Cyber Security & Public Key Infrastructure

Junu Rani Das Kailay

Controller of Certifying Authorities
Government of India

December 2019

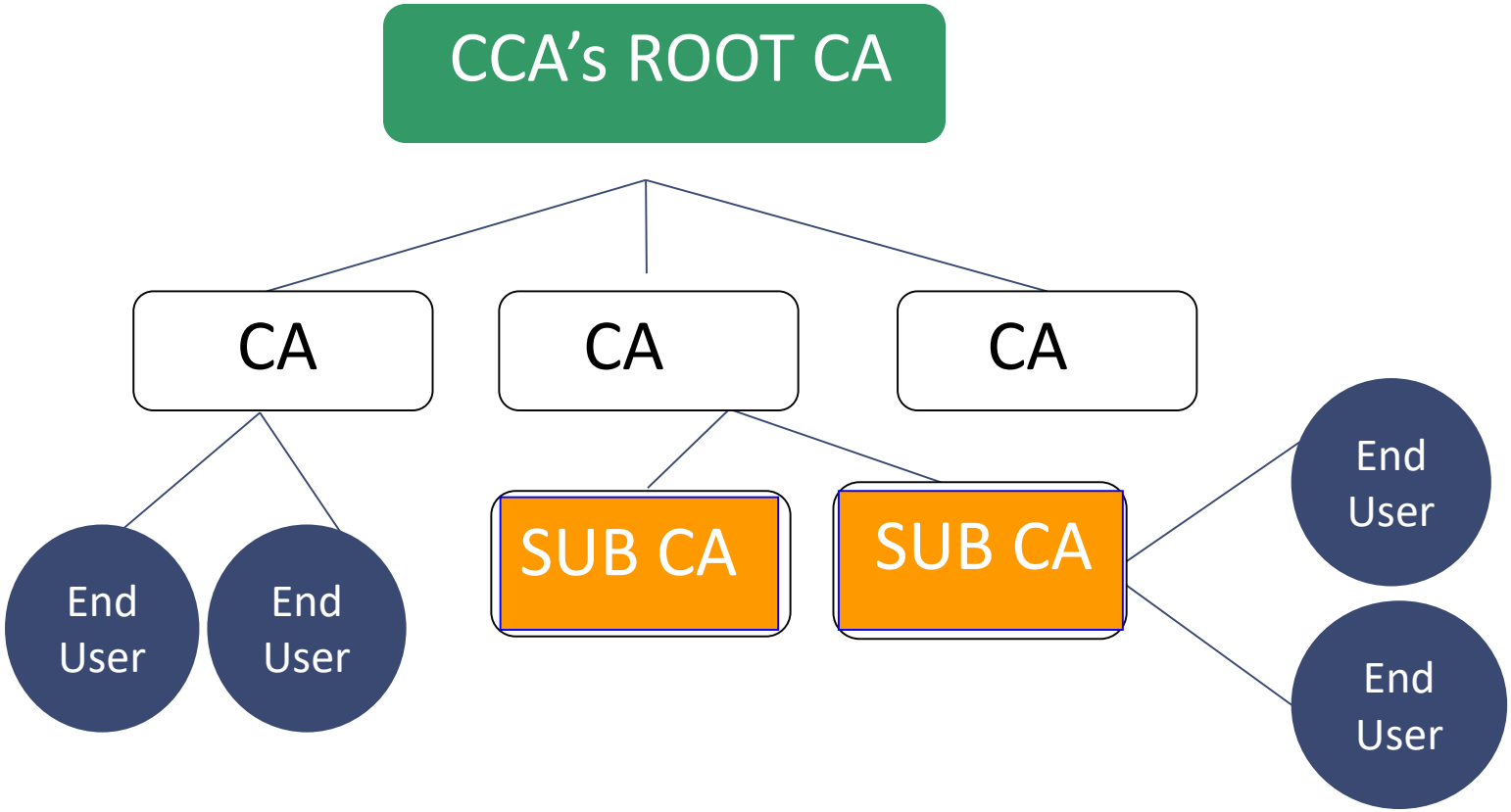
Information Technology (IT) Act, 2000

- The Information Technology Act 2000 facilitates acceptance of electronic records and digital signatures through a legal framework for establishing trust in e-Commerce and e-Governance.
- Controller of Certifying Authorities(CCA) is appointed under provision of the IT Act, 2000.

