Public Key Infrastructure & eSign in India

November 2015

Vikash Chourasia

CDAC Noida

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.

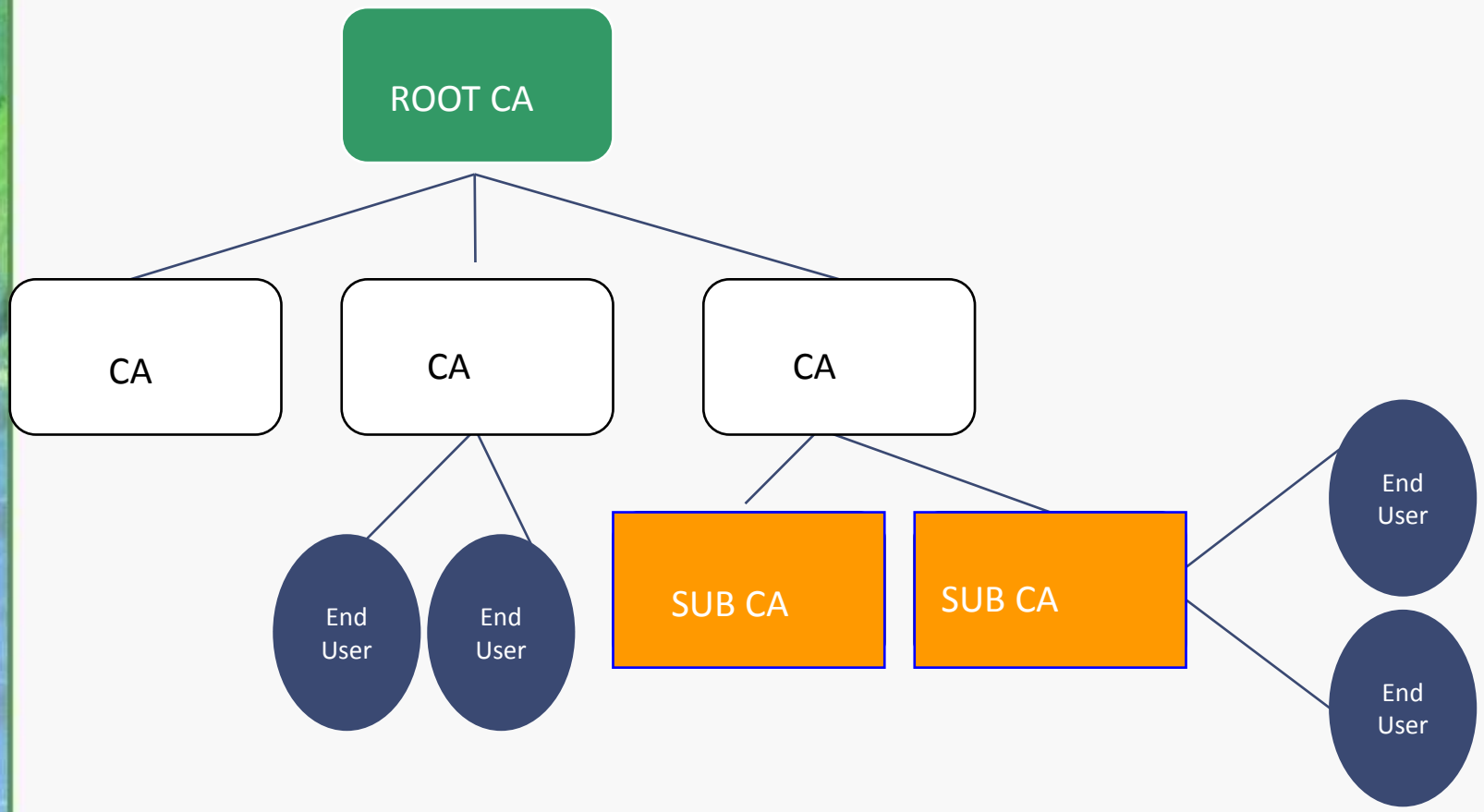
Functions of CCA

- 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



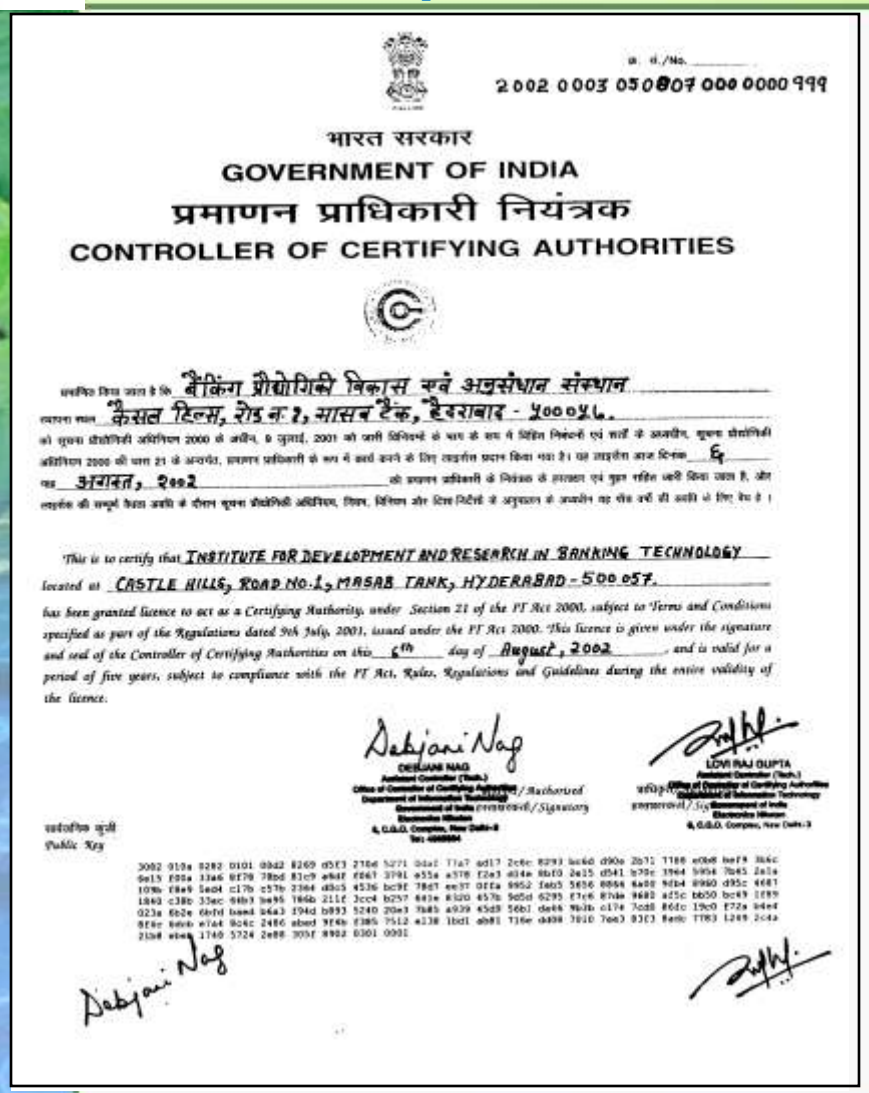
Controller of Certifying Authorities (CCA)

