distinction made between evidence for criminal proceedings and for civil proceedings?
- Is electronic evidence generated, stored or collected abroad admissible in judicial and administrative/regulatory proceedings? Are the rules about such “foreign” evidence different from those applicable to other kinds of “foreign” evidence?

B. Laws regarding paperless trade and single window systems

1. Laws relating to the establishment of a single window system/paperless trade system
• What legal instruments are used or need to be enacted to authorize or to establish the single window system and a paperless trading environment?
• Is there a national or coordinating agency to promote the domestic paperless trading environment (e.g., a single window system committee)? If so, does it have government and private representatives on it?
• Is there a dedicated budget to establish the single window system (or paperless trading platform)?
2. Legal aspects relating to information security
2 (a) Laws and regulations on information security and data confidentiality
• Do the national laws mandate information security standards?
• Do the national laws protect the confidentiality of electronic transactions/information?

B. Laws regarding paperless trade and single window systems

- Are there laws about cybercrimes, i.e., crimes using a computer (or other information and communication technologies) or targeting a computer or a network, such as unauthorized access to computers, introducing malware, interfering with proper operations, etc.?

2 (b) Laws and regulations relating to data accuracy and integrity when such data are shared for cross-border paperless trade systems

- Are there national laws/regulations establishing requirements for the accuracy and integrity of data submitted and processed for paperless trade? Are these laws of general application or specifically directed at paperless trade?
- Do these laws impose obligations on persons submitting such information and require processes to ensure correct attribution? Do they apply equally to paper and electronic communications? Are they consistent with the authentication and identity management rules mentioned earlier?

2 (c) Laws and regulations for accessing and sharing information and data between and among government agencies

- Are there agreements or policies for the sharing of data between government agencies within the country? Are there limits on such sharing based on personal privacy or commercial confidentiality?

B. Laws regarding paperless trade and single window systems

3. Service-level agreements and memorandums of understanding on paperless trade operations, e.g., operation of single window systems (service level agreements may be applicable for matters such as availability, reaction time, processing time, etc.)
• Are there service-level agreements or memorandums of understanding governing paperless trade operations? Who are the parties and what is their legal authority for making these agreements or memorandums of understanding?
• If yes, what level of service is expected from paperless trade service providers?
• What level of service is expected from single window system operators?

C. Cross-border aspects

1. Existing bilateral or regional agreements for cross-border paperless trade data exchange, including e-commerce and paperless trade facilitation provisions in regional trade agreements

- Is the country party to an international agreement, such as a regional trade agreement or a bilateral trade facilitation agreement, that requires or favours the legal recognition of electronic messages exchanged across the border?
- Is the country party to an international agreement providing legal recognition of electronic messages exchanged across the border?
- Are there arrangements that provide for mutual recognition of electronic messages and transmitted information? If yes, is mutual recognition granted on a bilateral or multilateral basis?
- Does the country recognize foreign electronic signatures and certificates? If so, on what basis?
- Are national laws relevant to paperless trade facilitation based on international models (e.g., United Nations Commission on International Trade Law (UNCITRAL), Council of Europe, Organization for Economic Cooperation and Development, etc.)?

C. Cross-border aspects

2. International standards/guidelines

- Do participants in cross-border trade use or rely on standards/regulations/guidelines for the exchange of electronic messages? United Nations Centre for Trade Facilitation and Electronic Business recommendations14,33, 35,36,37 and 38 on legal issues raised by cross-border interoperability are examples of such guidelines.
- Have international legal standards/regulations/guidelines been incorporated into a country's legal framework for its cross-border paperless trade? If so, how? Does the incorporation of such rules at the domestic level also affect cross-border activity?

3. Existing bilateral or multilateral technical/operational agreements

- Are there technical or operational agreements which provide for the unilateral or mutual recognition of electronic messages? Examples are the sanitary and phytosanitary exchange agreement between China and the Netherlands as well as the Association of Southeast Asian Nations' electronic Association of Southeast Asian Nations Trade in Goods Agreement programme.

C. Cross-border aspects

4. Other international legal instruments, regulations and standards relevant to enabling the use of data for cross-border paperless trade

- Which other laws may be relevant to cross-border paperless trade facilitation? For example, bilateral or multilateral agreements on cybercrime and the taking of electronic evidence abroad.