Controller of Certifying Authorities

- CCA licenses Certifying Authorities (CA) to issue Digital Signature Certificates under the IT Act.
- Digital Signature Certificates (DSC) issued by Certifying Authorities (CA).
- Twelve Certifying Authorities operational currently and the total number of DSC issued is over 120 million by November 2019.

Trust Hierarchy



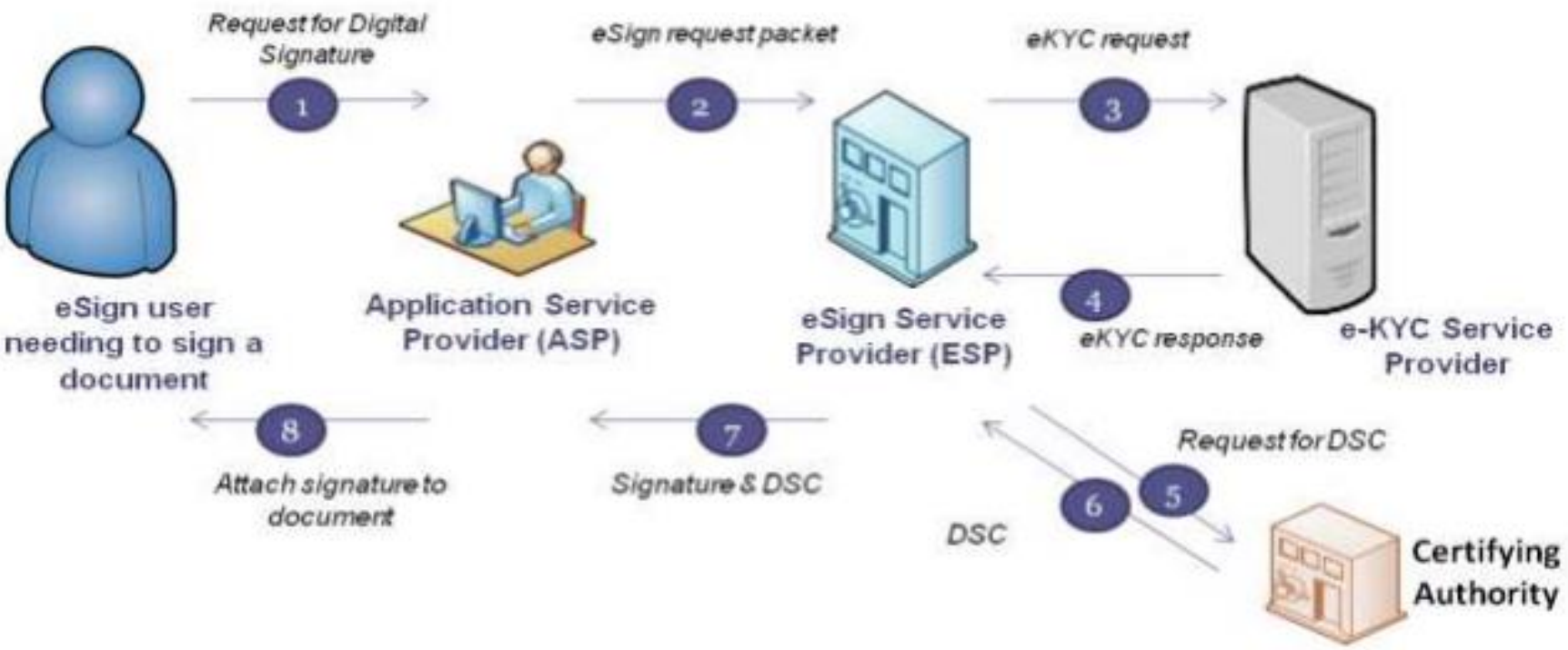
Information Technology (Amendment) Act, 2008

- Brought in technology neutrality through electronic signatures.
- Technology specific digital signatures retained as an electronic signature.
- New electronic signature technologies can be introduced through the Second Schedule of the IT Act.

