eSign Online Electronic Signature Service

Overview

What is eSign?
eSign facilitates digitally signing a document by an Aadhaar holder using an Online Service. eSign is designed for applying Digital Signature using authentication of signer through Aadhaar e-KYC service. This is an integrated service which facilitates issuing a Digital Signature Certificate and performing Signing of requested data by authenticating the Aadhaar holder. Aadhaar ID is mandatory for availing the eSign Service.

The Government has introduced Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015 in which the technique known as “e-authentication technique using Aadhaar e-KYC services” has been introduced for facilitating the eSign Service.

Examples of potential service delivery applications which can migrate to online paperless transactions through eSign are given below.

<table>
<thead>
<tr>
<th>S. n</th>
<th>Department/Sector</th>
<th>Service</th>
<th>Volume projections (per annum)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Digital Locker</td>
<td>Self Signing</td>
<td>2 crore</td>
</tr>
<tr>
<td>2</td>
<td>Income Tax</td>
<td>Pan Issuance</td>
<td>1 crore</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Return Filing</td>
<td>4 crore</td>
</tr>
<tr>
<td>3</td>
<td>Financial Sector</td>
<td>Account opening in Banks</td>
<td>10 crore</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Account opening in Post Office</td>
<td>2 crore</td>
</tr>
<tr>
<td>4</td>
<td>Passport</td>
<td>Issuance</td>
<td>0.6 crore</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Reissue</td>
<td>0.4 crore</td>
</tr>
<tr>
<td>5</td>
<td>Telecom</td>
<td>New Connection</td>
<td>6 crore</td>
</tr>
<tr>
<td>6</td>
<td>Rural Health Insurance</td>
<td>Application</td>
<td>0.3 crore</td>
</tr>
</tbody>
</table>
What Are the Expected Benefits of eSign

- **Easy and secure way to digitally sign information anywhere, anytime** – eSign is an online service that offers application service providers the functionality to authenticate signers and perform the digital signing of documents using Aadhaar e-KYC service. Hardware tokens are not required to be used.

- **Facilitates legally valid signatures** – eSign process involves consumer consent, Digital Signature Certificate generation, Digital Signature creation & affixing and Digital Signature Certificate acceptance in accordance with the provisions of the Information Technology (IT) Act, 2000. It enforces compliance, through API specification and licensing model of APIs. Comprehensive digital audit trail - in-built to confirm the validity of transactions is also preserved.

- **Flexible and easy to implement** - eSign provides configurable authentication options in line with Aadhaar e-KYC service and also records the Aadhaar ID used to verify the identity of the signer. The authentication options for eKYC includes biometric (fingerprint or iris scan) or OTP (through the registered mobile in the Aadhaar database). eSign enables millions of Aadhaar holders easy access to legally valid Digital Signature service.

- **Respecting privacy** - eSign ensures the privacy of the signer by requiring that only the thumbprint (hash) of the document be submitted for signature function instead of the whole document.

- **Secure online service** - The eSign Service is governed by e-authentication guidelines. While authentication of the signer is carried out using Aadhaar e-KYC services, the signature on the document is carried out on a backend server of the e-Sign provider. eSign services are offered by trusted third party service provider, currently Certifying Authorities (CA) licensed under the IT Act. To enhance security and prevent misuse, Aadhaar holders private keys are created on Hardware Security Module (HSM) and destroyed immediately after one time use.

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Save cost and time</td>
</tr>
<tr>
<td>2.</td>
<td>Improve User Convenience</td>
</tr>
<tr>
<td>3.</td>
<td>Easy to apply Digital Signature</td>
</tr>
<tr>
<td>4.</td>
<td>Verifiable Signatures and Signatory</td>
</tr>
<tr>
<td>5.</td>
<td>Legally recognized</td>
</tr>
<tr>
<td>6.</td>
<td>Managed by Licensed CAs</td>
</tr>
<tr>
<td>7.</td>
<td>Privacy concerns addressed</td>
</tr>
<tr>
<td>8.</td>
<td>Simple Signature verification</td>
</tr>
<tr>
<td>9.</td>
<td>Short validity certificates</td>
</tr>
</tbody>
</table>

**eSign Offerings**

eSign is an online service that can be integrated within various service delivery applications via an open Application Program Interface(API) to facilitate digitally signing a document by an Aadhaar holder. It is
designed for applying Digital Signature using authentication of consumer through Aadhaar authentication and e-KYC service.

Based on the verification of identity of the signer and storage of key pairs, three classes of certificates are issued in the traditional way of obtaining Digital Signatures Certificates from the Certifying Authorities. In the case of eSign Online Electronic Signature Service, the Digital Signature Certificates are issued in the following classes.

- **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.

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 secured by Hardware Security Module (HSM) of the eSign service provider and destroyed immediately after one time use at these assurance levels.

