5th International Conference on Public Key Infrastructure and its Applications (PKIA 2024)

A Joint Conference by IEEE CS & IAS Bangalore Chapter

September 5-6th, 2024

Bangalore, Karnataka, India

Deepak Kumar, *Scientist 'D'*

Controller of Certifying Authorities (CCA)
Ministry of Electronics and Information Technology (MeitY)
Electronics Niketan, 6, CGO Complex, New Delhi-110003

Information Technology Act, 2000

- Came into effect from October 17th, 2000 on the lines of the United Nation Commission of International Trade Law (UNCITRAL) Model Law

- The Information Technology Act 2000 facilitates acceptance of electronic records and Digital Signatures through a legal framework for establishing trust in e-Commerce & e-Governance.

- The IT Act, 2000 provides the legal recognition of digital signatures (Section 5, IT Act 2000)

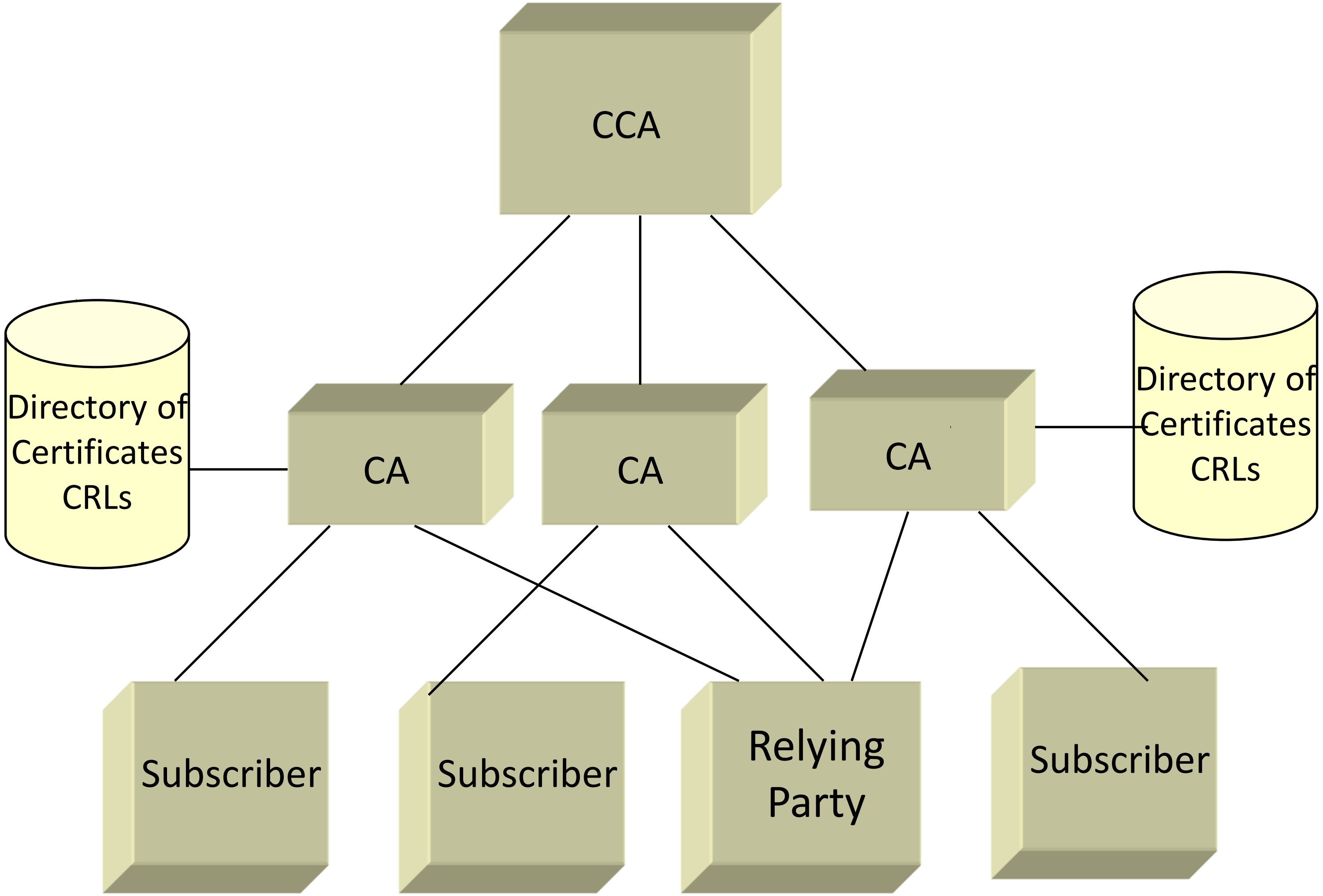
- Central Government appoints the Controller of Certifying Authorities (CCA) under Section 17 of the IT Act, 2000.

- 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.
  - ✓ New electronic signature technologies can be introduced through the Second Schedule of the IT Act.