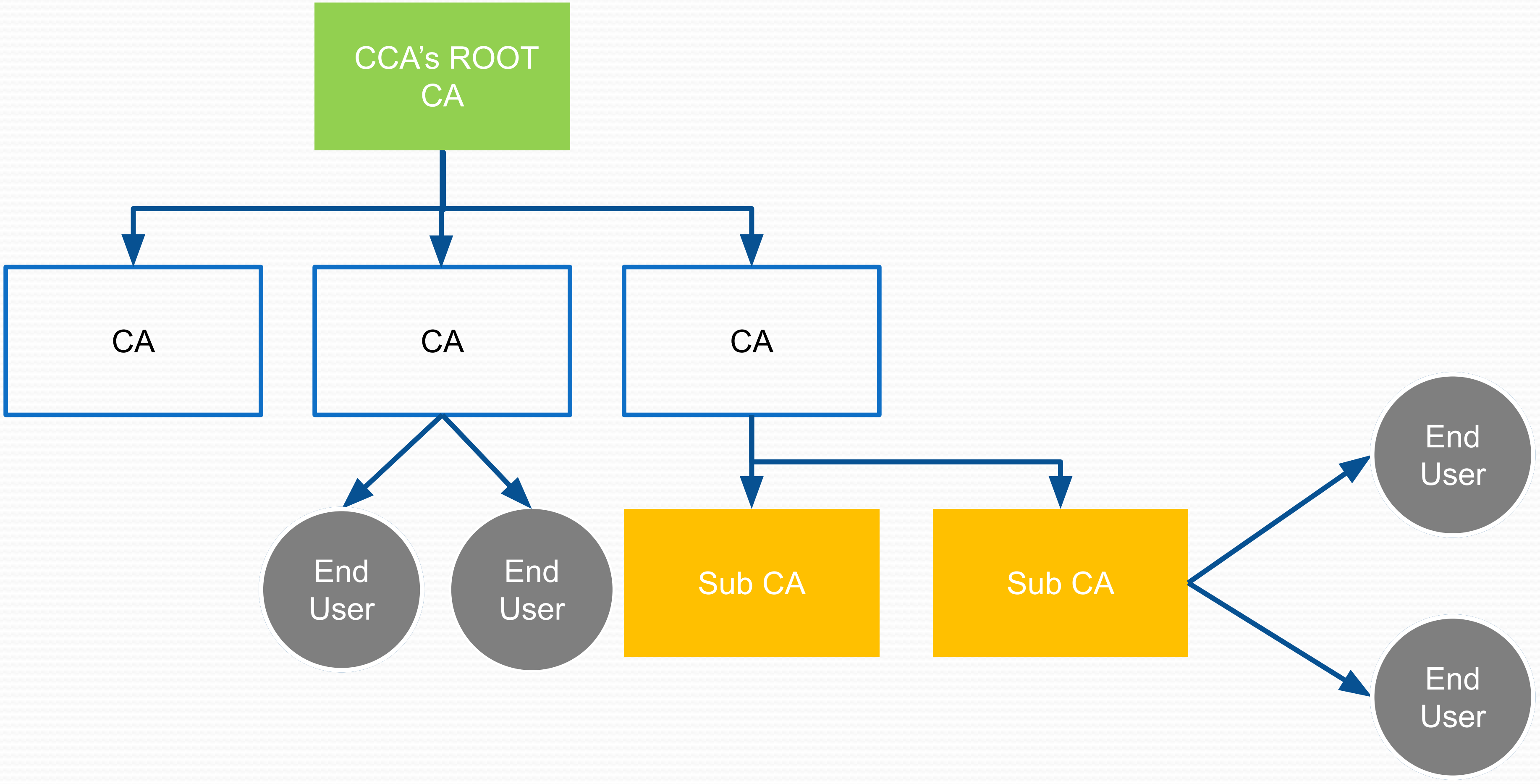
II. National initiatives (Indian)

- Journey of eTRADE project
- Cyber security, Electronic/Digital Signature Initiative
- Digital ID Initiative
- eSIGN Initiative
- Verifiable Credential & Digital Locker Initiative

