eSign – Online Digital Signature Service

Government of India
Ministry of Communications and Information Technology
Department of Electronics and Information Technology
Controller of Certifying Authorities

Agenda

1. Context
2. eSign Service
3. How eSign Works

1. Context
2. eSign Service
3. How eSign Works

The Information Technology (IT) Act 2000 & Controller of Certifying Authority (CCA)

Information Technology Act

- The IT Act, 2000 provides legal sanctity to electronic signatures
- Electronic signatures are accepted at par with handwritten signatures
- Electronic documents that have been electronically signed are treated at par with paper documents signed in the traditional way
- The IT Act provides the basic legal and administrative framework for e-commerce, and promotes its growth by creating trust in electronic environment

Controller of Certifying Authorities

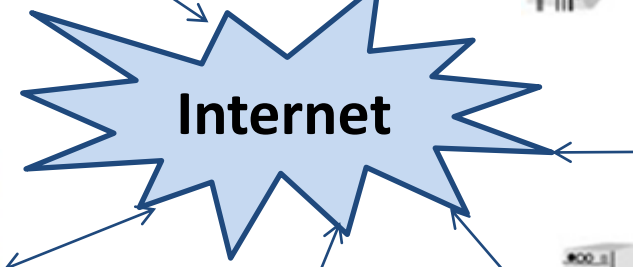
- The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities
- Certifying Authorities (CAs) issue Digital Signature Certificates (DSC) for authentication of users in cyberspace
- Prior to issuing a DSC, Certifying Authority (CA) is required to verify the credentials of the applicant as stated in the Application Form and supporting documents

Public Key Infrastructure (PKI)

- **The Public Key Infrastructure (PKI)** in the country comprises the CCA and the CAs, Users and Relying Parties, and policies and procedures
- The CCA is at the root of the trust chain hierarchy in India
- As the foundation for secure Internet applications, PKI ensures authentic communications that cannot be repudiated

Registration Authorities
Authorize the binding between Public Key and Certificate Holder