Functions of CCA

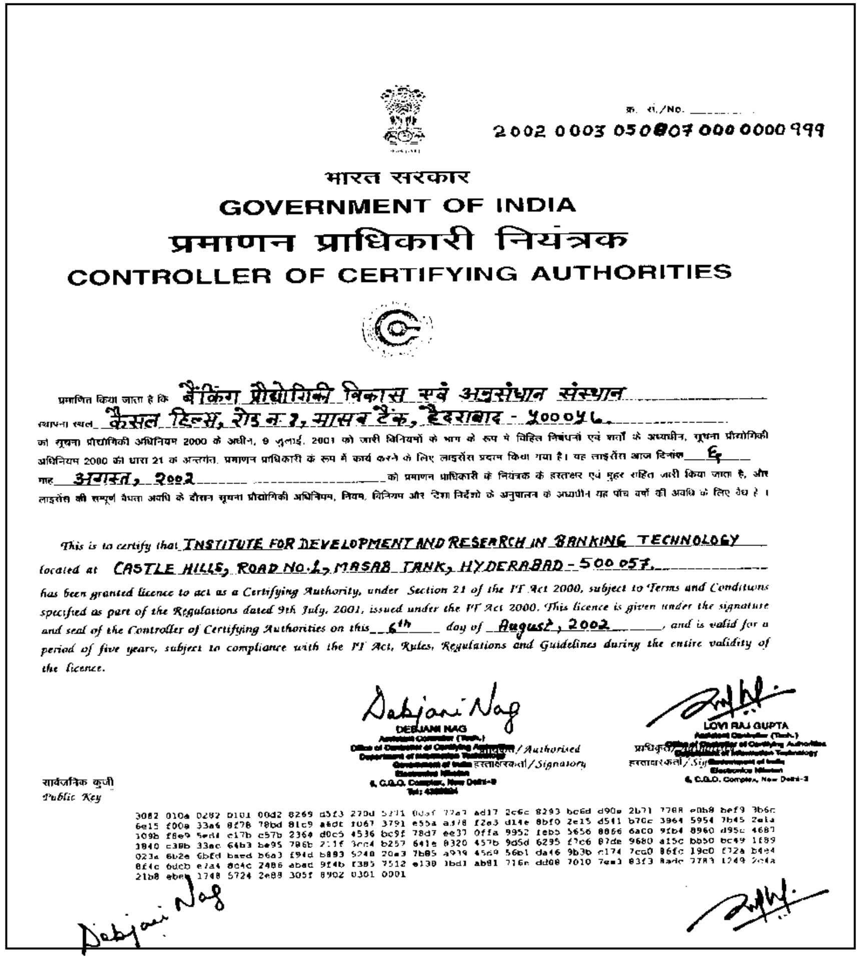
- Licensing of Certifying Authorities (CAs),
- Exercising supervision over the activities of the CAs
- Certifying public keys of the Certifying Authorities
- Laying down the standards to be maintained by the CAs
- Specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers
- Resolving any conflict of interests between the Certifying Authorities and the subscribers
- Auditing the physical and technical infrastructure of the applicants through a panel of auditors maintained by the CCA
- Maintaining disclosure record of every licenced CA, which shall be accessible to public
- Promotes the growth of E-Commerce and E-Governance through the wide use of Electronic (Digital) signatures

Trust Hierarchy


CCA
Directory of Certificates CRLs
CA
CA
CA
Directory of Certificates CRLs
Subscriber
Subscriber
Relying Party
Subscriber

CA Certificate

Paper



क्र. सं./No. ________
2002 0003 050807 000 0000 999

भारत सरकार

GOVERNMENT OF INDIA

प्रमाणन प्राधिकारी नियंत्रक

CONTROLLER OF CERTIFYING AUTHORITIES

प्रमाणित किया जाता है कि बैंकिंग प्रौद्योगिकी विकास एवं अनुसंधान संस्थान
स्थापना स्थल कैसल हिल्स, रोड न. १, मासब टैंक, हैदराबाद - ५०००५६.
को सूचना प्रौद्योगिकी अधिनियम 2000 के अधीन, 9 जुलाई, 2001 को जारी विनियमों के भाग के रूप में विहित निबंधनों एवं शर्तों के अध्यधीन, सूचना प्रौद्योगिकी अधिनियम 2000 की धारा 21 के अन्तर्गत, प्रमाणन प्राधिकारी के रूप में कार्य करने के लिए लाइसेंस प्रदान किया गया है। यह लाइसेंस आज दिनांक 6 माह अगस्त, २००२ को प्रमाणन प्राधिकारी के नियंत्रक के हस्ताक्षर एवं मुहर सहित जारी किया जाता है, और लाइसेंस की सम्पूर्ण वैधता अवधि के दौरान सूचना प्रौद्योगिकी अधिनियम, नियम, विनियम और दिशा निर्देशों के अनुपालन के अध्यधीन यह पांच वर्षों की अवधि के लिए वैध है।

This is to certify that INSTITUTE FOR DEVELOPMENT AND RESEARCH IN BANKING TECHNOLOGY
located at CASTLE HILLS, ROAD No.1, MASAB TANK, HYDERABAD - 500 057.
has been granted licence to act as a Certifying Authority, under Section 21 of the IT Act 2000, subject to Terms and Conditions specified as part of the Regulations dated 9th July, 2001, issued under the IT Act 2000. This licence is given under the signature and seal of the Controller of Certifying Authorities on this 6th *day of* August, 2002, *and is valid for a period of five years, subject to compliance with the IT Act, Rules, Regulations and Guidelines during the entire validity of the licence.*

