

Legal & Technology perspectives in India- Public Key Infrastructure

Harshprabha Aggrawal, Scientist 'G'



Controller of Certifying Authorities

Department of Electronics and Information Technology
Ministry of Communications and Information Technology



IT Act, 2000

- ❖ Based on UNCITRAL Model Law on E-Commerce (Jan-97)
- ❖ India Adopted in early stages

Information Technology Act

Date on which provisions came in to force : **17th Oct 2000**

Information Technology (Amendment) Act

Date on which provisions came in to force : **27th Oct 2009**



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) appointed under Section 17 (Chapter VI – Regulation of Certifying Authorities) of the IT Act, 2000
- Digital signature to be effected by use of asymmetric crypto system and hash function
- Appointment of Certifying Authorities and Controller of Certifying Authorities, including recognition of foreign Certifying Authorities

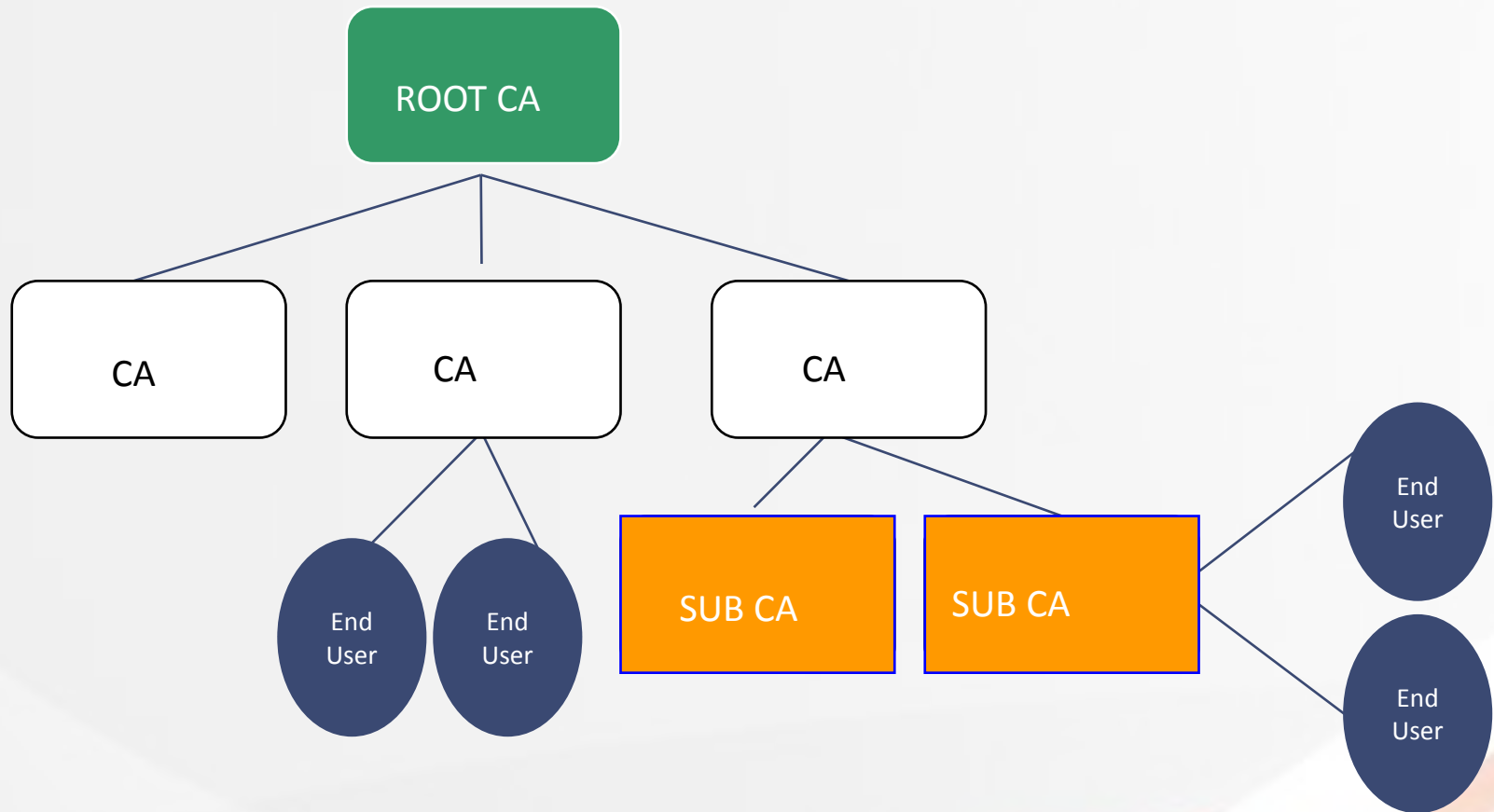


PKI in India

- Controller of Certifying Authority CCA operates the Root certifying authority, responsible for regulating Certifying Authorities (CAs).
- Controller certifies the association of CA with his public key.
- Certifying Authority (CA) is the trusted authority responsible for issuing Digital Signature Certificate.
- CA certifies the association of an individual with his/her public key.



India PKI Model





Section 5: Legal recognition of electronic signature

- Where any law provides that

- Information or any other matter shall be authenticated by affixing the signature or
- any document should be signed or
- bear the signature of any person then,

– notwithstanding anything contained in such law

- such requirement shall be deemed to have been satisfied,
- if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.



Functions of CCA

- exercising supervision over the activities of the Certifying Authorities;
- certifying public keys of the Certifying Authorities;
- laying down the standards to be maintained by the Certifying Authorities;
- specifying the conditions subject to which the Certifying Authorities shall conduct their business;



Functions of CCA

- specifying the form and content of a Digital Signature Certificate and the key;
- specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them;
- facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems;
- specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers;



Functions of CCA

- resolving any conflict of interests between the Certifying Authorities and the subscribers;
- laying down the duties of the Certifying Authorities;
- maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.



