# Authentication Scenarios India

*Ramachandran*

# India

- 1.2 billion residents
- -640,000 villages
- -~800 million mobile, ~200-300 mn migrant workers

# Authentication Scenarios

- Government – e-praman  authentication framework
  - PKI In Authentication
  - Aadhaar  based authentication
- Banking scenarios
- eSign Initiatives

# Government

# e-Pramaan – An e-Authentication Service

- e-Pramaan is a National Electronic Authentication Service for the Govt. Agencies to Authenticate the citizens to a desired level of assurance and confidence.
- It leverages on Aadhaar based Authentication of different levels to authenticate the citizens
- e-Pramaan provides solution to all the issues of Basic Authentication

# e-Pramaan – An e-Authentication Framework

- e-Pramaan maintains Two Repositories
  - Identity Repository: For user Identities
  - Credential Repository: For Authentication Credentials
- Authentication can be done for Internet based or Mobile based e-Gov services
- e-Pramaan will offer "e-Authentication as a service" to the citizens and Govt. Agencies
- e-Pramaan defines various Levels of Authentication for services with different sensitivity levels.

# e-Pramaan Authentication Levels

## Level 1


## Level 2



**One-Time Password**

## Level 3


**Crypto Token containing DSC**

## Level 4

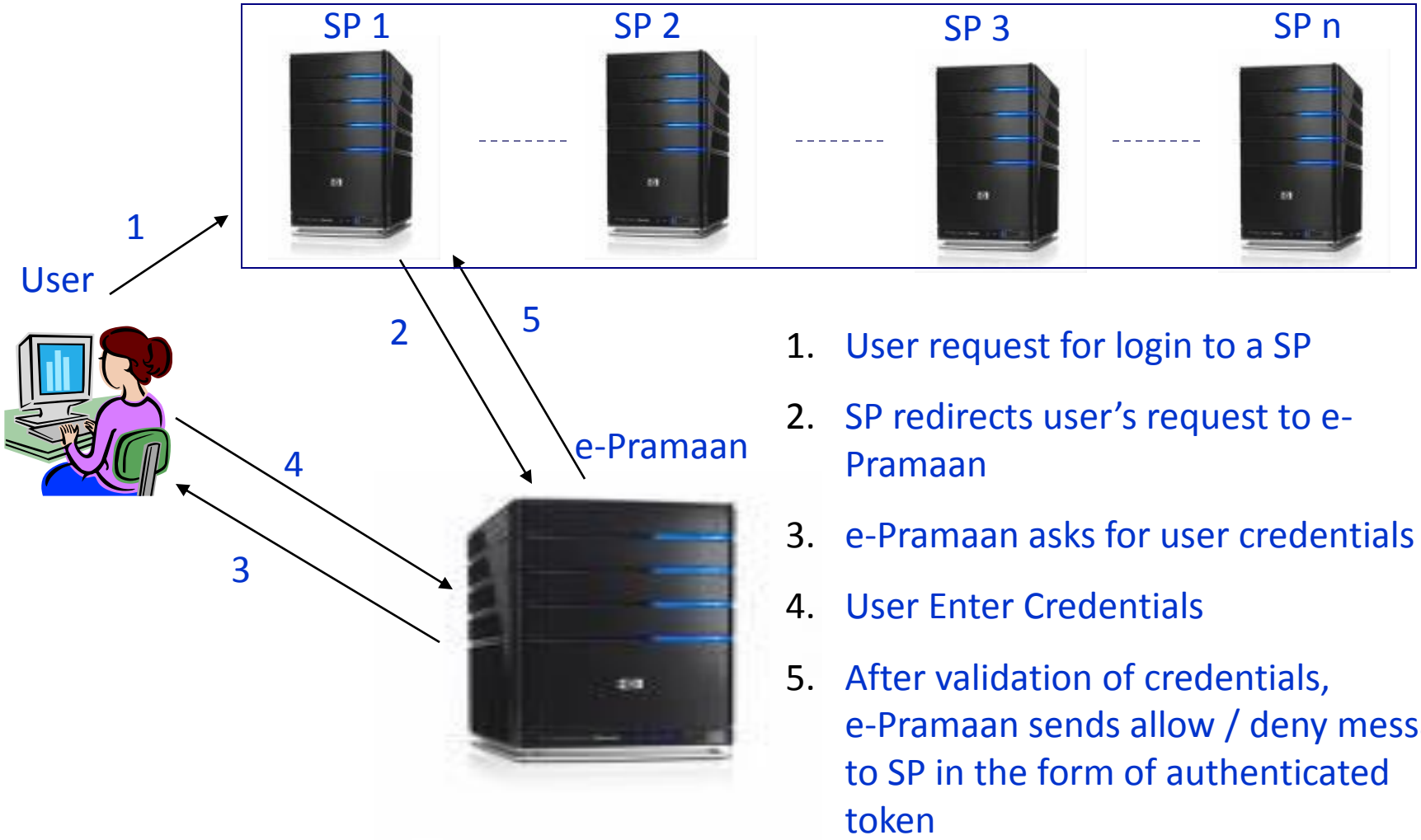


