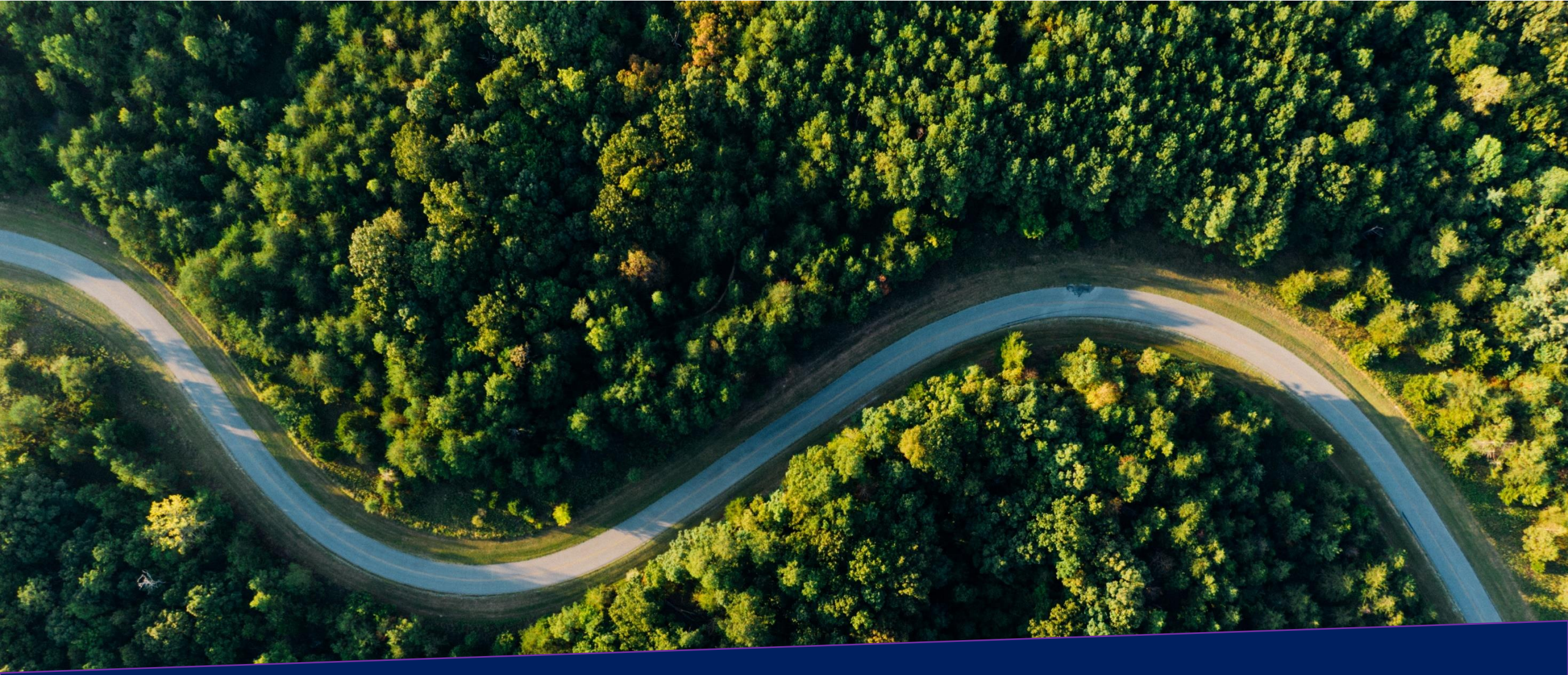
Need and Role of Trust Service Providers in Paperless Transformation