Relying Party Application
Validate Signatures and certificate paths



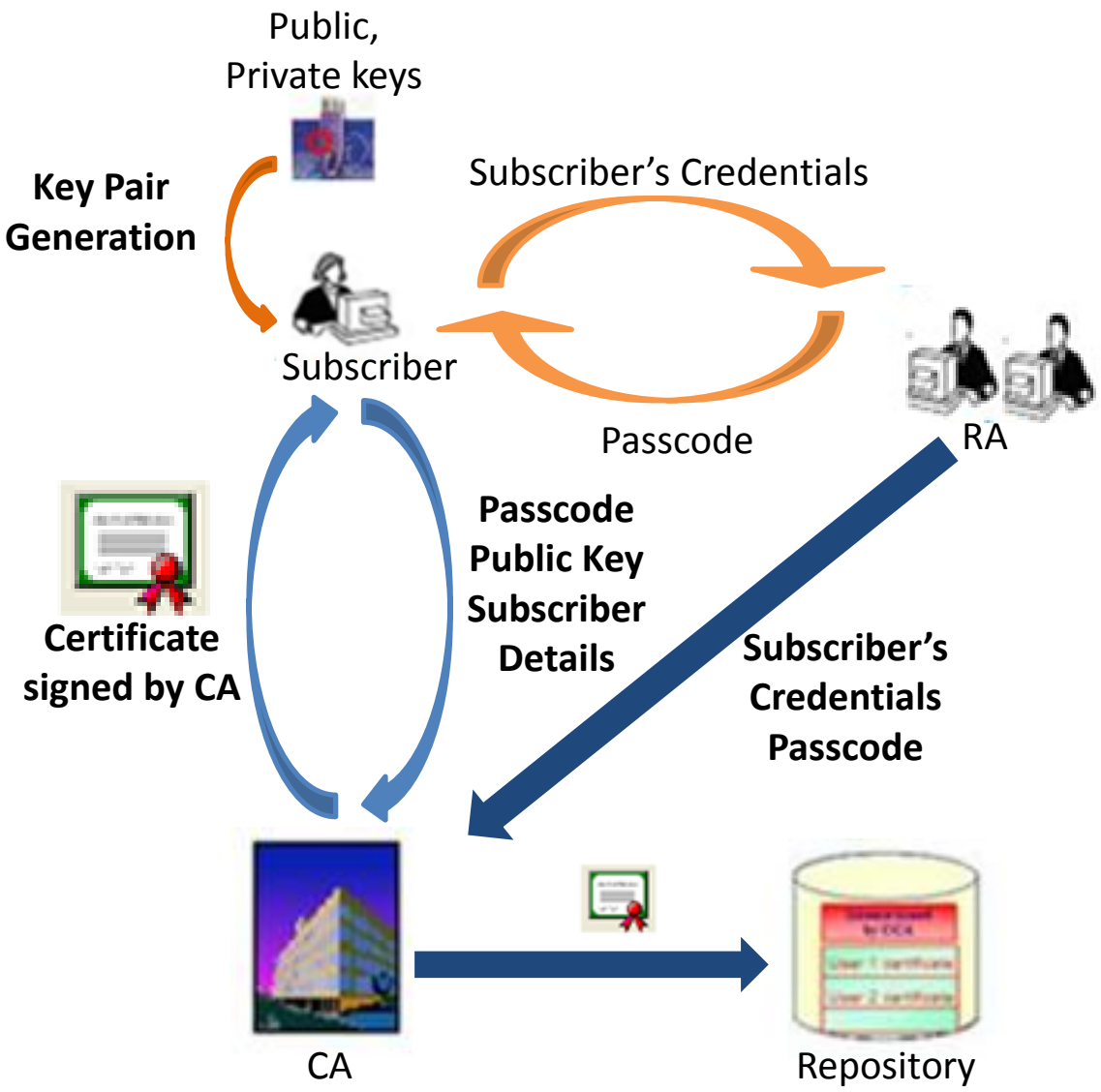
Certificate Holder
Subscriber

Certifying Authorities
Issuers

Web Server

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

Issuance of Digital Signature Certificate



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

Challenges in scaling up usage of Digital Signatures

Some of the major challenges faced while using traditional digital signature certificate are:

1. Personal digital signature requires person's **identity verification** and issuance of **USB dongle** having private key, secured with a **password/pin**

2. The **major cost** of the DSC is found to be the **verification cost**. Certifying Authorities **engage** Registration Authorities to carry out the verification of credentials prior to issuance of certificate

3. Physical **USB Dongle** compliant to **mandated standards** also adds to the **cost**

Current scheme of physical verification, document based identity validation, and issuance of physical dongles does not scale to a billion people. Relying on the DSC applicant's information already available on the public database is an alternate to manual verification and 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 of India

Data Collected for enrolment

- **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**

eKYC Process

- The UIDAI offers an authentication service to authenticate residents identity using **biometric** scan or **OTP** sent to mobile or email
- As part of the e-KYC process of Aadhaar, the resident authorizes UIDAI to provide their **demographic** data along with their **photograph** (**electronically signed and encrypted**) to service providers

1 Context

2 eSign Service

3 How eSign Works

eSign Service

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

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

eSign Service – Benefits

Some of the benefits that one can derive by using the eSign service are:

❖ 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

eSign Assurance Levels

In the case of eSign Online Electronic Signature Service, the Digital Signature Certificates are issued in the following classes:

1. OTP based eKYC

Aadhaar OTP class of certificates shall be issued for individuals use based on OTP authentication of subscriber through Aadhaar eKYC

These certificates will confirm that the information in Digital Signature certificate provided by the subscriber is same as information retained in the Aadhaar databases pertaining to the subscriber as Aadhaar holder