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



2002 0003 050807 000 0000 999

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

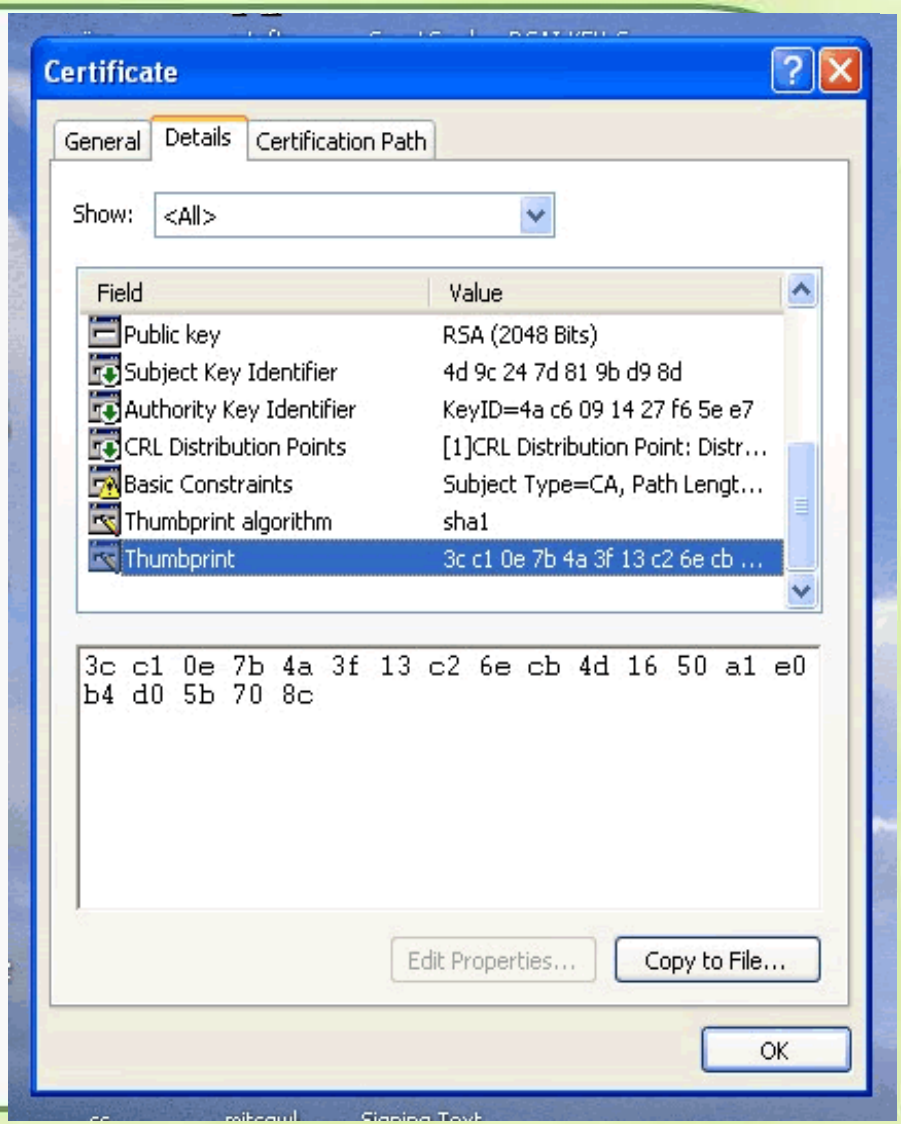
बैंकिंग प्रौद्योगिकी विकास एवं अनुसंधान संस्थान
कैसल हिल्स, रोड नं १, मासब टैंक, हैदराबाद - ५०० ०५७.
अगस्त, २००२

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
LOVI RAJ GUPTA

Public Key

Electronic



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.

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.