**Finger Print Biometric**

# Key Components of e-Pramaan

- Significant e-Pramaan Offerings:
  - **Single Sign-on** will enable the users to login to a level and thereby access all the services under that level using e-Pramaan Authenticated Token till the session is active
  - **Website Authentication** (to counter Phishing attack) using Digital Certificates
  - **User De-Registration** (in case of duplication/fraudulent users)
  - **Fraud Management**

# Authentication As a Service (AAS) using SSO




1. User request for login to a SP
2. SP redirects user's request to e-Pramaan
3. e-Pramaan asks for user credentials
4. User Enter Credentials
5. After validation of credentials, e-Pramaan sends allow / deny message to SP in the form of authenticated token

## e-Pramaan Website Authentication

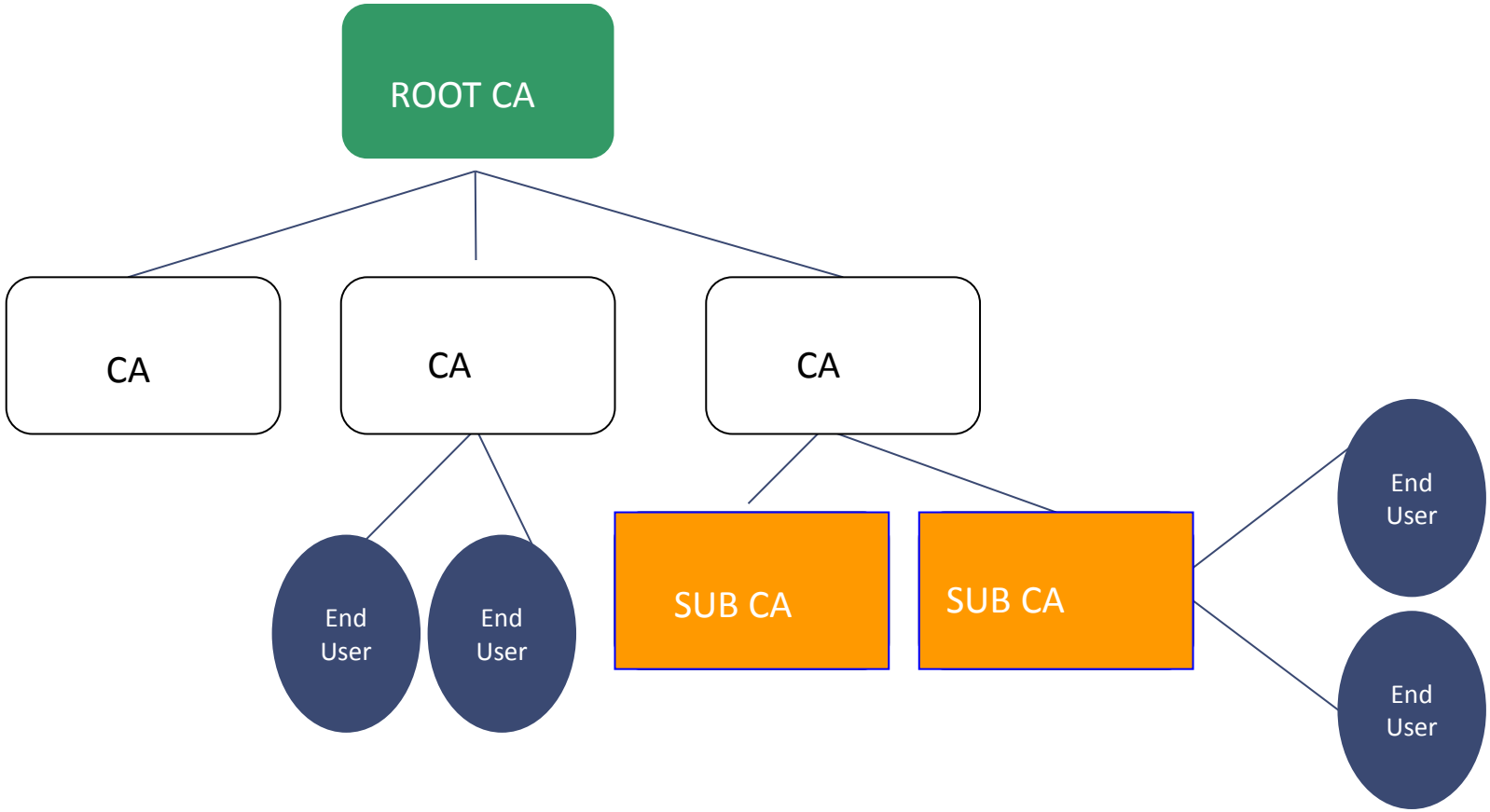
1. SP identifies the level of request & forward a Signed SAML request to e-Pramaan.
2. e-Pramaan verifies the SP, Creates an Authenticated Website Seal and asks the user to enter his credentials.
3. Verify client credentials
4. Once the credentials are verified, e-Pramaan redirects the digitally signed authenticated token to SP containing user's Aadhaar no. etc
5. If response is positive user is forwarded to respective service page.

