e-Sign and TimeStamping

Dr. Balaji Rajendran
Centre for Development of Advanced Computing (C-DAC)
Bangalore

Under the Aegis of

Controller of Certifying Authorities (CCA)
Government of India

Recent Developments: e-Sign – An Online Electronic Signature Service

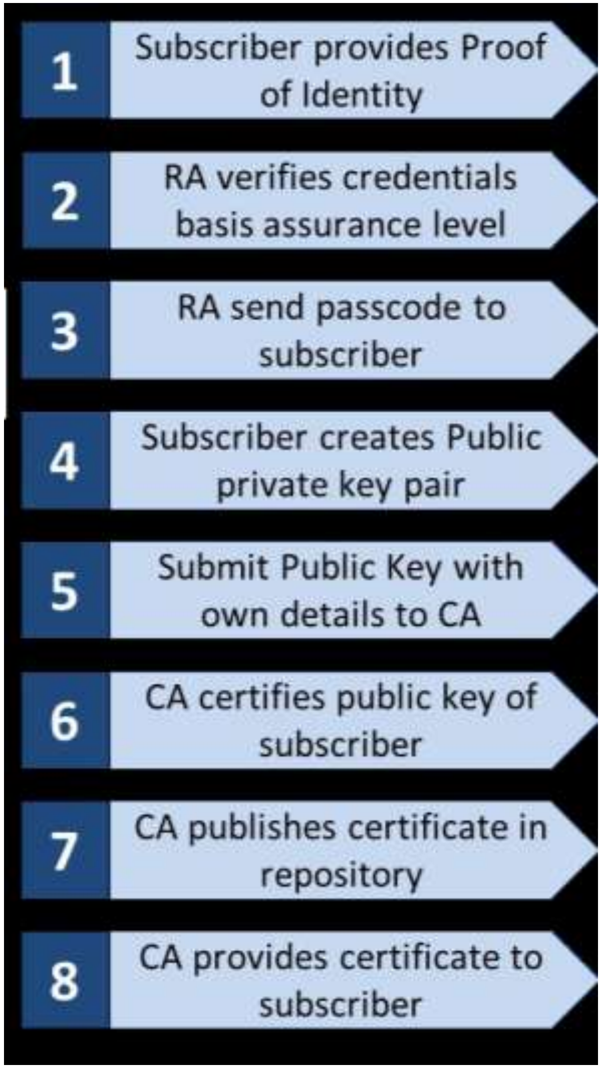
Electronic Signature

- An electronic signature to be legally accepted, should possesses the following requirements:
  - **Signature should 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 to be under the control of signatory, at the time of signing
  - **Alteration to be detectable:** Any alteration to the electronic signature made after affixing such signature is detectable
  - **Modification to be detectable:** Any modification to the information made after its authentication by electronic signature is detectable

Challenges in Present Digital Signature

- 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

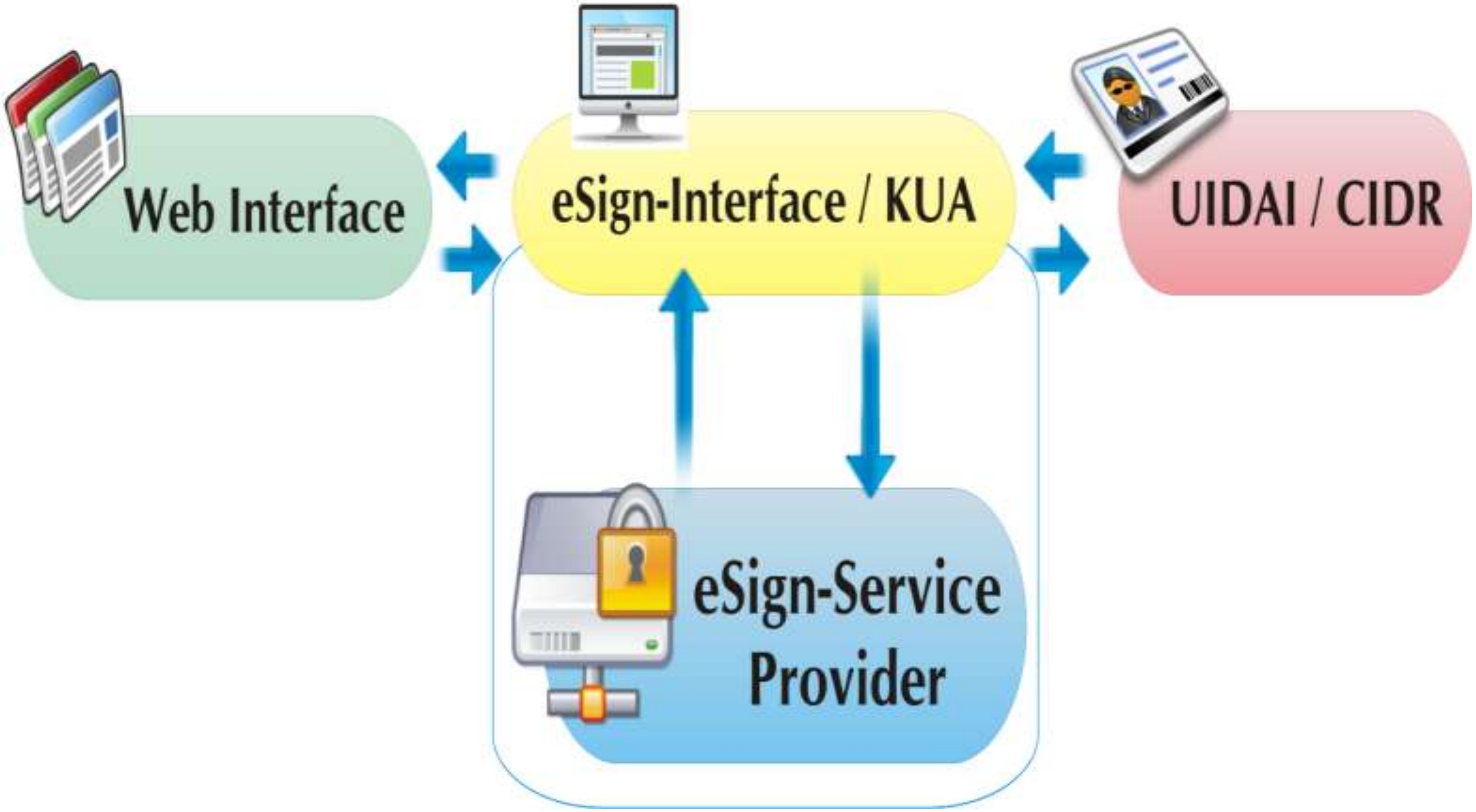


1. Subscriber provides Proof of Identity
2. RA verifies credentials basis assurance level
3. RA send passcode to subscriber
4. Subscriber creates Public private key pair
5. Submit Public Key with own details to CA
6. CA certifies public key of subscriber
7. CA publishes certificate in repository
8. CA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