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

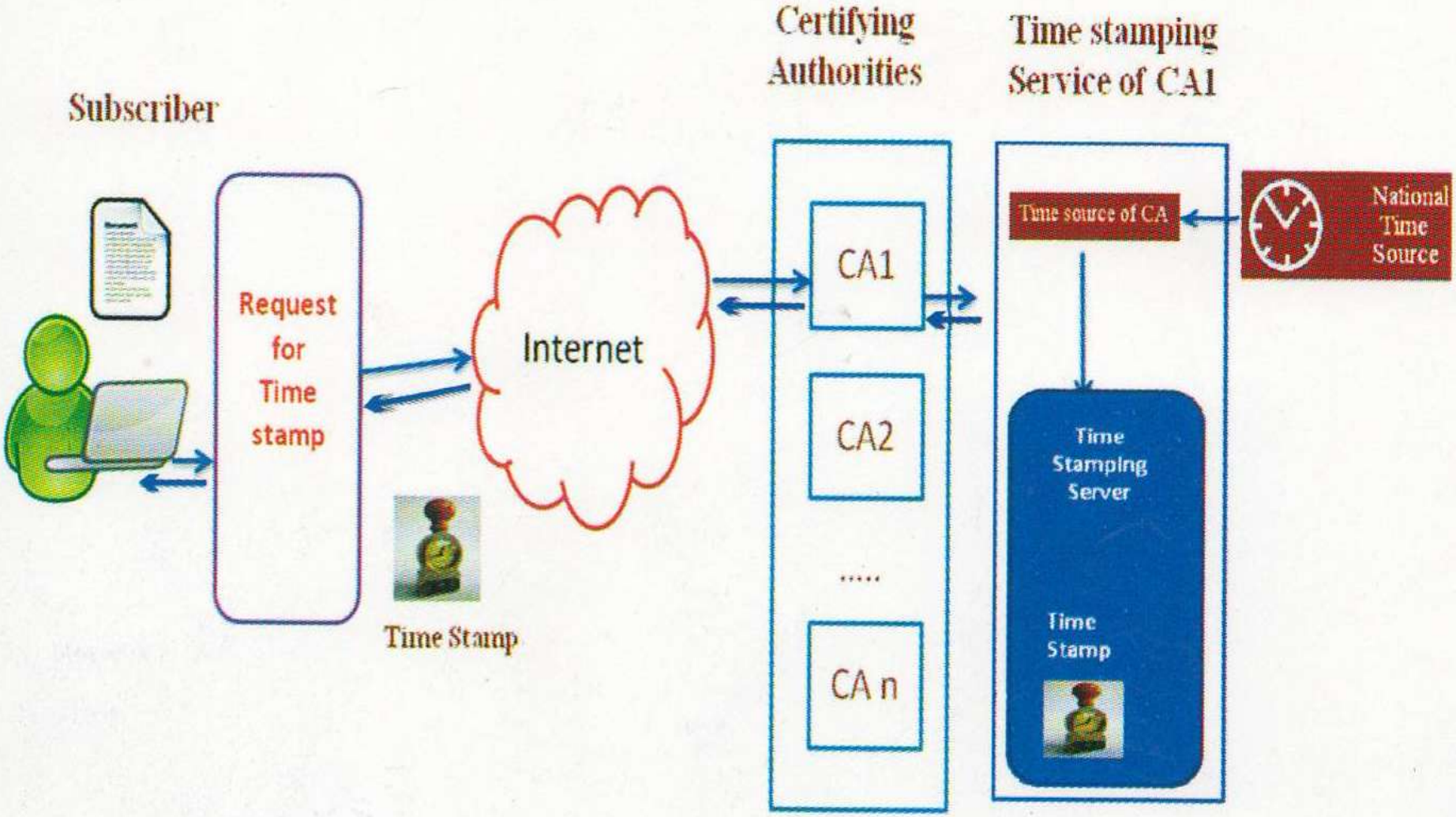
Thanking you

Vikash Chourasia
vikash@cca.gov.in

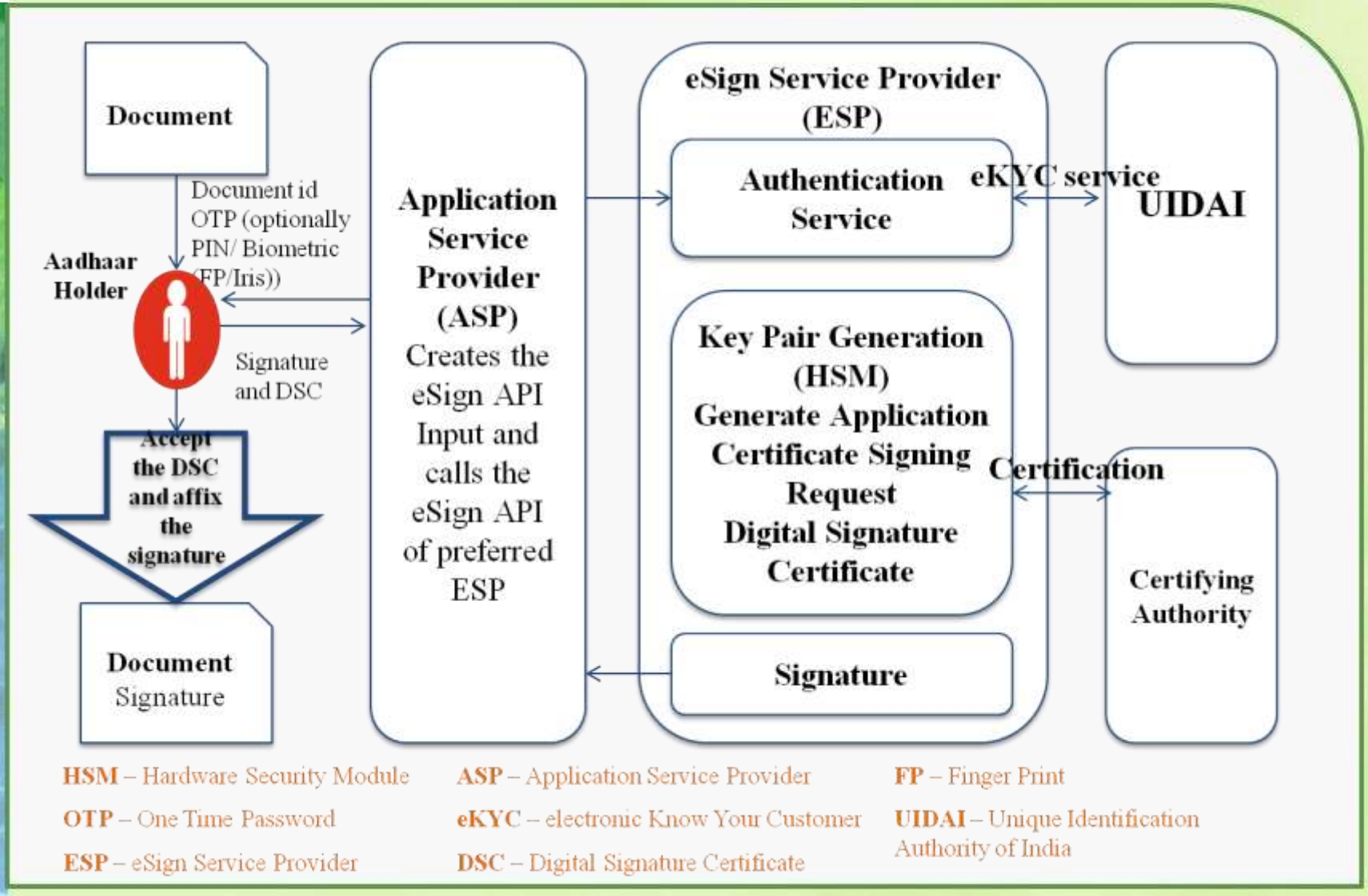
Controller of Certifying Authorities
Electronics Niketan,
6 CGO Complex, Lodhi Road,
New Delhi - 110003

Website : www.cca.gov.in

Time Stamping



eSign overview



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

eSign

Online electronic signature service

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.

