e-Sign – An Online Electronic Signature Service

Dr. Mohammed Misbahuddin
Centre for Development of Advanced Computing (C-DAC)
Bangalore

Under the Aegis of

Controller of Certifying Authorities (CCA)
Government of India

Agenda

- ✓ Electronic Signature
- ✓ Challenges in Digital Signature
- ✓ Current scenario of Certificate Issuance
- ✓ What is eSign
  - ✓ How eSign Works?
  - ✓ Assurance Levels
- ✓ Legal Validity of eSign
- ✓ eSign Services
- ✓ eSign API
- ✓ Use cases of eSign

Electronic Signature

Electronic Signature

An electronic signature to be legally accepted it shall possesses the following requirements:

- **Signature Data to be Linked to Signatory**: The signature creation data or the authentication data are, within the context in which they are used, linked to signatory.
- **The signature creation data under the control of signatory :** The signature creation data or the authentication data were, at the time of signing, under the control of signatory.
- **Alteration to be detectable:** Any alteration to the electronic signature made after affixing such signature is detectable. and
- **Modification to be detectable:** Any modification to the information made after its authentication by electronic signature is detectable.

Challenges in Present Digital Signature

Challenges in Present DS

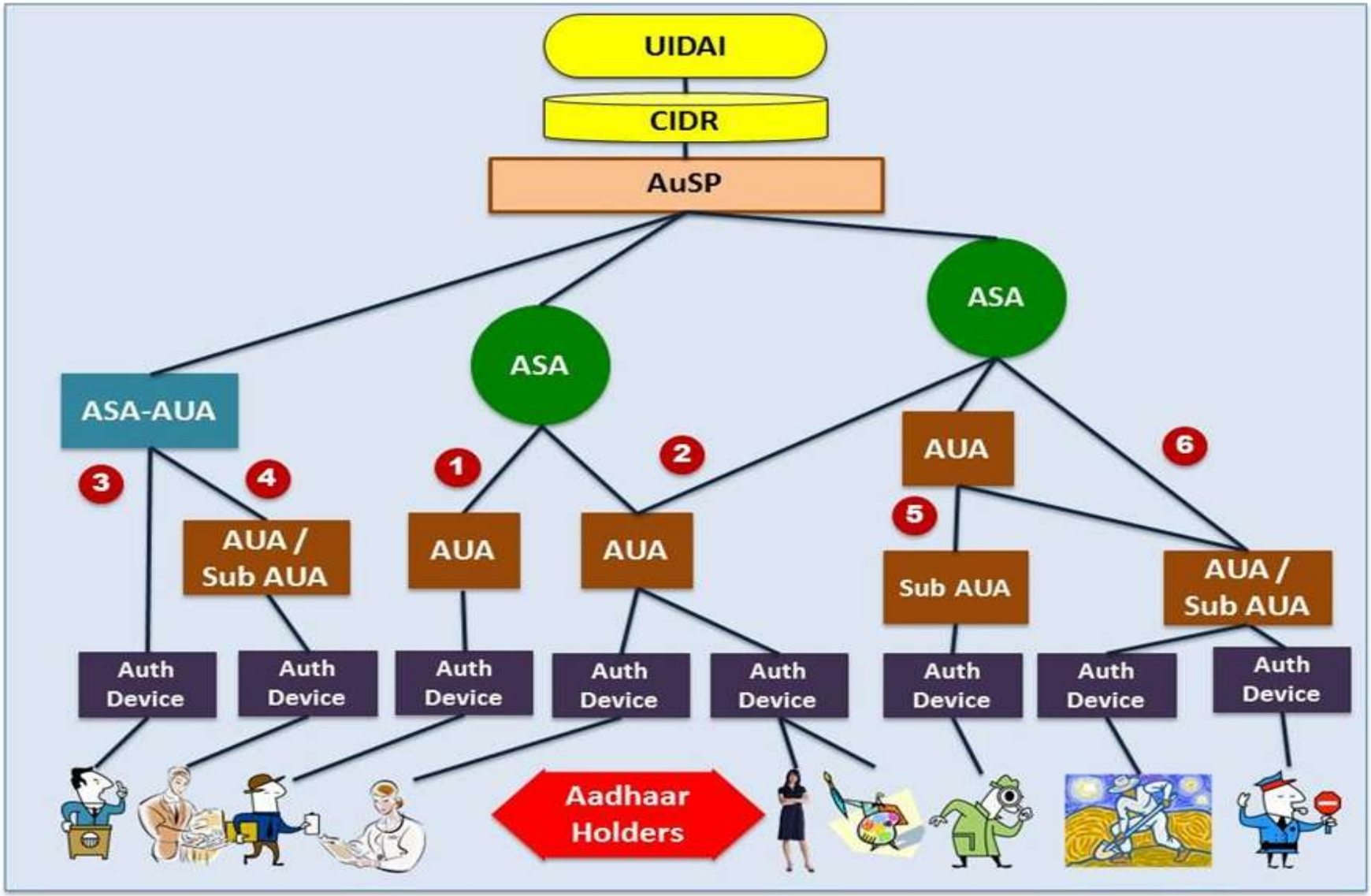
- Currently personal digital signature requires
  - Person's identity verification
  - Current scheme of physical verification, document based identity validation, and issuance of physical dongles does not scale to a billion people.
  - Certifying Authorities engage Registration Authorities to carry out the verification of credentials prior to issuance of certificate.
  - Issuance of USB dongle having private key, secured with a password/pin.
  - The major cost of the DSC is found to be the verification cost and cost of USB dongle.