Vijayakumar Manjunatha, Asia PKI Consortium

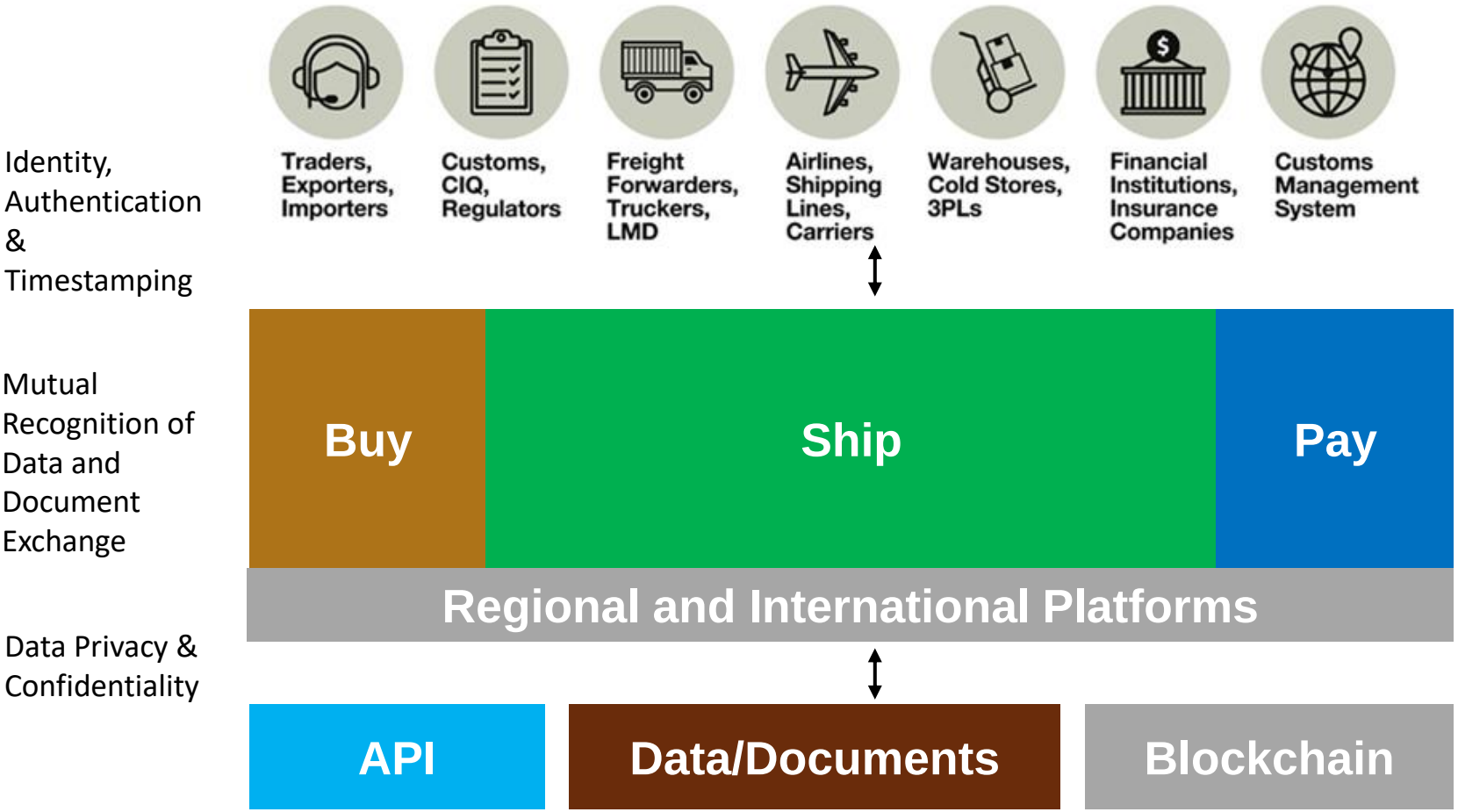
Content

1. **Transition from paper to paperless trade**
2. **Bilateral/Regional Initiatives**
3. **Statistics and Adoption in Asia Pacific**
4. **India Success Story**
5. **Role of Trust Service Providers**
6. **Future of trust services**
7. **Summary**



