e-Sign: An online Digital Signing Service

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

Under the Aegis of

Controller of Certifying Authorities (CCA)
Government of India

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

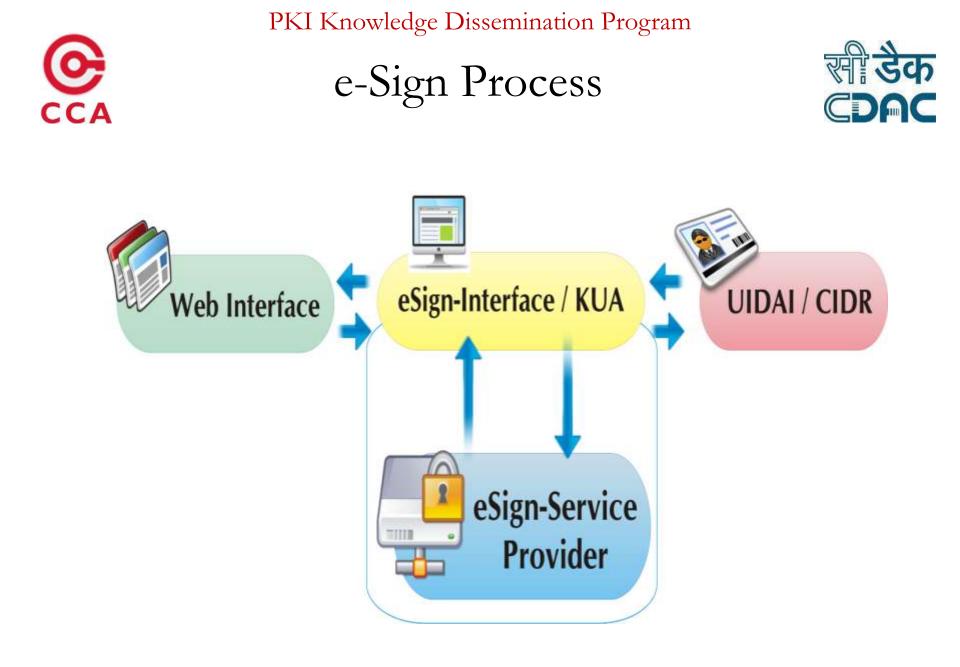# e-Sign – Electronic Signature

- 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.
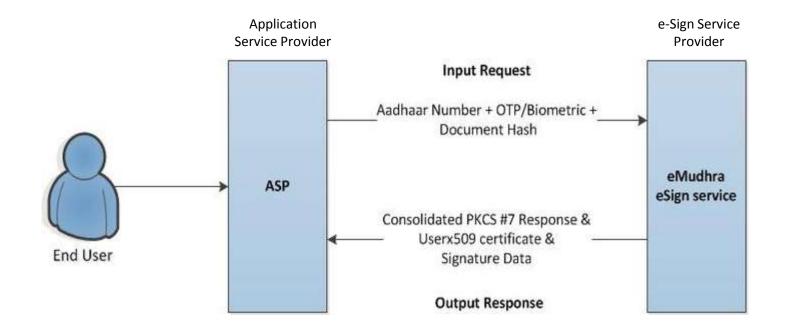
e-Sign Process