Debjani Nag
DEBJANI NAG
Assistant Controller (Tech.)
Office of Controller of Certifying Authorities
Department of Information Technology
Government of India
Electronics Niketan
6, C.G.O. Complex, New Delhi-3
Tel: [illegible]
प्राधिकृत/*Authorised*
हस्ताक्षरकर्ता/*Signatory*

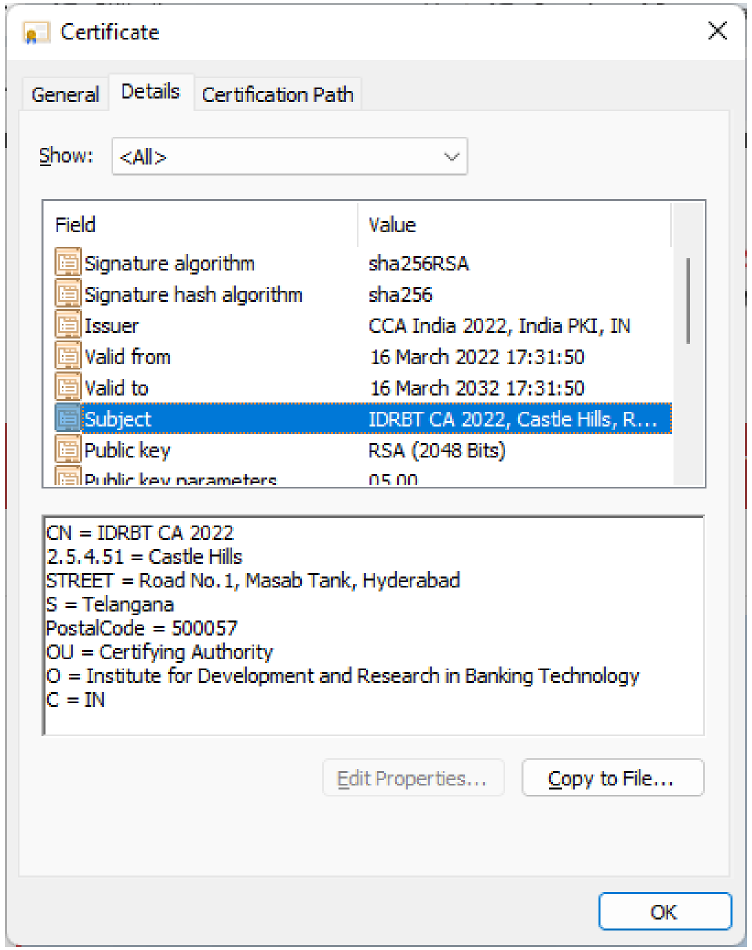
LOVI RAJ GUPTA
Assistant Controller (Tech.)
Office of Controller of Certifying Authorities
Department of Information Technology
Government of India
Electronics Niketan
6, C.G.O. Complex, New Delhi-3
प्राधिकृत/*Authorised*
हस्ताक्षरकर्ता/*Signatory*

सार्वजनिक कुंजी
Public Key

```
3082 010a 0282 0101 00d2 8269 d5f3 270d 5271 005f 72a7 ad17 2c6c 8293 bc6d d90e 2b71 7788 e0b8 bef9 3b6c
6e15 f00e 33a6 8f78 78bd 81c9 a6dc 1067 3791 e55a a178 f2e3 d14e 8bf0 2e15 d511 b70c 3964 5954 7b45 2e1a
109b f8e9 5ed1 c17b c57b 2364 d0c5 4536 bc9f 78d7 ee37 0ffa 9952 1eb5 5656 8866 6ac0 9fb4 8960 d95c 4687
1840 c38b 33ac 64b3 be95 786b 211f 3cc4 b257 641e 8320 457b 9d5d 6295 f7c6 87de 9680 a15c bb50 bc49 1f89
023a 6b2e 6bfd baed b6a3 f94d b893 5248 20e3 7b85 a939 4569 56b1 da16 9b3b c174 7cc0 86fc 19c0 f72a b4e4
8f4c 6dcb e7a4 8c4c 2486 abad 9f4b f385 7512 e130 3bd1 ab81 716e dd08 7010 7ee1 83f3 8adc 7783 1249 2e1a
21b8 ebe[illegible] 1748 5724 2e89 305f 8902 0301 0001
```

Debjani Nag

Electronic



Show: <All>

Field	Value
Signature algorithm	sha256RSA
Signature hash algorithm	sha256
Issuer	CCA India 2022, India PKI, IN
Valid from	16 March 2022 17:31:50
Valid to	16 March 2032 17:31:50
Subject	IDRBT CA 2022, Castle Hills, R...
Public key	RSA (2048 Bits)
Public key parameters	05 00

CN = IDRBT CA 2022
2.5.4.51 = Castle Hills
STREET = Road No. 1, Masab Tank, Hyderabad
S = Telangana
PostalCode = 500057
OU = Certifying Authority
O = Institute for Development and Research in Banking Technology
C = IN

Certifying Authority (CA)

Certifying authority is an entity which issues Electronic (Digital) Signature Certificates

- It is a **Trusted Third Party**
- Certifying Authorities are the important components of Public Key Infrastructure (PKI)