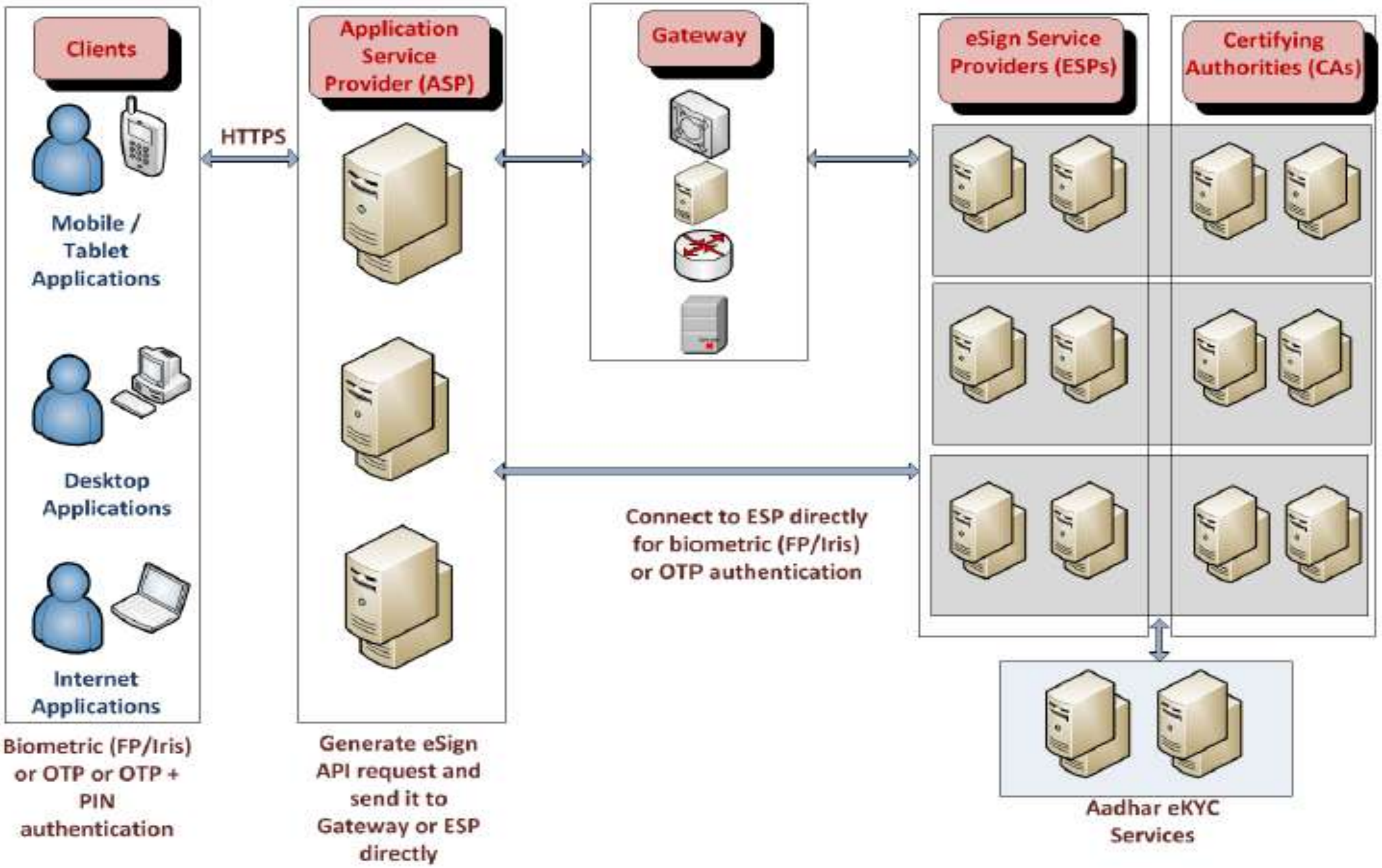
e-Sign – Electronic Signature

- 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.

e-Sign Process



Stakeholders in e-Sign Service

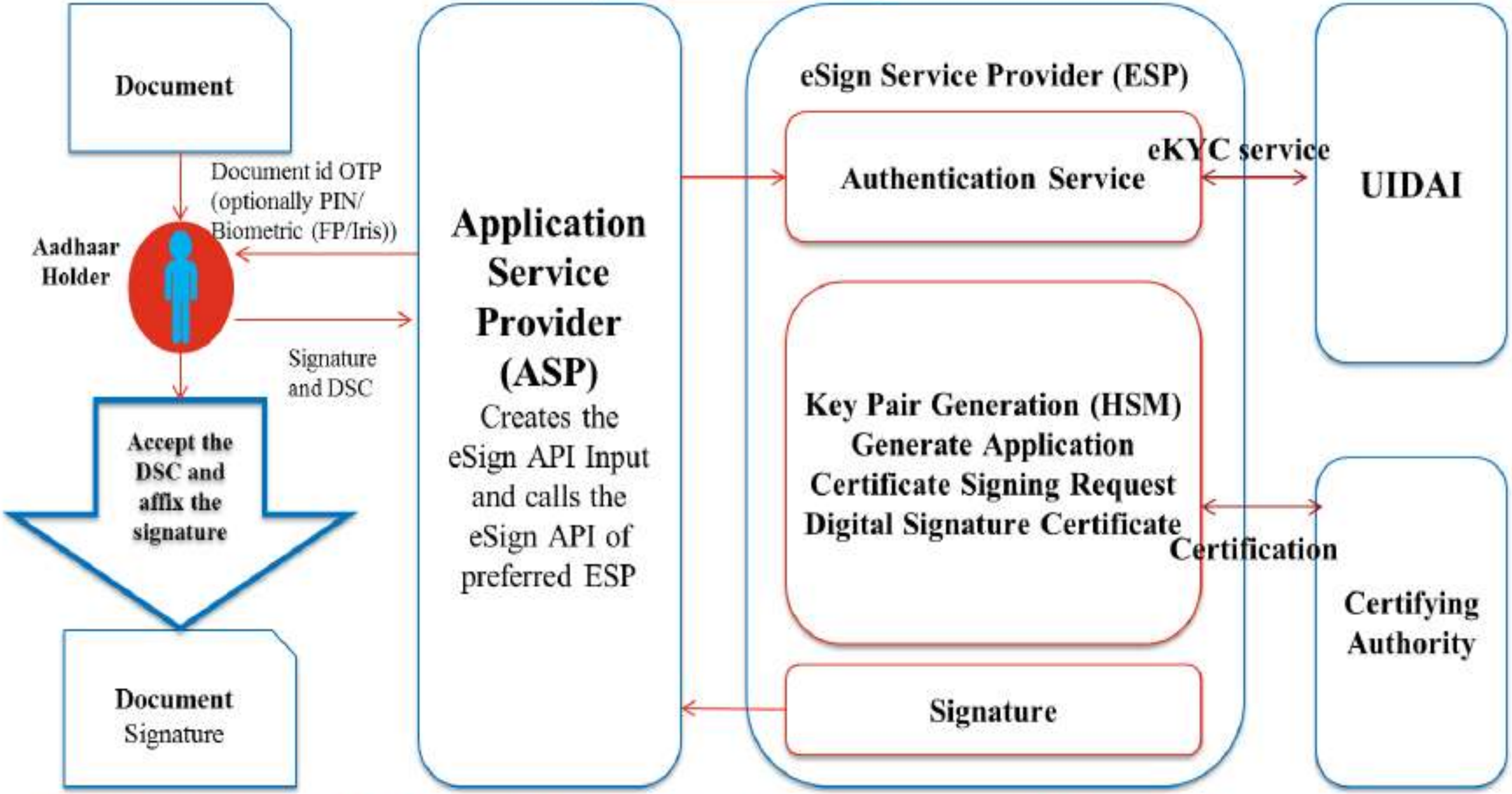

Clients
Mobile / Tablet Applications
Desktop Applications
Internet Applications
HTTPS
Application Service Provider (ASP)
Gateway
eSign Service Providers (ESPs)
Certifying Authorities (CAs)
Aadhar eKYC Services