The Unique Identification Authority of India (UIDAI)

The UIDAI offers an authentication service that makes it possible for residents to authenticate their identity

- Biometrically
- or through One Time Password (OTP) sent to the registered mobile phone or e-mail address

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 (electronically signed and encrypted) to service providers.

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

eSign - Benefits

❖ Save cost and time	❖ Aadhaar e-KYC based authentication
❖ Improve User Convenience	❖ Mandatory Aadhaar ID
❖ Easy to apply Digital Signature	❖ Biometric or OTP (optionally with PIN) based authentication
❖ Verifiable Signatures and Signatory	❖ Flexible and fast integration with application
❖ Legally recognized	❖ Suitable for individual, business and Government
❖ Managed by Licensed CAs	❖ API subscription Model
❖ Privacy concerns addressed	❖ Integrity with a complete audit trail
❖ Simple Signature verification	❖ Immediate destruction of keys after usage
❖ Short validity certificates	❖ No key storage and key protection concerns

Assurance levels

- OTP based eKYC
- Biometric based eKYC

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

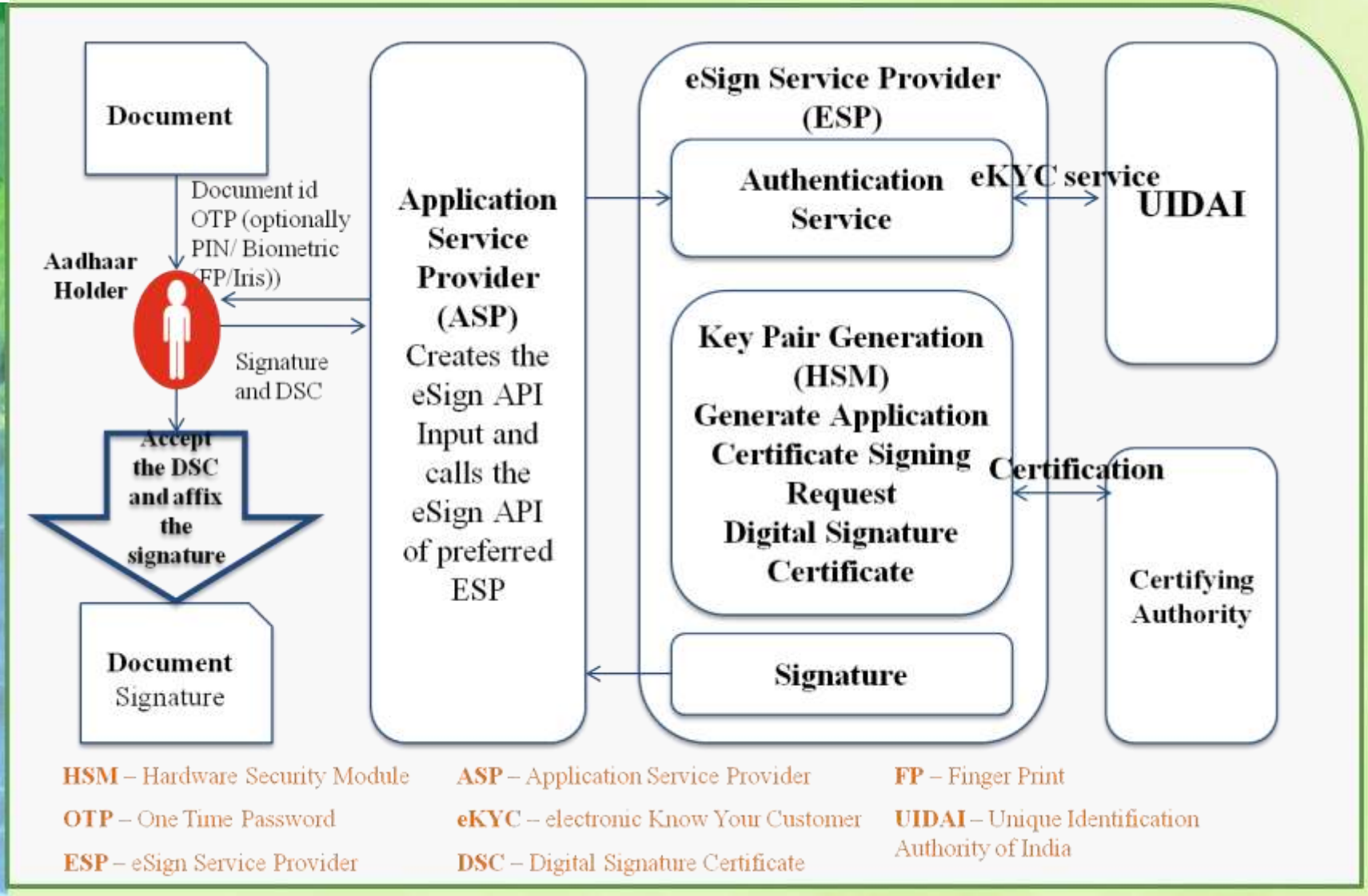
Addressing scalability through eSign

- An Aadhaar holder can sign any document with just Aadhaar biometric/OTP authentication requiring no physical device or paper-based application forms and supporting documents
- Authentication of the signer is carried out using eKYC of Aadhaar,
- the signature on the document is carried out on a backend server of the e-Sign provider.
- The service can be run by a trusted third party service provider - To begin with the trusted third party service shall be offered only by Certifying Authorities.