Information Technology Certifying Authorities Rules – Salient features

- Digital Signature creation and verification
- Licensing criteria for Certifying Authorities
- Cross certification
- Issue / Renewal / Suspension / Refusal of licence
- Digital Signature Certificate – Generation / Issue / Management / Archival / Revocation / Compromise
- Audit of Certifying Authority operation
- Information Technology Security Guidelines
- Security Guidelines for Certifying Authorities



Regulation of Certifying Authorities (CA)

- Licensing Certifying Authorities (CAs) under section 21 of the IT Act and exercising supervision over their activities.
- Controller of Certifying Authorities as the “Root” Authority certifies the technologies and practices of all the Certifying Authorities licensed to issue Digital Signature Certificates
- Addressing the issues related to the licensing process including:
 - Approving the Certification Practice Statement(CPS);
 - Auditing the physical and technical infrastructure of the applicants through a panel of auditors maintained by the CCA.



Regulation of Certifying Authorities

- There are eight licensed Certifying Authorities issuing Digital signature Certificates (DSC)
- More than 10 million Digital signature Certificates were issued by the licensed Certifying Authorities till December 2015



Licensed CAs

- ❖ SIFY Technologies
- ❖ National Informatics Centre (NIC)
- ❖ Institute for Development & Research in Banking Technology (IDRBT)
- ❖ Tata Consultancy services (TCS)
- ❖ (n)Code Solutions (GNFC)
- ❖ eMudhra Consumer Services (eMudhra)
- ❖ Indian Airforce (IAF)
- ❖ CDAC Pune



Classes of Certificates


Assurance Level	Assurance	Applicability
Class 0	This certificate shall be issued only for demonstration / test purposes.	This is to be used only for demonstration / test purposes.
Class 1	Class 1 certificates shall be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.	This provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance.
Class 2	These certificates will be issued for both business personnel and private individuals use. These certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases.	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial
Class 3	This certificate will be issued to individuals as well as organizations. As these are high assurance certificates, primarily intended for e-commerce applications, they shall be issued to individuals only on their personal (physical) appearance before the Certifying Authorities.	This level is relevant to environments where threats to data are high or the consequences of the failure of security services are high. This may include very high value transactions or high levels of fraud risk.