### Comparison between Existing DSC Process & eSign Process

<table>
<thead>
<tr>
<th>Stakeholders in DSC issuance</th>
<th>Stakeholders in eSign issuance</th>
</tr>
</thead>
<tbody>
<tr>
<td>o DSC Holders</td>
<td>o Aadhaar holders (= DSC holders)</td>
</tr>
<tr>
<td>o Relying Parties</td>
<td>o Application Service Providers (= Relying Parties)</td>
</tr>
<tr>
<td>o Registration Authorities (RA)</td>
<td>o eSign Service Provider(ESP) (CA operates as ESP)</td>
</tr>
<tr>
<td>o Certifying Authorities(CA)</td>
<td>o Certifying Authorities</td>
</tr>
<tr>
<td></td>
<td>o UIDAI (already has verified PoI, PoA data)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Activities:</th>
<th>Activities:</th>
</tr>
</thead>
<tbody>
<tr>
<td>o DSC applicant submit application</td>
<td>o Application user through ASP submits document hash, Aadhaar number and OTP or Biometric and consent for ESP to generate keys, submit request for DSC CA, and also to generate digital signature</td>
</tr>
<tr>
<td>o RA verify (one time verification PoA, PoI)</td>
<td>o ESP facilitates invoking eKYC request to UIDAI’s CIDR</td>
</tr>
<tr>
<td>o RA issue Hardware crypto Token</td>
<td>o ESP facilitates generation of key pair and submits application form.</td>
</tr>
<tr>
<td>o DSC applicant generate key</td>
<td>o ESP facilitates submission of request for DSC to CA.</td>
</tr>
<tr>
<td>o DSC applicant submit request for DSC to CA</td>
<td>o CA issues the DSC</td>
</tr>
<tr>
<td>o CA issue the DSC to applicant</td>
<td>o ESP facilitates generation of digital signature and sends along with DSC to ASP</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Highlights</th>
<th>Highlights</th>
</tr>
</thead>
<tbody>
<tr>
<td>o DSC issuance and apply of digital signature is independent process</td>
<td>o Integrated Digital signature and DSC issuance based on Aadhaar authentication</td>
</tr>
<tr>
<td>o Obtain DSC one time and use unlimited time till the validity of DSC</td>
<td>o Each time for digital signature, new DSC is issued. DSC is of 30 minutes validity only.</td>
</tr>
<tr>
<td>o CRL verification</td>
<td>o No CRL verification</td>
</tr>
</tbody>
</table>
eSign Operating Model Overview

Key Actors in eSign Ecosystem

Application Service Provider (ASP)
An organization or an entity using eSign service as part of their application to digitally sign the content. Examples include Government Departments, Banks and other public or private organizations. ASP may contact the ESP (eSign Service Provider) directly to avail the service within its framework.

Engagements
- ASPs need to engage with ESPs
- ASPs have to comply to the e-authentication guidelines laid down by CCA
- Examples of ASPs include banks, insurance companies, government departments, telcos etc

eSign Service Provider (ESP)
An organization or an entity providing eSign service. ESP is a “Trusted Third Party”, as per the Second Schedule of Information Technology Act. ESP must be a registered KYC User Agency (KUA) with UIDAI. ESP will facilitate subscriber’s key pair-generation, securing key pairs by hardware security module and creation of digital signature. ESP can be a Licensed Certifying Authority (CA), by themselves, or must be having an arrangement / integration with a CA for the purpose of obtaining Digital Signature Certificate for the generated Key-pair.

Engagements
- Only Certifying Authorities (CAs) can become ESPs. To offer eSign services, they need to adhere to the e-authentication guidelines laid down by CCA
- ESPs need to apply to UIDAI for becoming KUA and follow processes prescribed thereof
- ESP needs to engage with KSA to avail UIDAI’s eKYC service

Certifying Authorities (CA)
A CA is licensed by Controller of Certifying Authorities (CCA) under Information Technology Act to issue Digital Signature Certificates (DSC). CAs issue DSC for authentication of users in cyberspace.

Engagements
- Prior to issuing a DSC, the Certifying Authority (CA) is required to verify the credentials of the applicant as stated in the Application Form and in supporting documents that are attached.
- CAs issue DSC to Aadhaar holder applicant through eKYC authentication service of UIDAI
- CAs use their physical infrastructure and manpower resources for ESP.
An ASA or KSA is an agency that establishes secure leased line connectivity to the Central Identities Data Repository (CIDR) to transmit authentication request on behalf of AUAs or KUA and receive response back from CIDR. An ASA or KSA can serve more than one AUA or KUA. ASAs may also offer value added services to AUAs in addition to providing them with connectivity to CIDR. Such value added services are not managed by UIDAI.