Biometric (FP/Iris) or OTP or OTP + PIN authentication

Generate eSign API request and send it to Gateway or ESP directly

Connect to ESP directly for biometric (FP/Iris) or OTP authentication

e-Sign Overview


Document
Document id OTP (optionally PIN/ Biometric (FP/Iris))
Aadhaar Holder
Signature and DSC
Accept the DSC and affix the signature
Document Signature
Application Service Provider (ASP)
Creates the eSign API Input and calls the eSign API of preferred ESP
eSign Service Provider (ESP)
Authentication Service
eKYC service
UIDAI
Key Pair Generation (HSM) Generate Application Certificate Signing Request Digital Signature Certificate
Certification
Certifying Authority
Signature

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

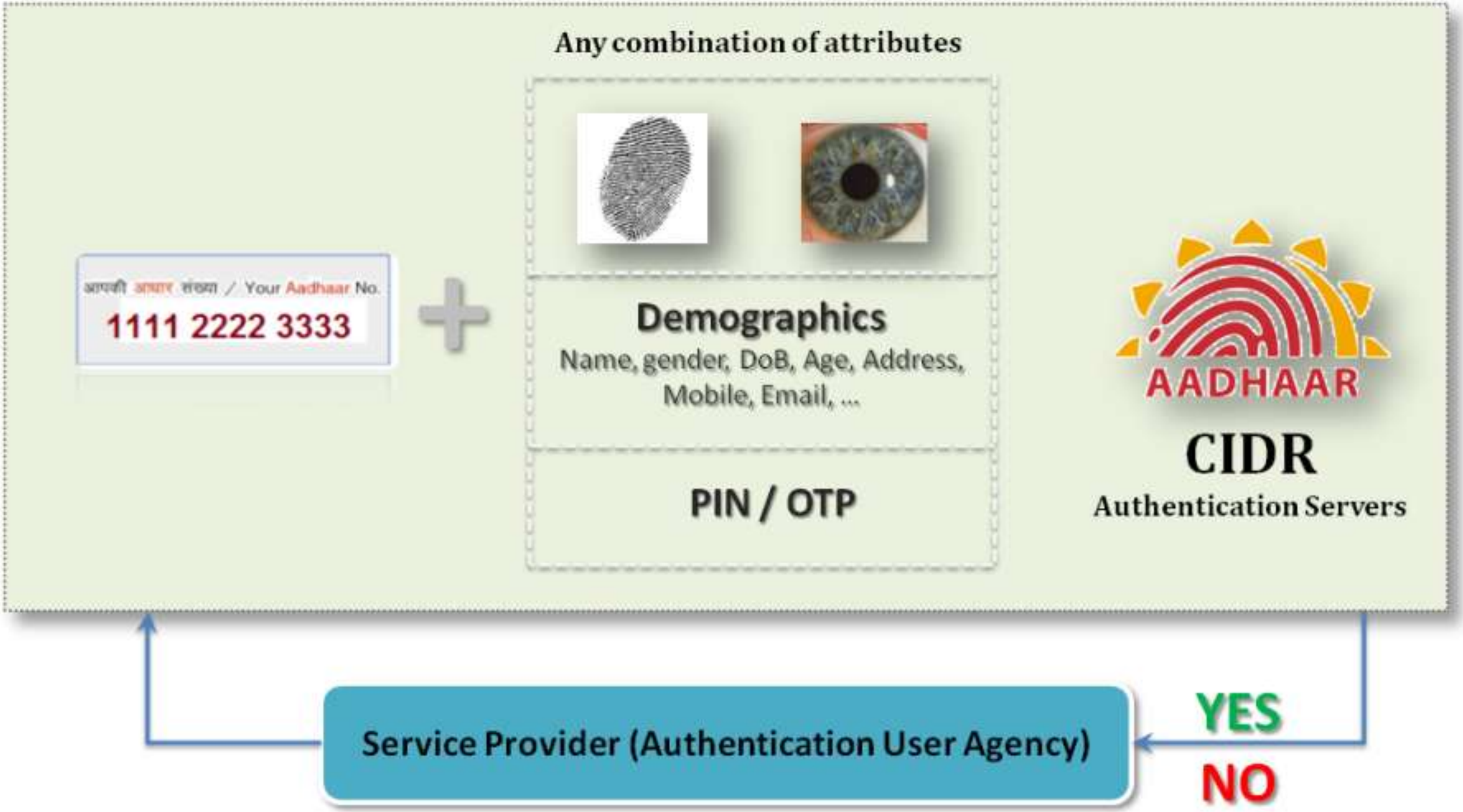
UIDAI – Unique Identification Authority of India

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

Aadhaar Authentication EcoSystem

A Typical Aadhaar Authentication



Any combination of attributes

आपकी आधार संख्या / Your Aadhaar No.

1111 2222 3333

+

Demographics

Name, gender, DoB, Age, Address, Mobile, Email, ...