Certificate

Paper

Electronic

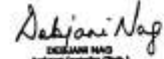



 भारत सरकार
GOVERNMENT OF INDIA
प्रमाणन प्राधिकारी नियंत्रक
CONTROLLER OF CERTIFYING AUTHORITIES



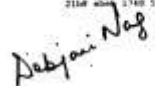
प्रमाणित किया जाता है कि बैंकिंग प्रौद्योगिकी विकास एवं अनुसंधान संस्थान
केसल हिल्स, रोड नं. १, मासब टैंक, हैदराबाद - ५०००५६.
 को मूलन संश्लेषित अधिनियम २००० में अधिन, ७ जुलाई, २००१ की धारा ११(१) के अन्तर्गत के रूप में प्रमाणित किया गया है। यह प्रमाणित किया गया है कि
 अधिनियम २००० की धारा २१ के अन्तर्गत, प्रमाणन प्राधिकारी के रूप में कार्य करने के लिए आवश्यक शर्तों को पूरा करता है। यह प्रमाणित किया गया है, और
 यह अवधि, २००२ को प्रमाणित किया गया है।

This is to certify that INSTITUTE FOR DEVELOPMENT AND RESEARCH IN BANKING TECHNOLOGY
located at CASTLE HILLS, ROAD NO. 1, MASSAB 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 in 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.


 ASHWANI KUMAR
 Assistant Controller (Tech.)
 Department of Information Technology
 Government of India (Ministry of Information & Public Relations)
 8, C.A.S.I. Complex, New Delhi-110 002


 LAXMI RAJ GUPTA
 Assistant Controller (Tech.)
 Department of Information Technology
 Government of India (Ministry of Information & Public Relations)
 8, C.A.S.I. Complex, New Delhi-110 002

प्रमाणित किया जाता है कि
 प्रमाणित किया गया है कि



Certificate

General Details Certification Path

Show: <All>

Field	Value
Serial number	27 48
Signature algorithm	sha1RSA
Issuer	CCA India, India PKI, IN
Valid from	Tuesday, August 06, 2002 12:...
Valid to	Sunday, August 05, 2007 12:...
Subject	Andhra Pradesh, idrbtca@idrb...
Public key	RSA (2048 Bits)
Subject Key Identifier	4d 9c 24 7d 81 9b d9 8d

```

30 82 01 0a 02 82 01 01 00 d2 82 69 d5 f3
27 0d 52 71 0d af 77 a7 ad 17 2c 6c 82 93
bc 6d d9 0e 2b 71 77 88 e0 b8 be f9 3b 6c
6e 15 f0 0a 33 a6 8f 78 78 bd 81 c9 a6 df
f0 67 37 91 e5 5a a3 78 f2 a3 d1 4e 8b f0
2e 15 d5 41 b7 0c 39 64 59 54 7b 45 2e 1a
10 9b f8 e9 5e d4 c1 7b c5 7b 23 64 d0 c5
45 36 bc 9f 78 d7 ee 37 0f fa 99 52 fe b5
56 56 88 66 6a 00 9f b4 89 60 d9 5c 46 87
  
```

[Edit Properties...](#) [Copy to File...](#)

OK





Digital Signature Enabled Applications

- 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



Digital Signature Enabled Applications

E-Procurement

- Indian Farmers Fertiliser Cooperative Limited (IFFCO)
- Directorate General of Supplies & Disposals (DGS&D)
- Oil and Natural Gas Corporation (ONGC)
- Gas Authority of India Ltd (GAIL)
- Air-India, Indian Railways etc.