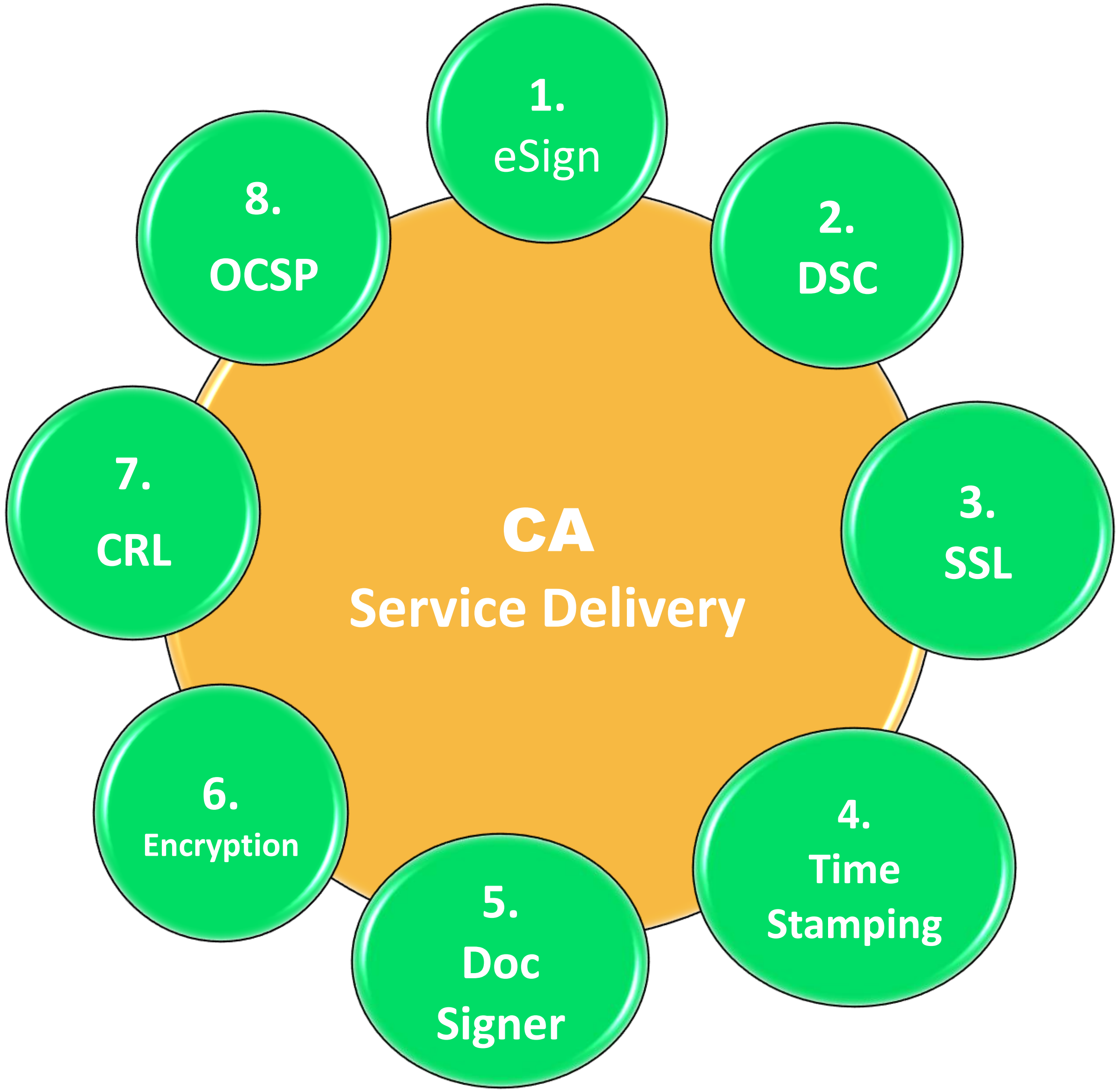
Responsibilities of CA

✓ Verify the credentials of the person requesting for the certificate
✓ Issue Digital Signature Certificates
✓ Revoke Digital Signature Certificates
✓ Generate and upload CRL

Certifying Authorities empanelled as **eSign Service Providers (ESPs)** provide eSign services (online electronic signature service) based on approved mode(s) of eKYC:

- Aadhaar online eKYC
- CA eKYC-offline Aadhaar eKYC, Banking eKYC, Organizational eKYC & PAN eKYC etc.