# PKI BASED AUTHENTICATION

# Electronic Signatures in India

- Digital Signatures created under the Information Technology (IT) Act, 2000 are legally valid
- Credential verification is one of the most important aspects of issuance of Digital Signature Certificate
- About 8 million Digital Signature Certificates issued.

# India PKI Model



# Electronic Signatures in India

- Validity of Digital Signature Certificates is for 3 years
- Three classes of Digital Signature Certificates
- Class 1 - based on verification from widely used databases (software driven)
- Class 2 - based on verification from widely used databases (hardware driven)
- Class 3 - based on verification from widely used databases and physical presence of subscriber (hardware driven)

# LICENSED CAs

- Sifi Technologies
- National Informatics Centre (NIC*)*
- Institute for Development & Research in Banking Technology (IDRBT*)*
- Tata Consultancy services (TCS)
- (n)Code Solutions (GNFC)
- eMudhra Consumer Services (eMudhra)
- Indian Airforce (IAF)

# Few PKI enabled Applications

**E-filing**
- MCA21
- Income Tax e-filing
- DGFT

**Banking Applications**
- RBI Applications (RTGS/SFMS)

**e-Procurement**

- IFFCO
- DGS&D
- ONGC
- GAIL
- Air-India
- Railways

**Others**
- IRCTC
- eOffice

# Recognition of Foreign Certifying Authorities

A foreign CA deemed as recognised if it has been authorised to issue DSCs by a recognised Regulatory Authority established under the laws of a country other than India

1. **Recognition of Foreign Certifying Authorities operating under a Regulatory Authority. Such CAs can be recognised if the following and other conditions are met:-**
   - The level of reliability of PKI environment of the country is at least equal that of India.
   - The Controller (CCA) enters into a MoU with the Regulatory Authority for Mutual Recognition of CAs.
   - Reliability assessment for equivalence

2 **Recognition of Foreign Certifying Authorities not operating under any Regulatory Authority**

**-**Any Foreign CA may apply to Controller for recognition. The recognition process should pass through examination of documents submitted by that CA:

The idea is to provide seamless authentication, message integrity, non-repudiation, & accessibility across jurisdictions facilitating e-commerce & e-Governance

# AADHAAR BASED AUTHENTICATION

# Aadhaar(Biometric)

**Create a Common"national identity" for every "resident‘**

- Biometric backed identity to eliminate duplicates.

