PKI SCENERIO IN INDIA

CCA India

Office of Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Electronics Niketan, 6, CGO Complex
New Delhi - 110003.

Controller of Certifying Authorities (CCA)

The Controller of Certifying Authorities (CCA) has been appointed by the Central Government under the provisions of Act

The Office of CCA came into existence on November 1, 2000.

CCA license & regulate Certifying Authorities (CAs) in the country with the aim of promoting the growth of e-Commerce and e-Governance through the wide use of electronic signatures.

CCA operates the “Root Certifying Authority of India (RCAI)” to issue public key certificate to Certifying Authorities (CA).

Indian IT Act, 2000

- Came into effect from **October 17th, 2000** on the lines of the UNCITRAL Model Law
- India is the 12th nation in the world to adopt digital signatures
- The Act applies to the whole of India and also applies to any offence or contravention
- IT Act 2000 was amended through the Information Technology **Amendment Act, 2008** which came into effect from October 27,2009
  - ✓ 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.

Digital India - Digital Infrastructure

AADHAAR

- 136 crore Aadhaar and over 8.6 thousand crore authentications

NSM
NATIONAL
SUPERCOMPUTING
MISSION

- Delivered over 24 PF capacity 18 super computers deployed 17000 manpower trained

MeghRaj CLOUD INITIATIVE

- Encourages standardized platforms and products, over 1,578 Users and more than 24,033 VMs
- 19 Private Cloud Service Providers

UPI
UNIFIED PAYMENTS INTERFACE

- 800+ crore monthly transactions worth Rs 12.99 lakh crore in Jan’23

NKN
National
Knowledge
Network

- High speed connectivity to 1,767 premier institutions + Universities

cert-in

- India # 10 in Global Cyber Security Index 2020 (ITU)