Faciliating paperless trade

Transition to paperless cross border trade



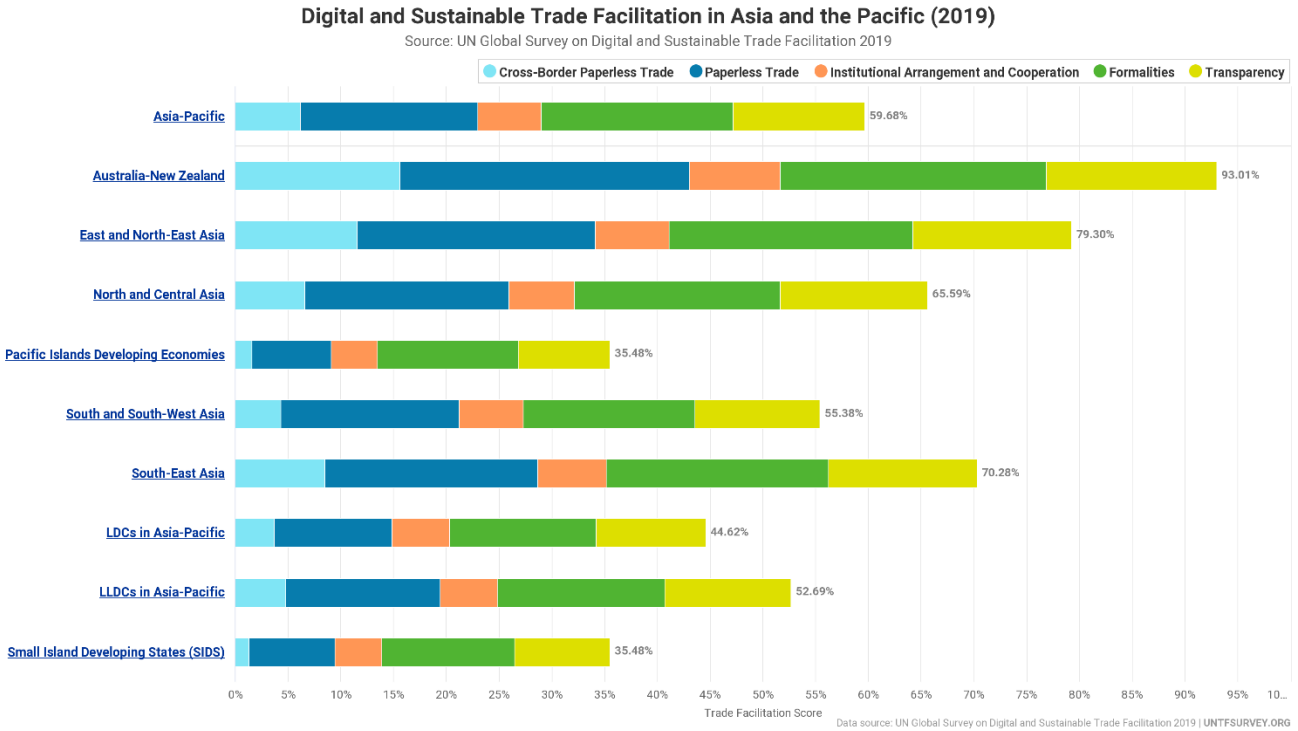
- Cross border trade results in exchange of a number of documents many of which are sensitive and require the need to establish trustworthiness
- Going from paper to paperless requires
  - Identification/KYC of participants in a reliable/seamless manner
  - Establishing authenticity of documents
  - Legal/technical framework supporting this transition
- All of this requires a framework without which
  - Cost of trade will be higher
  - GDP growth will be lower
  - Environmental impact can be significant

Bilateral/Regional Initiatives

- Some examples of bi-lateral/regional initiatives to facilitate mutual recognition
  - EU eIDAS - The European Union Electronic Identification, Authentication and Trust Services
  - EEU (The Eurasian Economic Union) initiative on electronic interaction
  - PAA – Pan Asian eCommerce Alliance
- In all of the above initiatives, digital identity and digital signatures play a vital role in ensuring trust worthiness between parties and documents exchanged across borders
- Some of these initiatives also focus on building capability to interact in a secure and paperless manner as part of single window, trade facilitation platforms
- The key would be to see how to internationalize and enable interoperability so that multiple countries can facilitate seamless and paperless global trade