PIN / OTP

AADHAAR

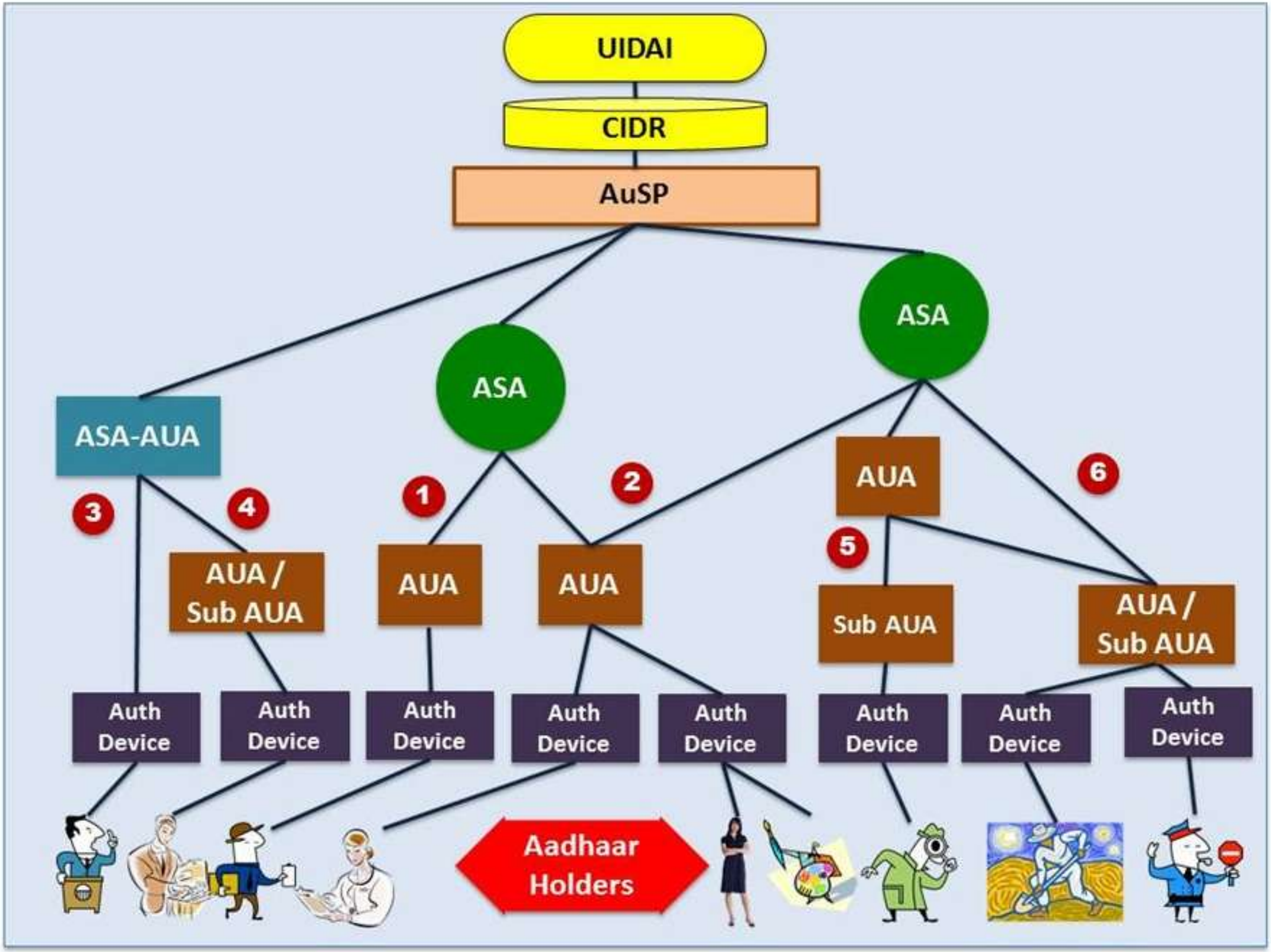
CIDR

Authentication Servers

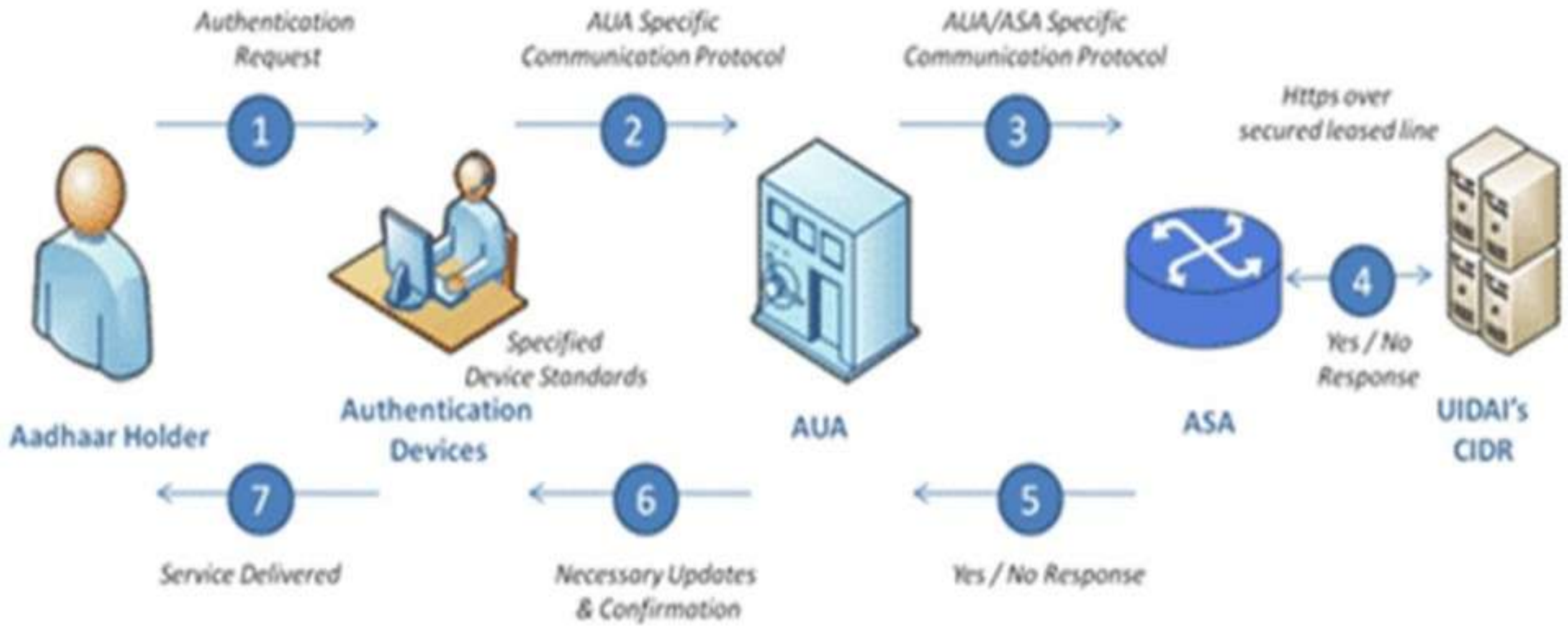
Service Provider (Authentication User Agency)

YES

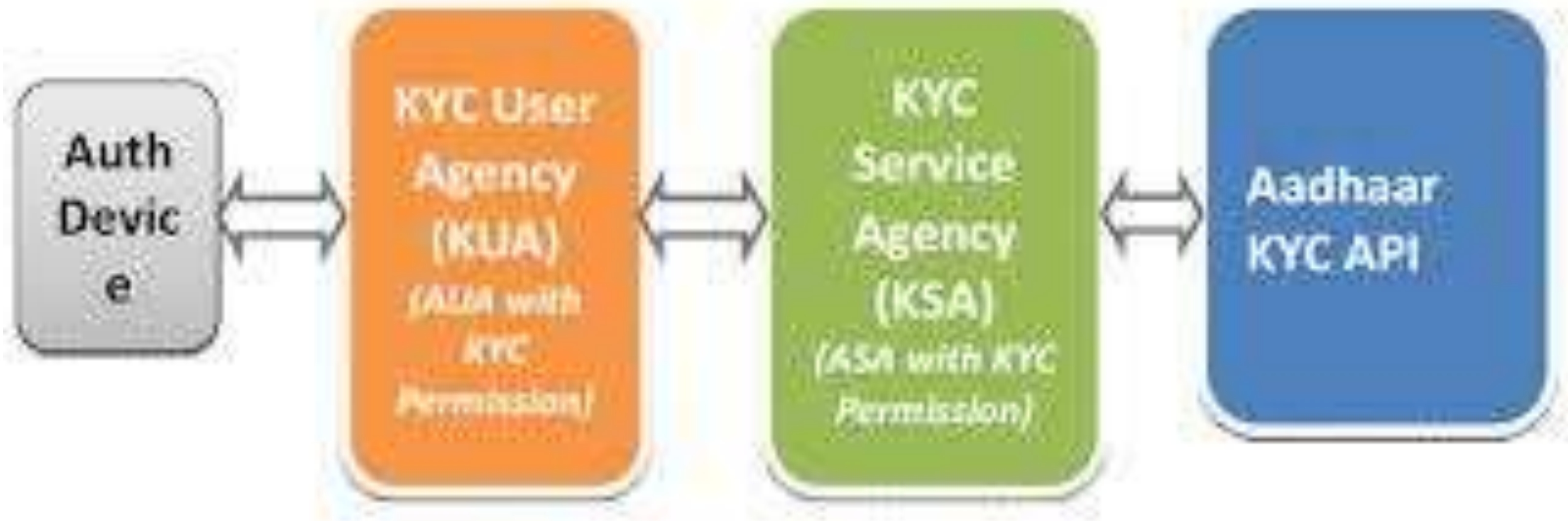
NO


UIDAI
CIDR
AuSP
ASA
ASA
ASA-AUA
3
4
1
2
AUA
6
5
AUA / Sub AUA
AUA
AUA
Sub AUA
AUA / Sub AUA
Auth Device
Auth Device
Auth Device
Auth Device
Auth Device
Auth Device
Auth Device
Auth Device
Aadhaar Holders

Authentication Flow (AUA & ASA)