e-Sign Service

Application Service Provider

e-Sign Service Provider

Input Request

Aadhaar Number + OTP/Biometric + Document Hash

ASP

eMudhra eSign service

Consolidated PKCS #7 Response & Userx509 certificate & Signature Data

End User

Output Response

Application Service Provider

- **Who is an ASP ?**

An agency which has integrated eSign service – It could 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
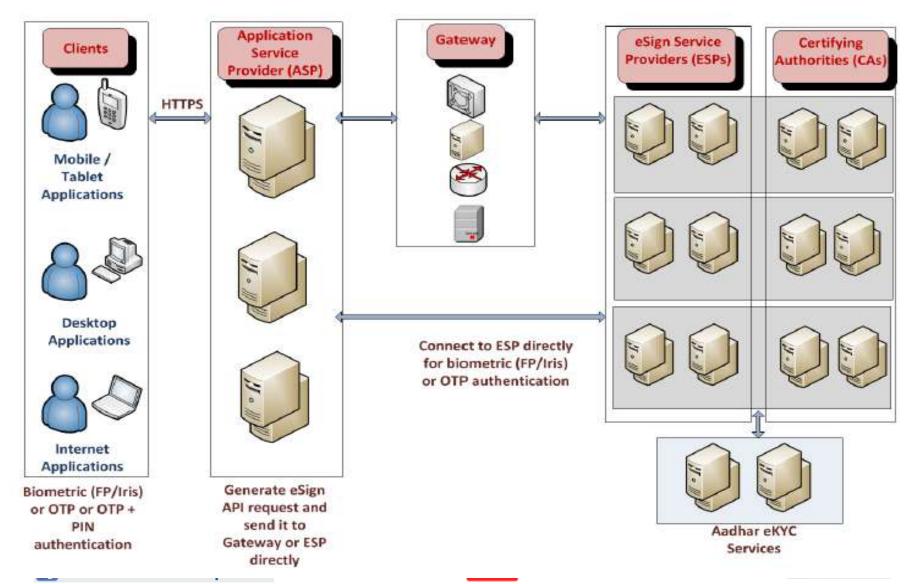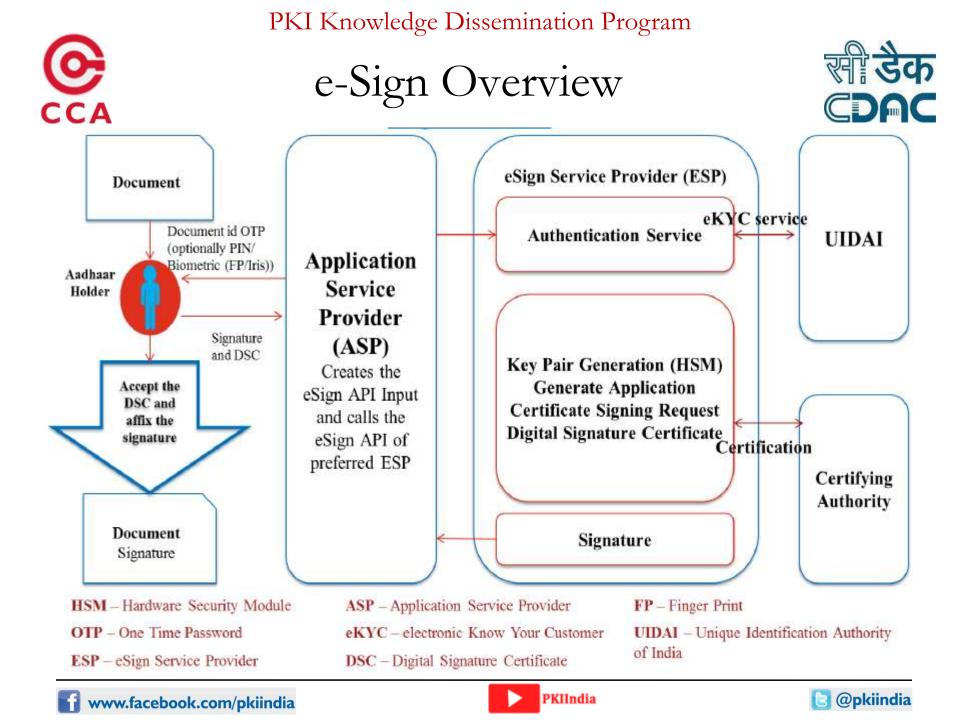
  – A legal entity registered in India