Sign online digital signature service

- eSign facilitates electronically signing a document using an Online Service.
- Electronic Signature is created using authentication of consumer through eKYC service.
- eSign is an integrated service that facilitates issuing a Digital Signature Certificate and performing Signing of requested data by authenticating users.
- Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015 have been notified to provide the legal framework for eSign.

eSign



eSign Process Flow

Stakeholders involved:

1. Application Service Provider (ASP),
2. eSign Service Provider (ESP),
3. Certifying Authority (CA) and
4. eKYC providers

Digital Signature Enabled Application s/w

- Ministry of Corporate Affairs MCA21 for e-filing
- Income Tax e-filing
- Indian Railway Catering & Tourism Corporation (IRCTC)
- Director General of Foreign Trade (DGFT)
- Reserve Bank of India (SFMS & RTGS)
- Digital Locker
- E-Procurement
- E-Office
- E-Gazette
- PFMS
- GeM

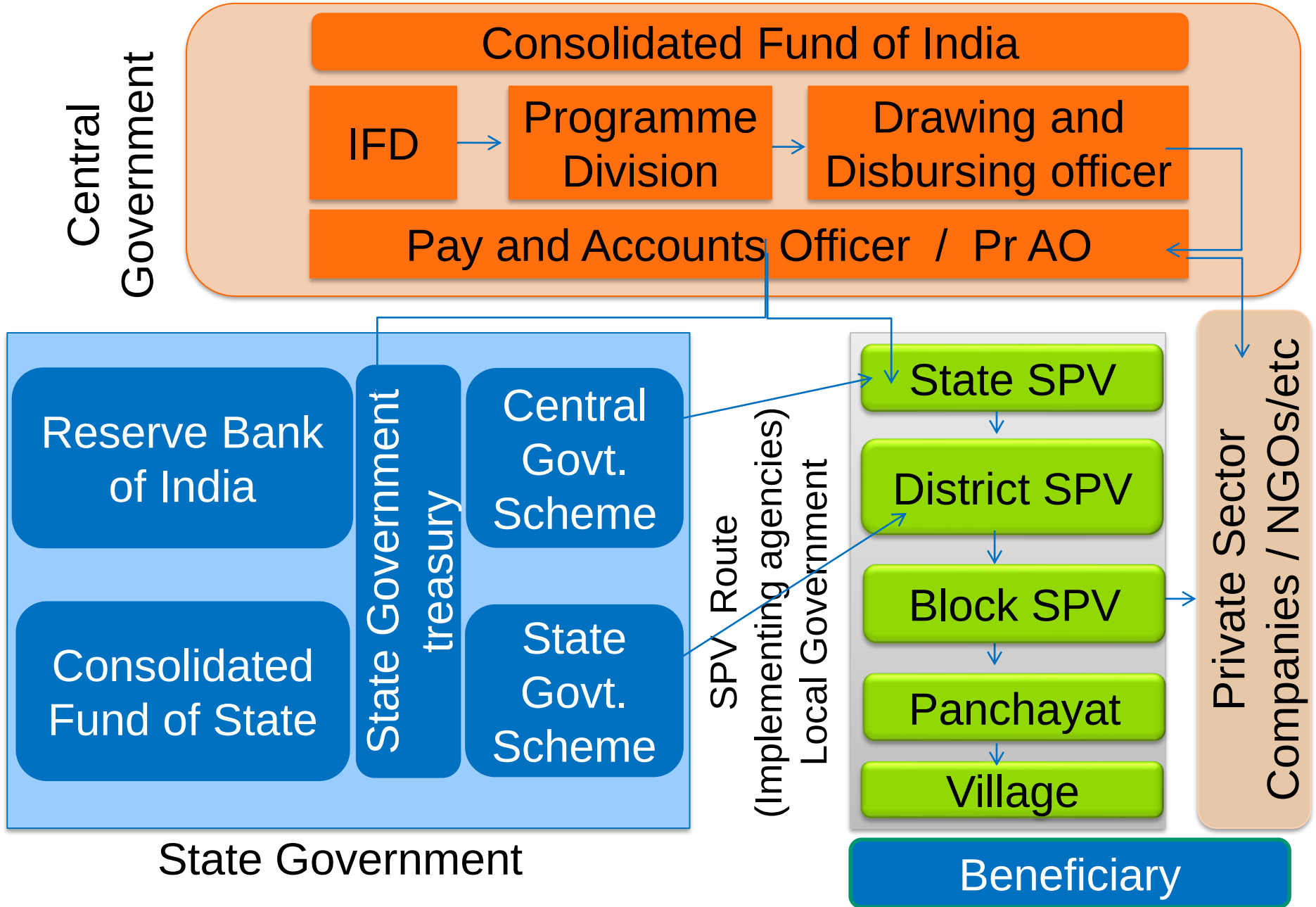
Public Financial Management System

The system is used for registering Implementing Agencies and facilitates budget allocation, sanction,

bill generation, fund disbursements, accounting, reconciliation, E-payments and beneficiaries' management both at

Central and sub-State level.

PFMS: Span of PFMS (Users of PFMS)



PKI Applications

- PKI on Mobile
- Hardware Security Modules
- Cloud Based Services
- Internet of Things
- Blockchain

PKI on Mobile

- A PKI enabled mobile solution facilitates Digital Signature and authentication for mobile applications, where transactions can take place directly from a mobile phone.
- The Mobile phone is used as a device for creation and storage of private credentials of the user.
- These credentials are then used for authenticating and digitally signing transactions.
- The options for enablement of PKI in mobile includes hardware implementations like Cryptographic SIM, Memory card as Cryptographic token and software implementations such as software cryptographic module in Mobile Phone.
- Though the options are available, major applications are still using crypto token based signatures.

Cloud based signature model

Centralized Key Pair Generation and Protection

- users belong to a specific organization and the certificates used for organization work, such as, signing the transactions, documents
  - provision must be made available to generate and protect the users keys centrally.
  - the user and only the user must securely and directly create their keys and authorize the keys for transactions to ensure the non-repudiation.