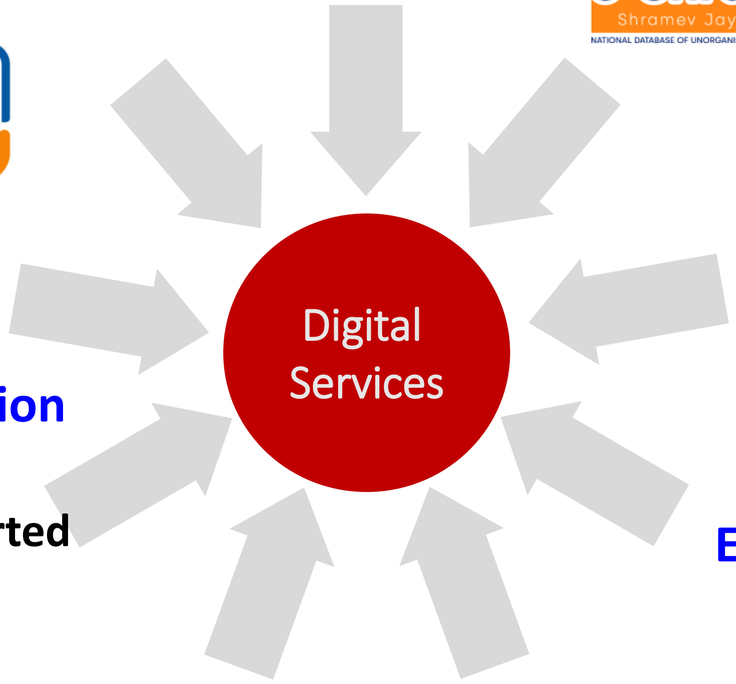
Digital India- Digital Services

200+
Major Projects

4000+
Services

43 crore
Average Daily Transactions

On Demand Services
from Central, State & Local Government



GeM
Government e Marketplace

66,572 Govt. Buyer &
58 lakh Organizations

PM-KISAN
Government of India

12th installment with Rs 16,000 cr released to farmers in October 2022

e-Shram
Shramev Jayate
NATIONAL DATABASE OF UNORGANISED WORKERS

More than 28.5 Cr UAN cards have been issued since the launch of portal

UMANG
1680+ Services
314 Departments
20,100+ utility services
5 Crore users

eNAM
उत्तम फसल, उत्तम इनाम

1.7 Cr Farmers onboard
1260 APMCs integrated

AADHAAR

Aadhaar Authentication Services to Govt.
150+ Applications Supported

E-District
709 Districts rolled out with 3,916 e-services

E-Hospital / ORS
1134 Hospitals onboarded

etaal

43 crore average daily transactions in 2022

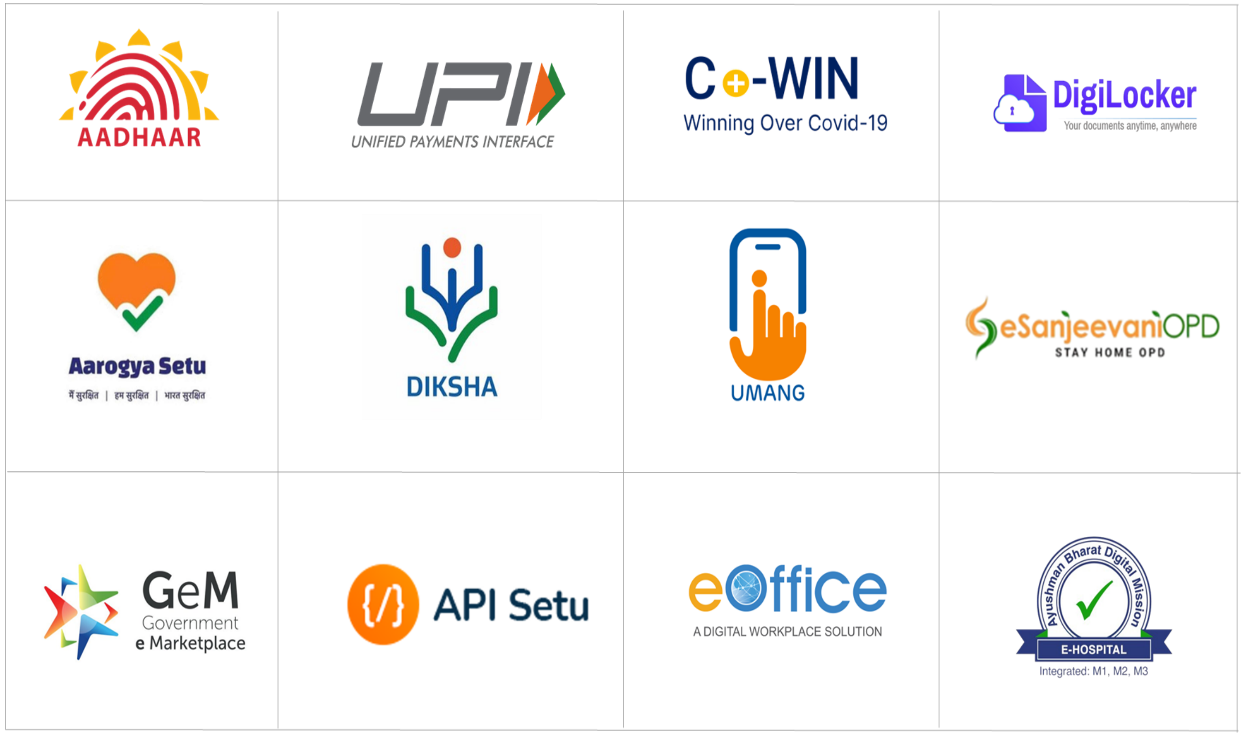
DigiLocker
Your documents anytime, anywhere

14.7 crore users
562 crore Issued documents

India Stack Global

- Presence-less, paper-less, cash-less and universal service layer
- Based on Open Standards, Open APIs & Interoperable
- Implemented at population scale
- Participation of Government and Industry
- Ever evolving and innovating with latest technologies
- Education, Healthcare, Financial services & more

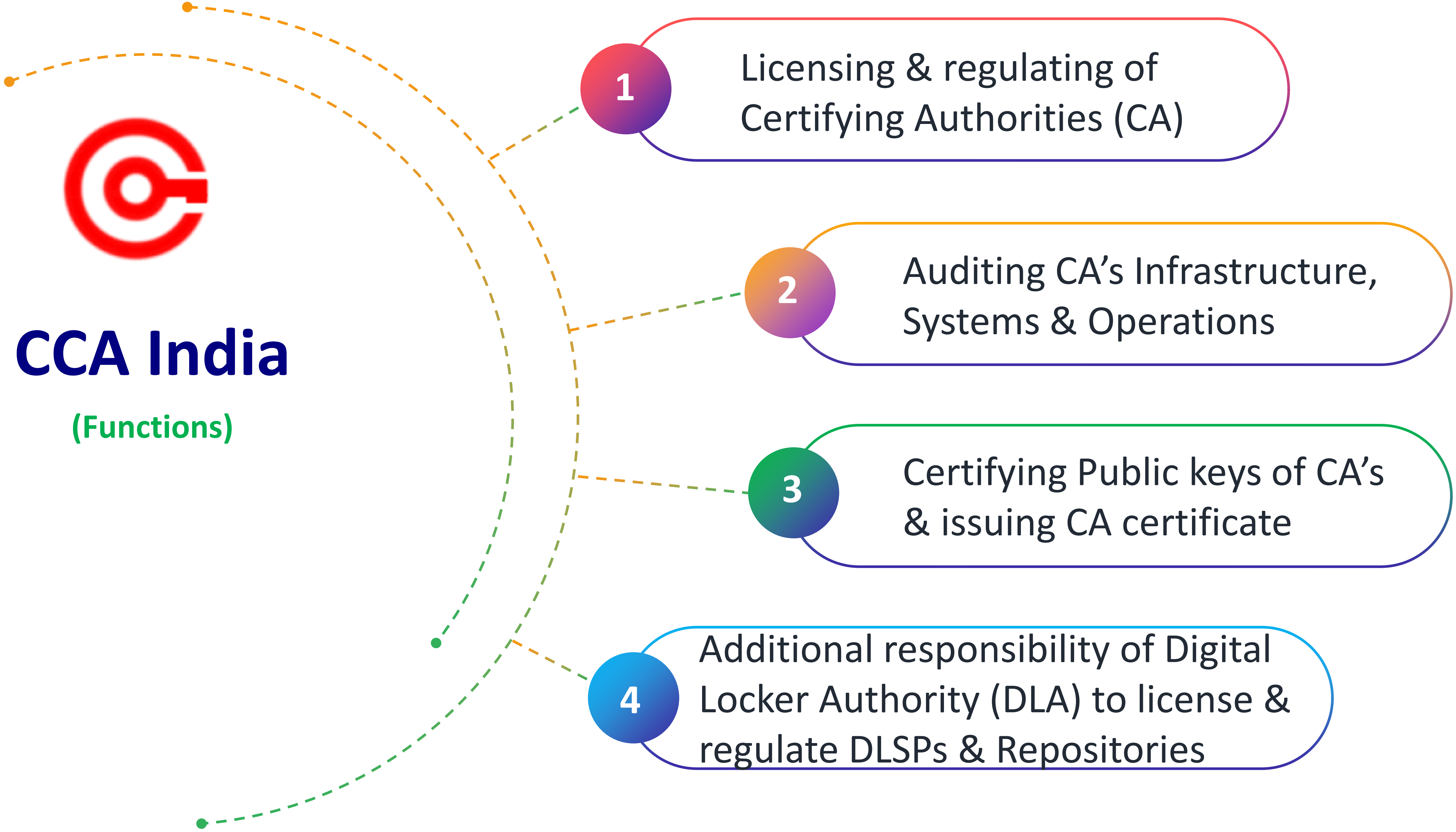
https://www.indiastack.global/



12 Solutions - Available in 6 UN languages

CCA India

(Functions)