**Engagements**
- An entity desiring to become KSA needs to approach UIDAI
- UIDAI’s website has a list of approved KSAs

**Unique Identification Authority of India (UIDAI)**

An authority established by Government of India to provide unique identity to all Indian residents. It also runs the e-KYC authentication service for the registered KYC User Agency (KUA).

**Engagements**
- UIDAI has the mandate of providing a Unique Identification Number (Aadhaar) to all residents
- Aadhaar is issued on the basis of biometric (fingerprint & iris) and de-duplication; Aadhaar database contains demographic data for residents – name, gender, age/DOB, address
- Through eKYC service of Aadhaar, a resident (after being duly authenticated) can authorize UIDAI to share his/her demographic data & photograph with requesting service providers

**Controller of Certifying Authorities (CCA)**

The IT Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities in compliance with the provisions of the Act. Certifying Authorities (CAs) issue Digital Signature Certificates for authentication of users in cyberspace. CCA is appointed under the IT Act to promote the use of Electronic Signatures in the Country.

**Engagements**
- The CCA is responsible for licensing CAs to issue DSCs under the IT Act and to supervise their activities. For eSign Online Electronic Signature Service, CCA issues the e-authentication guidelines and also facilitates the eSign API.
How ecosystem members engage

Overview of eSign API

eSign Application Programming Interfaces (API) specification defines the major architectural components and also the format and elements of communication among the eSign stakeholders including Application Service Provider, Certifying Authorities, Trusted Third Party eSign Service Providers and Aadhaar e-KYC service. The eSign API specification also contains details including API data format, operations, inputs, outputs, protocol, and security specifications. This eSign API enables Application Service Providers to integrate eSign service in their application.

The eSign service API can be used by ASPs for availing services from:
1. single eSign Service Provider
2. multiple eSign Service Providers

The use of single eSign Service Provider is a straightforward case. However, in case of multiple eSign providers, ASP shall have the above parameters configurable for each request. The routing of requests to each ESP can be in a round-robin manner, or a failure switchover, or an end-user selection basis, or any other manner implemented by ASP.

The Application Service Providers can choose any one of the following options to provide the eSign service to the end user:
- Directly connect to eSign Service Providers (ESP)
- Connect to eSign Service Providers (ESP) through a Gateway Service Provider (GSP)

eSign online service sequence diagram is given below.
Application Service Provider (ASP)

Application Service Providers (ASP) are the entities which will offer the end users, that is, the citizens various services online. The ASPs need to enter into an agreement with the eSign Service Provider (ESP) to provide online electronic signature service to the users through eSign.

ASP Eligibility Criteria

An agency which desires to integrate eSign service should either be:

A. A Central/ State Government Ministry / Department or an undertaking owned and managed by Central / State Government, or
B. An Authority constituted under the Central / State Act, or
C. A Not-for-profit company / Special Purpose organization of national importance, or
Legal entities eligible to apply to use eSign service, shall meet the following requirements:

1) Any organization incorporated under Companies Act, 1956, Registrar of Firms, LLP Registered; or
2) An association of persons or a body of individuals, in India, whether incorporated;
3) The entity should not have been blacklisted by any State Government, Central Government, Statutory, Autonomous, or Regulatory body.

ASP Readiness Stages

1) Registration

In order to register itself as an ASP, the agency must follow the following steps:

- An organization interested in using eSign sends a request to eSign Service Provider to enquire about the eSign service and to understand the process for getting access to it.
- The eSign Service Provider sends a suitable response to the requesting ASP, sharing the ASP related documentation requirements and proposes to conduct kick off session on the eSign services. ESP team shares the contact details of the team managing the organization engagement and provides access to eSign Services knowledge base which includes the documents listed below:
  1. eSign booklet
  2. ASP On-Boarding Guidebook
  3. ASP Application form
  4. ESP-AUA Agreement
  5. List of supporting documents and application process
- ASP submits the application with supporting documents as per the eligibility criteria provided
- ESP engagement team scrutinizes the ASP application and supporting documents as per the guidelines and specifications, list of supporting documents and application process and other documents published from time to time. ESP team will approve the application and inform the ASP
- The ASP On-Boarding Process is initiated to begin ASP’s engagement with ESP.

2) Contract and Agreement Signing

At this stage, an ASP is expected to understand the ESP services and agree to fulfill the requirements as per specifications including setting up infrastructure and aligning business process applications to the eSign services.

- Once both ASP and ESP are satisfied, they proceed to sign an agreement
- ESP and ASP enter into the agreement

3) Integration Kit

Once the agreement have been signed, the ASP is provided with the integration kit which shall include, but not be limited to, the following: API, URL, etc.