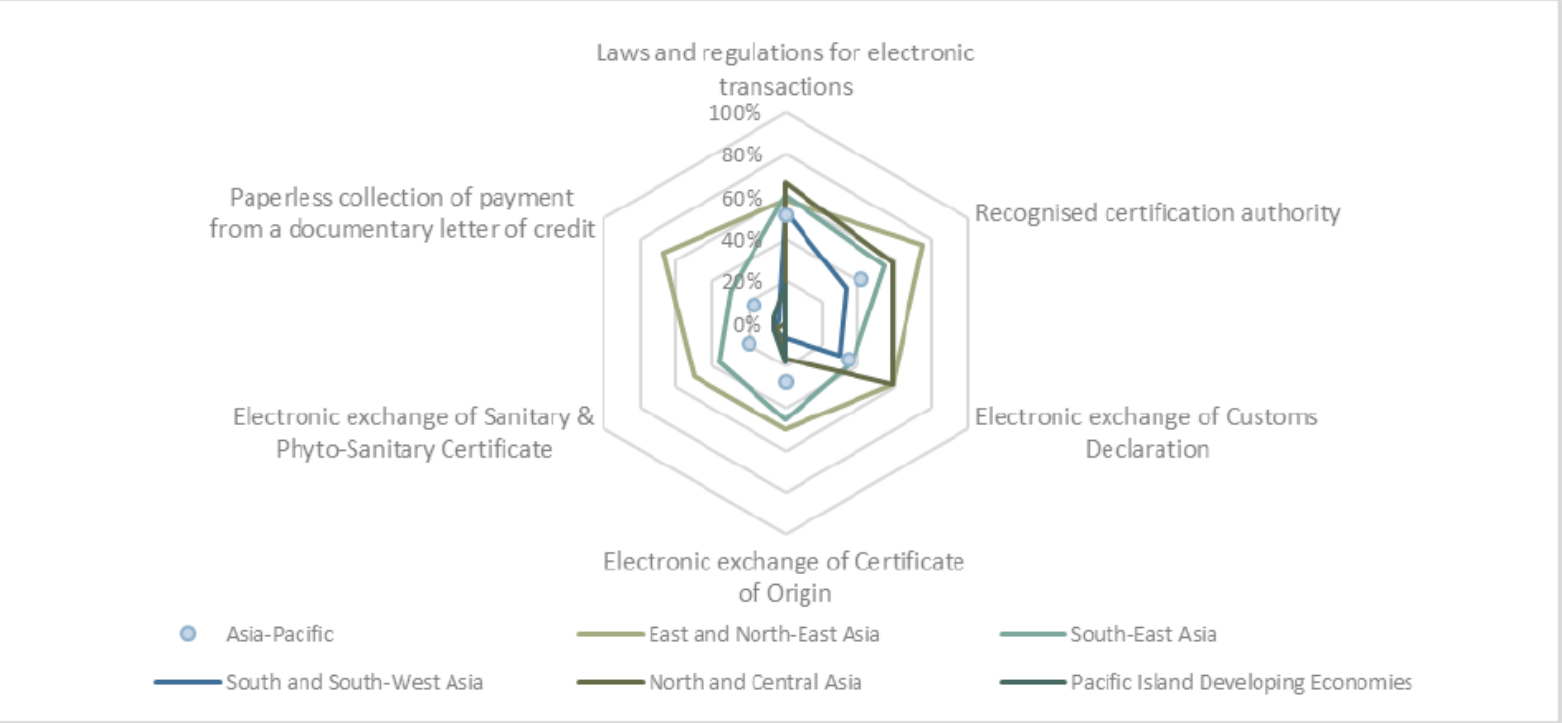
Some statistics

- Cross border paperless trade in implementation in Asia Pacific is 32%
- As defined in United Nations TF survey for Asia Pacific, among the six cross-border paperless trade measures, only laws and regulation for electronic transaction has seen a implementation level of more than 50%
- Implementation for other measures that are related to technology and electronic exchange of data such as Customs Declaration, CoO etc has been very slow
- The survey also highlights that the legal frameworks also may not be ready to support the legal recognition of electronic data or documents from other countries



Source: UN Global Survey on digital and sustainable trade facilitation 2019

Adoption in Asia Pacific



Source: UN Global Survey on Digital and Sustainable Trade Facilitation, untfsurvey.org, 2019

Trust Service Providers play an important role in bridging the trust deficit in cross border trade

Gaps and Roadmap

- The gaps generally noticed in the implementation of paperless trade systems include
  - Enabling the creation of legislative provisions for domestic or cross border electronic data exchange with acceptance of electronic data with regulatory agencies
  - Implementation of regulation, policy, operational processes and eSignature technology to facilitate paperless trade processes
  - Capacity gaps in the execution of such massive programmes, such as a lack of personnel with appropriate backgrounds or skills

In India, Controller of Certifying Authorities and the Government has built a robust digital signature infrastructure supported by active technology ecosystem to facilitate all of the above