Certificate holder's private keys are created on Hardware Security Module and destroyed immediately after one time usage at this assurance level

eSign Assurance Levels

In the case of eSign Online Electronic Signature Service, the Digital Signature Certificates are issued in the following classes:

2. Biometric based eKYC

Aadhaar biometric class of certificates shall be issued based on biometric authentication of subscriber through Aadhaar eKYC service

These certificates will confirm that the information in Digital Signature certificate provided by the subscriber is same as information retained in the Aadhaar databases pertaining to the subscriber as Aadhaar holder

Certificate holder's private keys are created on Hardware Security Module and destroyed immediately after one time usage at this assurance level

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

Addressing scalability through eSign (1/2)

eSign is a simple to use online service which allows everyone to have the ability to digitally sign electronic documents which will provide a hassle free fully paperless service to the citizens:

1. An Aadhaar holder can sign a document with Aadhaar Biometric/ OTP authentication requiring no physical device or paper-based application forms or documents

2. Authentication of the signer is carried out using eKYC of Aadhaar and the signature on the document is carried out on a backend server of the e-Sign provider

3. 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 (2/2)

4. The eSign facilitates issuing a Signature Certificate and performing Signing of requested data by authenticating Aadhaar holder

5. 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

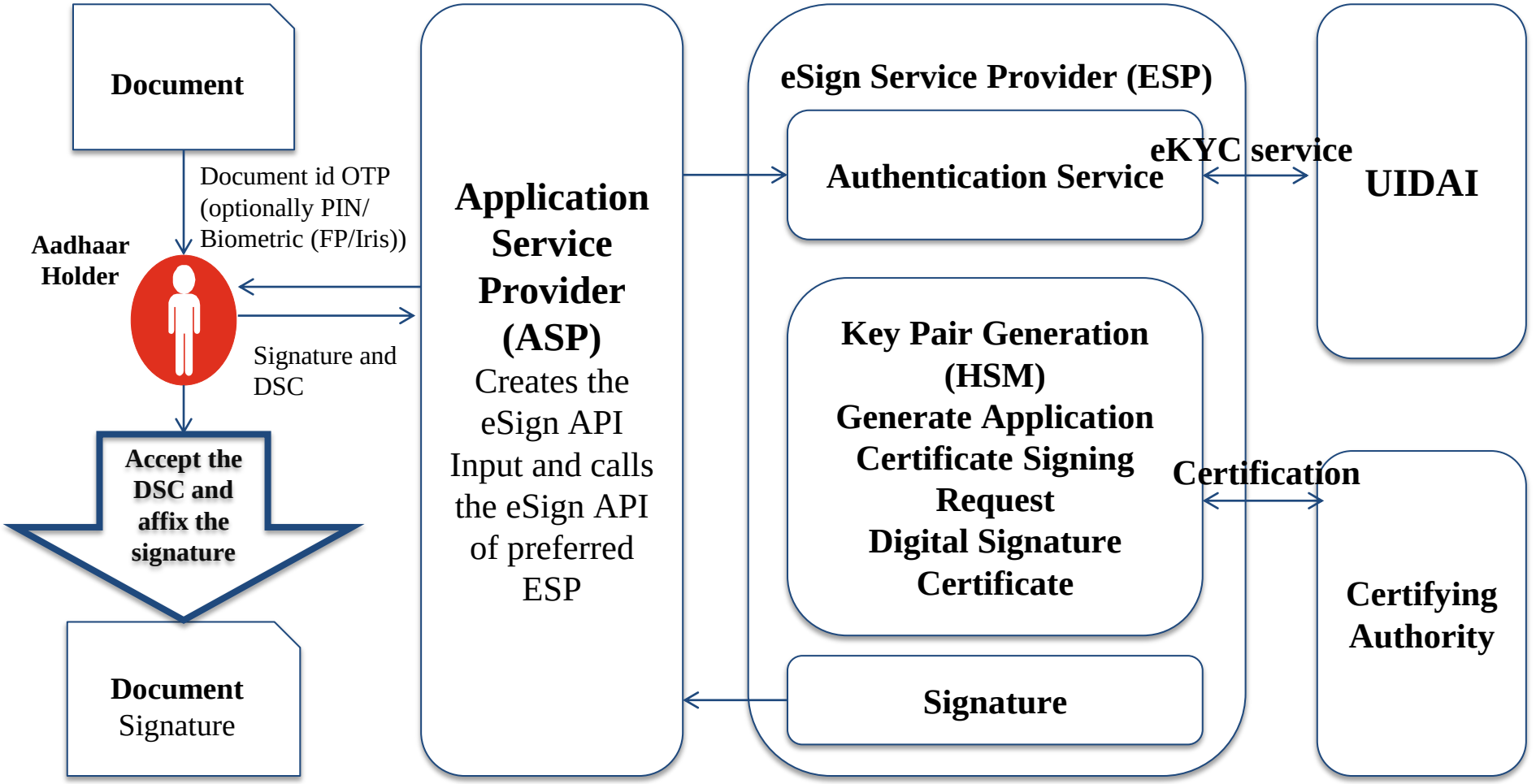
6. This service authenticates the person, does Aadhaar e-KYC, and then electronically signs the input within the e-Sign provider backend. Such scheme allows DSC to be scaled massively and allow many 3rd party applications to use the service via an open API and integrate DSC into their application