Addressing scalability through eSign

- The eSign facilitates issuing a Signature Certificate and performing Signing of requested data by authenticating Aadhaar holder.
- The certificate issued through eSign service will have a limited validity period and is only for one-time signing of requested data, in a single session.
- This service authenticates the person, does Aadhaar e-KYC, and then electronically signs the input within the e-Sign provider backend. Such scheme allows DSC to be scaled massively and allow many 3rd party applications to use the service via an open API and integrate DSC into their application.

eSign overview



eSign workflow

I At the Application Service Provider (ASP)

1. Asks the end user to sign the document
2. Creates the document hash (to be signed) on the client side
3. Captures Aadhaar number and authentication factor (OTP/OTP+PIN/Biometric)
4. Creates the input API for eSign
5. Calls the eSign API of the eSign provider

eSign workflow

II At the eSign Service Provider (ESP)

6. Validates the calling application input, and then creates the Aadhaar e-KYC input based on Aadhaar e-KYC API specification
7. Invokes the Aadhaar e-KYC API
8. On success, creates a new key pair for that Aadhaar holder
9. Sends public key and eKYC information to the Certifying Authority for certification

eSign workflow

III At the Certifying Authority(CA)

10. Based on the eKYC authentication information received from UIDAI, Digital Signature Certificate is issued and sent to the ESP.

eSign workflow

IV At the eSign Service Provider (ESP)

11. Signs the input document hash using the private key(Note: The original document never leaves the actual computer)
12. Creates an audit trail for the transaction
    - Audit includes the transaction details, timestamp, and Aadhaar e-KYC response
    - This is used for pricing and reporting
13. Sends the e-Sign API response back to the calling application after obtaining end-user acceptance

eSign workflow

V At the Application Service Provider (ASP)

14. Receives the signature from the e-Sign provider

15. Attaches the signature to the document

Stakeholders

Application Service Provider (ASP): An organization or an entity using eSign service as part of their application to electronically sign the content. (Government Departments, Banks and other public or private organizations)

End-User: An Individual using the application of ASP and represents himself/herself for signing the document under the legal framework. the end-user shall also be the 'resident' holding the AADHAAR number and 'applicant/subscriber for digital certificate', under the scope of IT Act.

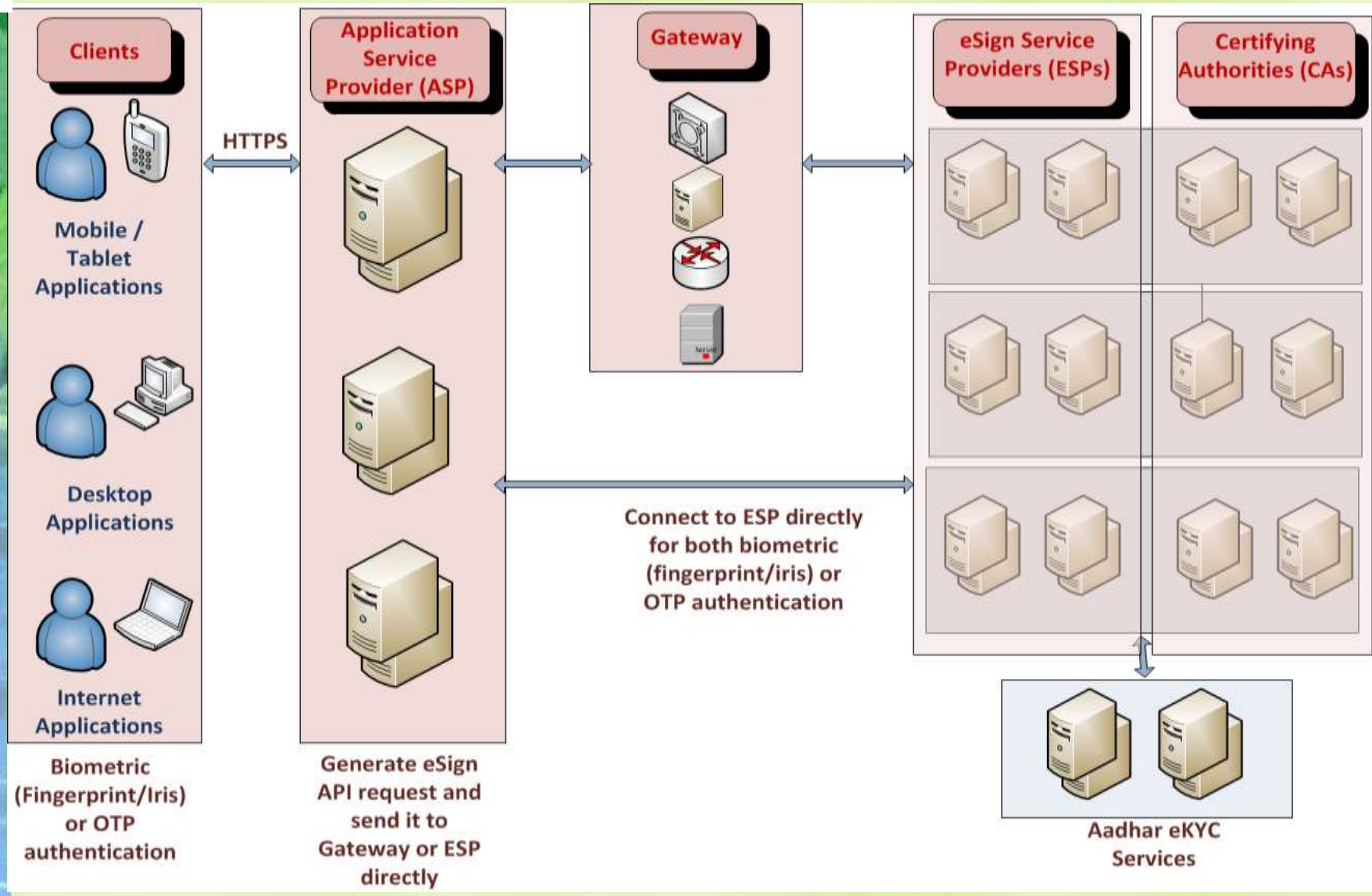
Stakeholders

eSign Service Provider (ESP): An organization or an entity providing eSign service. ESP is a “Trusted Third Party”, as per the definitions of Second Schedule of Information Technology Act. To begin with ESP is a Licensed Certifying Authority (CA).