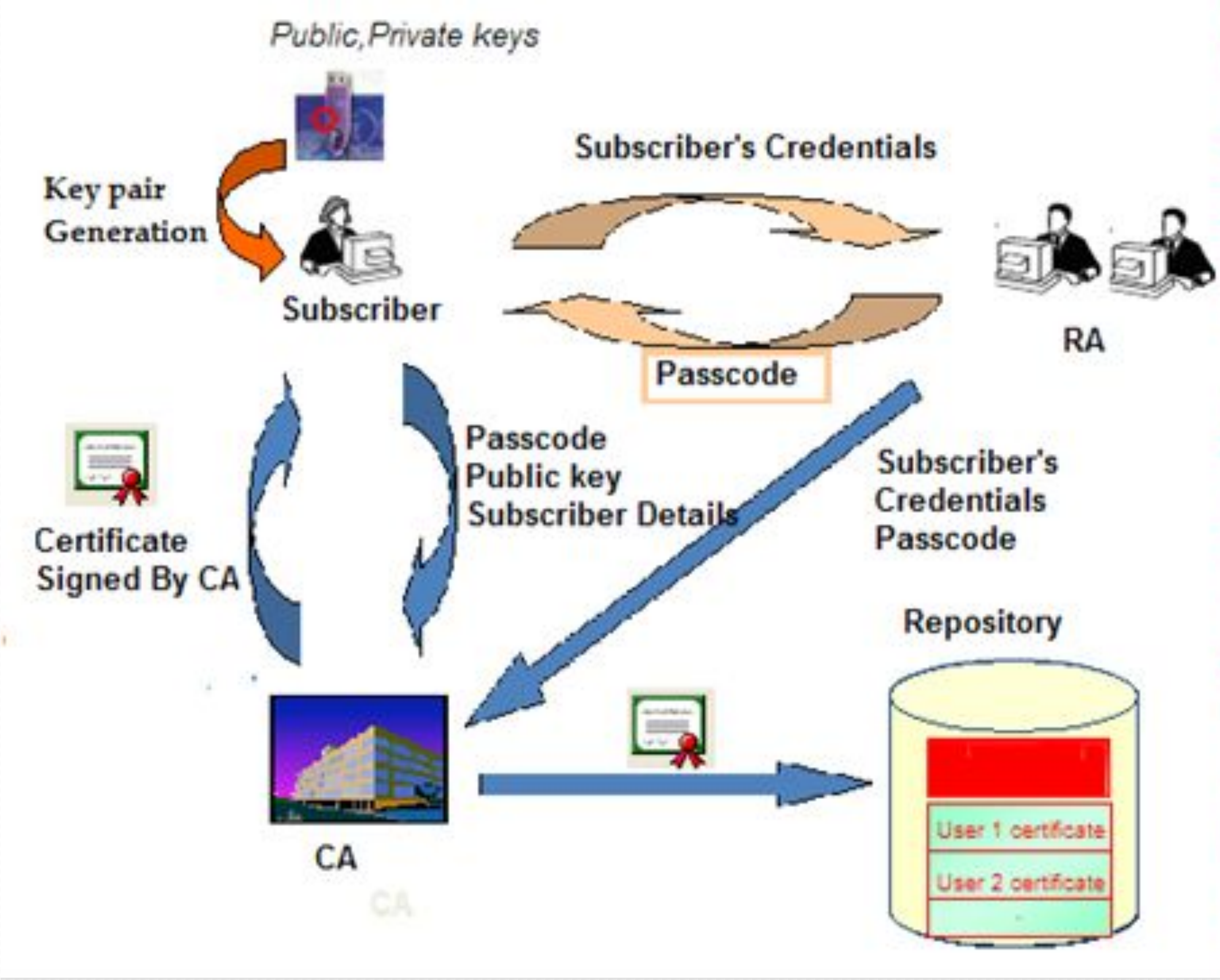
eTRADE

- Manifest filing
- Risk Assessment
- Trace & Track
- Paper elimination (Challenge)
- Duty Drawback (Challenge)
- Community Partner Interface (Challenge)
- IT Act

Trust Hierarchy



Issuance of DSC



1. Subscriber Provides Proof of identity

2. RA Verifies the Credential based on the assurance Level

3. RA send passcode to subscriber

4. subscriber create public private key pair

5. subscriber submits public key along with own details to CA

6. CA certifies the public key of subscriber

7. CA publish the certificate in their repository

8. CA provide certificate to subscriber

Credential Verification

- Verification of the Proof of Identity (PoI) and Proof of Address (PoA) is a pre-requisite for issuance of Digital Signature Certificates by Certifying Authorities.