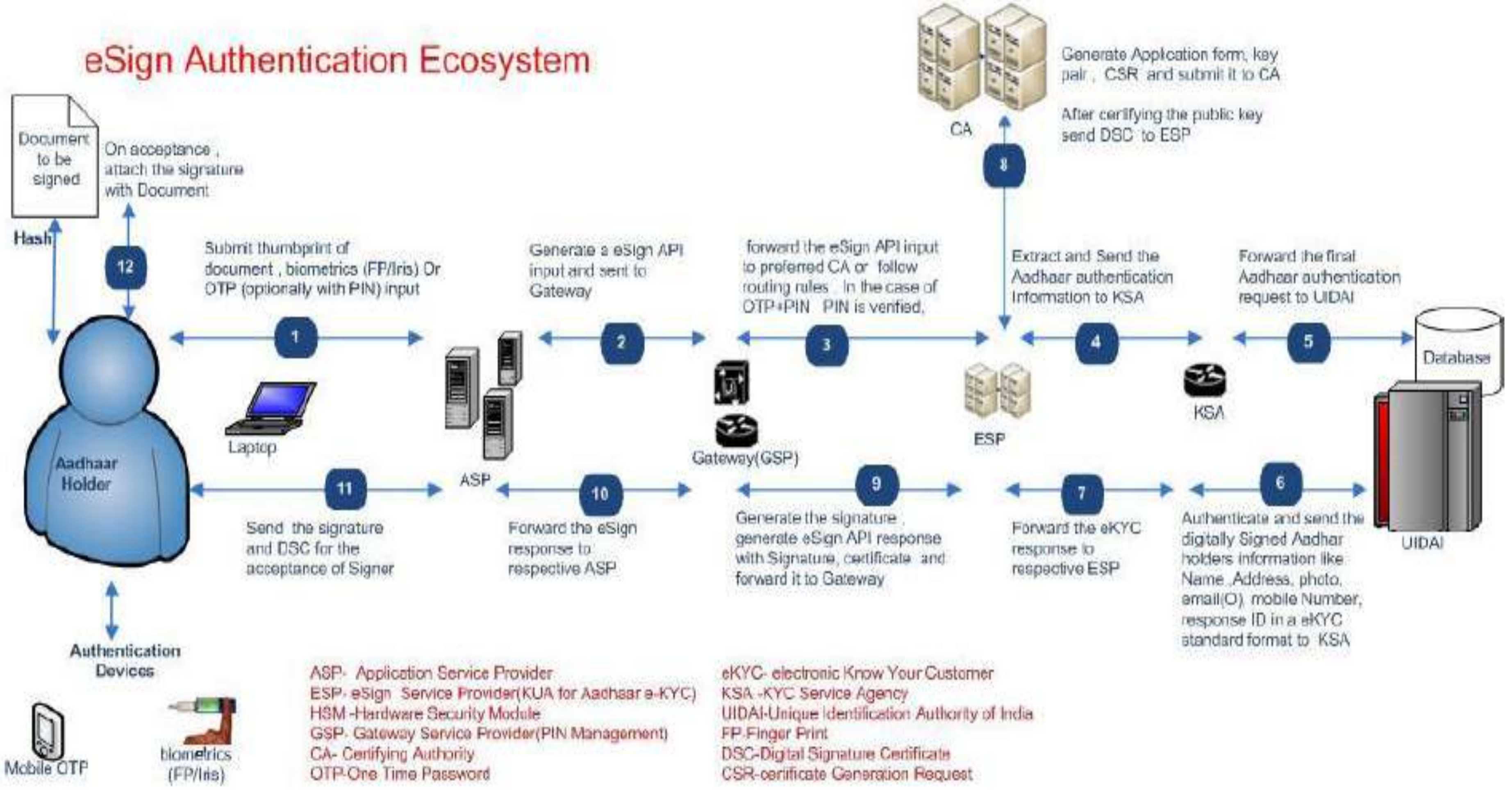

Authentication Request
1
AUA Specific Communication Protocol
2
AUA/ASA Specific Communication Protocol
3
Https over secured leased line
4
Yes / No Response
Specified Device Standards
Aadhaar Holder
Authentication Devices
AUA
ASA
UIDAI's CIDR
7
Service Delivered
6
Necessary Updates & Confirmation
5
Yes / No Response

Aadhaar eKYC – KUA & KSA


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

- Auth Device captures Aadhaar No. & Biometric; forwards encrypted packet to KUA
- KUA creates KYC XML and passes to KSA
- KSA forwards KYC XML to Aadhaar eKYC API
  - If Biometric Auth is successful, demographic data and photo is given to KSA in encrypted format
  - KSA then sends the packet to KUA, which formats for user

e-Sign Authentication Ecosystem



eSign Authentication Ecosystem

Document to be signed

On acceptance , attach the signature with Document

1 Submit thumbprint of document , biometrics (FP/Iris) Or OTP (optionally with PIN) input

2 Generate a eSign API input and sent to Gateway

3 forward the eSign API input to preferred CA or follow routing rules . In the case of OTP+PIN PIN is verified.

4 Extract and Send the Aadhaar authentication Information to KSA

5 Forward the final Aadhaar authentication request to UIDAI

6 Authenticate and send the digitally Signed Adhar holders information like Name ,Address, photo, email(O), mobile Number, response ID in a eKYC standard format to KSA

7 Forward the eKYC response to respective ESP

8 Generate Application form, key pair , CSR and submit it to CA

After certifying the public key send DSC to ESP

9 Generate the signature , generate eSign API response with Signature, certificate and forward it to Gateway

10 Forward the eSign response to respective ASP

11 Send the signature and DSC for the acceptance of Signer

12

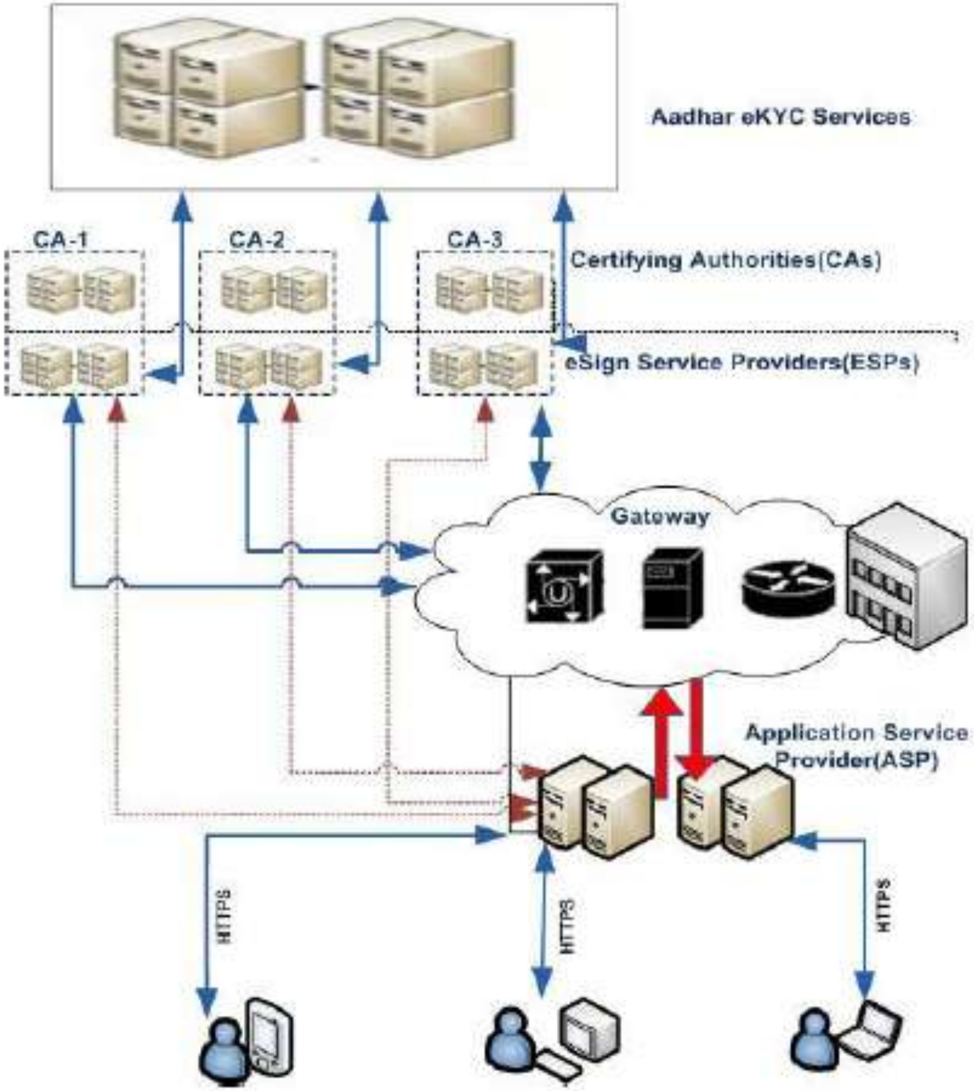
ASP- Application Service Provider
ESP- eSign Service Provider(KUA for Aadhaar e-KYC)
HSM -Hardware Security Module
GSP- Gateway Service Provider(PIN Management)
CA- Certifying Authority
OTP-One Time Password