India: The userbase

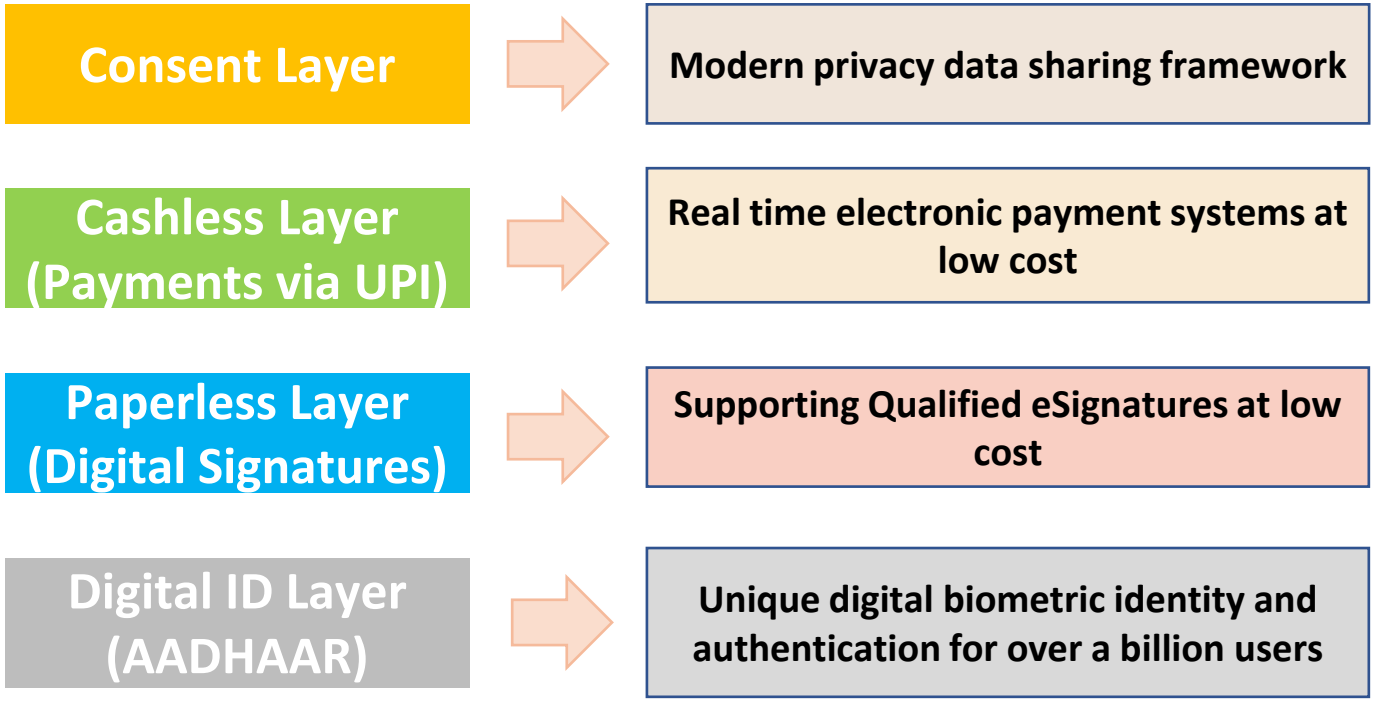
1. 10 Million+ Long Lived Certificate Users
2. 330 Million+ Short Lived Certificate users and growing.
3. Large scale paper to paperless revolution
4. Adopted across the Industry for e-Governance, Banking, Finance, Corporate / Enterprises, etc

Major Use cases

Use Case	Digital Signature	Adoption
GST Return Signing	JSON data signing	3-4mn / Mandatory
Income Tax Return Signing	Document Hash / Text data signatures	2mn+
MCA Return Signing	PDF Signature	2mn+ / Mandatory
Tax Letters (IT/GST) / Aadhaar	PDF Signature	Less Signers, More Docs
Tendering Portals	Document Hash / Text data signatures	Mandatory
UIDAI (AUA/KUA/etc)	XML Signatures (xml-dsig)	High Volume
Banking Transactions	XML / Text data signatures	More Transactions
G2B / G2C	PDF Signatures	Increasing
B2B / B2C	PDF Signatures	Increasing
Emails	SMIME CMS Signatures	Low adoption