Stakeholders in e-Sign Service

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

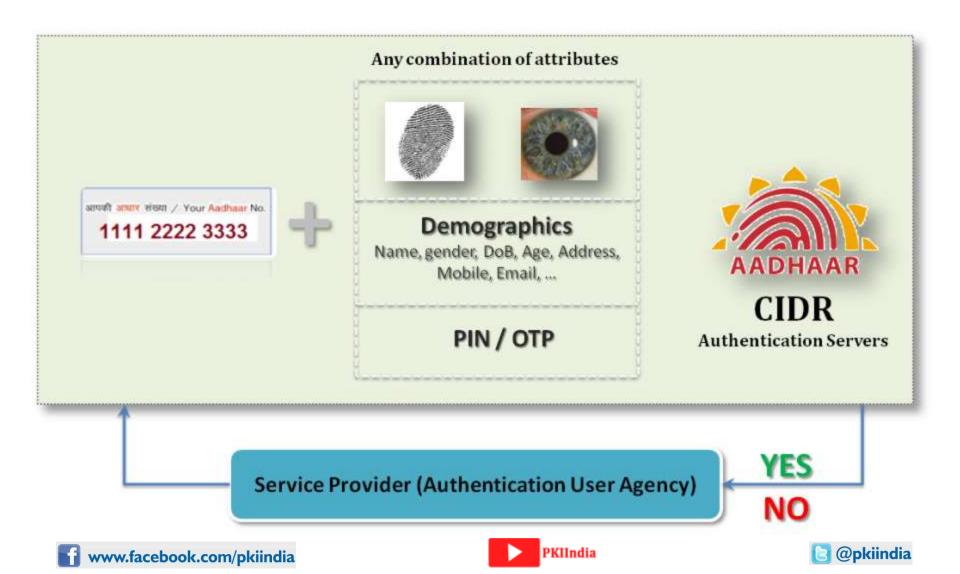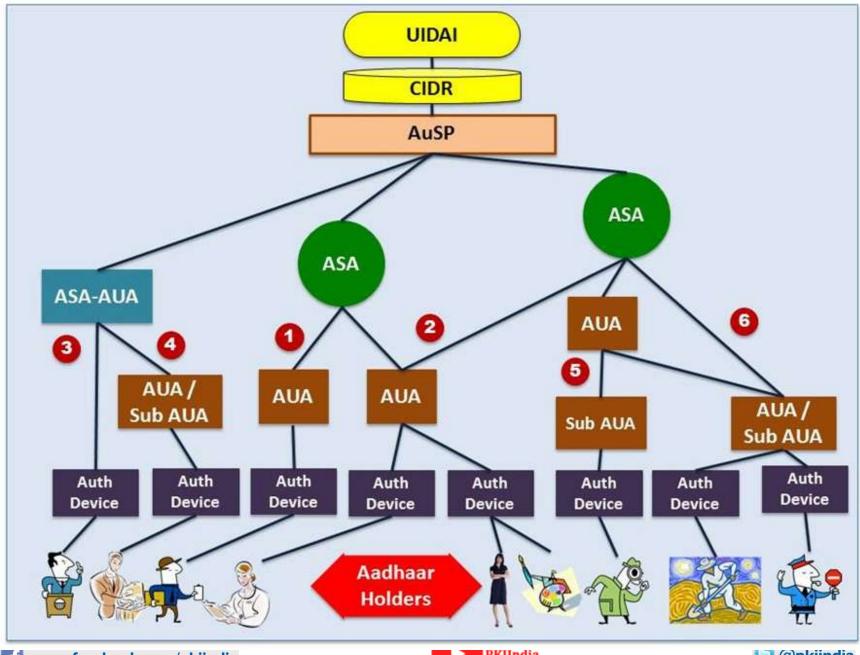| 7.	Invokes the Aadhaar e-KYC API
8.	On success, creates a new key pair for that Aadhaar holder
9.	Create a Certificate Generation Request(CSR) with the Aadhaar e-KYC input received, public key , Response Code
10.	Generate DSC Application form and CSR and submit them to CA
Certifying Authority(CA)	
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

Authentication Flow (AUA & ASA)
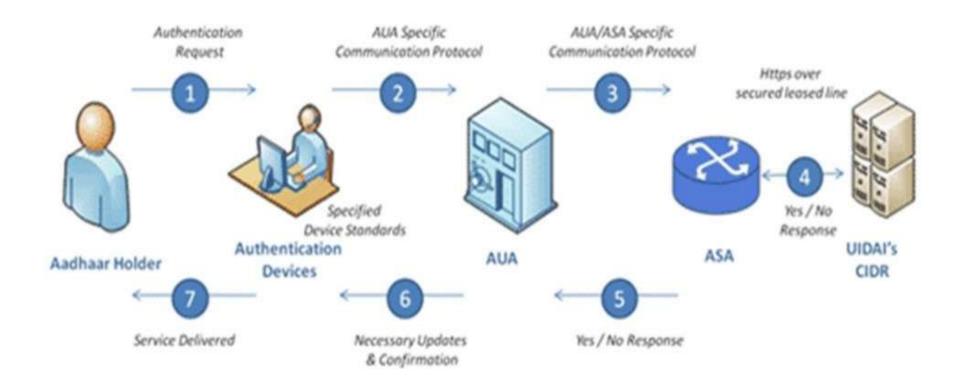
Aadhaar eKYC – KUA & KSA