- As part of the e-KYC process of Aadhaar, the resident authorizes UIDAI (through Aadhaar authentication using either biometric or OTP to provide their demographic data along with their photograph (electronically signed and encrypted) to service providers.

Addressing scalability through eSign

- An Aadhaar holder can sign any document with just Aadhaar biometric/OTP authentication requiring no physical device or paper-based application forms and supporting documents

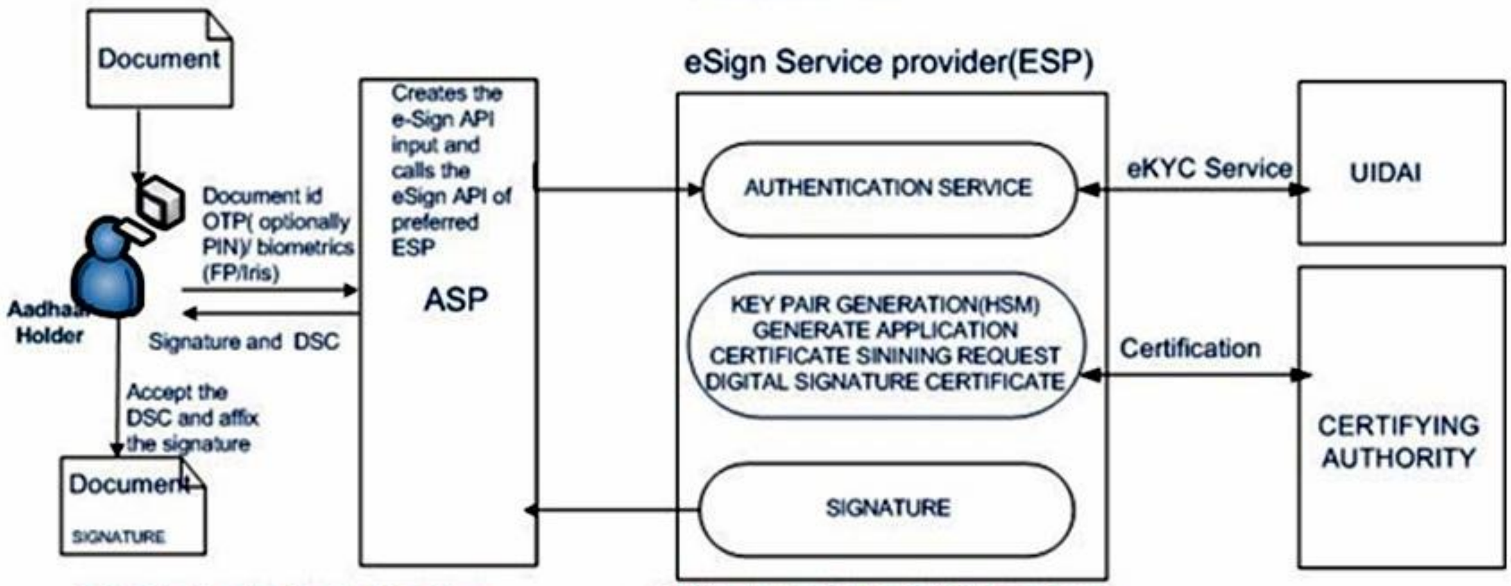
- Authentication of the signer is carried out using eKYC of Aadhaar,

- the signature on the document is carried out on a backend server of the e-Sign provider.

- The service can be run by a trusted third party service provider - To begin with the trusted third party service shall be offered only by Certifying Authorities.

