

Public Key Infrastructure & eSign in India

September 2015

Vikash Chourasia

CII Chandigarh



Controller of Certifying Authorities

Department of Electronics and Information Technology

Ministry of Communications and Information Technology



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 of the IT Act, 2000 to promote the use of Digital Signatures for e-Governance & e-Commerce.



Functions of CCA

- 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
- Laying down the standards to be maintained by the CAs,
- 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.

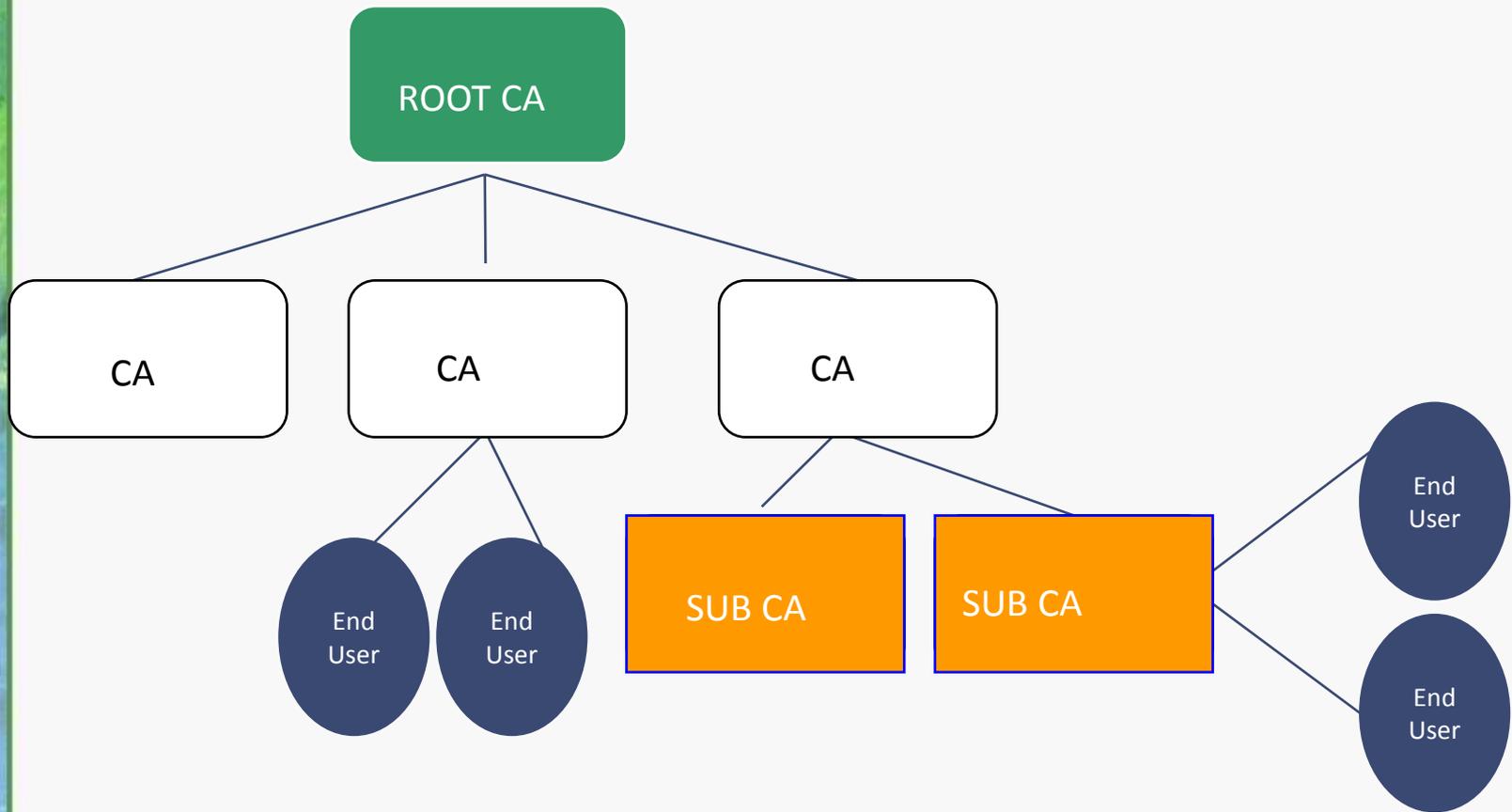


Regulation of Certifying Authorities

- CCA promotes the growth of E-Commerce and E-Governance through the wide use of Electronic (Digital) signatures
- There are seven licensed Certifying Authorities issuing Digital signature Certificates (DSC)
- More than 90,00,000 Digital signature Certificates were issued by the licensed Certifying Authorities till date