1 Licensing & regulating of Certifying Authorities (CA)

2 Auditing CA’s Infrastructure, Systems & Operations

3 Certifying Public keys of CA’s & issuing CA certificate

4 Additional responsibility of Digital Locker Authority (DLA) to license & regulate DLSPs & Repositories

CCA India Responsibilities

As per IT Act 2000, the following functions are stated:

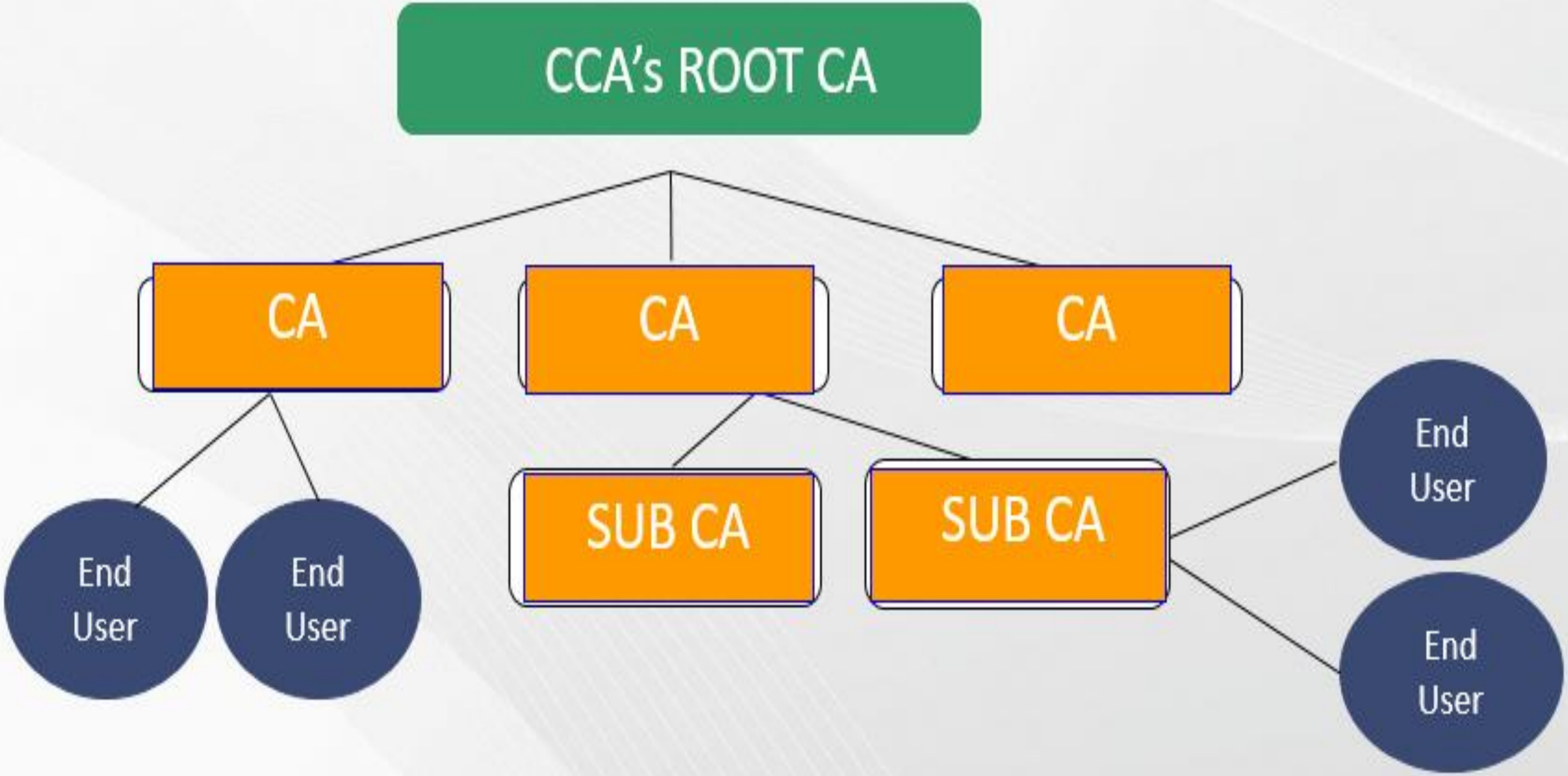
1. Exercising supervision over the activities of the Certifying Authorities.
2. Certifying public keys of the Certifying Authorities
3. Laying down the standards to be maintained by the Certifying Authorities;
4. Specifying the qualifications and experience which employees of the Certifying Authorities should possess;
5. Specifying Authorities shall conduct their business Specifying the content of written, printed or visual material and advertisements that may be distributed or used in respect of a Electronic Signature Certificate and the Public Key;
6. Specifying the form and content of a Electronic Signature Certificate and the key.
7. Specifying the form and manner in which accounts shall be maintained by the Certifying Authorities;

