**eSign FAQ**

**What is the online eSign Electronic Signature Service?**

eSign Electronic Signature Service is an innovative initiative by allowing easy, efficient, and secure signing of electronic documents by authenticating signer using Aadhaar eKYC services. With this service any Aadhaar holder can digitally sign an electronic document without having to obtain a physical digital signature dongle. Service providers can integrate this service within their application to offer Aadhaar holders a way to sign electronic forms and documents without having to have a printed paper and physical signature.

The Digital Signature Issuance and applying of signature to an electronic content is carried out in few seconds. Through the interface provided by Application Service Provider, users can apply signature on any electronic content by authenticating biometric or OTP using Aadhaar eKYC services. The interfaces are provided to user on variety of devices like computer mobile etc. At the backend, eSign electronic signature service provided by Certifying Authority issue a Digital Signature Certificate and applies the Digital Signature of the user same will be applied to the document on acceptance of user.

**What are the challenges to be addressed using eSign- Online Digital Signature Service?**

Currently personal digital signature requires person’s identity verification and issuance of USB dongle having private key, secured with a password/pin. Current scheme of physical verification, document based identity validation, and issuance of physical dongles 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 to allow everyone to have the ability to digitally sign electronic documents.

**What are the objectives of eSign online Electronic Signature Service?**

An eSign electronic signature offers various applications a mechanism to replace manual paper based signatures by integrating this service within their applications and enable an Aadhaar holder to electronically sign a form/document anytime, anywhere, and on any device.. eSign service facilitate transactions to significantly reduce paper handling costs, improve efficiency, and offer convenience to customers.

**Whether eSign online Electronic Signature Service is a replacement for the existing Digital Signature?**

No. The existing method of obtaining Digital Signature by submission of an application form to a Certifying Authority, key pair generation of individual, Certification of public key of user by a Certifying Authority, signature generation as and when required using signature generation tools/utilities , safe custody of key pairs on Crypto tokens by individuals till the expiry of Digital Signature Certificate, etc. will continue to exist along with eSign Online Digital Signature Service provided by Certifying Authority .

The Application Service Provider can determine the suitability and support of signature requirements in their application.

**5. What are the major difference between traditional digital Signatures eco system 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 lost or key compromise. The verification of the individual’s signature requires the verification of whether the DSC is issued under India PKI and also the revocation status of the Certificates. Key pairs are stored in Crypto Tokens which are complied with standards mentioned in the Information Technology Act & Rules to prevent the duplication of keys. It is individual’s obligation for safe custody of this Crypto Tokens and signature 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 pairs are generation, the certification of the Digital Signature Request containing public key along with authenticated response received from Aadhaar eKYC services by Certifying Authority and digital signature of document are facilitated by eSign online Electronic Signature Service provider instantaneously within a single online service. The key pairs 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 make 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.

**Is my privacy protected?**

Yes. Document content that is being signed is not sent to eSign service provider. The privacy of individual’s information is protected by sending only one way hash of the document to eSign online Electronic Signature Service provider. Each signature requires a new key-pairs and certification by a Certifying Authority and this back-end process is completely transparent to individual. In addition, Aadhaar eKYC data is not sent back to application and is used only within the eSign provider as the KYC audit record.

**Whether it is a legally valid signature?**

Yes. The Electronic Signatures facilitated through eSign Online Electronic Signature Service is legally valid provided with eSign 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*.

**Who can provide eSign- Online Digital Signature Service?**

At present, eSign Online Digital Signature Service is operated CAs. CAs use their physical infrastructure and manpower resources for eSign Service. The security requirement for this service is mandated as the same level as being currently maintained by the CA. A CA should Sign KYC User Agency (KUA) agreement with UIDAI to enable access e-KYC service.

**Who can integrate eSign- Online Digital Signature Service in their application?**

Any Government or legal entity registered in India is eligible to integrate eSign- Online Digital Signature Service in their application**.** Such entities are referred as “Application Service Providers” (ASP).

**What are the requirements for integrating eSign- Online Digital Signature Service in an application?**

* The ASP can apply to eSign Online Service of Certifying Authority to integrate eSign- Online Digital Signature Service in their application as mentioned in the on-boarding process manual. The ASP should be a sub-KUA of CA. The eSign- Online Digital Signature Service provider allows access to ASPs after fulfilling the criteria mentioned in the on-boarding process manual. An agreement need to be executed between eSign- Online Digital Signature Service provider and ASP.
* ASPs 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.
* Develop a software application that should integrate both eSign API and e-KYC API as per the eSign API issued by Controller and eKYC API defined by UIDAI .

**What are the requirements for using eSign- Online Digital 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.

**10. Where does someone get assistance for integration of their application with eSign- Online Digital Signature Service?**

The communication between Application Service Provider and eSign- Online Digital Signature Service is operated in accordance with eSign API Specifications and also and eKYC API defined by UIDAI. In the initial phase , Office of CCA help Application Service provider to select one eSign Online Service provider for testing and Integration.

**How do 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, use the name of the eSign Online Service provider and communication link as mentioned in the eSign API. In the case of multiple eSign Online Service providers, the ASP can manage the service by local integration or avail the service of Gateway. CDAC is functioning as Gateway.