CA Service Delivery



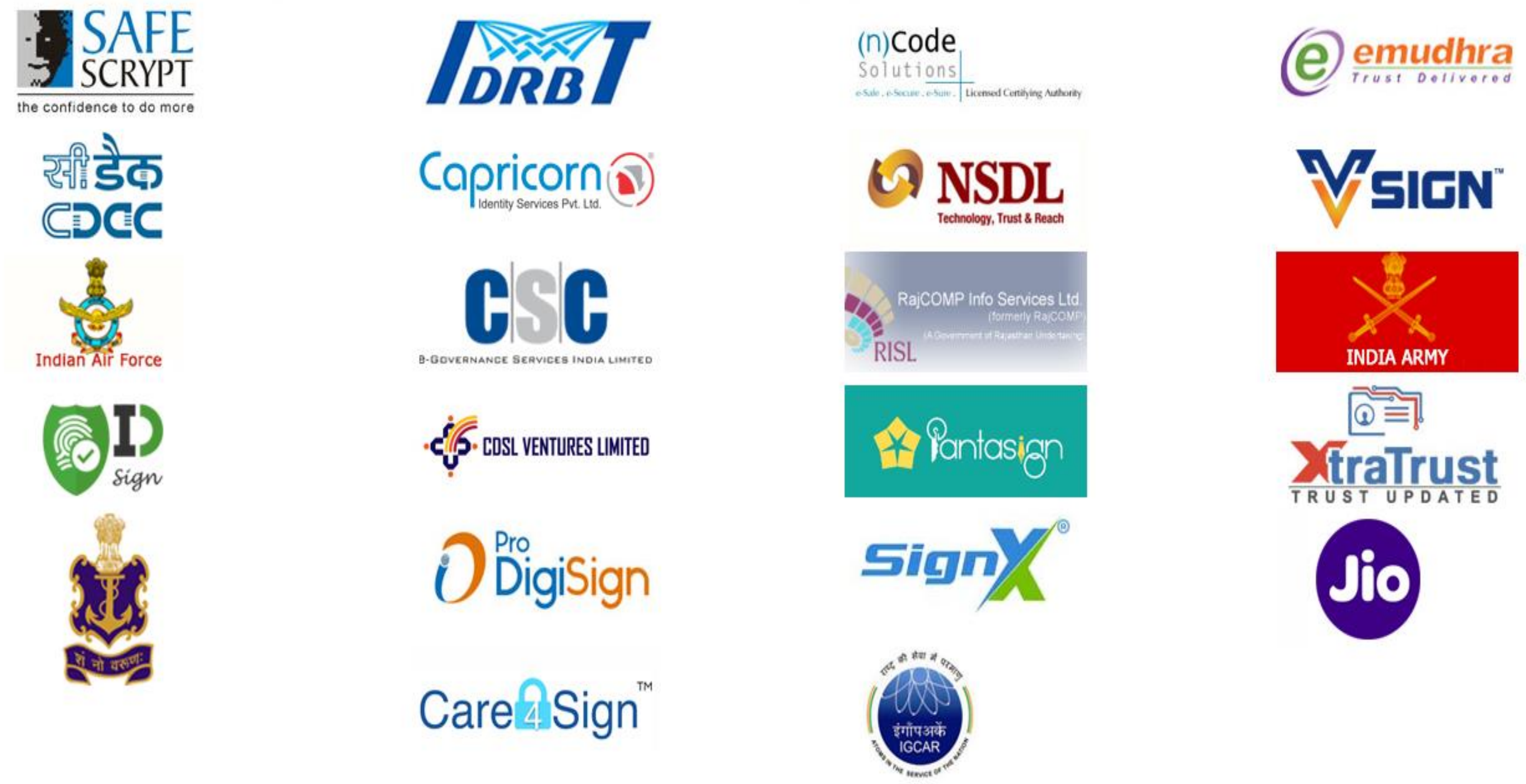
CCA India Licensed CAs – 22 Nos.

DSC Providers (17 CAs)