Certifying Authority (CA): An organization or an entity licensed under CCA for issuance of Digital Signature Certificate and carrying out allied CA operations.

UIDAI: An authority established by Government of India to provide unique identity to all Indian residents. It also runs the eKYC authentication service for the registered KYC User Agency (KUA).

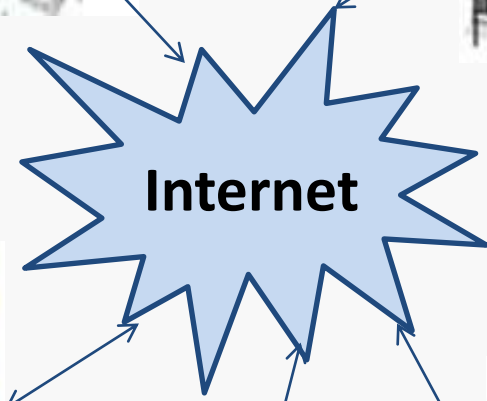
Stakeholders interaction



Public Key Infrastructure

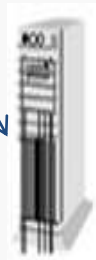
Registration Authorities
Authorize the binding between Public Key and Certificate Holder

Relying Party Application
Validate Signatures and certificate paths



Certificate Holder
Subscriber

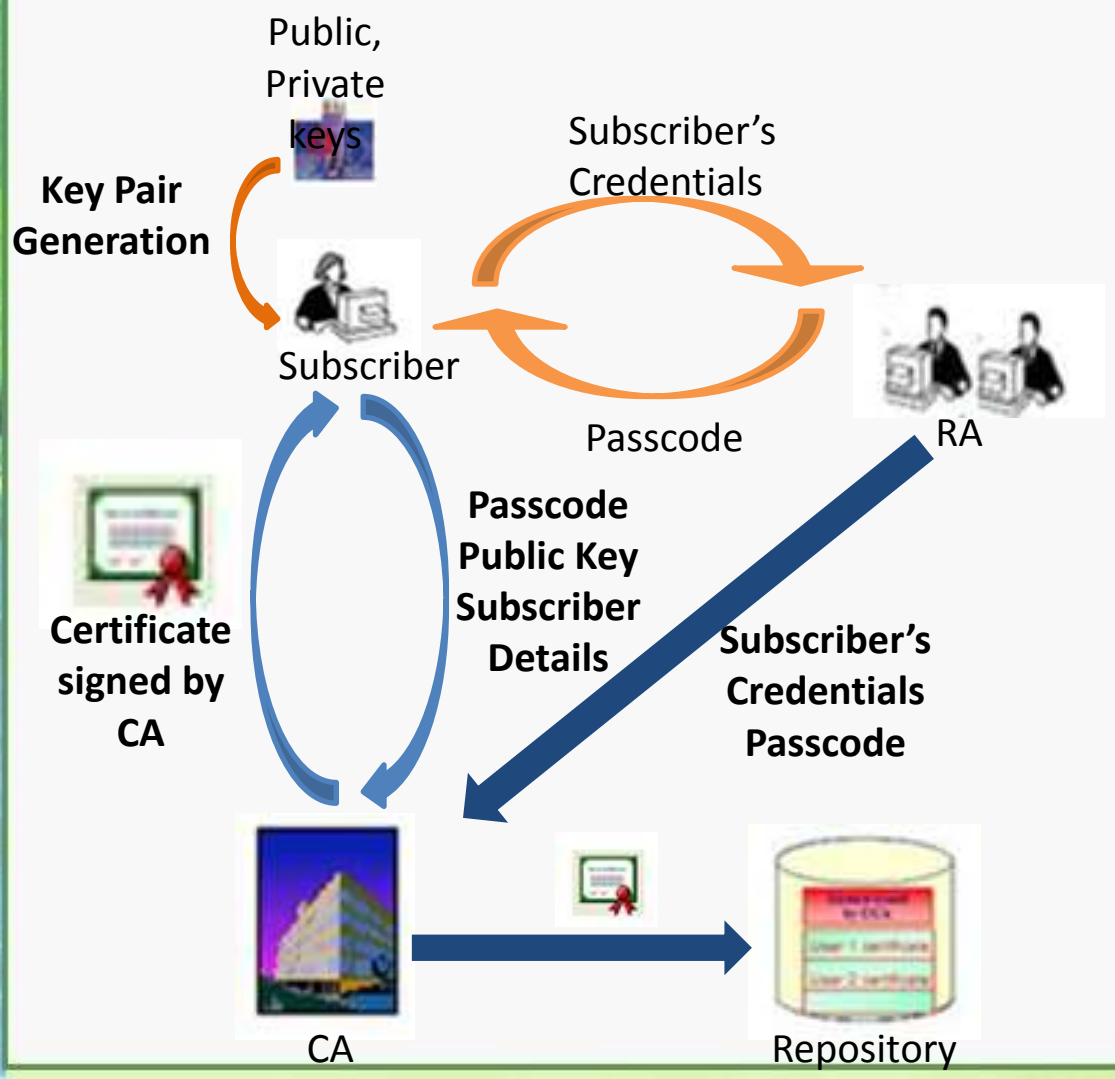
Certifying Authorities
Issuers



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.