- Based on interaction during the previous steps of the process and inputs, an ASP assesses the level of support it requires for go-live readiness
- If the ASP team feels that it requires assistance in setting up its services, it can seek help of ESP.
- ASP team engages with an ESP to define the schedule and agenda of on boarding process which provides access to preparation material on eSign services to better prepare an ASP for the process
• ASP builds the required infrastructure for adopting eSign service with support provided by the approved agency. Once the required infrastructure for eSign service is ready, ASP will request the ESP to send the request for pre-production environment access

4) **Pre-Production Testing:**

- ESP support team provides access to pre-production environment and enables the ASP to establish end to end connectivity to carry out eSign services testing
- ESP support team responds to pre-production access request by sharing the ASP code to enable ASP to conduct end to end testing.
- ASP performs end to end testing on ESP pre-production test bed. The timeline suggested for testing is 7-10 days (in addition to normal ASP on-boarding testing time). The testing will be carried out in following manner:
  - ASP will test the domain application by transmitting transaction request on pre-production environment
  - ASP is expected to test the connectivity on testing environment as it is critical for integration testing of transmitting end user request to ESP
  - ASP should conduct at least 200 successful transactions in the pre-production stage
- Post successful end to end testing ASP engages an ISA certified Auditor to conduct the compliance audit

5) **Audit Report Submission and Security Assessment (Audit report of ASP to be submitted to ESP)**

• Audit report/ certificate duly signed by an ISA certified auditor should be submitted to the ESP as per below schedule
  a. ASP should submit the report/ certificate to ESP prior to the commencement of operations
  b. ASP should submit annual compliance report, upon request by ESP, within 30 days of such request by ESP
• A complete detailed checklist for Audit has been provided as given in on-boarding manual
• The Application Service Provider is required to get a detailed security and risk assessment of its application before getting the final approval from the ESP.

6) **Go-Live – Readiness and Approval**

• ASP notifies ESP Business team about its readiness for migration to production environment
• Subsequently ASP completes the go live checklist and submits the request for go live with the following documents:
  o Go Live checklist
  o Audit certificate as proof of compliance to current standards and specifications
• ESP engagement team scrutinizes the ASP go live request as per the Go-Live checklist and supporting documentation and seeks internal approvals for Go Live

7) **Generate License for Production and Go-Live**

• ESP provides access to ASP admin portal for accessing ASP code and ASP generates the public key certificate for mapping and authentication
• Post migration & testing, ASP shall establish production release and operation management mechanism
• ASP goes live and updates status to ESP
This process ends when the ASP systems are aligned to ESP terms & condition and is ready for eSign service delivery

Key ASP Responsibilities

1) ASPs are liable to comply with provisions mentioned in the Information Technology Act and online eSign service guidelines issued by Controller
2) Mandatory login/password authentication for signatory prior to using OTP option of eSign Service.
3) ASP is responsible for capturing the consent of signatory for signature creation based on the Aadhaar based authentication
4) ASP should make sure that the signatory should accept the Digital Signature certificate prior to affixing the signature and DSC to document
5) ESP is responsible for maintaining all logs and certificates.
6) The signature validation should be carried out with respect to signature affixing time.

Mandatory Security & Technology Requirements

- ASP should have mechanism to authenticate user prior to using the eSign Service.
- The meta data and the responses should be logged for audit purposes.
- Encrypted Personal Identity Data (PID) block and license keys that came as part of authentication packet should never be stored anywhere in its system (if applicable).
- Network between ASP and ESP should be secure.

eSign Service Provider (ESP)

An ESP is a trusted third party for facilitating key pair generation, DSC application form generation and submission to CA, perform digital signature function for users and also interact with UIDAI and CA for identity verification and certification functions. An ESP can serve more than one ASP. At present, only CAs are allowed to provide eSign service. A CA can use the same physical infrastructure and manpower resources for eSign Service. Security requirements for this eSign service, is at the same level as being currently maintained by the CA. The Audit of the e-authentication service is carried out along with the audit of CA facilities.

ESP Eligibility Criteria
At present, only CAs are allowed to provide eSign service. To become ESP, the entity should have license to operate as a Certifying Authority.

ESP Readiness Stage
- The ESP should be a Certifying Authority. If ESP is not a CA, they should become CA first.
- The ESP should function as AUA and e-KYC agent of UIDAI.
- The Audit of the ESP should be carried out along with compliance audit of CA.
- Application Service Provider should have gone through an approval process of ESP and should have agreement between them.
Key ESP Responsibilities

- Authentication of Aadhaar holder: ESP should verify that the consent of Aadhaar holder has been obtained. Aadhaar e-KYC service should provide digitally signed information that contains name, address, email id (optional), mobile phone number (optional), photo and response code to the applicant. The mode of e-authentication should be biometric or OTP in accordance with Aadhaar e-KYC Services specification.

- ESP should build software, hardware and procedural controls to facilitate authentication of Aadhaar holder, key pair generation, Electronic Application form generation, Certificate Request submission to CA systems, digital signature on document.