1 Context

2 eSign Service

3 How eSign Works

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 Workflow (1/5)

At Application Service Provider (ASP) | At eSign Service Provider (ESP) | At Certifying Authority (CA) | At eSign Service Provider (ESP) | At 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. Capture Aadhaar number and authentication factor (OTP/Biometric)
4. Creates the input API for eSign
5. Calls the eSign API of the eSign provider

eSign Workflow (2/5)

At Application Service Provider (ASP) | **At eSign Service Provider (ESP)** | At Certifying Authority (CA) | At eSign Service Provider (ESP) | At Application Service Provider (ASP)

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 (3/5)

At Application Service Provider (ASP) | At eSign Service Provider (ESP) | **At Certifying Authority (CA)** | At eSign Service Provider (ESP) | At Application Service Provider (ASP)

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

eSign Workflow (4/5)

At Application Service Provider (ASP) | At eSign Service Provider (ESP) | At Certifying Authority (CA) | **At eSign Service Provider (ESP)** | At Application Service Provider (ASP)

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 (5/5)

At Application Service Provider (ASP) | At eSign Service Provider (ESP) | At Certifying Authority (CA) | At eSign Service Provider (ESP) | **At Application Service Provider (ASP)**

14. Receives the signature from the e-Sign provider

15. Attaches the signature to the document

Stakeholders

Application Service Provider

- An organization or an entity using eSign service as part of their application to electronically sign the content
- Example: Govt. Departments, Banks, other public/ private organizations

End User

- An Individual using the application of ASP and represents himself/ herself for signing the document under legal framework
- Also a resident holding the Aadhaar number and applicant/ subscriber for digital certificate

eSign Service Provider

- Trusted Third Party as per the definitions of Second Schedule of Information Technology Act to provide eSign service
- To begin with ESP is a Licensed Certifying Authority (CA)