Current Scenario of Certificate Issuance

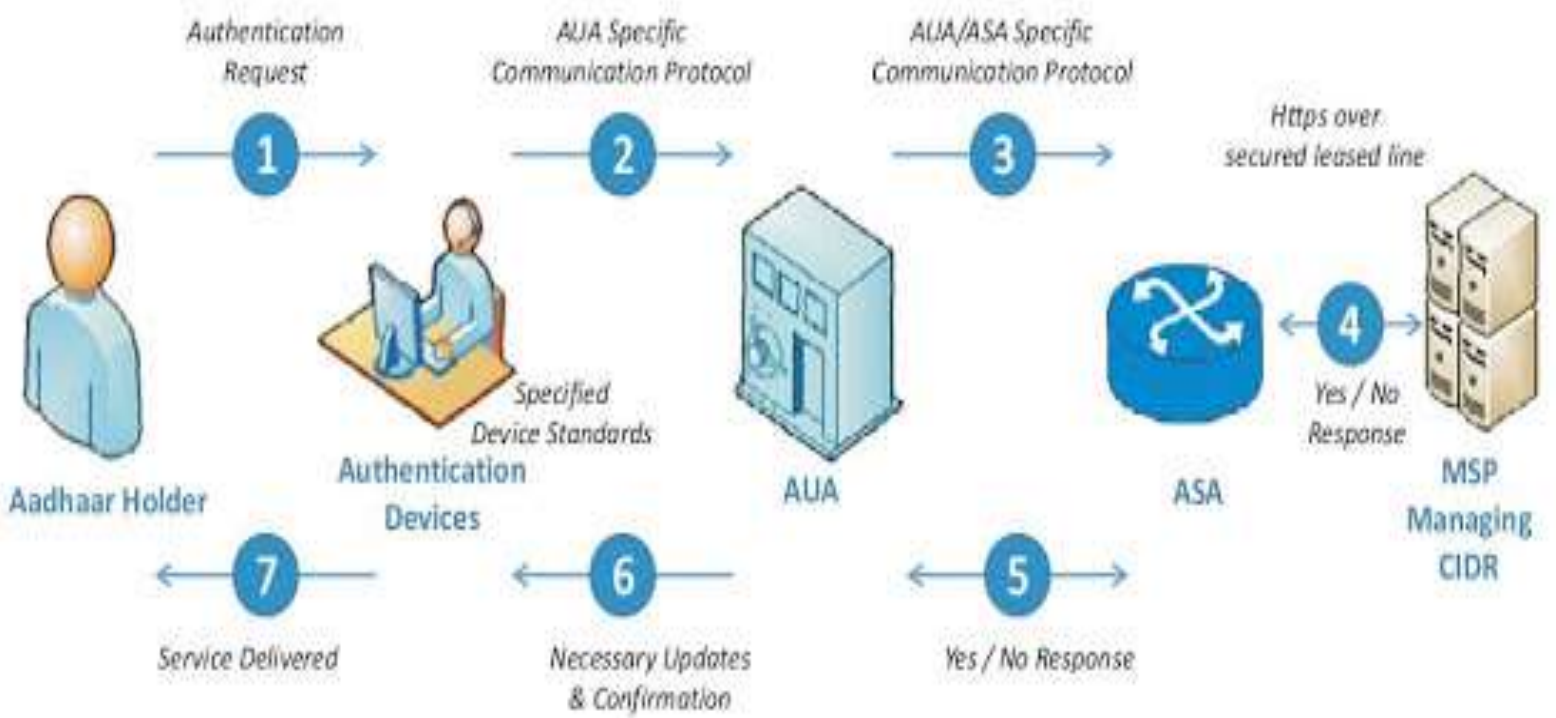
Current Issuance Process

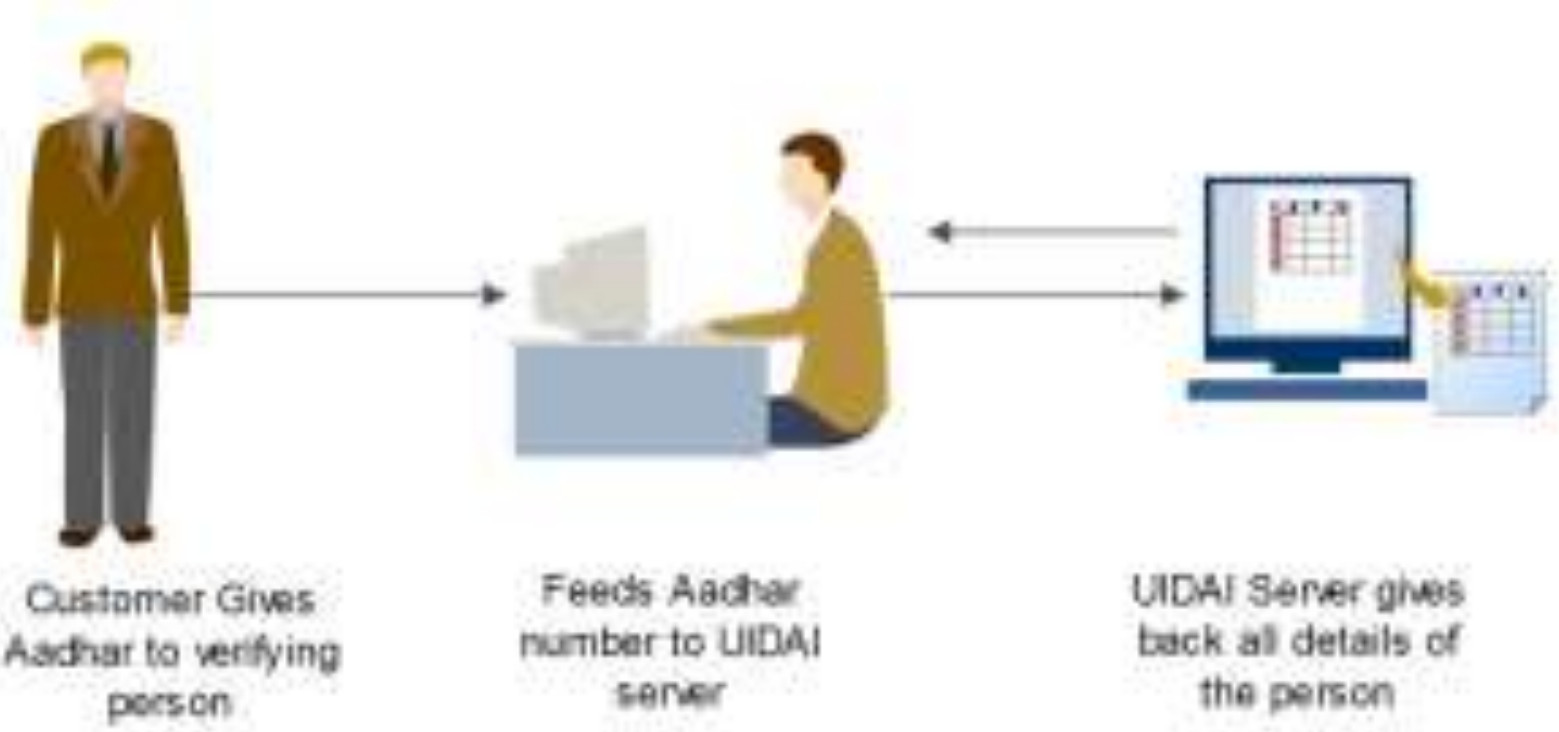
Aadhaar Authentication Ecosystem

Aadhaar Authentication



Authentication Flow (AUA & ASA)




Customer Gives Aadhar to verifying person
Feeds Aadhar number to UIDAI server
UIDAI Server gives back all details of the person