-"Verifiable online identity" for portability.

**Application ecosystem using open APIs**

-Aadhar enabled bank account and payment platforms

-Aadhar enabled electronic, paperless KYC

# Aadhaar(Biometric)

- **Enrolment**

  -One time in a person's lifetime

  -Minimal demographics

  -Multi-model biometrics(Fingerprints,Iris)

  -12-digit unique Aadhar number assigned

- **Authentication**

  -Verify "you are who claim to be"

  -Open API based

  -Multi-device, multi-factor

# Digital Signature using Aadhaar based Authentication

Leveraging Aadhaar based authentication onto combined DSC issuance and signing of a document :

- has high potential to scale up the usage of DSC in many applications like Income TAX returns.
- May require some changes in the rules under the Information Technology Act.

# Authentication

Matching of Aadhaar no. and biometrics with the data maintained in the UIDAI's back-end system to enable residents to prove their identity electronically for availing services and benefits

# Aadhaar e-KYC

- provides a convenient  mechanism for agencies to offer an electronic, paper-less KYC experience to Aadhaar holders eliminating insecure and costly paper process

# Verification Requirements for DSCs

Digital Signature Certificates are issued after identity and address verification of DSC applicant.

For higher level assurance level like Class 3 certificate , physical verification is required.

Addhaar e-KYC service can substitute both identity and address verification.

With biometric authentication, Class 3 certificates can be issued to DSC applicant.

# Requirements for e-KYC service

## CAs should function as e-KYC agency

- e-KYC agency is an organization or an entity using Aadhaar authentication as part of its applications to provide services to residents.
- If CAs function as e-KYC agency, the verification requirements for DSC issuance can be substituted with Aadhaar based Authentication .
- Three CAs are in the process of pilot run and e-KYC services will be adopted soon after examining feasibility

# Banking scenario

# Internet Banking authentication

The following security mechanism is available currently on our Net Banking platform every time after login:

- Secure financial site
- „ All communication between customer and the site is encrypted  with SSL encryption is in use.
- „The address bar turns green after accessing the website indicating that the site is secured with an SSL Certificate that meets the Extended Validation Standard.(Supports all leading browsers e.g. Internet Explorer, Mozilla Firefox, Opera, Safari, Google chrome etc.)

## For Retail Customer

1. User Id and Password for Login
2. SMS alert after accessing profile Section.
3. Mandatory SMS based OTP for addition of beneficiary
4. SMS alert on random times during beneficiary approval process.
5. Mandatory SMS based OTP transactions above Rs 10,000 for third party and above Rs 5,000 for merchant transactions.
6. SMS alert for every debit transaction on the registered mobile number.

**Now all the banks should provide PKI based authentication to customers in addition to other mechanisms**

## For corporate customer

1. User Id and Password for Login
2. SMS based OTP or OTP through Hardware Token for Login
3. SMS alert after accessing profile Section
4. Maker Checker Concept for addition of beneficiary and performing transaction
5. Transaction Password to Authorize the transaction
6. Optional SMS based OTP to Authorize the transaction
7. SMS alert for every INB originated debit transaction on the registered mobile number.
8. Digital Signature Certificate (DSC) in lieu of SMS based OTP or OTP through Hardware Token for Login in