eSign overview

eSign Overview

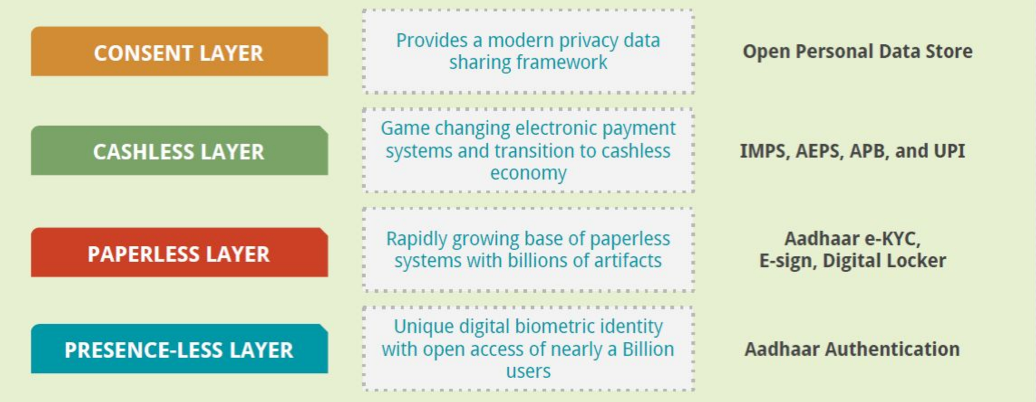


ASP- Application Service Provider
ESP- eSign Service Provider
HSM -Hardware Security Module
OTP-One Time Password

eKYC- electronic Know Your Customer
UIDAI-Unique Identification Authority of India
FP-Finger Print
DSC-Digital Signature Certificate

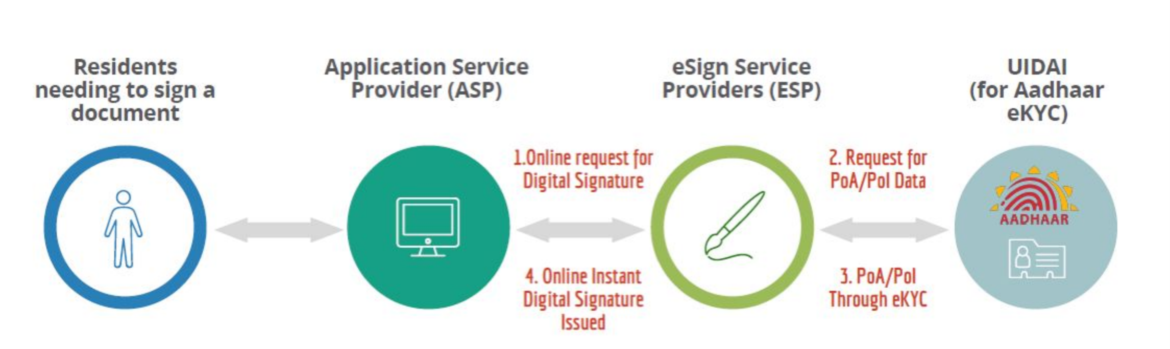
Experiences from India

- 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



CONSENT LAYER	Provides a modern privacy data sharing framework	Open Personal Data Store
CASHLESS LAYER	Game changing electronic payment systems and transition to cashless economy	IMPS, AEPS, APB, and UPI
PAPERLESS LAYER	Rapidly growing base of paperless systems with billions of artifacts	Aadhaar e-KYC, E-sign, Digital Locker
PRESENCE-LESS LAYER	Unique digital biometric identity with open access of nearly a Billion users	Aadhaar Authentication