eKYC- electronic Know Your Customer
KSA -KYC Service Agency
UIDAI-Unique Identification Authority of India
FP-Finger Print
DSC-Digital Signature Certificate
CSR-certificate Generation Request

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.
  - **Aadhaar-eKYC – Biometric (FP/Iris**):
    - This class of certificate shall be issued based on biometric authentication of subscriber through Aadhaar e-KYC service.

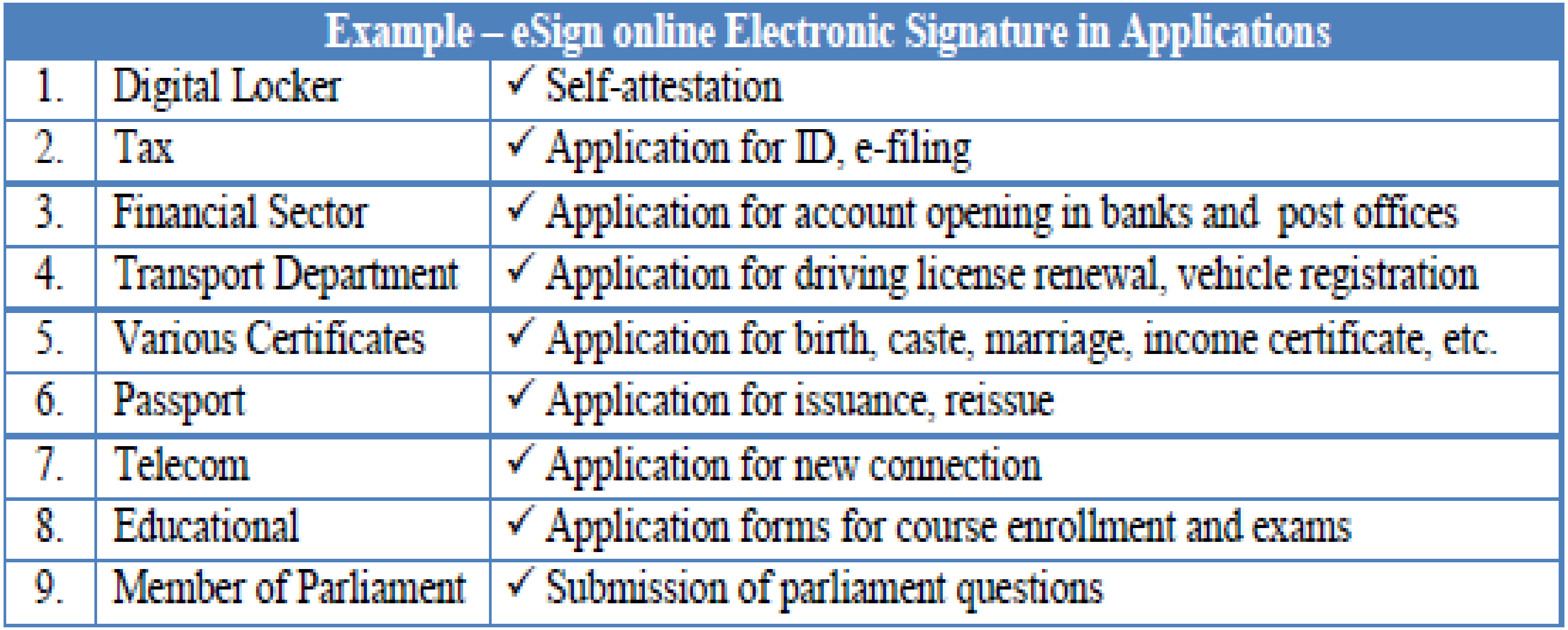
e-Sign Services (Operational Scenario)


Aadhar eKYC Services
CA-1
CA-2
CA-3
Certifying Authorities(CAs)
eSign Service Providers(ESPs)
Gateway
Application Service Provider(ASP)
HTTPS
HTTPS
HTTPS

Two Options for Operating e-Sign Services

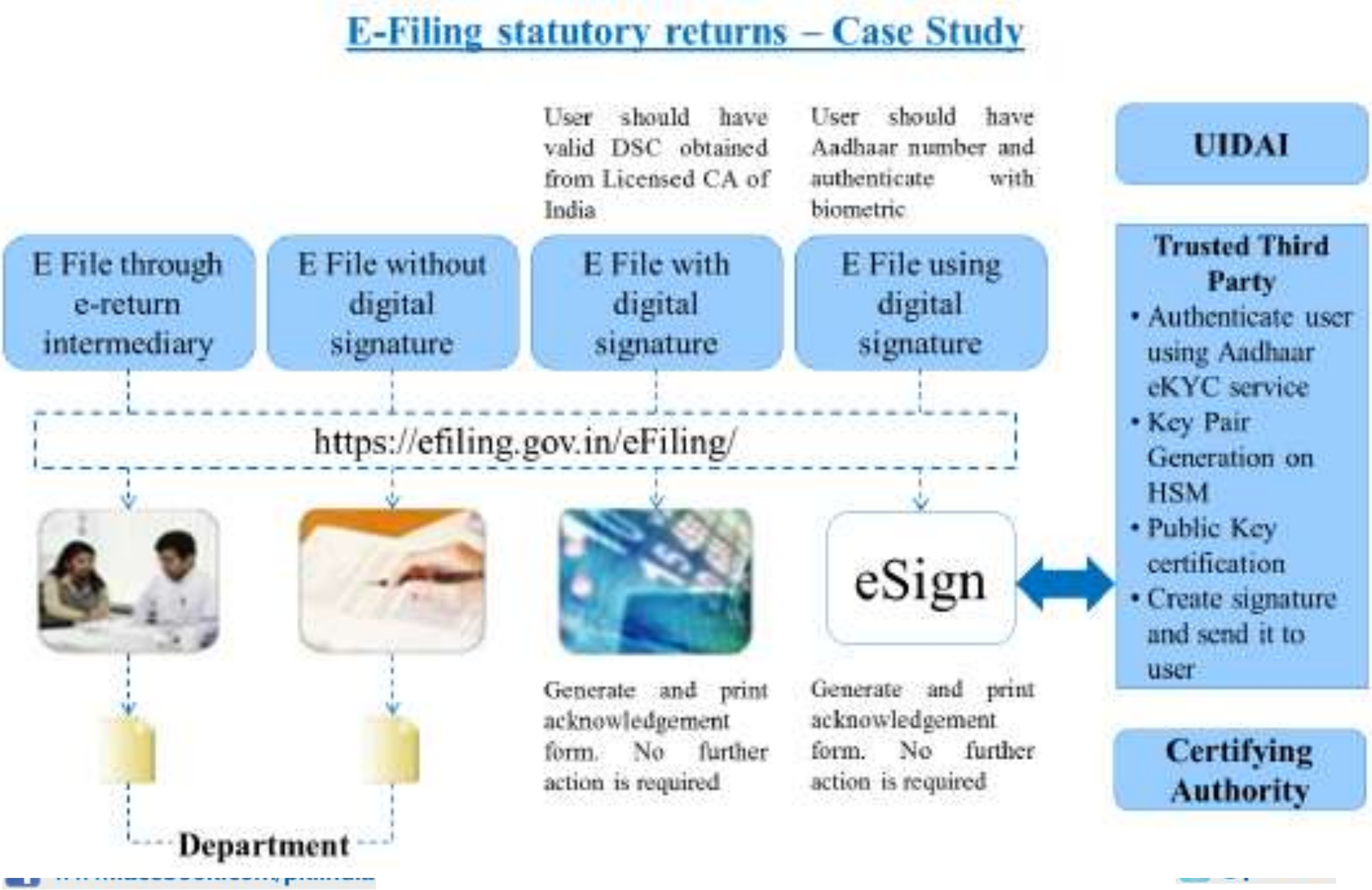
1) Directly Connecting to ESP
2) Using a Gateway Service Provider