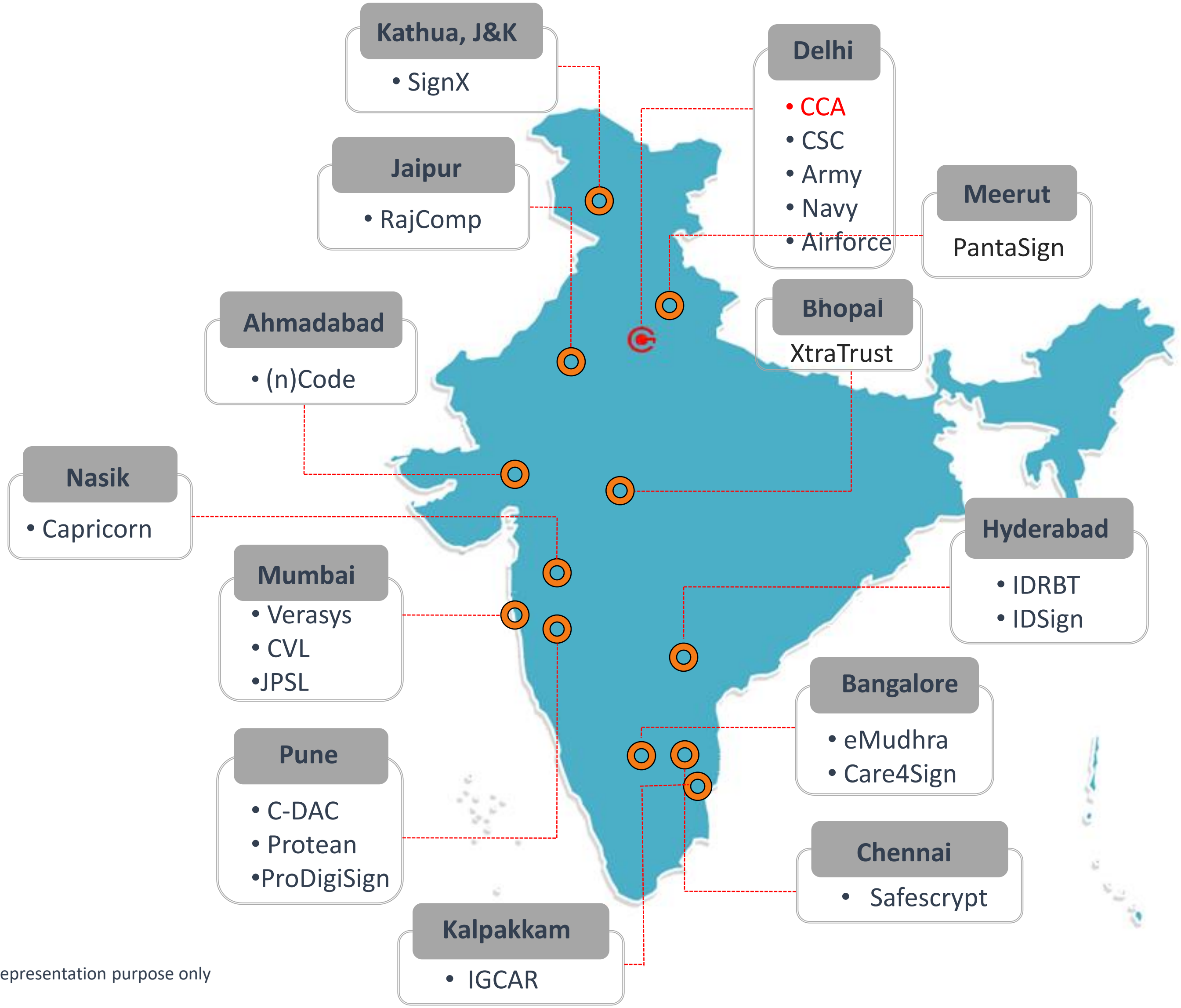
- Dongle/Crypto token based DSC

eSign Service Providers (18 ESPs)

- Online electronic signature service


SAFE SCRYPT
the confidence to do more
सी-डैक 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 TM
(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
इंगांपअकें
IGCAR
emudhra
Trust Delivered
VSIGN
INDIA ARMY
XtraTrust
TRUST UPDATED
Jio