KUA and KSA

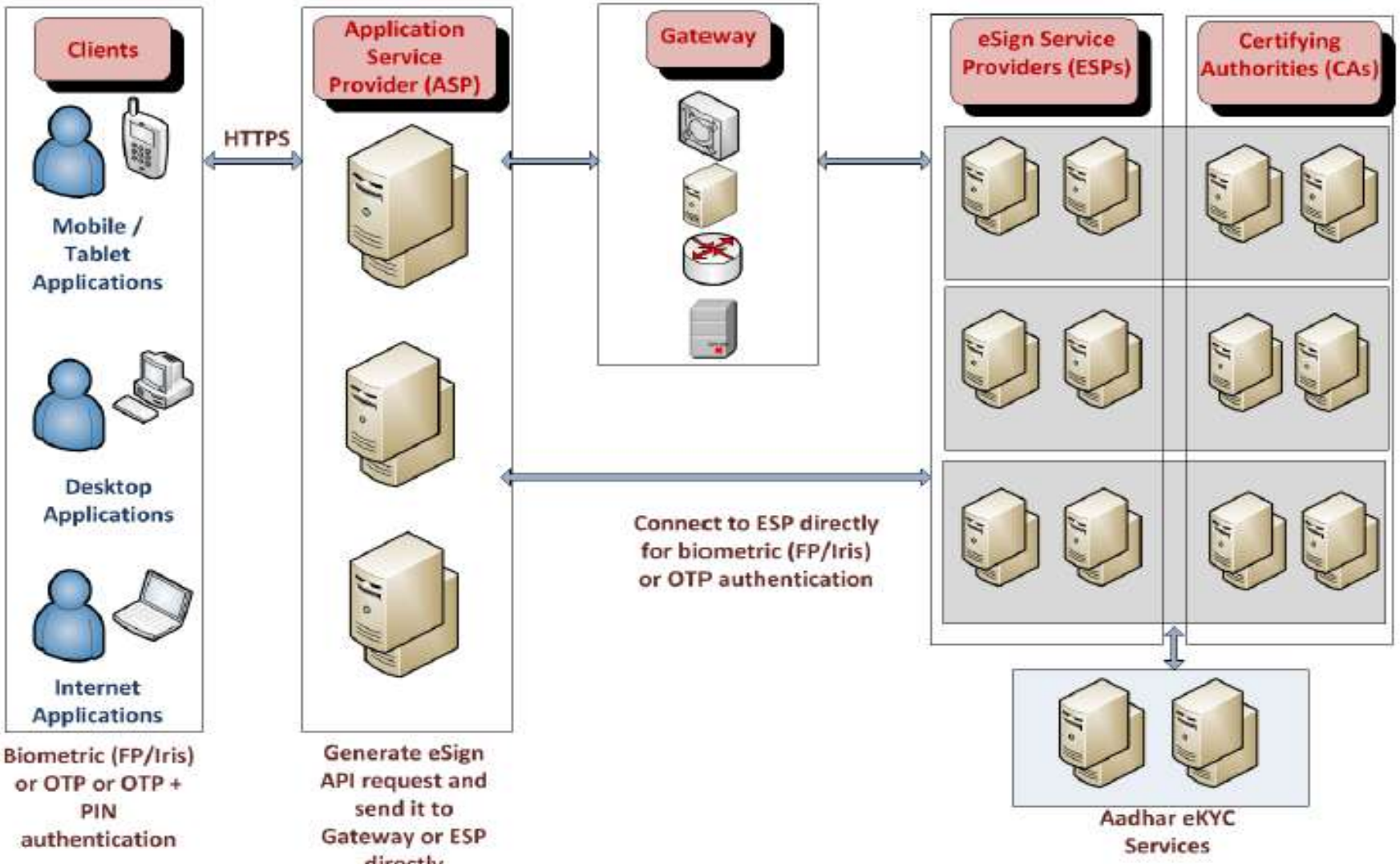

Auth Device
KYC User Agency (KUA)
(AUA with KYC Permission)
KYC Service Agency (KSA)
(ASA with KYC Permission)
Aadhaar KYC API
Auth API