Use Cases 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

Case Study : e-Filing



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

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

Generate and print acknowledgement form. No further action is required

Generate and print acknowledgement form. No further action is required

Department

UIDAI

Trusted Third Party

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

Certifying Authority

Benefits of e-Sign

- No need of Hardware Tokens
- No Physical Verification of user is required
  - Instead of manual verification process, eSign utilizes Aadhaar based e-Authentication (an online service)
- Multiple ways to authenticate a user
  - eSign facilitates authentication based on One-Time Password (through registered mobile as in Aadhaar database) or Biometric (fingerprint or iris-scan).
    - C-DAC currently uses Aadhaar-OTP based service for Authentication
- Privacy is preserved
  - As only the thumbprint (i.e. hash) of the document is obtained for digital signature, instead of whole document

C-DAC's e-Sign Service

- e-Hastakshar offers on-line platform to citizens for **instant signing** of their documents securely in a legally acceptable form, under the Indian IT Act
- C-DAC through its **e-Sign/e-Hastakshar** initiative enables citizens with valid Aadhaar ID and registered mobile number to carryout digital signing of their documents on-line.
  - DSC offered by C-DAC CA through eSign service to the applicant is for **one-time signing usage** and shall be of class **"Aadhaar-eKYC – OTP"**.
  - C-DAC utilizes the service of Unique Identification Authority of India (**UIDAI**) for on-line e-authentication and Aadhaar eKYC Service.
  - As a provider of DSC and eSign services, C-DAC plays the role of a Certifying Authority (**CA**) under the Controller of Certifying Authorities (CCA)

Time Stamping

Need for Timestamping

- To support assertions of proof
  - Certificates or Messages can be signed after a signing key has expired or been revoked and could be "back-dated"
- Required for documents meant for wide distribution or for long term storage and archiving purposes
- Generally operated as a Trusted Third Party Service

Applications

- Office automation workflows
- Financial Transactions
- E-filing
- Share trading
- E-mails, Contracts
- Medical records
- E-tendering, E-procurement
- Patent, Trademark & Geographical Indicators (GI) filing
- Code Signing etc.,

How Time stamping is done?

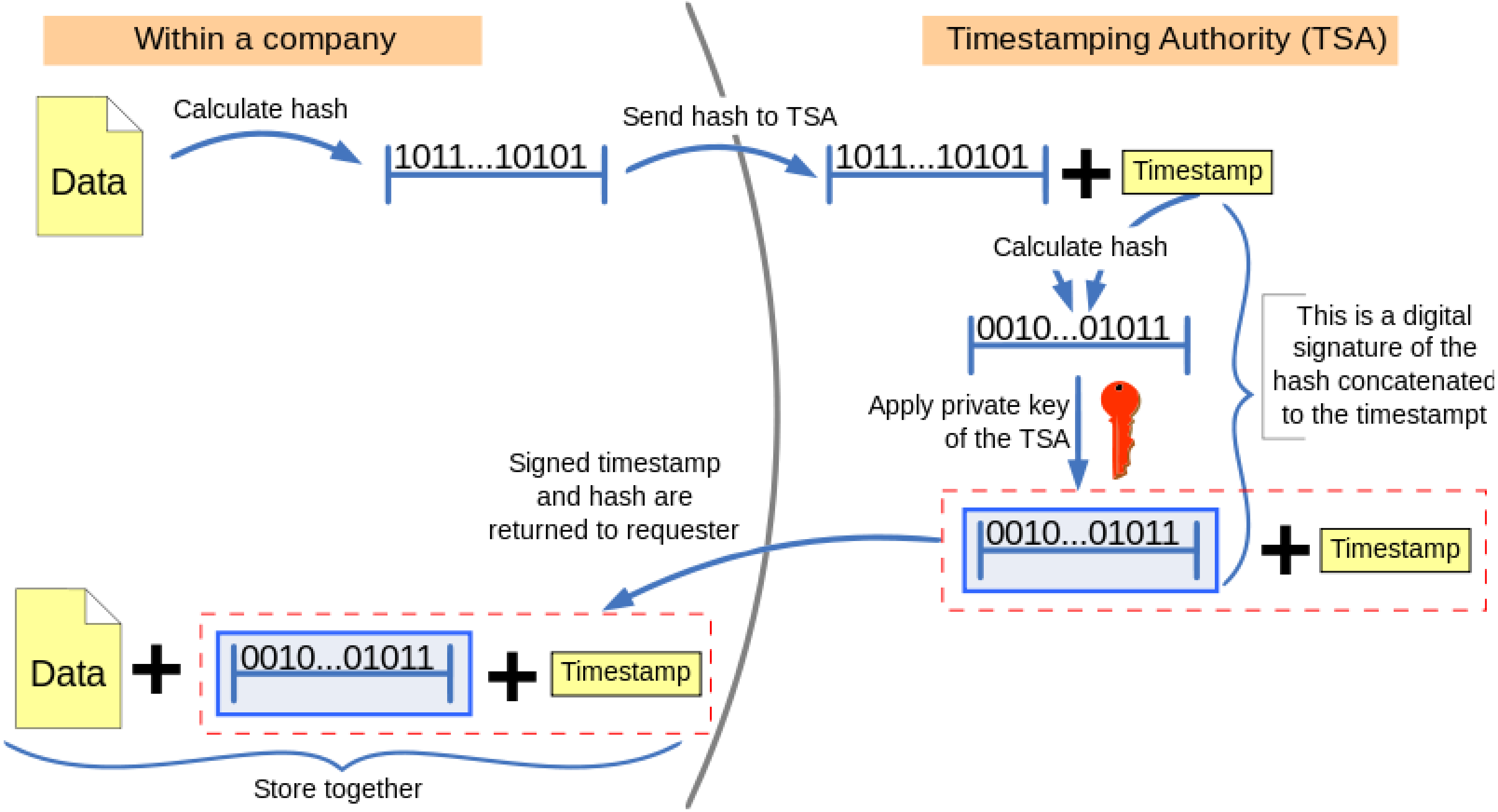
- Time stamping Client
  - Your application
- Time stamping Server
  - Time stamping Authority (TSA)
  - Ex: Verisign, GlobalSign etc…

How Time stamping is done?