eSign

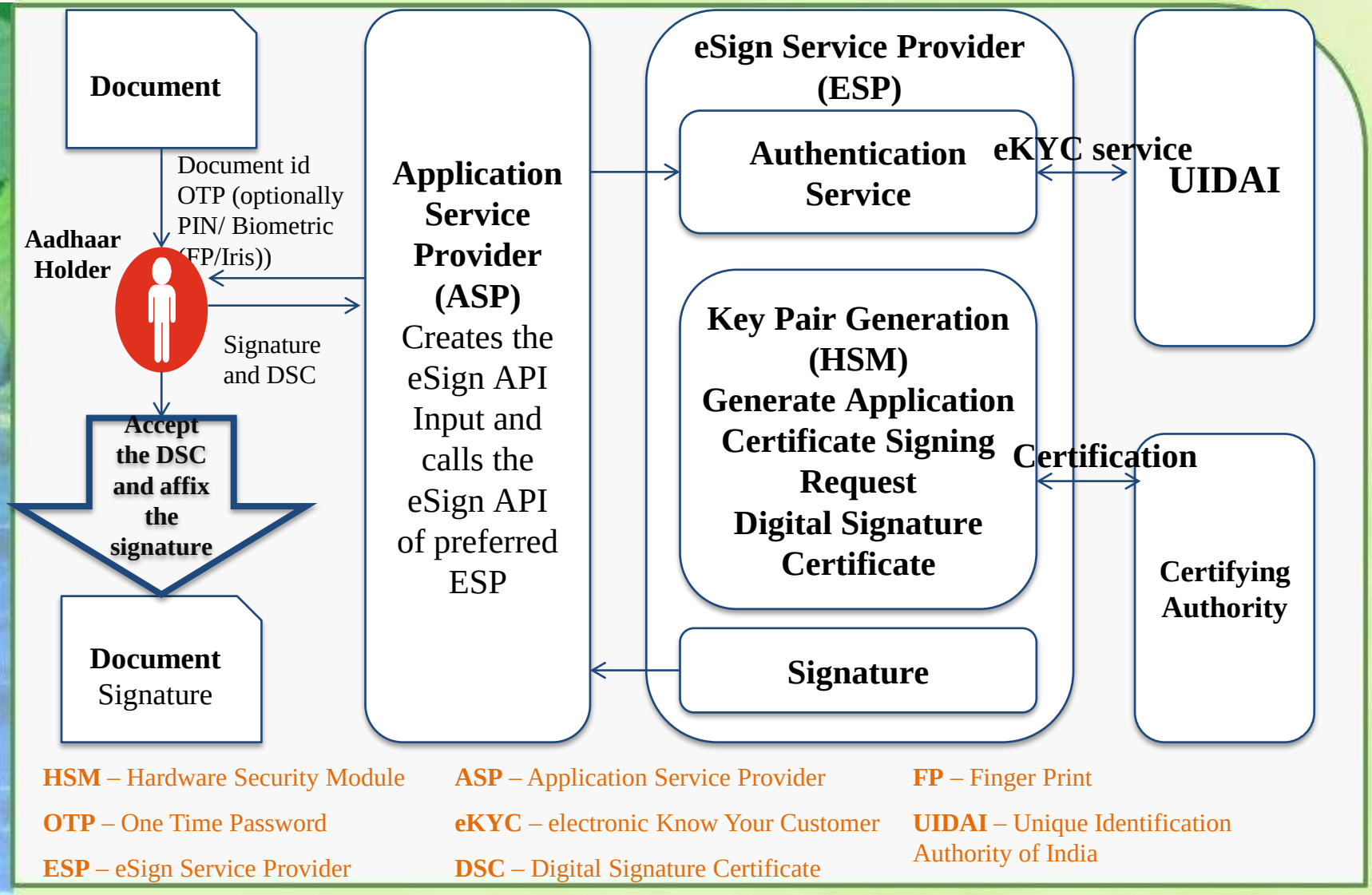
eSign facilitates electronically signing a document by an Aadhaar holder using an Online Service. Aadhaar ID is mandatory for availing this service

Authentication of the Aadhaar holder through UIDAIs eKYC service is the basis on which the Digital Signature Certificate is issued to the prospective signer

eSign is an integrated service that facilitates issuing a Digital Signature Certificate and performing Signing of requested data by authenticating Aadhaar holder

Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015 has been notified to provide the legal framework