Licensed Certifying Authorities



Kathua, J&K
- SignX

Jaipur
- RajComp

Ahmadabad
- (n)Code

Nasik
- Capricorn

Mumbai
- Verasys
- CVL
- JPSL

Pune
- C-DAC
- Protean
- ProDigiSign

Kalpakkam
- IGCAR

Delhi
- CCA
- CSC
- Army
- Navy
- Airforce

Meerut

PantaSign

Bhopal

XtraTrust

Hyderabad
- IDRBT
- IDSign

Bangalore
- eMudhra
- Care4Sign

Chennai
- Safescrypt

Note: Map not as per scale & representation purpose only

Licensed CAs

Govt/Semi Govt Sector

○ C-DAC
○ CSC eGovernance
○ RajCOMP Info Services Ltd. CA
○ IGCAR

Banking Sector

○ IDRBT

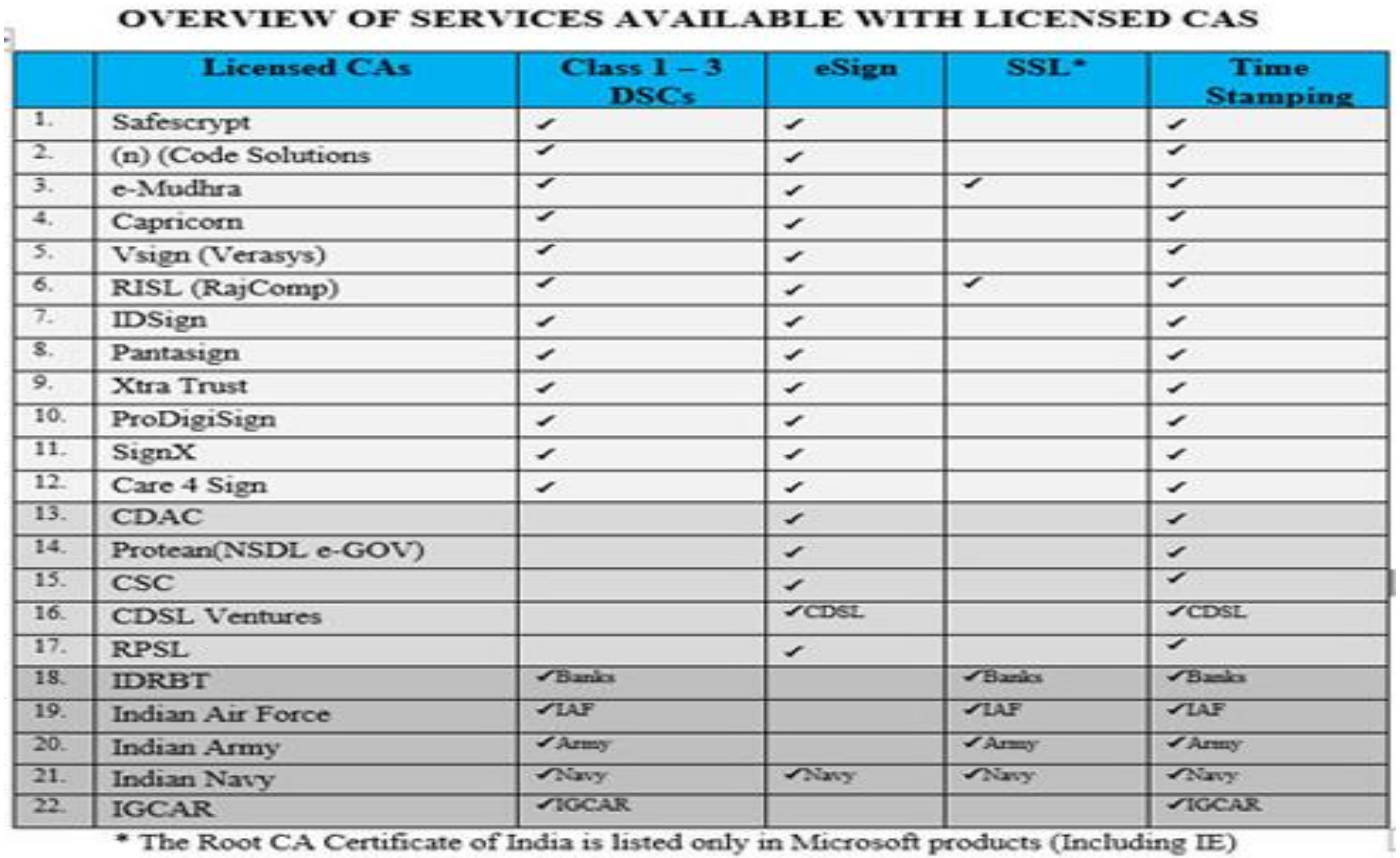
Private Sector

○ Safescrypt
○ eMudhra
○ (n)Code
○ Capricorn
○ PantaSign
○ Protean (formerly NSDL)
○ Verasys
○ IDSign
○ CDSL Ventures Ltd.(CVL) CA
○ XtraTrust
○ ProDigiSign
○ SignX
○ Care4Sign
○ JPSL

Defence Sector

○ India Air force
○ Indian Army
○ Indian Navy

CAs Services Overview



OVERVIEW OF SERVICES AVAILABLE WITH LICENSED CAS

	Licensed CAs	Class 1 – 3 DSCs	eSign	SSL*	Time Stamping
1.	Safescrypt	✓	✓		✓
2.	(n) (Code Solutions	✓	✓		✓
3.	e-Mudhra	✓	✓	✓	✓
4.	Capricorn	✓	✓		✓
5.	Vsign (Verasys)	✓	✓		✓
6.	RISL (RajComp)	✓	✓	✓	✓
7.	IDSign	✓	✓		✓
8.	Pantasign	✓	✓		✓
9.	Xtra Trust	✓	✓		✓
10.	ProDigiSign	✓	✓		✓
11.	SignX	✓	✓		✓
12.	Care 4 Sign	✓	✓		✓
13.	CDAC		✓		✓
14.	Protean(NSDL e-GOV)		✓		✓
15.	CSC		✓		✓
16.	CDSL Ventures		✓CDSL		✓CDSL
17.	RPSL		✓		✓
18.	IDRBT	✓Banks		✓Banks	✓Banks
19.	Indian Air Force	✓IAF		✓IAF	✓IAF
20.	Indian Army	✓Army		✓Army	✓Army
21.	Indian Navy	✓Navy	✓Navy	✓Navy	✓Navy
22.	IGCAR	✓IGCAR			✓IGCAR

* The Root CA Certificate of India is listed only in Microsoft products (Including IE)

eSign: Online Electronic Signature, **DSC**: Dongle/Token based Electronic Signature Certificate, **SSL**: Server Certificate, **TS**: Timestamping Certificate

DSC & eSign Statistics

Year	No. of CA licensed	No. of DSC (in Lakh)	No. of eSign (in Lakh)
2002-13	5	67.90	---
2014	-	25.92	---
2015	1	23.68	5.38
2016	2	40.50	97.94
2017	-	38.64	351.68
2018	1	44.75	198.01
2019	2	46.83	314.82
2020	4	47.20	439.68
2021	2	46.22	984.17
2022	4	51.70	1454.96
2023	1	51.96	2027.38
2024 (till 30th June)	-	25.58	1439.40
Total	22	510.88 (~5.1 Cr)	7313.42 (~73.1 Cr)