e-Sign – Online Electronic Signature

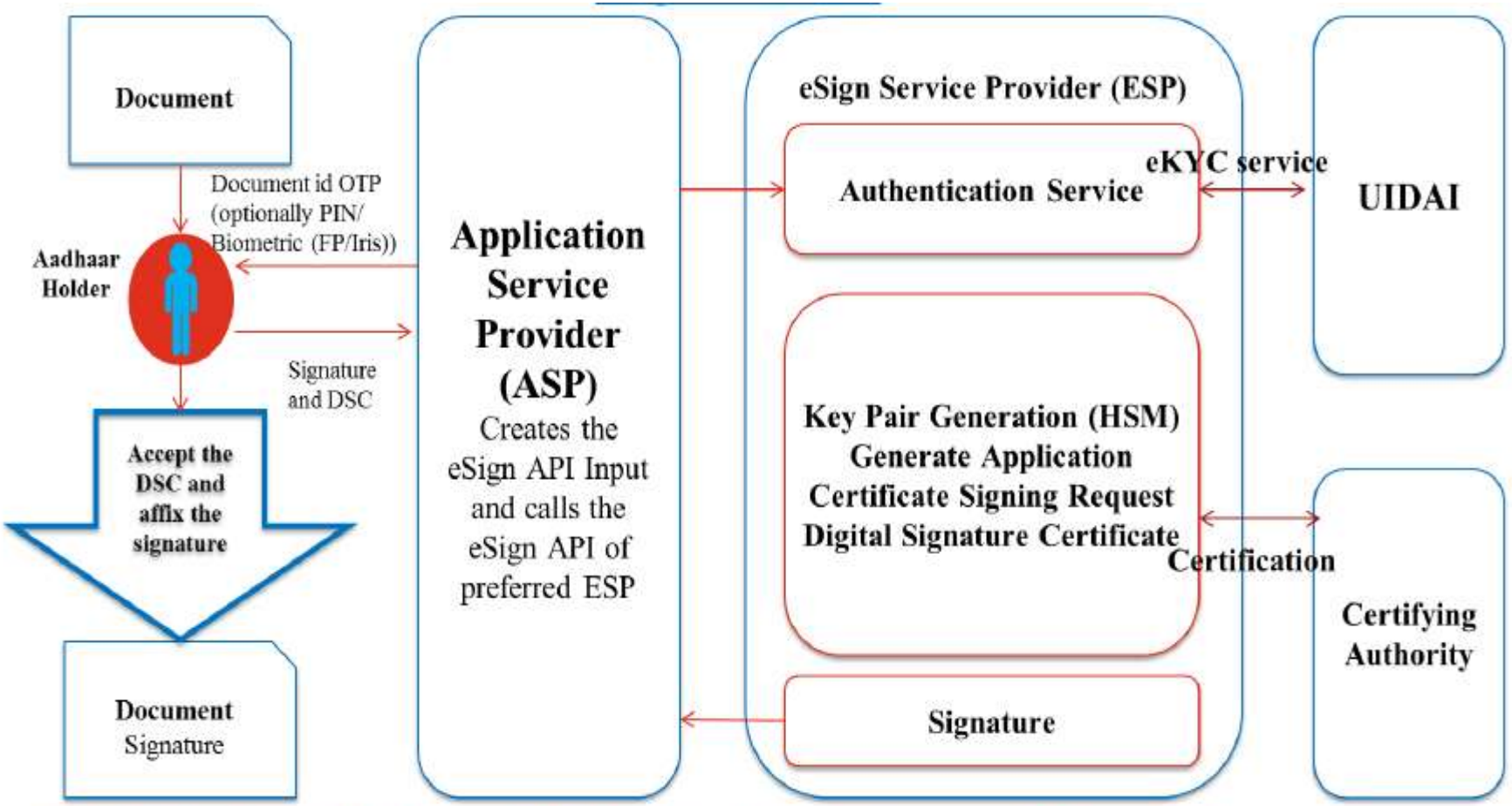
e-Sign Electronic Signature

- An innovative initiative for allowing easy, efficient, and secure signing of electronic documents by authenticating signer using Aadhaar eKYC services.
- Any Aadhaar holder can digitally sign an electronic document without having to obtain a hardware dongle.
- Application Service Providers (ASPs) can integrate this service within their application to offer Aadhaar holders a way to sign electronic forms and documents.
- The need to obtain DSC through a printed paper application form with ink signature and supporting documents will not be required.