India PKI Model





Controller of Certifying Authorities (CCA)

Certifying Authorities(CA) licensed by CCA to issue Digital Signature Certificates(DSC)

- 1) Sify
- 2) IDRBT
- 3) NIC
- 4) TCS
- 5) (n)Code Solutions
- 6) eMudhra
- 7) IAF



IDRBT Certificate

Paper

Electronic


 2002 0003 050807 000 0000 9999

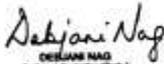
भारत सरकार
GOVERNMENT OF INDIA
प्रमाणन प्राधिकारी नियंत्रक
CONTROLLER OF CERTIFYING AUTHORITIES



प्रमाणित किया जाता है कि बैंकिंग प्रौद्योगिकी विकास एवं अनुसंधान संस्थान
 केसल हिल्स, रोड नं. १, मासब टैंक, हैदराबाद - ५०००५८.

को प्रमाणन प्राधिकारी अधिनियम २००० के अंतर्गत, ० जुलाई, २००१ को जारी अधिनियम के अंतर्गत के रूप में स्वीकृत किया गया था। यह प्रमाणन प्रमाण प्रमाणन प्राधिकारी अधिनियम २००० की धारा २१ के अंतर्गत, प्रमाणन प्राधिकारी के रूप में जारी करने के लिए प्रमाणन प्रदान किया गया है। यह प्रमाणन प्रमाणन प्राधिकारी अधिनियम २००० के अंतर्गत, २००२ के अंतर्गत जारी किया गया है।

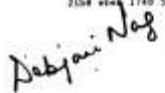
This is to certify that INSTITUTE FOR DEVELOPMENT AND RESEARCH IN BANKING TECHNOLOGY
 located at CASTLE HILLS, ROAD NO. 1, MASAB TANK, HYDERABAD - 500 057.
 has been granted licence to act as a Certifying Authority, under Section 21 of the IT Act 2000, subject to Terms and Conditions specified as part 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.


ASHWANI NAG
 Additional Controller (Tech.)
 Office of Controller of Certifying Authorities/Bankers of
 Department of Information Technology
 Government of India (CERTIFICATE)/Signatory
 Electronic Offices
 4, G.S.D. Complex, New Delhi-110 004


LEELRAJ GUPTA
 Additional Controller (Tech.)
 Office of Controller of Certifying Authorities
 Department of Information Technology
 Government of India (CERTIFICATE)/Signatory
 Electronic Offices
 4, G.S.D. Complex, New Delhi-110 004

प्रमाणित मुझे
 Public Key

3002 010a 5282 0101 0922 8269 0517 2764 5271 04a1 71a7 0d17 2c4c 8293 0a60 090a 2071 7188 e068 0e7f 064c
 0e13 202a 1340 0178 730d 8109 e84f 0847 3791 a55a a378 12a3 404a 8043 2a35 0541 575c 3964 5954 7045 2a1a
 1076 1840 1e04 c170 c57b 2304 4805 4536 bc9f 7807 ee37 0f2a 9952 1a05 5856 805a 8a95 0d84 8940 d95c 4487
 1843 c38c 33ac 94b7 0a95 164b 211f 3cc4 5257 8a1e 8520 6576 905d 6295 1716 874a 8a82 a25c 0a50 1c49 1879
 023a 8e2e 007d 0a0d 0443 194d 0b93 5240 20a3 784b 4029 4526 7061 0a7a 0a1a c17a 7028 804c 1903 172a 044d
 814e 0a0a 014d 0a4c 248c a04d 9f4a 0385 7512 4338 1b01 a081 716e 0a08 7010 7ea3 8313 8a1e 7783 1288 2c4a
 2184 0a0a 1740 5724 2488 303f 8902 0301 0001


Ashwani Nag

Certificate

General Details Certification Path

Show: <All>

Field	Value
Public key	RSA (2048 Bits)
Subject Key Identifier	4d 9c 24 7d 81 9b d9 8d
Authority Key Identifier	KeyID=4a c6 09 14 27 f6 5e e7
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Basic Constraints	Subject Type=CA, Path Lengt...
Thumbprint algorithm	sha1
Thumbprint	3c c1 0e 7b 4a 3f 13 c2 6e cb ...