Contd…

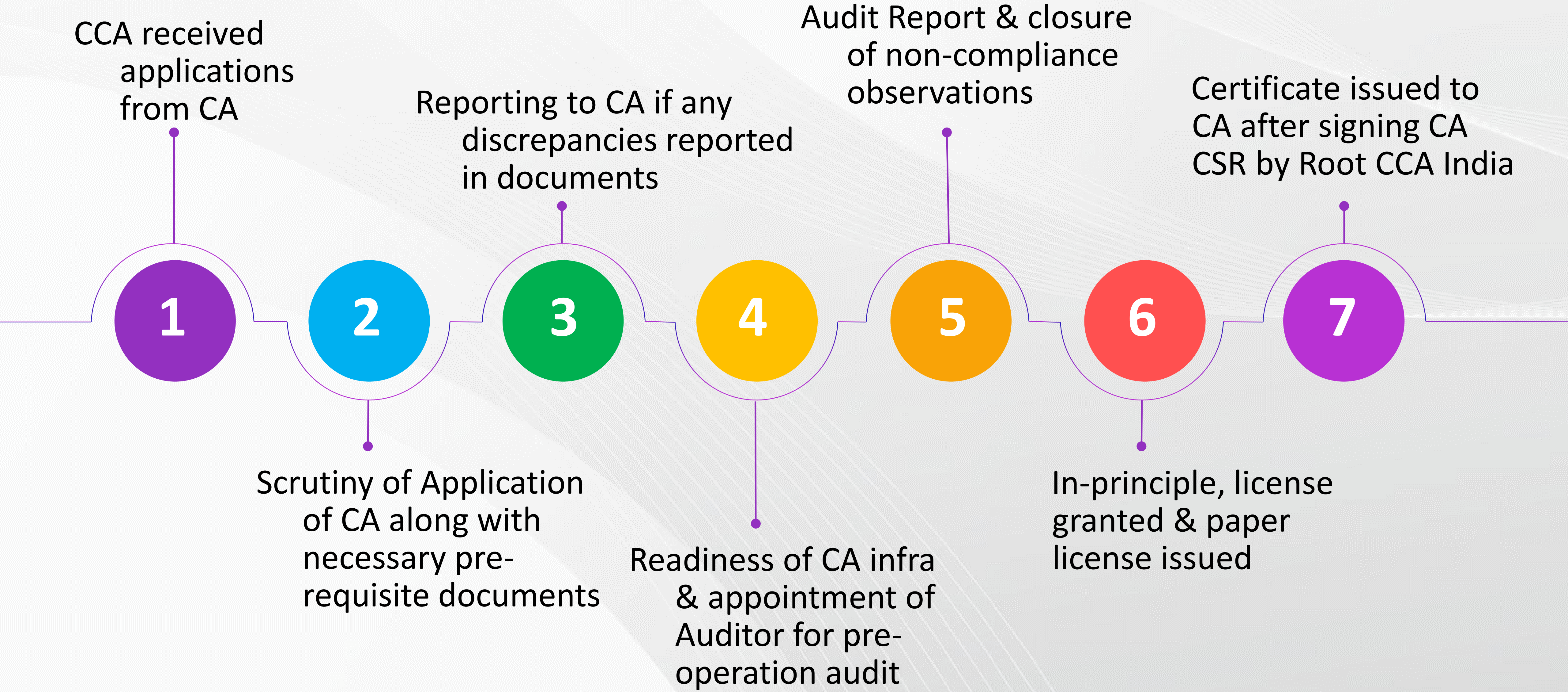
CCA India Responsibilities

8. Specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them.
9. Facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
10. Specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;
11. Resolving any conflict of interests between the Certifying Authorities and the subscribers;
12. Laying down the duties of the Certifying Authorities;
13. Maintaining a data-base containing the disclosure record of every Certifying Authority containing such particulars as may be the conditions subject to which the Certifying specified by regulations, which shall be accessible to public.
14. CCA has entrusted an additional role* as **Controller of Digital Locker Authority (CDLA)** for licensing & regulating of Digital Locker Service Providers (DLSPs) & DL Repositories.