- DSC Application Form: DSC application form is to be electronically generated after successful authentication of DSC applicant by Aadhaar e-KYC services.

- ESP should facilitate generation of key pairs on their Hardware Security Module. The key pairs are generated after Aadhaar eKYC based authentication which is unique to the subscriber. The private key will be destroyed after one time use.

- On successful key generation the Certificate Signing Request is sent to CA by ESP for issuing the DSC.

- ESP should facilitate the digital signature creation and send the Digital Signature and DSC received from CA to ASP.

- Audit logs: Record all relevant information concerning the e-authentication of DSC applicant for generation of key pair and subsequent certification functions and preserve for a minimum period of 7 years. Record all relevant information concerning the e-authentication of subscriber for accessing the key pair and preserve for a minimum period of 2 years.

- Make available eSign Integration kit to ASPs.

- ESP will process the application received from ASP for on-boarding.

Mandatory Security & Technology Requirements

- The private key of the subscriber shall be secured by Hardware security module (HSM) in accordance with FIPS 140-2 level 3 recommendations for Cryptographic Modules Validation List.

- HSM of ESP should be separate from that of CAs for DSC issuance.

Certifying Authority (CA)

The office of Controller of Certifying Authorities (CCA) has been established under the Information Technology Act 2000 for promoting trust in the electronic environment in India. CCA licenses the Certifying Authorities (CAs) to issue the Digital Signature Certificates (DSC) under the Information Technology Act. A CA provides services to its subscribers and relying parties as per its Certification Practice Statement (CPS) which is approved by the CCA as part of the licensing procedure.

Current Responsibilities & Obligations of CAs

- The issuance process of DSC involves the identity and address verification of the user at the time of submission of application form. The user needs to submit an attested copy of the identity and address...
proof to the CA. A similar process is followed for renewal of certificates as well. For issuing a digital signature certificate, it is a pre-requisite that the verification of credentials of the subscriber is carried out and in case of a class 3 certificate, physical verification is also required. The digital signature certificate will be issued by the CAs only after the application form and supporting documents (duly attested) have been physically received and verified at the CA premises.

- The Registration Authority (RA) functions as an agent of the CA, for the purpose of collecting and authenticating each subscriber’s identity and address information and forwarding accepted applications for DSC. The Certifying Authorities have agreements with their Registration Authorities to perform their functions and duties.

- On successful verification, CA issues DSC and publishes them in the repository of CAs. CAs are responsible for Issuing Certificate Revocation Lists (CRL) at periodic intervals or immediately after revocation. CA publishes a list of invalid (revoked) Digital Signature Certificates.

- A CA should verify the source of a DSC request before issuance. Issued DSCs shall be checked to ensure that all fields and extensions are properly populated.

- CAs are responsible for the following functions in respect of DSC life cycle
  a) DSC Application Processing: It is the responsibility of the CA to verify that the information in DSC applications is accurate.
  b) Approval or Rejection of DSC Applications: A CA may approve or reject a DSC application.
  c) DSC Issuance: Upon receiving a request for a DSC, the CA shall respond in accordance with the requirements set forth in its CPS.
  d) Notification to Subscriber of Certificate Issuance: A CA shall notify a subject (End Entity Subscriber) of DSC issuance.
  e) DSC Revocation and Suspension: DSC revocation requests must be authenticated. Request to revoke a DSC may be authenticated using that DSC's associated private key, regardless of whether or not the private key has been compromised.
  f) Publication of DSC Information: DSC and DSC status information shall be published.

- Apart from the certification function, CAs provide the following services to relying parties
  - Online Certificate Status Protocol (OCSP)
  - Time stamping service

**CAs role in eSign**

a) CA should function as AUA and e-KYC agent of UIDAI.

b) CA should have dedicated certification issuance systems in place for eSign service to facilitate eSign service in an auto issuance mode.

c) Audit and obtain approval for ESP/CA system to start eSign service.

d) The routine audit of the ESP should be carried out along with CA systems audit and compliance.

**Mandatory Security & Technology Requirements**
The CA system for issuing Aadhaar eKYC class based DSCs should be completely independent of CA systems used for other classes of DSCs.

The CA system should accept only digitally signed Certificate Signing Request (CSR) from designated ESP systems over a dedicated link.

UIDAI Ecosystem

The Unique Identification Authority of India (UIDAI) has been created, with the mandate of providing a unique identity (Aadhaar) number to all residents of India and also defining usages and applicability of Aadhaar for delivery of various services. Towards Aadhaar-enabling delivery of various services, UIDAI proposes to provide online authentication using demographic and biometric data.