- 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
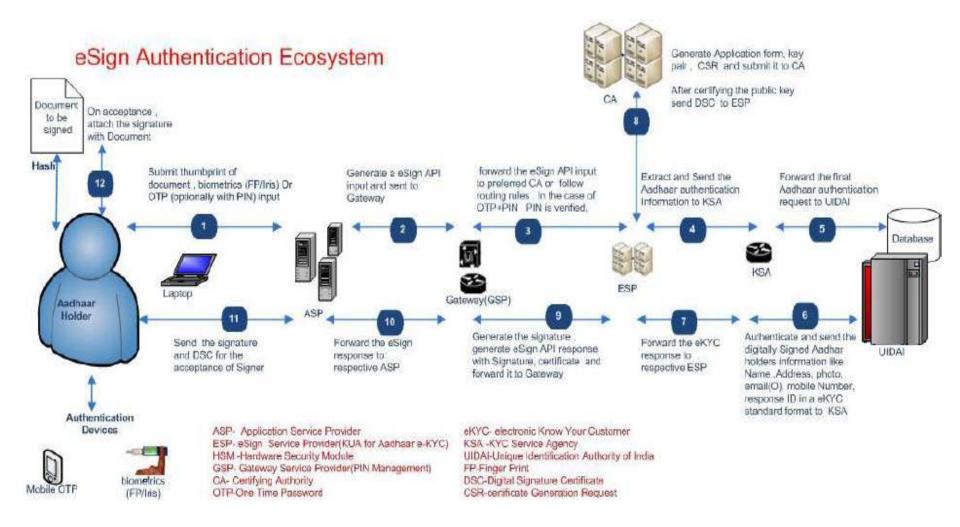 - KSA then sends the packet to KUA, which formats for user

e-Sign Authentication Ecosystem

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.
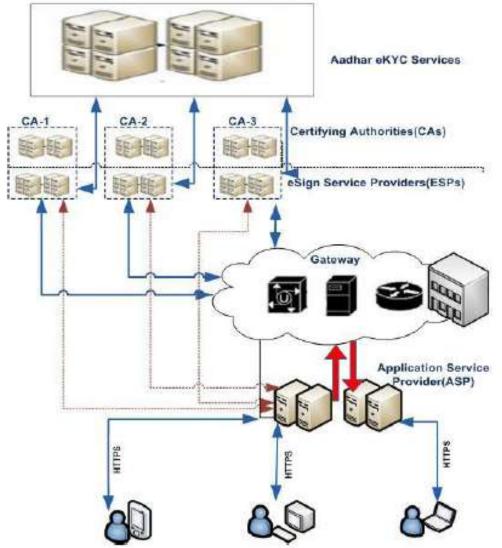
e-Sign Services (Operational Scenario)

Two Options for Operating e-Sign Services
1) Directly Connecting to ESP
2) Using a Gateway Service Provider

Case Study : e-Filing

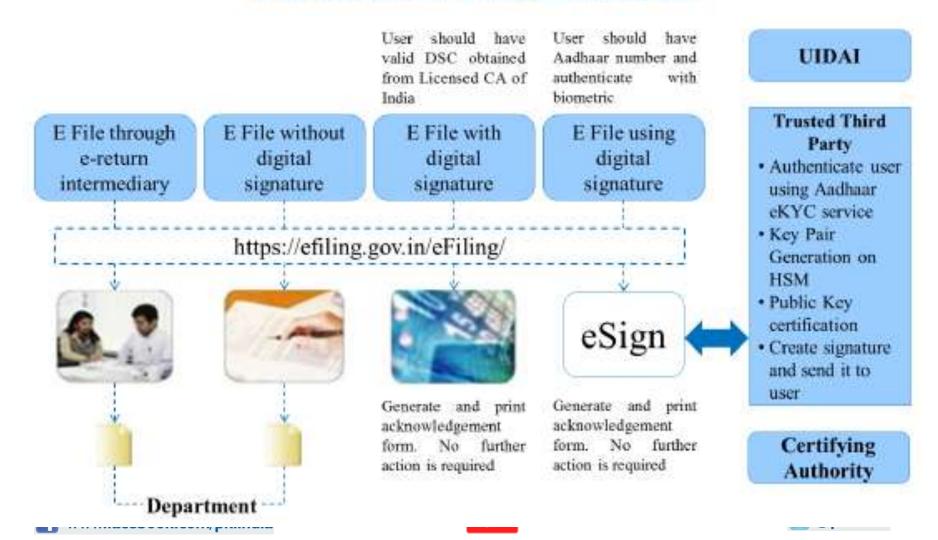## E-Filing statutory returns – Case Study

		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

UIDAI

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

Use Cases of e-Sign Services

S.No	e-Sign Application	Purpose
1	Digital Locker	Self Attestation
2	Income Tax	e-Filing
3	Banks & Financials	Application for Account Opening
4	Transport Department	Application for License Renewal, Vehicle Registration
5	Certificates	Application for Birth, Caste, Marriage, Income etc…
6	Passport	Application for Issuance, Reissue
7	Telecom	Application for new connection
8	Education	Application for Course enrollment, Scholarships, Exam etc..
9	Members of Parliament	Submission of Parliament Questions

Recent e-Sign Applications

- Account Opening – Axis Bank

- Demat & Trading Account Opening – Motilal Oswal

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)

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**

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

Thank You

pki@cdac.in