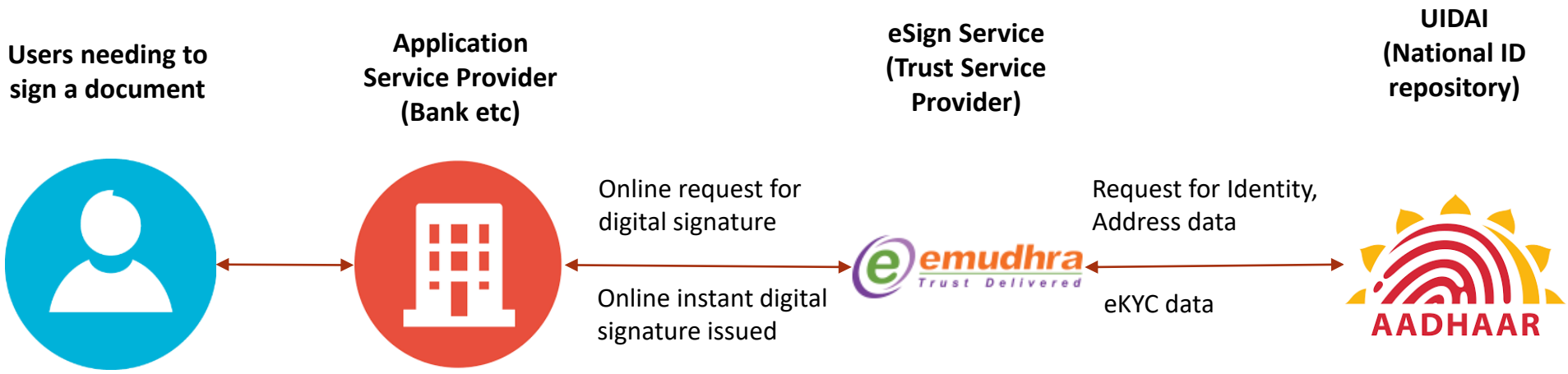
Digital Trust Landscape in India

"Digital India" vision has given huge impetus to creation of a paperless, presenceless and cashless society



Trust Service Providers play an important role in all layers of the above stack by providing digital signature certificates that are used for securing critical infrastructure and for signing data/documents

Facilitating signing at scale



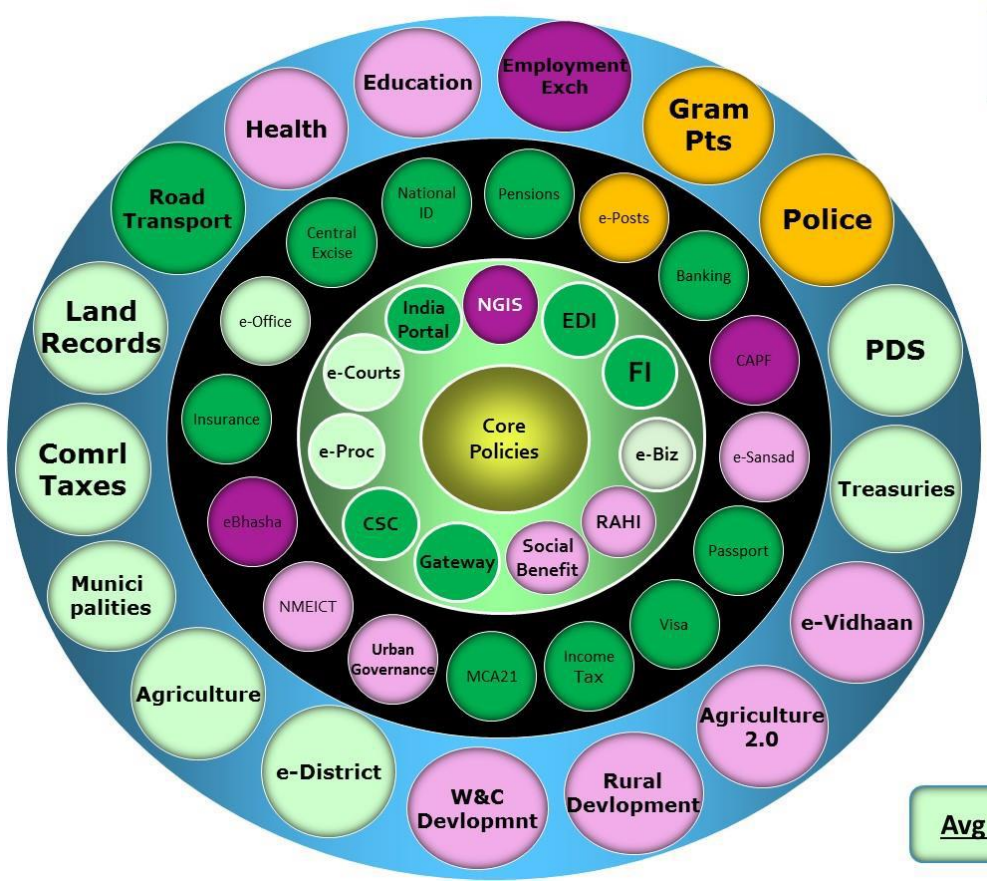
- In 2015, India introduced eSign based on AADHAAR
- eSign is similar to remote signing in eIDAS, uses short lived certificates for signing requests
- eSign can also be based on existing KYC‘s done by regulated entities specifically Banks
- eSign equivalent to Qualified Electronic Signatures based on reliable identity data
- eSign Service Providers licensed, regulated and audited by Ministry of IT (based on comprehensive audit criteria)