UIDAI Mandate

The Unique Identification Authority of India (UIDAI) has been established with the mandate of providing a Unique Identification Number (Aadhaar Number) to all residents. During enrolment, the following data is collected:

- 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 Overview

UIDAI offers the eKYC service, which enables a resident having an Aadhaar number to share their demographic information and photograph with a UIDAI partner organization in an online, secure, auditable manner with the residents consent. The consent by the resident can be give via a Biometric authentication or an One Time Password (OTP) authentication.

Some of the key features of the eKYC service are:

- Paperless: The service is fully electronic, enabling elimination of KYC document management
- Consent based: Data is shared by the resident consent through Aadhaar authentication, thus protecting resident privacy.
- Secure and compliant with the IT Act: Data transfer are secured through the use of encryption and digital signature as per the Information Technology Act, 2000 making e-KYC document legally equivalent to paper documents.
- Non-repudiable: The use of resident authentication for authorization, the affixing of a digital signature by the service provider originating the e-KYC request, and the affixing of a digital

The UIDAI offers an authentication service that makes it possible for residents to authenticate their identity biometrically through presentation of their biometric or using a One Time Password (OTP) sent to the registered mobile phone or e-mail address

Verification of the Proof of Identity (PoI) and Proof of Address (PoA) is a pre-requisite for issuance of Digital Signature Certificates by Certifying Authorities. As part of the e-KYC process, the resident authorizes UIDAI
(through Aadhaar authentication using either biometric or OTP to provide their demographic data along with their photograph (digitally signed and encrypted) to service providers.

eKYC containing authenticated information about Aadhaar holders can therefore be used in issuing them a DSC as well as carrying out online digital signatures - making it possible for service providers to provide instant service delivery to residents

**Key requirements and steps for becoming a AUA**

AUA On-Boarding Process: For cases if applicant is not engaged with UIDAI as AUA, then as per e-KYC Policy, the applicant has to first apply for AUA. Initiate the AUA On-Boarding Process to begin applicant’s engagement with UIDAI as AUA. The detailed steps to be carried out by prospective AUA for on boarding are covered in the AUA On-Boarding Process. It is recommended that in parallel prospective AUA shall also initiate the process for KUA by filling and submitting the KUA Request Form. Thus, this will facilitate the applicant to engage with UIDAI as AUA and at the same time it can also avail the e-KYC service as KUA. The following are the general steps for an entity to become AUA. For more details ref [https://uidai.gov.in](https://uidai.gov.in)

**Key requirements and steps for becoming a KUA**

The existing AUA providers should explicitly register with UIDAI to enable them for providing eKYC service to their customer base. The e-KYC service responds with resident demographic/photograph information to authorize the resident and uses the information to provide additional services. The following are the general guidelines for an AUA to become KUA. For more details ref [https://uidai.gov.in](https://uidai.gov.in)

**Step 1 - Application Submission along with Supporting documents**
- KUA Application Form duly Signed and Stamped
- Letter of Authority or Power of Attorney or Board resolution copy of the Authorised signatory along with the specimen signatures of the authorised signatory by the higher official
- Scope/Purpose of utilizing e-KYC services
- Letter of engagement from KSA
- Two copies of Blank Stamp paper(s) of requisite denomination as per the State
- Covering letter for the submission of documents mentioned above

**Step 2 - Application Approval, Agreement Signing and Pre-Production Access**

**Step 3 - Go Live & Audit Compliance Checklist Submission & Acceptance**
- KUA Go Live Checklist
- KUA Audit Compliance (if there is a change in modality from AUA to KUA)
- Production access is provided after verifying Go Live and audit compliance checklist Go Live!!
FAQs

For residents

Q) What is the online eSign Electronic Signature Service?

eSign Electronic Signature Service is an innovative initiative for allowing easy, efficient, and secure signing of electronic documents by authenticating the signer using Aadhaar eKYC services. With this service, any Aadhaar holder can digitally sign an electronic document without having to obtain a cryptographic device. Application Service Providers can integrate this service within their application to offer Aadhaar holders a way to sign electronic forms and documents. The need to obtain Digital Signature Certificate through a printed paper application form with ink signature and supporting documents will not be required.

The Digital Signature Certificate issuance and applying of signature to electronic content is carried out in few seconds with eSign. Through the interface provided by the Application Service Provider (ASP), users can apply electronic signature on any electronic content by authenticating themselves through biometric or OTP using Trusted Third Party (TTP) Aadhaar eKYC services through eSign Service Provider. At the backend, eSign service provider facilitates key pair generation and Certifying Authority issues a Digital Signature Certificate. The eSign Service Provider facilitates creation of the Digital Signature of the user for the electronic document. This signature will be applied to the document on acceptance by the user.

Q) Where the eSign Online Electronic Signature Service can be used?