PKI HIERARCHY

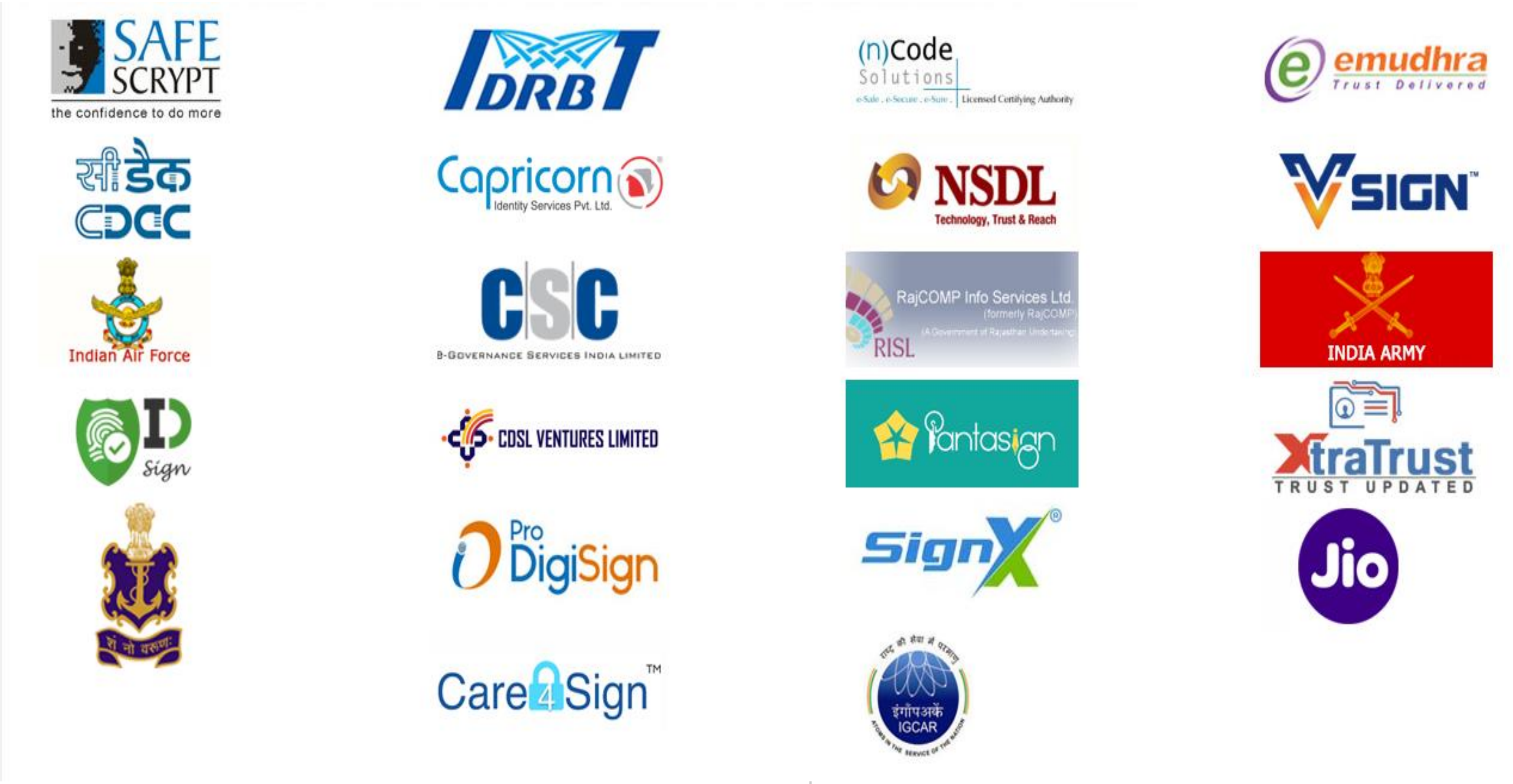


Steps for Licensing Certifying Authority (CA)