3c c1 0e 7b 4a 3f 13 c2 6e cb 4d 16 50 a1 e0
 b4 d0 5b 70 8c

Edit Properties... Copy to File...

OK



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.	This provides a basic level of assurance These are given on soft tokens.
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. Address proof and Identity Proof are required along with the application form.	This level is relevant to environments where risks and consequences of data compromise are moderate. These are issued on hardware tokens.
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. These are issued on hardware tokens.



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)
- Court Application



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.



Promoting the use of Digital Signatures

Awareness creation

Advertisements in leading newspapers regarding :

- The issuance process for Digital Signature Certificates
- The dos-and-dont's for using Digital Signatures



Promoting the use of Digital Signatures

Awareness creation

Targeted workshops/meetings for specific sectors

Finance

Procurement

Trading Community

Income Tax

Customs

Judiciary

Industry

Government



Promoting the use of Digital Signatures

- Working with RBI & IBA towards facilitating Digital Signatures for Internet Banking



DSC validation

- Provide certificate validation services based on the Online Certificate Status Protocol (OCSP) in accordance with RFC 2560
- White Listing of DSCs issued
- Validation of trust path leading up to the Root
- According legal validity to other PKI based signatures (XML, CMS, ..)



Incorporation of CCAs Root Certificate in Browsers & other products

- Microsoft – commenced in 2009
- Adobe – in 2015
- Mozilla, java - in progress



Mutual recognition of other electronic Signature regimes

For a Digital Signature Certificate issued by a Foreign Certifying Authority to be recognized in India, gazette Notification containing two sets of Regulations have been issued.

- Foreign Certifying Authorities operating under a PKI Regulatory Authority comparable to that in India.
- Foreign Certifying Authorities which are not operating under a PKI Regulatory Authority.

- ***MoU for former and application for latter?***

Enabling Digital Signatures on Mobile phones

- Hardware based
 - Cryptographic SIM cards
- Software based
 - Through APPs incorporating cryptographic algorithms



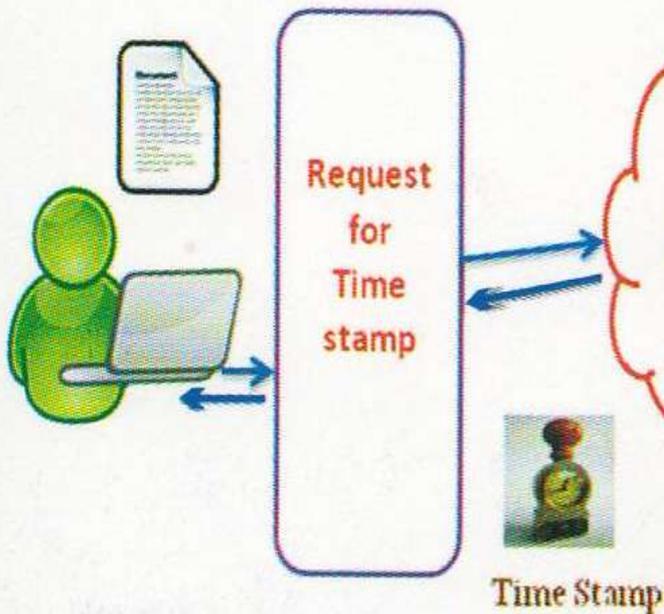
Time Stamping Service

- 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.