Uses of Electronic Signatures

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

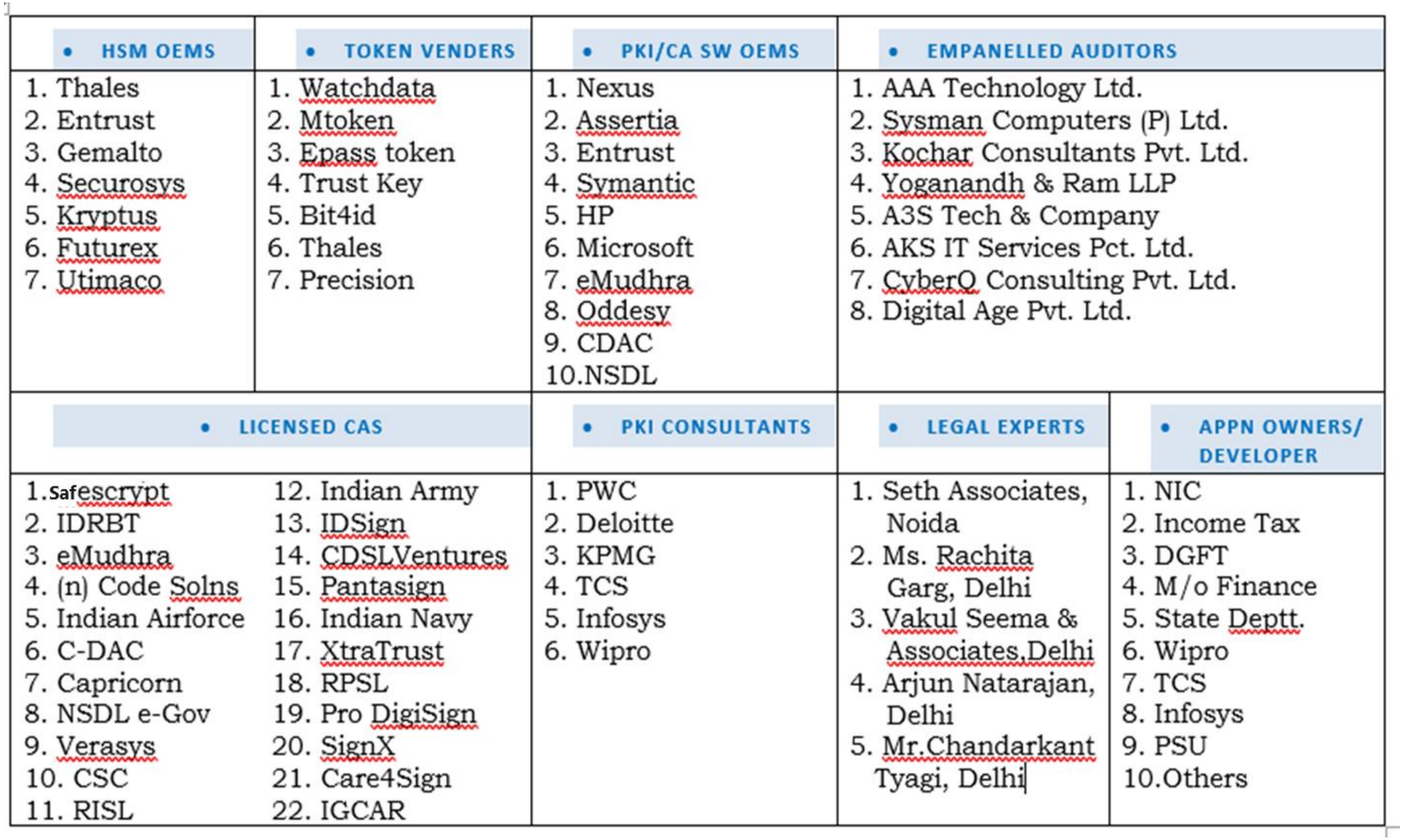
Judicial

- ✓ 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

Players/Stakeholders in PKI Eco System



• HSM OEMS	• TOKEN VENDERS	• PKI/CA SW OEMS	• EMPANELLED AUDITORS
1. Thales	1. Watchdata	1. Nexus	1. AAA Technology Ltd.
2. Entrust	2. Mtoken	2. Assertia	2. Sysman Computers (P) Ltd.
3. Gemalto	3. Epass token	3. Entrust	3. Kochar Consultants Pvt. Ltd.
4. Securosys	4. Trust Key	4. Symantic	4. Yoganandh & Ram LLP
5. Kryptus	5. Bit4id	5. HP	5. A3S Tech & Company
6. Futurex	6. Thales	6. Microsoft	6. AKS IT Services Pct. Ltd.
7. Utimaco	7. Precision	7. eMudhra	7. CyberQ Consulting Pvt. Ltd.
		8. Oddesy	8. Digital Age Pvt. Ltd.
		9. CDAC	
		10.NSDL	

• LICENSED CAS		• PKI CONSULTANTS	• LEGAL EXPERTS	• APPN OWNERS/ DEVELOPER
1.Safescrypt	12. Indian Army	1. PWC	1. Seth Associates, Noida	1. NIC
2. IDRBT	13. IDSign	2. Deloitte	2. Ms. Rachita Garg, Delhi	2. Income Tax
3. eMudhra	14. CDSLVentures	3. KPMG	3. Vakul Seema & Associates,Delhi	3. DGFT
4. (n) Code Solns	15. Pantasign	4. TCS	4. Arjun Natarajan, Delhi	4. M/o Finance
5. Indian Airforce	16. Indian Navy	5. Infosys	5. Mr.Chandarkant Tyagi, Delhi	5. State Deptt.
6. C-DAC	17. XtraTrust	6. Wipro		6. Wipro
7. Capricorn	18. RPSL			7. TCS
8. NSDL e-Gov	19. Pro DigiSign			8. Infosys
9. Verasys	20. SignX			9. PSU
10. CSC	21. Care4Sign			10.Others
11. RISL	22. IGCAR			

CCA’s Initiatives

- ❖ Development of PKI-based Digital Certificates for IoT Device Security
- ❖ Common API Platform
- ❖ Webtrust Compliance to RCAI
- ❖ Indian Browser Open Challenge
- ❖ Secure Post Quantum Cryptography (PQC)
- ❖ Blockchain based DSCs content validation & Storage system
- ❖ Establishment of WebTrust certified SSL Root CCA/CA
- ❖ Next Generation PKI Awareness Program
- ❖ Analytics Dashboard & Portal for Licensing & Audit of CAs
- ❖ Mutual Recognition Framework & Cross Certification

Thank you!

Controller of Certifying Authorities
Electronics Niketan,
6 CGO Complex, Lodhi Road,
New Delhi - 110003

Website : https://www.cca.gov.in
E-mail Id: deepak.sukhija@cca.gov.in