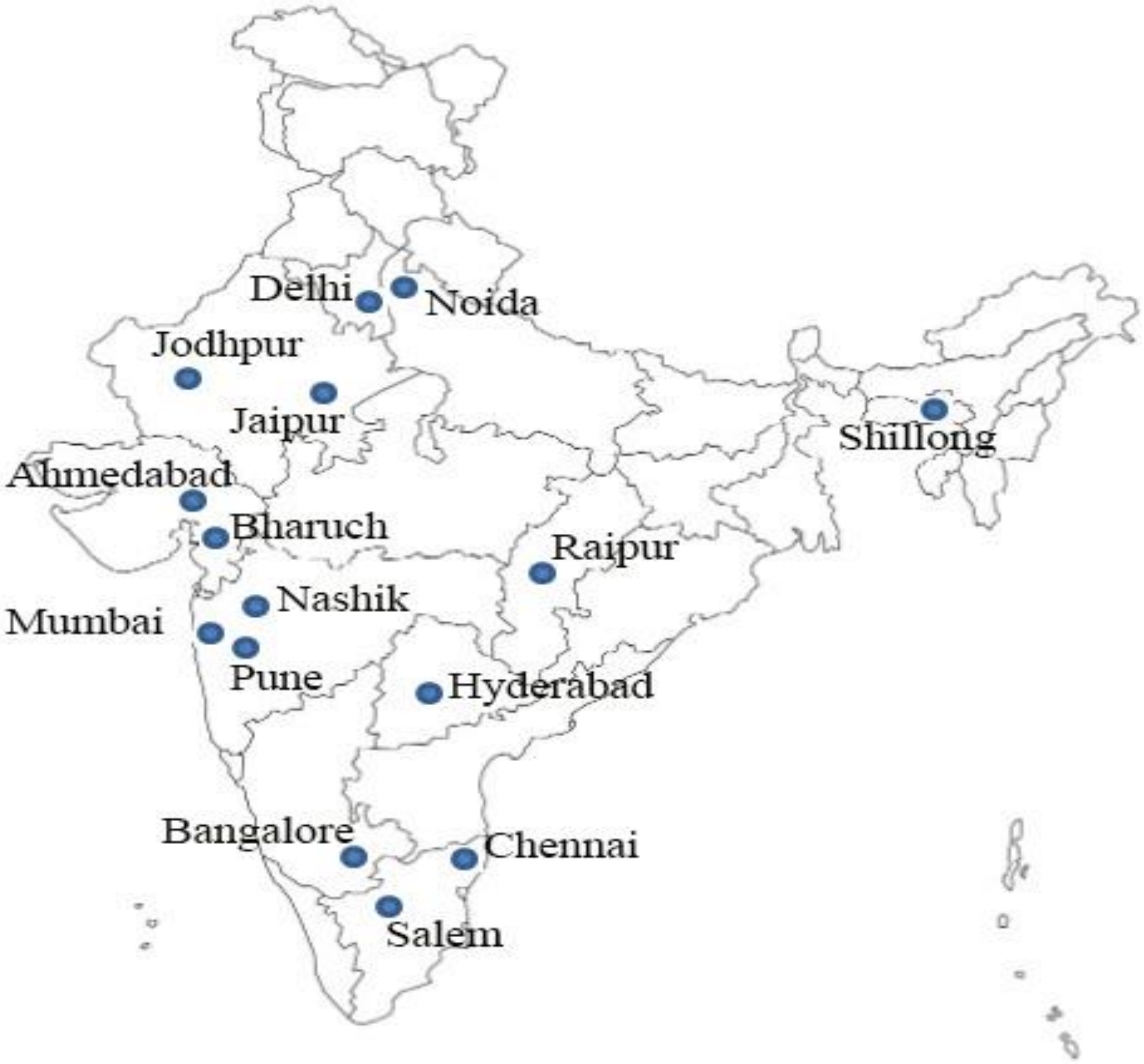


1. CCA received applications from CA
2. Scrutiny of Application of CA along with necessary pre-requisite documents
3. Reporting to CA if any discrepancies reported in documents
4. Readiness of CA infra & appointment of Auditor for pre-operation audit
5. Audit Report & closure of non-compliance observations
6. In-principle, license granted & paper license issued
7. Certificate issued to CA after signing CA CSR by Root CCA India

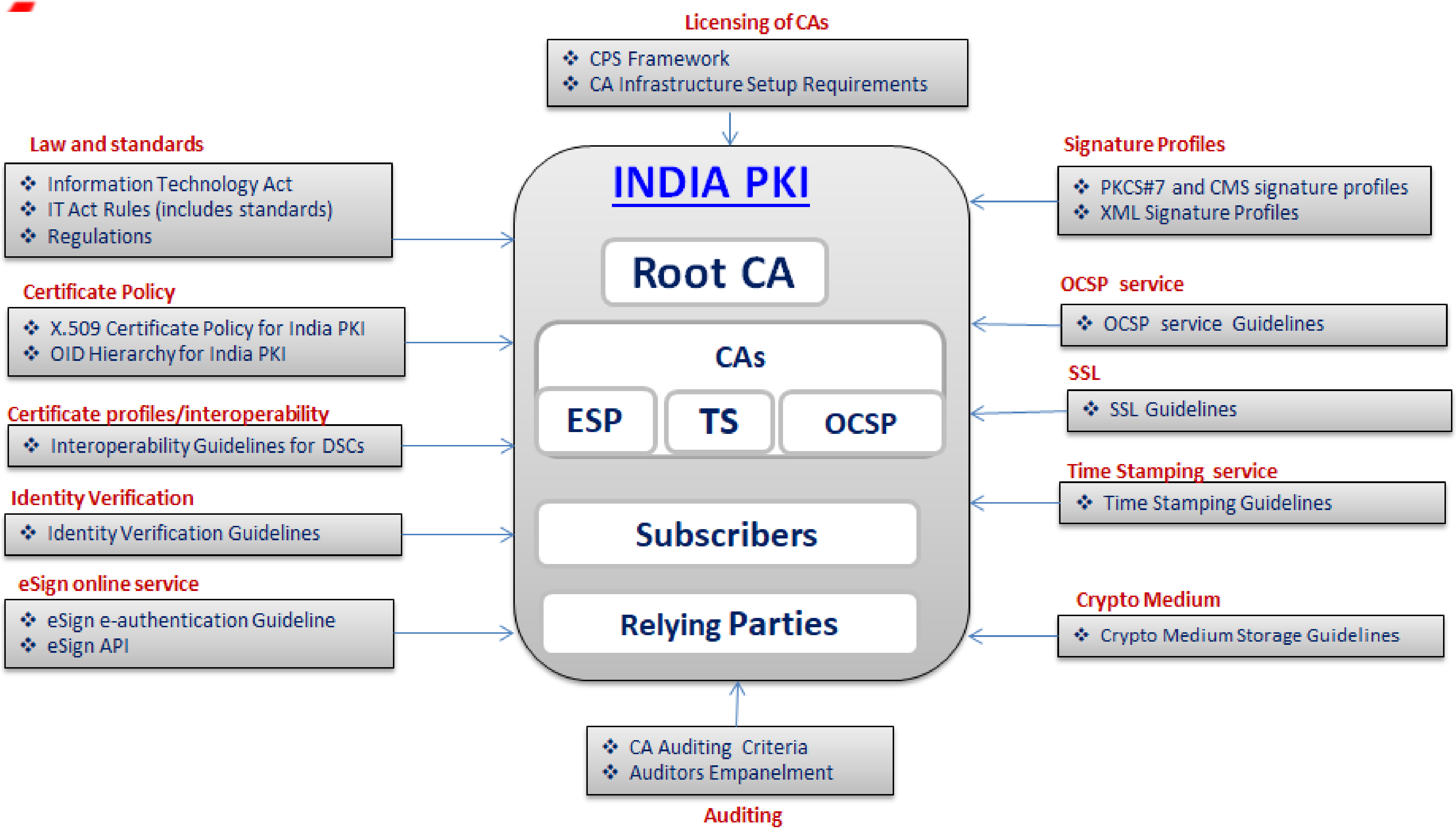
CCA India Licensed CAs – 22 Nos.