Implications

- Pricing per transaction
- This resulted in a changed business model where intermediaries such as Banks, Insurance companies pick up the cost of signing on behalf of the customer and save huge costs themselves

Mission Mode Projects & Digital Signatures

- As part of Mission Mode projects of Digital India program, the government is aiming to **drive better transparency and quicker approvals using digital signatures**
- There are 44 projects where both G2C and over time C2G interactions will be made paperless using digital signatures over time
- The key projects include Financial Inclusion (public distribution, agriculture etc), Company Administration, Taxes, Land Records, Police, Public Distribution, Judiciary, Posts, Procurement, Education, Health etc



Digital Identity (AADHAAR) and Digital Signatures are the backbone for Mission Mode projects

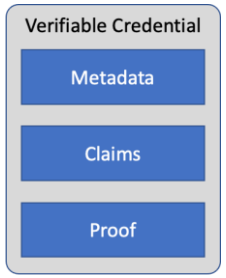
Role of Trust Service Providers

Role of Trust Service Providers

- To facilitate cross border paperless trade, trust providers can play the ideal bridge to facilitate mutual recognition as they
  - Are licensed/accredited by a Govt body under respective country Electronic Transactions Act or Information Technology Act giving users and relying parties assurance
  - Provide reliable verification and exchange of user information
  - Operate infrastructure to issue digital signature certificates which are legally recognized and non-repudiable
  - Provide services such as Remote Signing for seamless user experience and Timestamping for time authenticity
- Interesting examples of international mutual recognition include ePassports which work on a principle of cross recognition based on common trust list maintained by ICAO

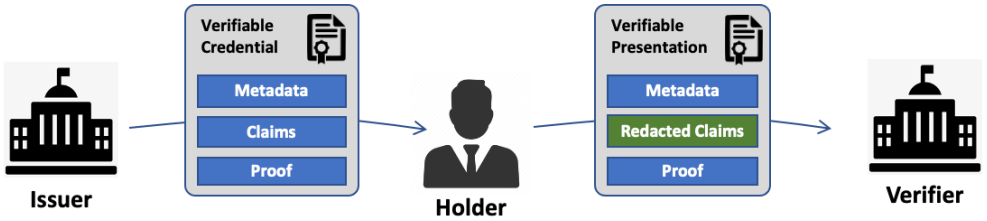
Future of Trust Services – Verifiable Claims

- The world is moving towards Derived Credentials and Verifiable Claims both of which are built on the foundation of cryptographic trust
- This presents an interesting opportunity for trust service providers as they
  - Verify user identity and potentially associated details (education, employment)
  - Provide keys that provide cryptographic legal binding
- The same model can be extended to issue other types of user claims around Education, Employment, Ownership of Assets, Bank Accounts or even complex claims relating User Identity and Asset Ownership etc
- The underlying model can leverage both centralized or decentralized stores depending on who intends to own/control data and manage interactions
- Key properties of verifiable claims
  - Could be centralized or decentralized
  - Supports online and offline (through the use of QR Codes)
  - Privacy Preserving
  - Cryptographically secure and legally binding