An Application Service Provider (ASP) can integrate eSign online electronic signature service so that the users of that ASP will be able to use eSign. A physical paper form/document which is currently used to obtain digital signature certificate can be replaced by its electronic form and thereby facilitate electronic signature of the signer through eSign.

ASPs who can be potential users of eSign include Government agencies, Banks and Financial Institutions, Educational Institutions etc.

Q) What are the challenges to be addressed using eSign- Online Electronic Signature Service?

Personal digital signature certificate requires person’s identity verification and issuance of physical cryptographic device to store private key. The access to private key is secured with a password/pin. Current scheme of physical verification, document based identity validation, and issuance of physical cryptographic device does not scale to a billion people. For offering hassle-free fully paperless citizen services, mass adoption of digital signature is necessary. A simple to use online service is required so as to allow everyone to have the ability to digitally sign electronic documents.

Q) What are the objectives of eSign online Electronic Signature Service?

eSign Online electronic signature service, offers applications a mechanism to replace manual paper based signatures by integrating this service within their applications. An Aadhaar holder can electronically sign a form/document anytime and anywhere. eSign service facilitates significant reduction in paper handling costs, improves efficiency, and offers convenience to customers.

Q) Is my privacy protected?

Yes. Document content that is being signed is not sent in the clear to the eSign service provider. The privacy of signer's information is protected by sending only the one-way hash of the document to the eSign Service.
provider. Each signature requires a new key-pair and certification of the new Public Key by a Certifying Authority. This back-end process is completely transparent to the signer. In addition, Aadhaar eKYC data is not sent back to the Application Service Provider and is retained only within the eSign provider as the eKYC audit record.

Q) Whether it is a legally valid signature?
Yes. The Electronic Signatures facilitated through eSign Online Electronic Signature Service are legally valid provided the eSign signature framework is operated under the provisions of Second Schedule of the Information Technology Act and Guidelines issued by the Controller of Certifying Authorities. Please refer Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015 - e-authentication technique using Aadhaar e-KYC services.

Q) What are the different classes of certificates in the eSign Electronic Signature Service?
Based on the verification of identity of individuals and storage of key pairs, three classes of certificates are issued in the traditional way of obtaining Digital Signature Certificates from Certifying Authorities. In the case of eSign Online Electronic Signature Service, the Digital Signature Certificates are issued in the following classes.

- **Aadhaar-eKyc – OTP** Aadhaar-eKyc - OTP class of certificates is issued to individuals based on OTP authentication of subscriber through Aadhaar e-KYC. For additional security PIN facility can be availed.
- **Aadhaar-eKyc - Biometric (FP/Iris)**: Aadhaar-eKyc - Biometric (FP/Iris) class of certificate is issued based on biometric authentication of subscriber through Aadhaar e-KYC service.

Q) Whether Electronic Signatures can be applied to any electronic content of individual's choice?
An individual can obtain Digital Signature Certificate from the existing DSC issuance framework and can digitally sign the electronic content of choice subject to the acceptability of such class of certificate by the relying parties and the validity of the DSCs.
eSign Online Electronic Signature Service are offered to individuals by Application Service providers. In the eSign Online Electronic Signature Service, the choice of type of electronic content on which electronic signatures can be applied are limited to options provided by ASPs.

Q) How do I know my signature and certificate is the one which was applied to the document?
The content of DSC is shown to signatory prior to affixing the signature within the ASP application. The ASP needs to provide necessary tool to verify the signature.

For ASPs

Q) Whether eSign online Electronic Signature Service is a replacement for the existing Digital Signature?
No. The existing method of obtaining Digital Signature Certificate by submission of a paper application form to a Certifying Authority, key pair generation by applicant Certification of public key of applicant by a Certifying Authority, signature generation as and when required using signature generation tools/utilities, safe custody of key pairs on Crypto tokens by DSC holder till the expiry of Digital Signature Certificate, etc. will continue to exist along with eSign Online Electronic Signature Service.
The Application Service Provider determines the suitability of eSign Online Signature service in their application.

Q) What are the major differences between traditional digital Signature ecosystem and new eSign online Electronic Signature Service?

In the traditional Digital Signature system, an individual is responsible for applying for a Digital Signature Certificate to CA, key pair generation and safe custody of keys. The Certifying Authorities issue Digital Signature Certificate to individuals after verification of credentials submitted in the application form. Such Digital Signature Certificates are valid for 2-3 years. Individual can affix digital signature any time during the validity of Digital Signature Certificate. The certificates are revoked in case of loss or compromise of keys. The verification of the individual's signature requires the verification of whether the DSC is issued under India PKI and also ascertaining the revocation status of the DSC. Key pairs are stored in Crypto Tokens which comply with standards mentioned in the Information Technology Act & Rules to prevent the duplication of keys. It is individual's obligation for safe custody of Crypto Tokens. The signatures are created using the keys certified by CA.