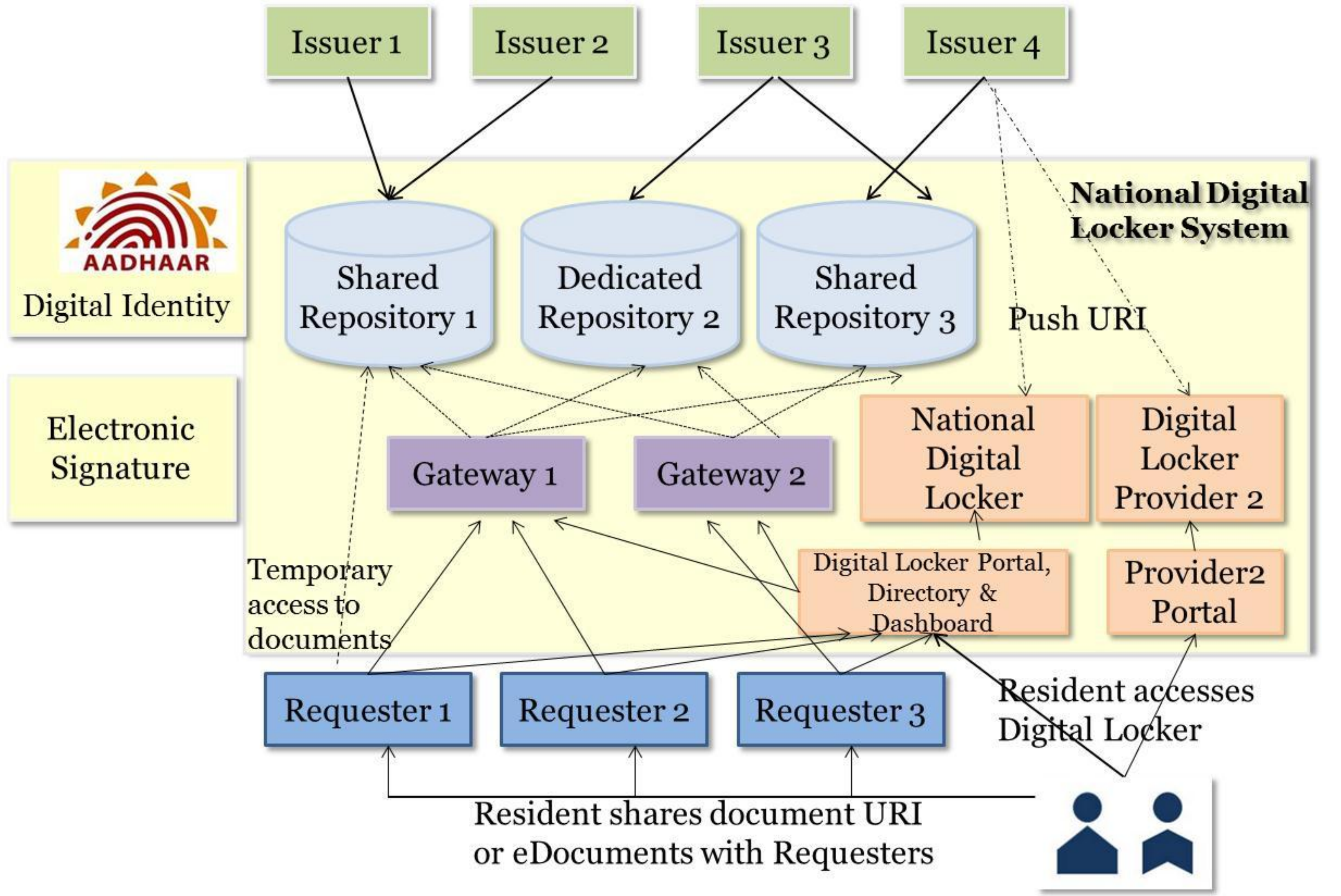
- AADHAAR eSign – Digital Id based electronic signatures


Residents needing to sign a document
Application Service Provider (ASP)
eSign Service Providers (ESP)
UIDAI (for Aadhaar eKYC)
1.Online request for Digital Signature
4. Online Instant Digital Signature Issued
2. Request for PoA/PoI Data
3. PoA/PoI Through eKYC
AADHAAR

Verifiable Credentials - Digital Locker

- Enable **digital empowerment** of residents by providing them with Digital Locker on the cloud
- Enable e-Signing of **documents** and make them available electronically and **online**
- Minimize the **use of physical documents**
- Ensure **Authenticity** of the e-documents and thereby eliminating usage of fake documents
- **Secure access** to Govt. issued documents through a web portal and mobile application for residents
- **Reduce administrative overhead** of Govt. departments and agencies and make it easy for the residents to receive services
- **Anytime, anywhere access** to the documents by the resident
- **Open and interoperable standards** based architecture
- Architecture to support a **well-structured standard document format** to support easy sharing of documents across departments and agencies
- Ensure **privacy and authorized access** to residents' data.

DLTS Architecture



III. UN/CEFACT initiatives

(https://unece.org/trade/uncefact)

- Blockchain for Trade Facilitation
- IoT for Trade Facilitation
- Digital ID for Trade Facilitation
- Cross-border inter-ledger exchange for Pref. CoO
- AI for Trade Facilitation
- Verifiable Credentials for Cross-border Trade Facilitation etc.