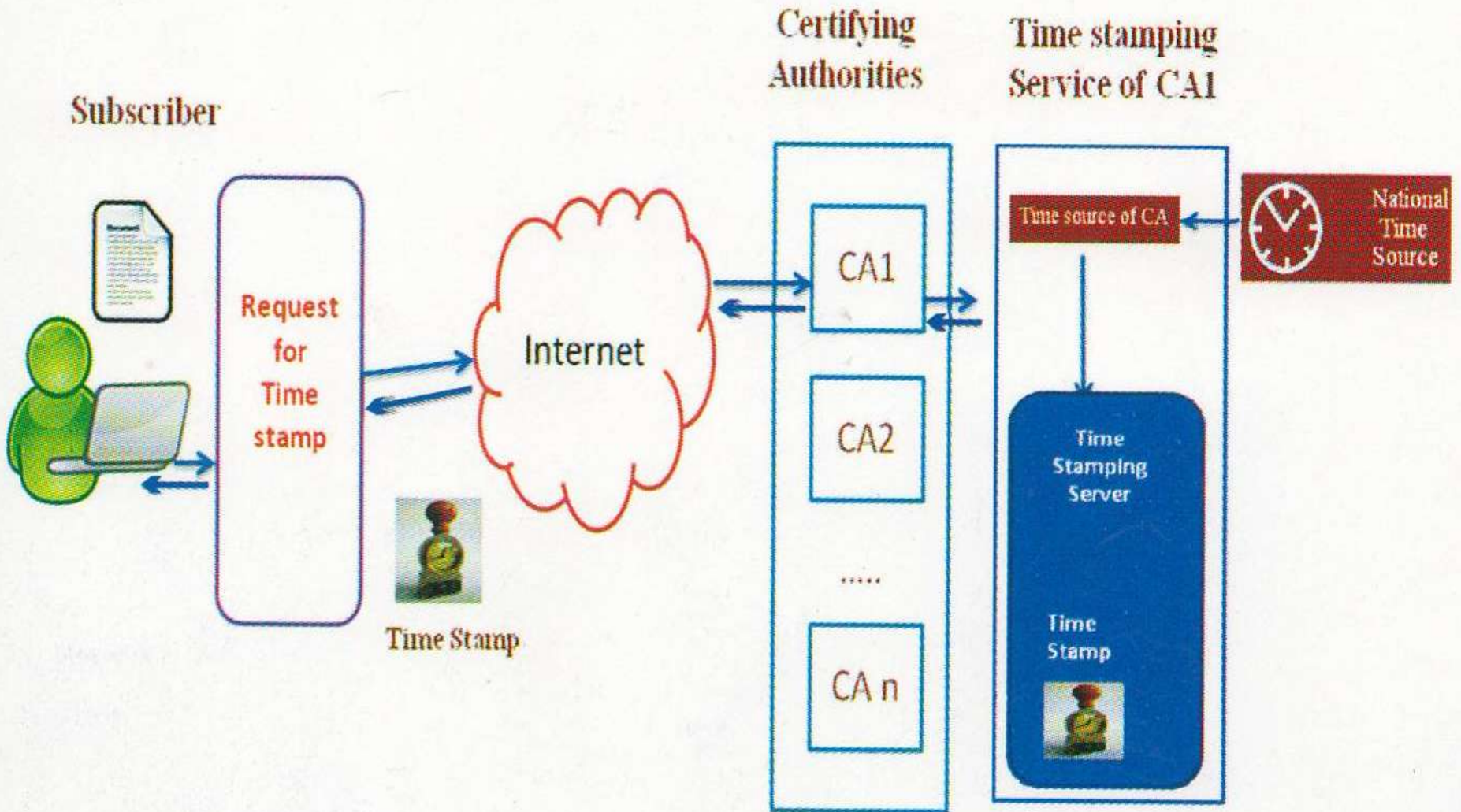


Time Stamping Service

- The IT (CA) Regulations mandate provisioning of Time Stamping Services by Certifying Authorities (CA) who issue Digital Signature Certificates(DSC) under the Information Technology (IT) Act, 2000
- Digitally signed **Time stamps** are based on time derived from National time source
- Time stamps can be verified to establish the time when a document or transaction was created.



Time Stamping





Time Stamping Service - Applications

- eProcurement
- eTendering
- ePatent and Copyright
- eFiling of statutory returns
- eBanking
- eMail
- eContracts and other electronic documents



eSign

Online electronic signature service



eSign

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



Empanelled eSign service provider

- eMudhra CA
- CDAC CA
- nCode (in the process)