SAFE SCRYPT
the confidence to do more
सीडैक
CDAC
Indian Air Force
ID Sign
शं नो वरुणः
IDRBT
Capricorn
Identity Services Pvt. Ltd.
CSC
E-GOVERNANCE SERVICES INDIA LIMITED
CDSL VENTURES LIMITED
Pro DigiSign
Care4Sign™
(n)Code Solutions
e-Sale . e-Secure . e-Sure . Licensed Certifying Authority
NSDL
Technology, Trust & Reach
RajCOMP Info Services Ltd.
(formerly RajCOMP)
(A Government of Rajasthan Undertaking)
RISL
Pantasign
SignX®
राष्ट्र की सेवा में परमाणु
इंगांपअकें
IGCAR
ATOMS IN THE SERVICE OF THE NATION
emudhra
Trust Delivered
VSIGN™
INDIA ARMY
XtraTrust
TRUST UPDATED
Jio

Distribution of Licensed CAs



Electronic Signatures Policy Framework



Licensing of CAs

- CPS Framework
- CA Infrastructure Setup Requirements

Law and standards

- Information Technology Act
- IT Act Rules (includes standards)
- Regulations

Certificate Policy

- X.509 Certificate Policy for India PKI
- OID Hierarchy for India PKI

Certificate profiles/interoperability

- Interoperability Guidelines for DSCs

Identity Verification

- Identity Verification Guidelines

eSign online service

- eSign e-authentication Guideline
- eSign API

INDIA PKI

Root CA

CAs

ESP

TS

OCSP

Subscribers

Relying Parties

Signature Profiles

- PKCS#7 and CMS signature profiles
- XML Signature Profiles

OCSP service

- OCSP service Guidelines

SSL

- SSL Guidelines

Time Stamping service

- Time Stamping Guidelines

Crypto Medium

- Crypto Medium Storage Guidelines

- CA Auditing Criteria
- Auditors Empanelment

Auditing

Certifying Authority(CA) eSign Service Provider(ESP) Secure Socket Layer(SSL)
Time Stamping(TS) Online Certificate Status Protocol(OCSP) Relying Party(RP)

Electronic Signature options for subscribers

1. Crypto token/Mobile key storage based long term validity DSCs

2. eSign Service based one time usage & short term validity DSCs

3. Remote Key Storage based Long term validity DSC & eSign

INTEROPERABILUTY

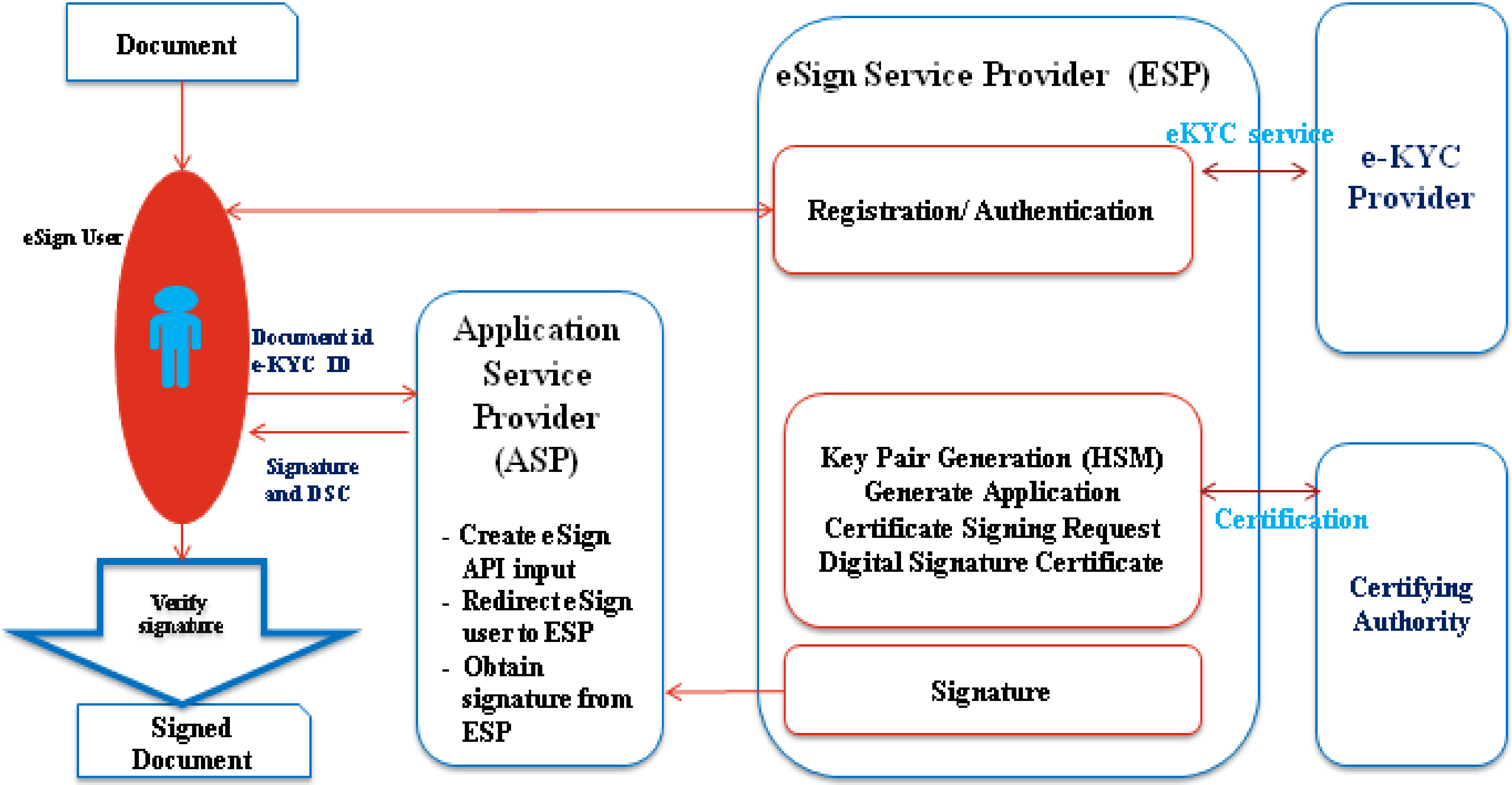
In order to facilitate interoperability , Licenced CAs follow common policy and procedures for similar assurance types of DSCs. CA follows