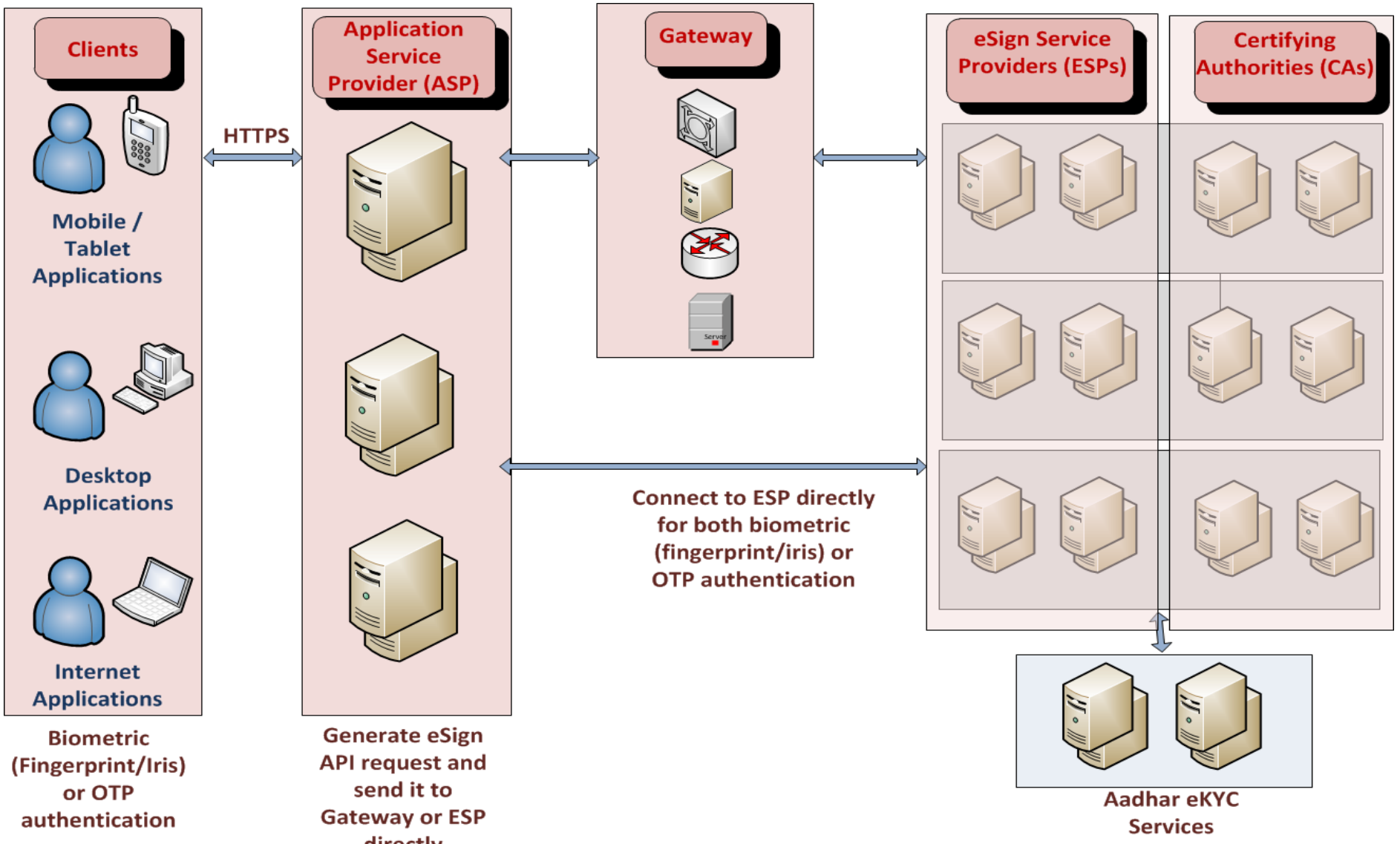
Certifying Authority

- An organization or an entity licensed under CCA
- Issues Digital Signature Certificate and carries out allied CA operations

UIDAI

- Provide unique identity to all Indian residents
- Provides eKYC authentication service to registered KUAs

Stakeholders Interaction



Availing eSign Service

The various steps for integration the eSign in the application are defined below:

1. Apply to ESP for integrating eSign Service in their application
2. Perform testing in the staging environment
3. Submit audit report and checklist to ESP/GSP
4. Obtain license key and test in the production environment

On boarding process to integrate eSign Service in application

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

Applications from legal entities registered in India who seeks to use eSign service to enable online digital Signature on its application, will be referred to the ESP/GSP approval for their consideration

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