Public Key Infrastructure

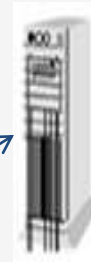
Registration Authorities

Authorize the binding between Public Key and Certificate Holder



Relying Party Application

Validate Signatures and certificate paths



Internet

Certificate Holder
Subscriber



Certifying Authorities

Issuers



Web Server



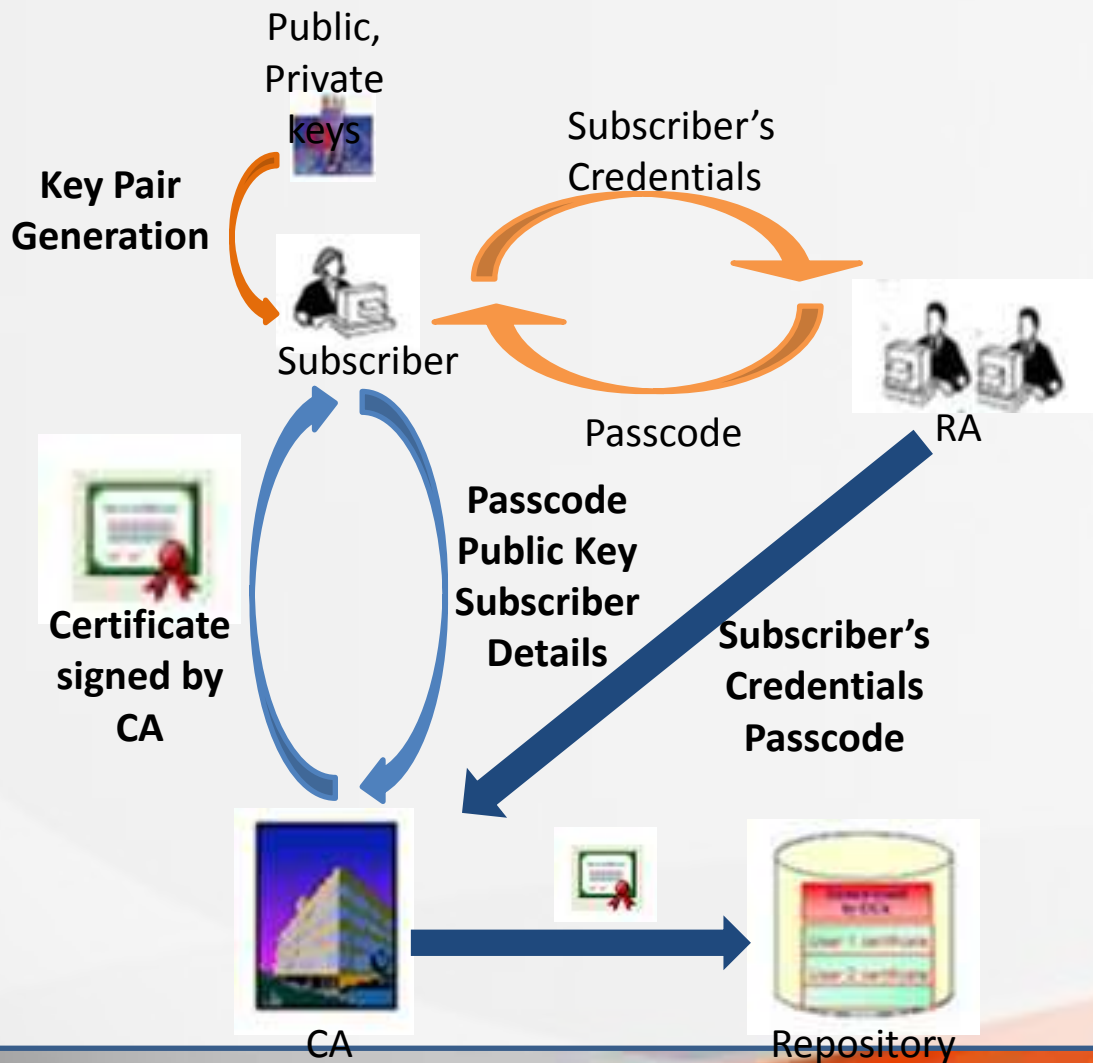
Repository

Store and distribute certificate & status: expired, revoked, etc.





Issuance of DSC



- 1 Subscriber provides Proof of Identity
- 2 RA verifies credentials basis assurance level
- 3 RA send passcode to subscriber
- 4 Subscriber creates Public private key pair
- 5 Submit Public Key with own details to CA
- 6 CA certifies public key of subscriber
- 7 CA publishes certificate in repository
- 8 CA provides 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 (digitally signed and encrypted) to service providers.

Thanking you

[Harshprabha Aggrawal](#)
harsh@cca.gov.in



Controller of Certifying Authorities

Electronics Niketan,
6 CGO Complex, Lodhi Road,
New Delhi - 110003

Website : www.cca.gov.in