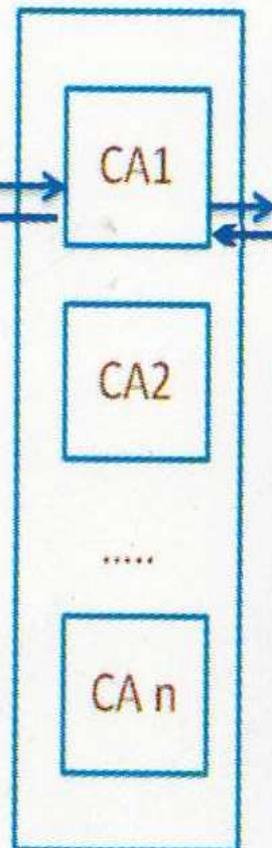


Time Stamping

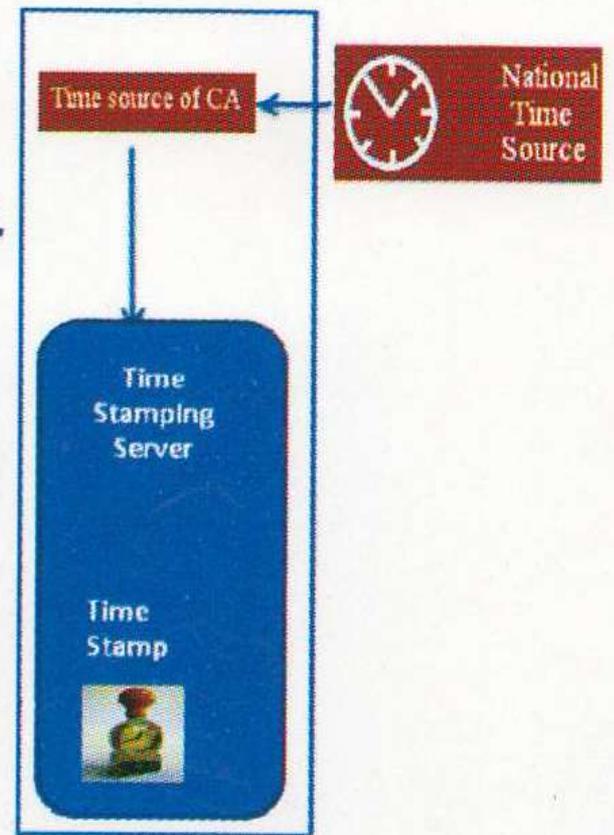
Subscriber



Certifying Authorities



Time stamping Service of CA1





Time Stamping Service - Benefits

- Accurate time in conformance with Government Guidelines
- Digitally signed time stamps – verifiable in future
- Assured Integrity and Non-repudiability
- Electronic Notary
- Fraud detection
- Time Stamped content is protected from public exposure
- The only legally acceptable time stamping service



Time Stamping Service - Applications

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



Challenges in scaling up usage of electronic Signatures

- Personal digital signature requires person's identity verification and issuance of USB dongle having private key, secured with a password/pin.
- Current scheme of physical verification, document based identity validation, and issuance of physical dongles does not scale to a billion people.
- The major cost of the DSC is found to be the verification cost. Certifying Authorities engage Registration Authorities to carry out the verification of verification of credentials prior to issuance of certificate.
- Physical USB Dongle compliant to mandated standards also adds to the cost.
- Relying on the DSC applicant's information already available on the public database is an alternate to Manual verification. UIDAI provides one such alternative.