- Interoperability Guidelines for DSCs
- X.509 Certificate Policy for India PKI
- PKCS#7 and CMS & XML signature profiles
- OID Hierarchy for India PKI
- Security Requirements for Crypto Devices
- Audit Criteria for CAs
- eSign e-authentication Guidelines & eSign API

AUDIT CRITERIA

- The Audit Criteria for the Licenced CAs covers ACT and WebTrust/ETSI requirements
- Licenced CAs are audited by the auditors empanelled by CCA
- Annual audit by empanelled auditors and internal audit is mandatory.
- The empanelment of auditors are carried out by CCA and valid for 2 years

eSign Services



Document

eSign User

Document id
e-KYC ID

Signature and DSC

Verify signature

Signed Document

Application Service Provider (ASP)

- Create eSign API input
- Redirect eSign user to ESP
- Obtain signature from ESP

eSign Service Provider (ESP)

Registration/ Authentication

Key Pair Generation (HSM)
Generate Application
Certificate Signing Request
Digital Signature Certificate

Signature

eKYC service

e-KYC Provider

Certification

Certifying Authority

HSM – Hardware Security Module

OTP – One Time Password

ASP – Application Service Provider

e-KYC – electronic Know Your Customer

DSC – Digital Signature Certificate

ESP – eSign Service Provider

eSign Services

- eSign is an online Electronic Signature Service, based on successful authentication of individual using e-KYC services
- Electronic signature of the electronic document are facilitated by the ESP instantaneously within a single online service.
- The key pairs are used only once and the private key is deleted after one time use.
- The Digital Signature Certificates are of 30 minutes validity, and this makes verification simple by eliminating the requirements of revocation checking.
- Document that is signed using eSign will contain a valid digital signature that can be easily verified using standard methods.

The eSign is carried out based on the

1. Aadhaar Authentication
2. CA eKYC account authentication

eSign Authentication methods

eSign was introduced with OTP as the default authentication method. The authentication for eSign has been further enhanced with options

1. T-OTP
2. Mobile access token
3. FIDO2 over mobile
4. Public Key Authentication

eKYC of subscribers

- An eKYC account with CA is mandatory for issuance of DSCs.
- Physical verification is mandatory for signature certificates
- One time registration of applicant and the KYC can be used for a period of 2 years.
- Applicants are required to submit the information to CA and CA carryout a verification to establish the information submitted by the applicant is genuine.
- CA may employ one or more of the following online verification mechanisms:-

  Aadhaar authentication, PAN (Income tax), Bank KYC online & CA direct verification

Foreign CA Regulations

For a Digital Signature Certificate issued by a Foreign Certifying Authority to be recognized in India, notification contains two sets of Regulations –

1. **Recognition of Foreign Certifying Authorities operating under a Regulatory Authority. Such CAs can be recognised if the following and other conditions are met:-**
   - The level of reliability of PKI environment of the country is at least equal that of India.
   - The Controller (CCA) enters into a MoU with the Regulatory Authority for Mutual Recognition of CAs.
   - Reliability assessment for equivalence

- **2 Recognition of Foreign Certifying Authorities not operating under any Regulatory Authority**
- **-**Any Foreign CA may apply to Controller for recognition. The recognition process should pass through examination of documents submitted by that CA

Use of PKI in e-Governance

Government

- ✓ Ministry of Corporate Affairs (MCA 21)
- ✓ E-Procurement Project of Govt. of AP
- ✓ Indian Customs & Excise Gateway
- ✓ e-Procurement System, Karnataka Govt.
- ✓ DGS&D & DGFT
- ✓ PFMS, MoF
- ✓ GeM Portal, MoC&I
- ✓ E-Office, State & Central Govt. offices
- ✓ DigiLocker, NeGD
- ✓ ITR filing & returns
- ✓ RTI reply
- ✓ Online Money Orders
- ✓ E-education
- ✓ IRCTC ticketing & reservations
- ✓ E-voting
- ✓ Public Information Record
- ✓ Online file movement system
- ✓ Online Govt. orders/treasury orders
- ✓ Issuing forms & licenses
- ✓ Email & Messaging service
- ✓ **Govt. e-Services**
  - e-Invoice
  - e-Tax Filing
  - e-Customs
  - e-Passport
  - e-Governance
  - e-Payment
  - e-Billing
  - e-Procurement
  - e-Insurance
  - e-Treasury

Telcom

- ✓ Subscriber's services management
- ✓ Shifting of telephones, Accessories (Clip, Cordless)
- ✓ Small payments through telephones
- ✓ Mobile Authentication of SMS
- ✓ Inter/Intra offices authentic communications
- ✓ Procurement of material
- ✓ Network Management

E-Commerce

- ✓ Online shopping
- ✓ Payments
- ✓ Sellers verification
- ✓ Purchase verification

Judicial

- ✓ Instant posting of Judgment online
- ✓ Secure electronic communications within judiciary
- ✓ Authentic archiving of Judicial records
- ✓ Submission of Affidavits
- ✓ Issuing certified copies of the judgment

Banking

- ✓ Money transfer
- ✓ e-KYC
- ✓ Payments
- ✓ Account opening & Access
- ✓ Non-financial transactions
- ✓ Tax payment
- ✓ Online trading
- ✓ Insurance opening

Objectives, Goals, Targets

1. Be the trust anchor for digital transactions
2. Promote Digital Transactions and e-Commerce
3. Increase Usage of Digital Signatures
4. WebTrust certification of CAs
5. Cross country recognition
6. Addressing new technology Challenges
7. Support and fulfil our country’s vision

Thank you