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

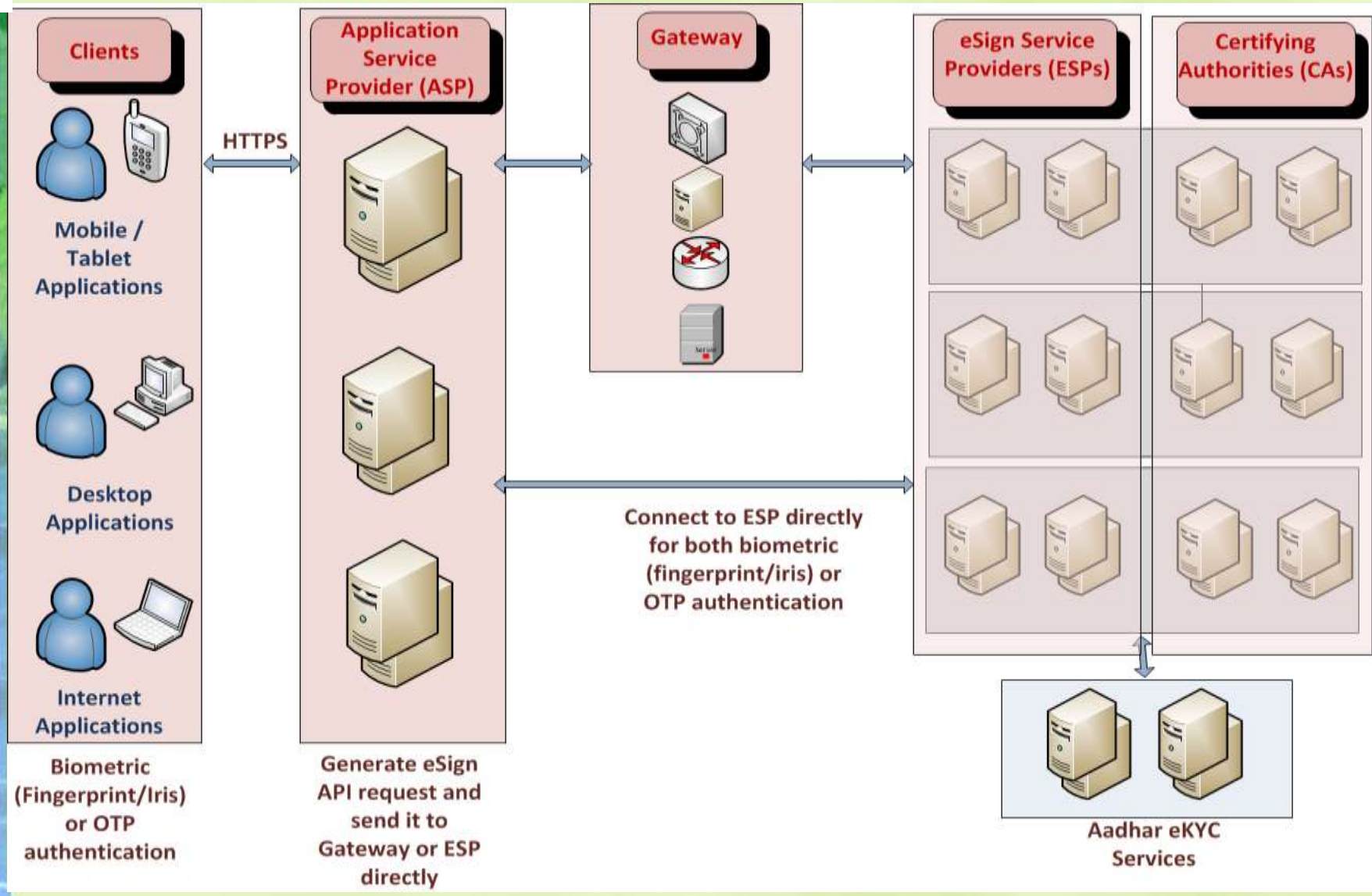
FP – Finger Print

UIDAI – Unique Identification Authority of India

eSign - Benefits

❖ Save cost and time	❖ Aadhaar e-KYC based authentication
❖ Improve User Convenience	❖ Mandatory Aadhaar ID
❖ Easy to apply Digital Signature	❖ Biometric or OTP (optionally with PIN) based authentication
❖ Verifiable Signatures and Signatory	❖ Flexible and fast integration with application
❖ Legally recognized	❖ Suitable for individual, business and Government
❖ Managed by Licensed CAs	❖ API subscription Model
❖ Privacy concerns addressed	❖ Integrity with a complete audit trail
❖ Simple Signature verification	❖ Immediate destruction of keys after usage
❖ Short validity certificates	❖ No key storage and key protection concerns

Stakeholders interaction



Application Service Provider (ASP)

The agency who intends to integrate eSign service should either be:

- A Central/ State Government Ministry / Department or an undertaking owned and managed by Central / State Government, or
- An Authority constituted under the Central / State Act, or
- A Not-for-profit company / Special Purpose organization of national importance, or
- A bank / financial institution / telecom company, or
- A legal entity registered in India

On-Boarding for offering eSign services

- For an Application Service Provider (ASP) to integrate eSign into the service, it has to apply to a eSign Service Provider (ESP) by filling the form and submitting the required documents as prescribed.

- Once the ESP has satisfied itself, the two parties (ESP and ASP) enter into an agreement to decide the scope of services, service level agreements and other terms of business.

- The ASP will then be given an integration kit to kick start the Pre-production work.

On-Boarding for offering eSign services

- The ASP accesses the pre-production environment and performs end to end testing. The testing phase lasts for usually 7-10 days
- Once it is complete, the ASP can send a request for approval to Go-Live.
- The ESP satisfies itself about the readiness of the ASP to go live.

On-Boarding for offering eSign services

- Once approval is received from the ESP, the ASP needs to obtain access to the production environment.
- Once the migration from pre-production to production stage is completed, the ASP can roll out the application to provide eSign service to various Aadhaar holders

Using the eSign service

The ASP can choose any of the following options to provide the eSign service to the end user:

- Directly connect to ESP
- Connect to ESP through the Gateway Service Provider (GSP)

Using the eSign service

Option1:

- The eSign service API can be used by ASPs through:
  - Single eSign Service Provider
  - Multiple eSign Service Provider
- In case of multiple eSign service providers, ASP shall have parameters configurable for each request.
- The routing of requests can be a round-robin, a failure switchover, an end-user selection basis, or any other manner implemented by ASP.

Using the eSign service

Option2:

The ASP can also use a Gateway Service Provider which integrate with one or more ESP and route the request accordingly.

- The Gateway Service provider may also have additional validation process, where a one-time registration of end-user may happen, and a secure pin is provided to access the gateway. This will form a secure second factor protection in case of OTP based authentication, if required.

- GSP can also ensure that at peak times traffic can be managed effectively by routing eSign request to different ESPs

Potential Services

Services which are consumed on a individual capacity has a potential to be migrated to eSign

	Department	Service	Transaction	Advantage
1	Digital Locker	Self Signing	2 crore/ year*	D
2	Income Tax	Pan Issuance	1 crore/ year	D
		Return Filing	3–4 crore/ year	D
3	Financial Sector	Account opening in Banks	10 crore/ year	V
		Account opening in Post Office	2 crore/ year	V

Legend: V No Visit D Digital / No Paper

Note: * 1 million users signing about 15-20 documents in a year

Potential Services

	Department	Service	Transaction	Advantage
4	Transport Department	Driving License	1.2 crore/ year	D
		Vehicle Registration	15 crore total	D
5	Passport	Fresh applications	0.75 crore/year	D
		Reissue existing	0.25 crore/year	V
6	Telecom	New Connection	6 crore/ year	V
7	Rural Health Insurance	Application	2 crore total 0.3 crore/ year	V

Legend: V No Visit D Digital / No Paper

Other Services

Other services which can be explored for migration to eSign are:

Department		Service		Transaction	Advantage
1	Various Certificates	Birth	Tribe	9 crore/year	V
		Death	Domicile		
		Caste	Marriage		D
		Income	Residence		

Legend: V No Visit D Digital / No Paper

Where we stand currently. . .

To enhance the demand of eSign service in the market, a number of steps have been taken and DeitY is engaging with a number of prospective ASPs. These include:

- ***Income Tax Department***
- ***Digital Locker team***
- ***External Affairs Ministry – Passport Office***
- ***Department of Telecom***

A number of materials/ resources have been developed which could be leveraged by prospective agencies to become ASP or gain an understanding of eSign:

- eSign API Specifications
- eSign Booklet
- e-Authentication Guidelines
- Gazette Notification
- Template agreement between ASP-ESP
- ASP On Boarding Document

Thank you

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

Website : www.cca.gov.in Email : info@cca.gov.in