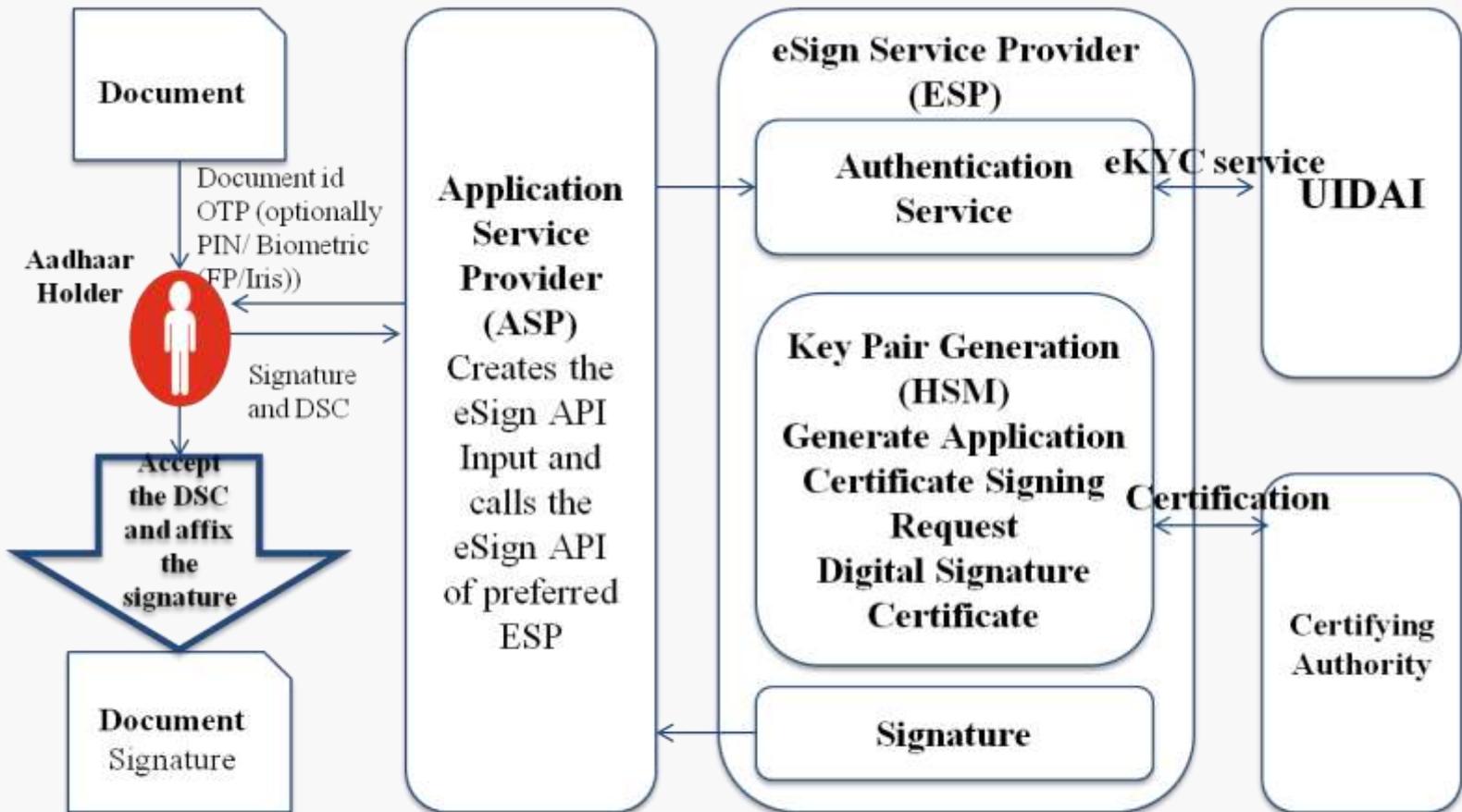


The Unique Identification Authority of India (UIDAI)

- The Unique Identification Authority of India (UIDAI) has been established with the mandate of providing a Unique Identification Number (Aadhaar Number) to all residents.
- During enrolment, the following data is collected:
 - Demographic details such as the name of the resident, address, date of birth, and gender;
 - Biometric details such as the fingerprints, iris scans, and photograph; and
 - Optional fields for communication of such as the mobile number and email address.



eSign overview



HSM – Hardware Security Module

OTP – One Time Password

ESP – eSign Service Provider

ASP – Application Service Provider

eKYC – electronic Know Your Customer

DSC – Digital Signature Certificate

FP – Finger Print

UIDAI – Unique Identification Authority of India

Use Cases- eSign Online Electronic Signature Services

- ✓ eSign online Electronic Signature Service can be effectively used in scenarios where signed documents are required to be submitted to service providers – Government, Public or Private sector.
- ✓ The agencies which stand to benefit from offering eSign online electronic signature are those that accept large number of signed documents from users.

Use Cases- eSign Online Electronic Signature Services

Digital Locker	✓ Self attestation
Tax	✓ Application for ID, e-filing
Financial Sector	✓ Application for account opening in banks and post office
Transport Department	✓ Application for driving licence renewal, vehicle registration
Various Certificates	✓ Application for birth, caste, marriage, income certificate etc
Passport	✓ Application for issuance, reissue
Telecom	✓ Application for new connection
Educational	✓ Application forms for course enrollment and exams
Member of Parliament	✓ Submission of parliament questions

Thanking you

Vikash Chourasia

vikash@cca.gov.in



Controller of Certifying Authorities

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

Website : www.cca.gov.in