Stakeholders in e-Sign Service



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

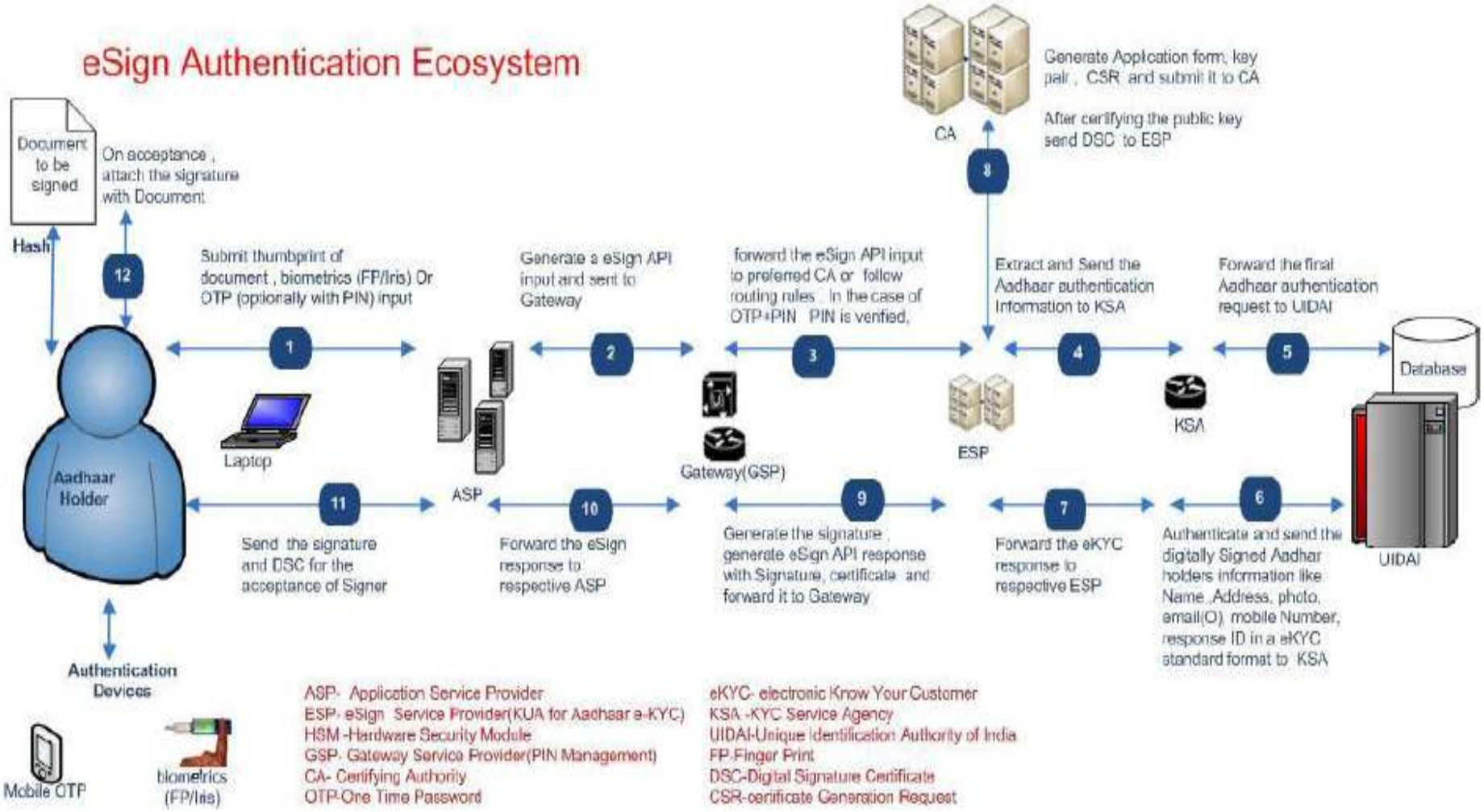
FP – Finger Print

UIDAI – Unique Identification Authority of India

Application Service Provider	
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/OTP+PIN/Biometric)
4.	Creates the input API for eSign
5.	Calls the e-Sign API of the eSign provider
eSign Provider (a KUA as per Aadhaar e-KYC model)	
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.	Create a Certificate Generation Request(CSR) with the Aadhaar e-KYC input received, public key , Response Code
10	Generate DSC Application form and CSR and submit them to CA
Certifying Authority(CA)	
11	Validate the eSign provider calling application, CSR and DSC application form and generate DSC
12	Send the DSC to calling application of eSign provider
eSign Provider (a KUA as per Aadhaar e-KYC model)	
13	Signs the input document hash using the private key (Note: The original document will not be sent to eSign provider) Creates an audit trail for the transaction a. Audit includes the transaction details, timestamp, and Aadhaar e-KYC response
	b. This is used for pricing and reporting
14	Sends the e-Sign API response (signature & DSC) back to the calling application
Application Service Provider	
15	Obtain the acceptance of DSC from end user
16	On DSC acceptance by end user, attaches the signature to the document

eSign Authentication Ecosystem



Certificate Assurance Levels

- Following classes of Certificates are issued.
- Aadhaar-eKYC – **OTP**: This class of certificates shall be issued for **individuals use** based on OTP authentication of subscriber through Aadhaar e-KYC. 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.

- Aadhaar-eKYC – **Biometric (FP/Iris)**:

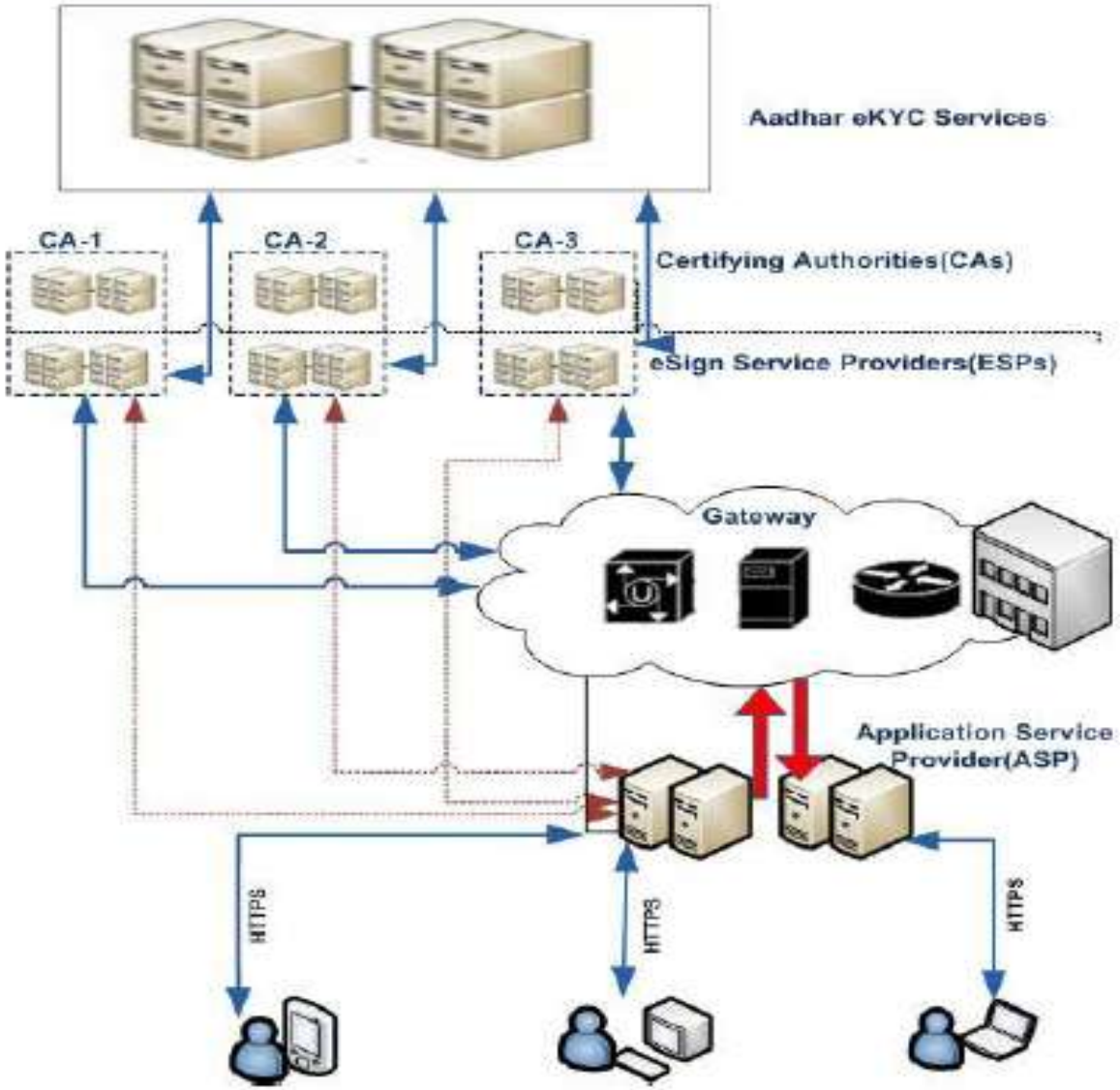
  This class of certificate shall be issued based on biometric authentication of subscriber through Aadhaar e-KYC service. These certificates will confirm that the information in Digital Signature certificate provided by the subscriber is same as information retained in the Aadhaar databases pertaining to the subscriber as Aadhaar holder.

Legal Validity of e-Sign

Legal Validity of eSign

- eSign process involves consumer consent, DSC generation, Digital Signature creation and affixing and DSC acceptance in accordance with provisions of Information Technology Act.
- The Electronic Signatures facilitated through e-Sign Service are legally valid provided the e-Sign signature framework is operated under the provisions of Second Schedule of the Information Technology Act and Guidelines issued by the Controller.
- Please refer *Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015 – e-Authentication technique using Aadhaar e-KYC services.*

e-Sign Services (Operational Scenario)



Two Options for Operating e-Sign Services

1) Directly Connecting to ESP
2) Using a Gateway Service Provider

Usecases of e-Sign Services

Example – eSign online Electronic Signature in Applications		
1.	Digital Locker	✓ Self-attestation
2.	Tax	✓ Application for ID, e-filing
3.	Financial Sector	✓ Application for account opening in banks and post offices
4.	Transport Department	✓ Application for driving license 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

e-Filing Case Study

E-Filing statutory returns – Case Study

User should have valid DSC obtained from Licensed CA of India

User should have Aadhaar number and authenticate with biometric

UIDAI

E File through e-return intermediary	E File without digital signature	E File with digital signature	E File using digital signature

https://efiling.gov.in/eFiling/

eSign

Trusted Third Party

- Authenticate user using Aadhaar eKYC service
- Key Pair Generation on HSM
- Public Key certification
- Create signature and send it to user

Generate and print acknowledgement form. No further action is required

Generate and print acknowledgement form. No further action is required

Certifying Authority

Department

Conclusion

- While PKI and Digital Signatures have been transforming the way traditional transactions happen, the e-Sign will confirm to most of the Digital India implementations
- e-Sign Ecosystem offers
  - Easy and secure way to digitally sign information anywhere, anytime
  - Facilitates legally valid signatures
  - Flexible and easy to implement
  - Respecting privacy
  - Secure online service

References

- http://www.cca.gov.in/cca/?q=eSign.html