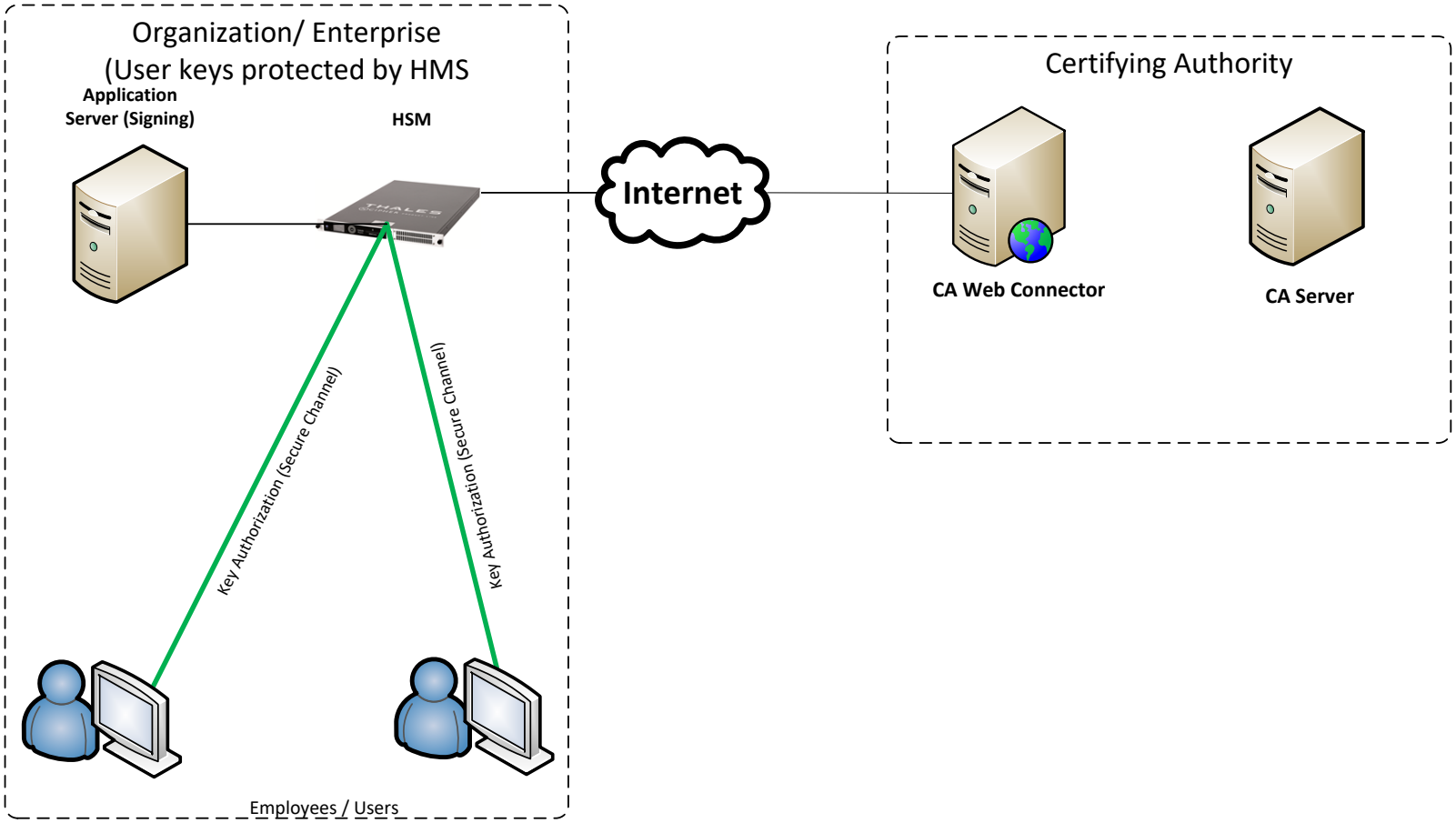


Figure:Centralized key management for organization / enterprise users

Procedure for signing and key generation

The following must be ensured for secure access / authorization:

- The HSM used must be at least FIPS 140-2 Level 3 certified.
- User keys must always be protected by the HSM.
- Users must directly authorize their respective key generation and key use on the HSM. The authorization code must be executed within the secure boundary of the HSM, that is, HSM's secure code execution server. The authorization must not be through any other application outside HSM secure boundary.
- The authorization must be with user PIN/Password/Biometric.
- The channel from the user device to HSM's secure code execution server must be encrypted.
- The authorization PIN/Password/Biometric must be encrypted on user device (PC/ Laptop/ Tablet/ Mobile) and sent to the HSM.
- Audit trails of the key use must be maintained by the HSM secure code execution server.

Requires

- A separate rule for specifying security procedures, the role, responsibilities and functions to be performed during the key-life cycle like key generation, renewal, revocation audit.
- Standard API for interoperability and also to extent signing facility for application other than of parent organisation.
- on-boarding guidelines.
- Authentication guidelines.

International Cooperation

- Many countries accord legal validity to digitally signed documents when verified using Digital Signature Certificates (DSC) issued by Certifying Authorities recognized by their Regulatory Authorities/ Government.
- This works within the country but does not facilitate cross-border transactions.
- The CAs Licenced under Indian Root are allowed to offer certificates to individuals of other countries in order to enable participation in bidding process.
- The guidelines are in place for the verification of individuals of foreign nation.
- In order to facilitate cross-border transactions and also to mutually recognize DSCs issued by licensed Certifying Authorities of other countries, regulations for recognition of foreign CAs were notified in 2103.

Thank you

www.cca.gov.in