- Process
  - Compute hash of your data
  - Send your hash to TSA
    - TSA generally ask you to sign to your hash
  - TSA concatenates a timestamp to the hash and calculates hash of this concatenation. This hash is then digitally signed by TSA.
  - This signed hash + timestamp is sent back to your application which appends it to the original data, and could be sent to the receiver.

How Timestamping is done?

Trusted timestamping


Within a company

Timestamping Authority (TSA)

Data

Calculate hash

1011...10101

Send hash to TSA

1011...10101 + Timestamp

Calculate hash

0010...01011

Apply private key of the TSA

This is a digital signature of the hash concatenated to the timestampt

0010...01011 + Timestamp

Signed timestamp and hash are returned to requester

Data + 0010...01011 + Timestamp

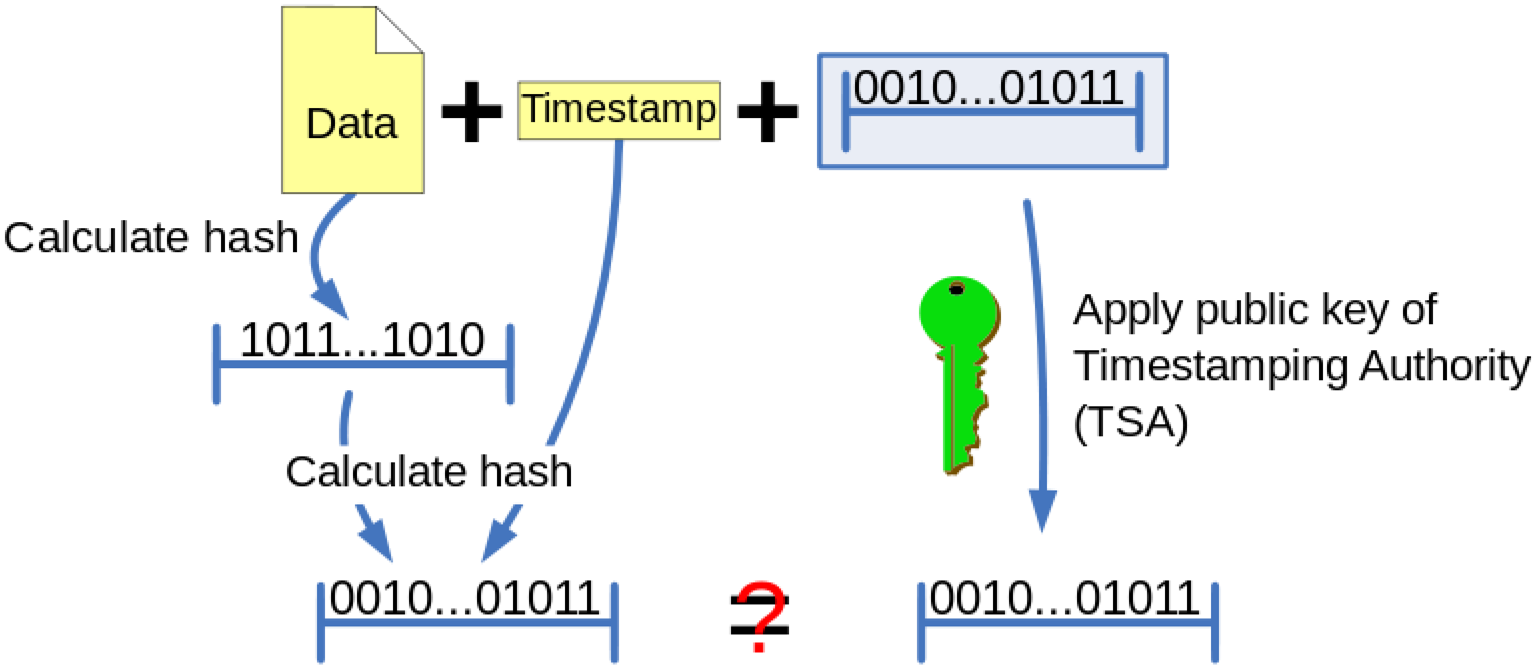
Store together

Validation of Timestamp

- First the hash of the original data is calculated
- Timestamp given by TSA is then appended to the above hash
- Hash of the above is calculated (Let's call it A)
- Digital signature of TSA is validated, which will get the hash of (the original message + timestamp) (Let's call it B)
- If A and B are equal then the timestamp and message has not been altered and timestamp was issued by TSA
- If not either the timestamp was not issued by TSA or the timestamp was altered

Validation of Timestamp

Checking the trusted timestamp



If the calculated hashcode equals the result of the decrypted signature, neither the document or the timestamp was changed and the timestamp was issued by the TTP. If not, either of the previous statements is not true.

Time Stamping Services in India

- In India, time stamping services are provided by CA's and CCA have mandated the CA's to provide the same
- Key points that were mentioned in the Time stamping Guidelines for CAs by CCA are:
  - The CA shall not issue a Time stamping certificate other than for its own time stamping service.
  - The Time stamping service provided by CA should be logically & physically separate from the CA systems.
  - However CA can use the same physical infrastructure and resources.

Time Stamp Requirements

- The National Physical Laboratory, India (NPLI), is responsible for maintenance and development of the Indian Standard Time (IST) .
- NPLI maintains the time scale of Indian Standard Time (IST) with the help of a commercial cesium atomic clock.
- The time scale maintained by NPLI is designated as UTC.
- All the TSAs should synchronize their master clocks with the NPLI based time scale with in the accuracy.

Key Benefits

- Accurate time in conformance with Government Guidelines
- Digitally Signed timestamps
- Verifiable in future
- Assured Integrity and Non-repudiation
- Fraud Detection
- Electronic Notary
- Content to be time stamped is protected from public exposure

Conclusion

- PKI and Digital Signatures have been transforming the way traditional transactions happen
- PKI Ecosystem has the potential to usher
  - Transparency
  - Accountability
  - Time, Cost & Effort-savings
  - Speed of execution and to be an integral part of
  - **Digital India and bring in Digital Identity**

References

- Cryptography and Network security – Principles and Practice by William Stallings
- Applied Cryptography: Protocols, Algorithms, and Source Code in C by Bruce Schneier
- Handbook of Applied Cryptography, by Alfred Menezes and Paul Van Oorschot
- Ryder, Rodney D, Guide to Cyber Laws, 3rd Edition, Wadhwa & Company, New Delhi
- Digital Certificates: What are they?: http://campustechnology.com/articles/39190_2
- Digital Signature & Encryption: http://www.productivity501.com/digital-signatures-encryption/4710/
- FAQ on Digital Signatures and PKI in India - http://www.cca.gov.in/cca/?q=faq-page
- Controller of Certifying Authorities – www.cca.gov.in
- e-Sign: http://www.cca.gov.in/cca/?q=eSign.html
- More Web Resources
  - Social Media: www.facebook.com/pkiindia @pkiindia

C-DAC Activities in PKI Domain

- PKI Knowledge Dissemination Program
  - An effort to spread awareness and build competencies in the domain across the country
- PKI Body of Knowledge
  - To develop a BoK with inputs from various sections of users
    - Researchers – Algorithms and new directions in PKI
    - Developers – PKI Administration and implementation issues
    - Policy Makers - Laws
    - End Users and Applications

CCA

सी डैक
CDAC

Thank You

pki@cdac.in