A VC has the following parts

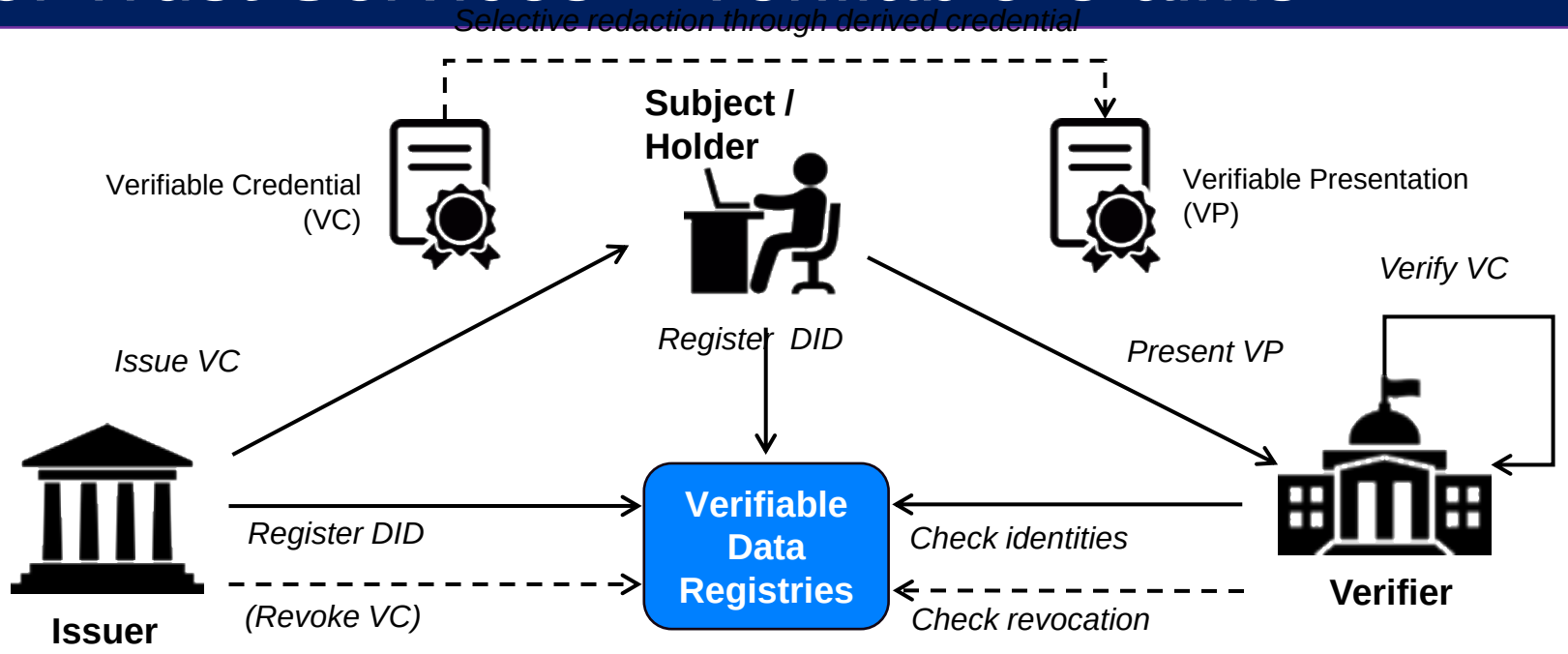
- Metadata (type of credential such as ID, Degree certificate who the issue is)
- Claims (data elements such as Name, DoB, Gender or something more detailed as Joe has a Master's Degree)
- Proof (cryptographic assertion)



A VC can be issued to the holder or the verifier based on holder consent

Key is to ensure data sharing ensures privacy and claims are shown only on a need to know basis

Future of Trust Services – Verifiable Claims



Can be implemented using any of centralized or decentralized registries

- Verifiable Claims are forming the bedrock of future web transactions particularly in the context of shift towards Decentralized networks
- Short-term key pairs offer an ideal scenario for privacy preserving cryptography where claims are specific to the assertion required (“Am I old enough to drive” -> “Yes”) as against sharing the full certificate. This will move the business model to transaction based pricing
- Trust Service Providers (given their trust anchorship to the Govt Root) can act as an ideal provider of VC’s for compliance and binding and interoperability with the Electronic Transactions Act
- An interesting example of a platform that enables this in India is the “Digi Locker” platform

Summary

Summary

- In Summary, trust services will continue to play a crucial role in facilitating cross border trade but the following issues need to be tackled
  - Defining the right model – Cross certification or cross recognition or bridge CA approaches
  - Establishing KYC baseline – mapping equivalence between identity vetting and levels of assurance
  - Technical interoperability – certificate profiles, trust list
  - Legal recognition and dispute resolution mechanism etc

Thank you

Vijayakumar Manjunatha

Chair of Technology & Standards Working Group, Asia PKI Consortium

SVP & CTO, eMudhra

vijay@emudhra.com | +91 9739342828