Transfer of MLETR-compliant titles

- UNCITRAL Model Law on Electronic Transferable Records
  - Using the Negotiable Maritime Bill of Lading as an example
- Exploring aspects of the MLETR and how this can be addressed through blockchain
  - Uniqueness / Singularity, Exclusive Control, Integrity, signature, endorsement, change of medium
- Ways in which blockchain allows to address these
  - Tokens / token owner, verifiability, confidentiality, data protection
- Importance of UN/CEFACT standards and semantics

Cross border inter-ledger exchange for Pref CoO

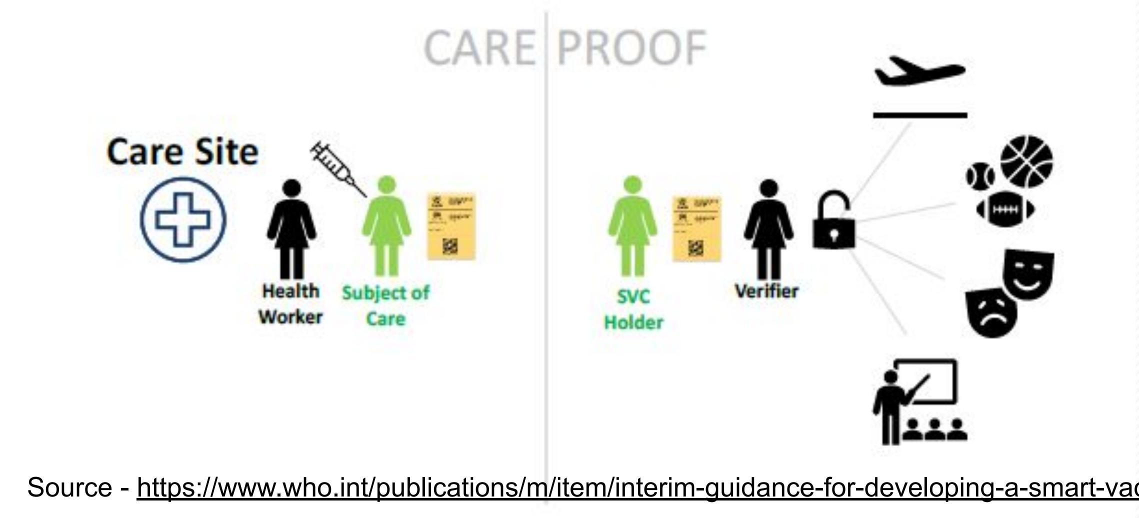
- Using blockchain technology to build a platform that facilitates the exchange of digital preferential certificates of orgin
  - Intergovernmental Ledger (IGL)
  - Genuinely scalable and decentralised model
- Issuing high integrity digital trade documents
  - Authenticated, provenance traced, digitally processed
  - Issued by one government authority and verifiable by any stakeholder
- Use of quick reference codes (QR-codes)
  - Enabling immediate verification for authenticity and integrity
- Preferential certificates of origin are the first trial – should be able to be scaled out to other trade documents
- Pilot being performed between Australia, Singapore and China

Digital ID for Trade

- This project has been discussed over the last few forums where a gap and need for standardization has been identified for digital business identity management in both **B2B and B2G use cases** for facilitating cross border trade
- Discussions so far have focussed on facilitation of interoperability/standardization with emerging developments in this area (ex: Blockchain, Verifiable Credentials, Decentralized Identifiers etc) to support solving key challenges
  - Ability to develop trustworthiness between participants in the supply chain
  - During paper-paperless transition, how does one reliably verify what’s claimed on paper using a digital twin
  - Managing compliance in a complex world – KYC guidelines, GDPR etc?
  - How does one extend Identity systems with IoT, Blockchain

Digital ID and Verifiable Credentials – Example - Smart Vaccination Certificates

- How does this work?



Source - https://www.who.int/publications/m/item/interim-guidance-for-developing-a-smart-vaccination-certificate

- Summary
  - Certificates are digitally issued as verifiable credentials using digital cryptographic identifiers by which any Member State can trust that medical documents issued by another Member State are authentic and have not been tampered with
  - WHO defines standards for issuance and reliance of such certificates
  - Focus on Equity, Accessibility, Privacy and Scalability and sustainability
- More information can be found at https://www.who.int/groups/smart-vaccination-certificate-working-group

Thanking you

takhan@meity.gov.in