In the new eSign online Electronic Signature Service, on successful authentication of individual using Aadhaar eKYC services, the key pair generation, the certification of the public key based on authenticated response received from Aadhaar eKYC services, and digital signature of the electronic document are facilitated by the eSign online Electronic Signature Service provider instantaneously within a single online service. The private key pair are used only once and the private key is deleted after one time use. The Digital Signature Certificates are of 30 minutes validity, and this makes verification simple by eliminating the requirements of revocation checking. Document that is signed using eSign will contain a valid digital signature that can be easily verified using standard methods.

Q) Who can provide eSign- Online Electronic Signature Service?

At present, eSign Online Electronic Signature Service is offered by CAs. The security requirement for this service is mandated as the same level as currently mandated for CAs. A CA should Sign KYC User Agency (KUA) agreement with UIDAI to enable access to e-KYC service.

Q) Who can integrate eSign- Online Electronic Signature Service in their 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

Such entities are referred to as “Application Service Providers” (ASP).

Q) What are the requirements for integrating eSign- Online Electronic Signature Service in an application?

The ASP can apply to eSign Service Provider for integrating eSign- Online Electronic Signature Service in their application as mentioned in the on-boarding process manual. The ASP should be a sub-AUA of eSign Service Provider. The eSign- Online Electronic Signature Service provider allows access to ASPs after fulfilling the
criteria mentioned in the on-boarding process manual. An agreement is needed to be executed between eSign-Online Electronic Signature Service provider and ASP.

ASPs have to deploy hardware and software for deployment of e-KYC service across various delivery channels. For biometric authentication, these should be STQC certified biometric scanners at ASPs customer interface locations as per UIDAI specification.

ASPs have to develop a software application that should integrate eSign API as per the eSign API specifications issued by the Controller of Certifying Authorities.

Q) What are the requirements for using eSign- Online Electronic Signature Service for application users?
The user should have 12 digit Aadhaar Number. For OTP based authentication, the mobile number should be registered with Aadhaar Database.

Q) Where does someone get assistance for integration of their application with eSign- Online Electronic Signature Service?
The communication between Application Service Provider and eSign- Online Electronic Signature Service is operated in accordance with eSign API Specifications.

Q) How does an application provider avail services of more than one eSign Online Service provider?
eSign APIs are designed to interact with one or more eSign Online Electronic Signature Service providers. If application provider desires to interact with only one CA, it should use the name of the eSign Online Service provider and communication link as mentioned in the eSign API specifications. In the case of multiple eSign Online Service providers, the ASP can manage the service by local integration or by availing the services of the Gateway.

Q) What is the role of the Gateway?
To implement Aadhaar eKYC OTP based authentication with an additional optional PIN authentication, the PIN needs to be managed at a central location. For the purpose of eSign integration with PIN, Gateway will manage the PIN function. ASP can directly integrate with eSign provider if they choose to do so. The optional PIN facility will not be available in such integration (only biometric and OTP will be available).

Q) How can one ensure that the authentication to ASP and to ESP is by the same person?
In the ASP implementation, an individual is identified using a code or number instead of name. For example in the case of income TAX e-filing, the person is identified by a PAN number. It is a challenge for ASP to ensure that the individual who has logged in using PAN id is the same person who has signed the documents using eSign. Mapping (seeding) the individual’s application specific ID with their Aadhaar number in the ASP database is recommended to enable the authenticity of the signature.

For ESPs

Q) What are the requirements for enabling ASP with eSign Electronic Signature Service?

- ESP should be KUA of UIDAI to provide eKYC service
- ASP should be a sub-AUA of ESP to integrate eKYC service
o ASP should be Service Integrator of eSign online Electronic Signature Service for one or more ESPs. (includes a contract between CA and ASP)
o Integrate eSign API and Aadhaar eKYC API in the application of ASP
o Audit, as per the guidelines of UIDAI and CCA.
o Subscriber should have Aadhaar Number (and registered mobile for OTP based authentication).
   For biometric based authentication, the individual should have access to biometric capturing device
o ASP database should be seeded with Aadhaar number to ensure that authenticity of the signer is verifiable by ASP.

Q) What is the validity of Digital Signature Certificate?
The Digital Signature Certificate used to verify the signature will be valid for 30 minutes and the private key will be immediately destroyed after signing. This eliminates any misuse of the certificate and simplifies the need for checking revocation list during signature verification.

Q) Whether the Digital Signature Certificate is revocable?
Revocation of certificate is not necessary as the certificate validity is 30 minutes and private key is deleted immediately after signature creation.

Q) Who is responsible for archival of signature? Both eSign online Electronic Signature Service provider and Application Service providers are responsible for archival of their data and application logs. The eSign online Electronic Signature service provider’s logs should include the information received from ASP and also the signature created.