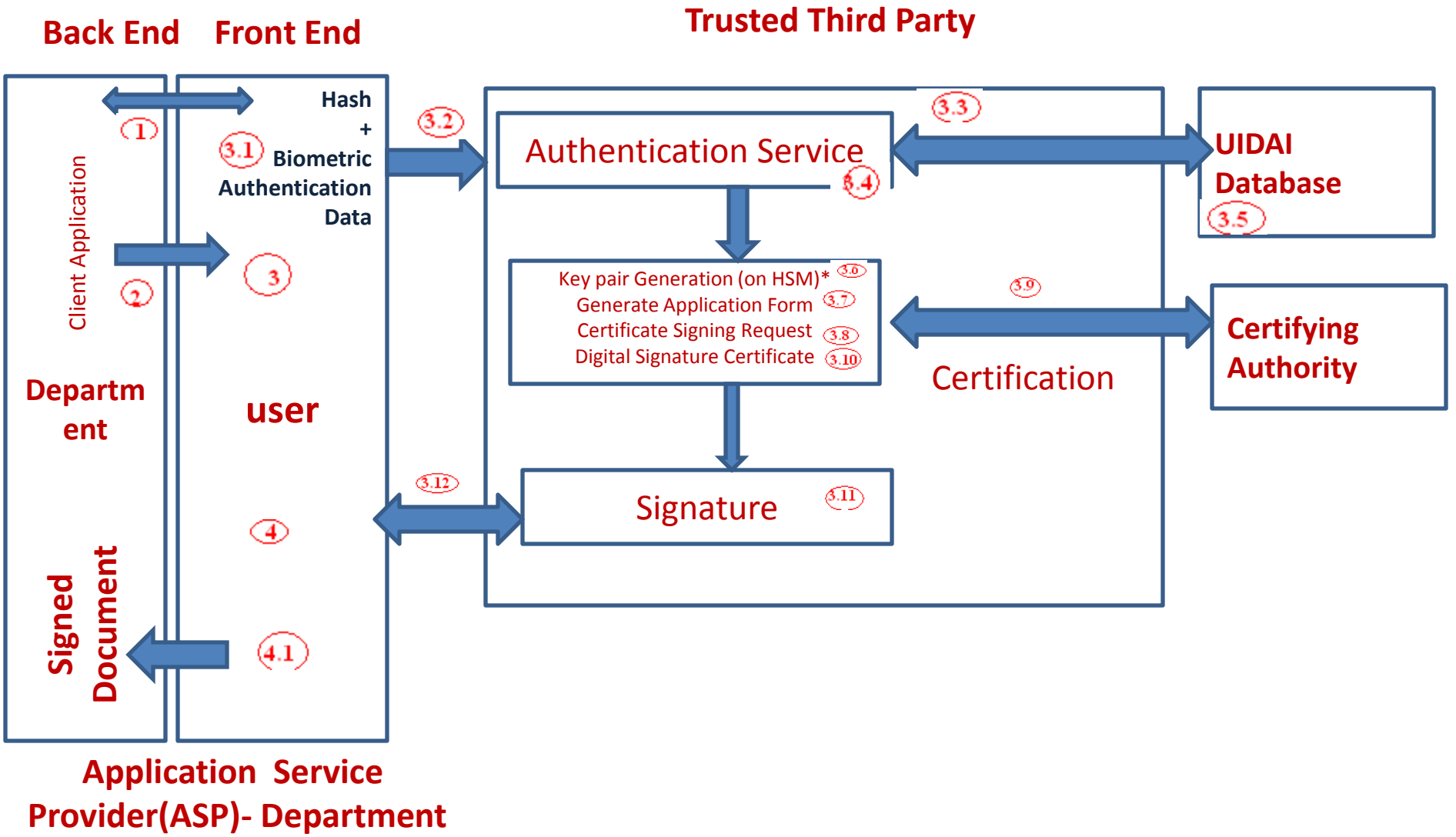
**Recently RBI made the DSC mandatory for corporate customers**

# eSign

# e-Sign

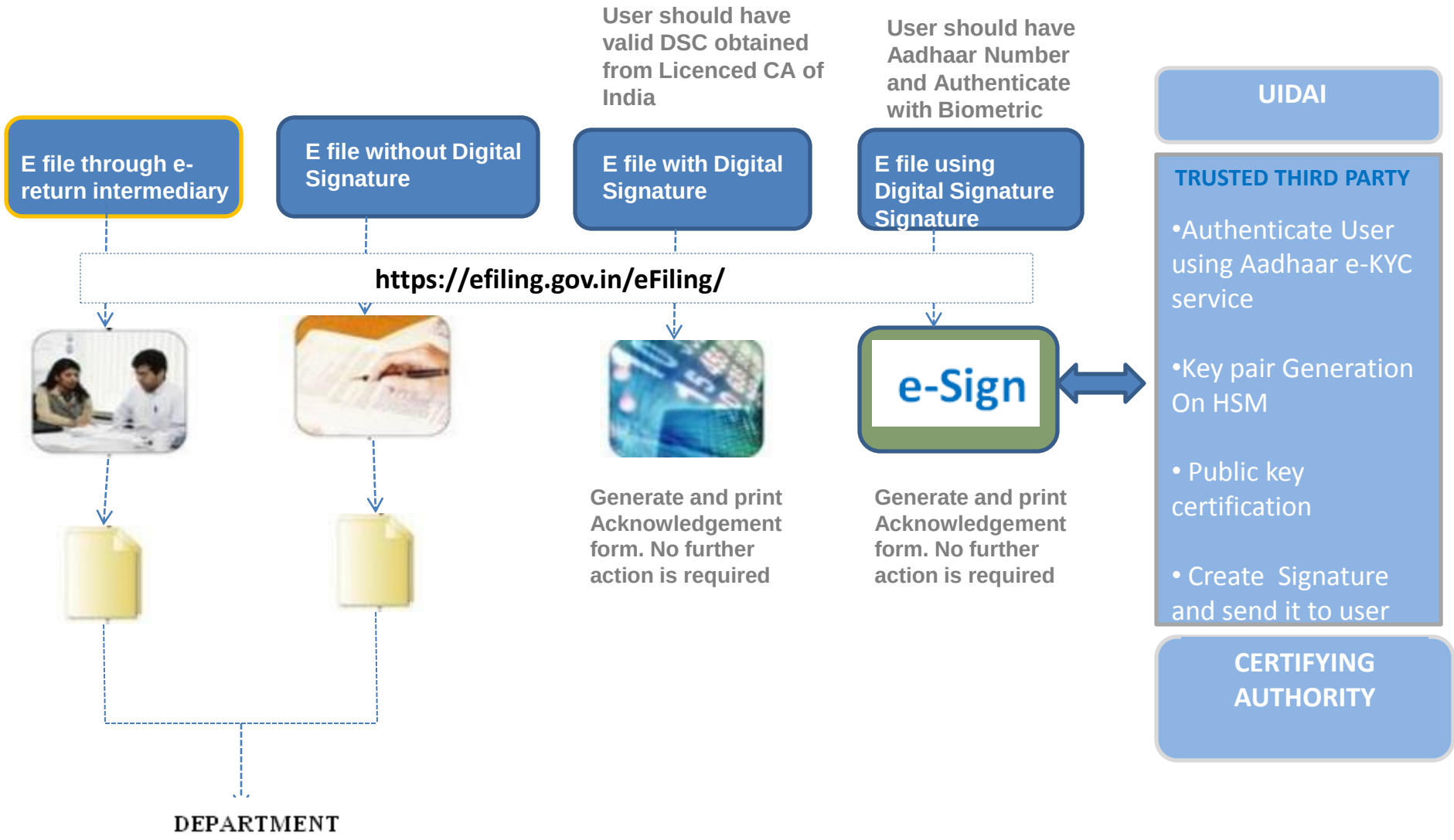
- To enhance and scale up the use of Digital signatures, it is proposed to use Aadhaar(biometric) based Authentication for Digital Signatures of individual(e-Sign).
- The e-Sign proposes digitally signing a document by an Aadhaar holder using an Online Service.
- While authentication of the signer is carried out using e-KYC of Aadhaar, the signature on the document is carried out on a backend server, which is the e-Sign provider.
- The service can be run by a trusted third party service provider.
- The solution has potential to facilitate large scale implementation of Digital Signatures .

# e-Sign




* Hardware Security Module

# E-Filing-statutory returns - case study



# Benefits

- Signature requirements of many applications can be fulfilled with legally valid Digital Signature.
- Digital Signature Certificate enable much larger segment of the population to sign digitally
- Digital Signature Certificates will be of short validity(10 minutes)

Thank you