**What is the role of Gateway in eSign Online Electronic Signature Service?**

CDAC is the only Gateway for the eSign Online Electronic Signature Service. The routing of the requests to respective CAs and optional PIN Management is the major role of Gateway.

**Why CDAC is the only Gateway?**

To implement Aadhaar eKYC OTP based authentication with an additional optional PIN authentication, the PIN need to be managed at a central location. For the purpose of eSign integration with PIN, CDAC is functioning as Gateway and PIN management. ASP can directly integrate with eSign provider if they choose to do so, except that optional PIN facility will not be available in such integration (biometric and OTP will be available).

**Is there any additional authentication is required in the case of Aadhaar eKYC OTP option?**

Yes, the following are the options

* **ASP level logon/Password authentication**: Though Aadhaar eKYC OTP option is relevant to environments where the risks and consequences of data compromise are low and they are not considered to be of major significance, an application level authentication is recommended for eSign Online Electronic Signature Service . This is mainly to mitigate following the risks

1. An individual might have registered the one mobile number for entire family in the Aadhaar Database.

2. Surrendering of mobile number and not changing the mobile number in the

Aadhaar Database.

* **PIN** : If Aadhaar eKYC OTP based authentication is used eSign Online Electronic Signature Service, a Gateway level PIN authentication which is linked to Aadhaar number can also be used an alternate option.

Once immediate linking of Aadhaar databases with Telecom directory a reality, the above mentioned restriction will be reviewed.

**15. What are the options to ensure the authentication to application and signer is same person?**

In the application 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 an PAN number. It is a challenge for application to ensure that the individual who have logon using PAN id is the person who has signed the documents. 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.

**Where the eSign Online Electronic Signature Service can be used?**

If an Application Service Provider (ASP) decides to integrate eSign online electronic signature service, the users of that ASP will be able to use eSign. A physical paper form/document is currently used to obtain signatures can be replaced by its electronic form/document form with digital signature of the individual(s) who is signing. Some of the examples are:

1. Signing documents while availing various Government services by the citizens as well as Government officers (e.g., within e-file application).

2. Tax Application Signature - signing the tax submission either online or at the accountant’s office.

3. Account opening forms and other service subscription forms in banks, SIM card issuance forms, Insurance forms, etc.

4. Other personal documents such as University certificates, bank Loan document, telephone application, office automation, etc

**What is the role of UIDAI in eSign Online Electronic Signature Service?**

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.

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

**What are the key features of the eKYC service which are used in eSign Online Electronic Signature Service for authenticating signer?**

[Ref UIDAI] 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 signature by UIDAI when providing the e-KYC data makes the entire transaction non-repudiable by all parties involved.
* Instantaneous: The service is fully automated, and KYC data is furnished in real-time, without any manual intervention
* Regulator friendly: The service providers can provide a portal to the Ministry/Regulator for auditing all e-KYC requests.

**Can you provide a sample usage scenario for eSign online Electronic Signature Service ?**

Individuals having Aadhaar number can use Digital Locker (http://digitallocker.gov.in/) to store the electronic copy of their identities/Certificates/etc at a central location. The electronic documents placed in the repository of Digital Locker can be accessed or shared the link for verification. These electronic documents can be electronically signed (self-attestation) using eSign Online Electronic Signature Service for integrity and authenticity**.**

**20 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 class of certificates are issued in the traditional way of obtaining Digital Signatures Certificates from a 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 use based on OTP authentication of subscriber through Aadhaar e-KYC. These classes of certificates are relevant to use in the environments where consequences of data compromise are low and they are not considered to be of major significance.
* 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. These classes of certificates are relevant to use in the environments where consequences of data compromise are medium level of confidence in the asserted identity and risks and consequences of data compromise are moderate.

**Whether Electronic Signatures can be applied to any electronic content of individual's choice?**

An individual can obtain Digital Signature Certificate from the established DSC issuance framework and can be used to digitally sign the electronic contents of choice subjected to the acceptability of such class of certificate to relying parties and validity of 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 contents on which electronic signatures can be applied are limited to option provided by ASPs.

**How the trustworthiness of the eSign Online Electronic Signature Service is ensured?**

Upon the biometric or OTP authentication of the individual with the already verified information kept in the database of UIDAI, key pairs are generated and such submit public key along with information received from UIDAI to CA for certification. Immediately after signature is generated with the private key of individual and key pairs are removed. The key pairs are generated on Secure Hardware Security Module to ensure security and privacy.

Audit log files are generated for all events relating to the security of the eSign- Online Digital Signature Service, such the security audit logs are automatically collected and digitally signed by ASPs. All security audit logs, both electronic and non-electronic, shall be retained and are audited periodically.

**Who own the eSign Electronic Signature Service and who are the beneficiaries?**

Certifying Authorities owns the eSign Online Electronic Signature Service and Application Service Providers and individual availing service of ASP are beneficiaries. eSign Online Electronic Signature Service enable ASP to create an paperless environment and individual service beneficiaries of ASP save cost and time by using this remote signature capability

**Who are the providers of eSign Electronic Signature Service at present?**

At present following providers offer this service. In future, more providers may be added. Please check CCA website for updated information.

1. Safescrypt CA
2. (n)Code Solutions CA
3. e-Mudhra CA

**How much does it cost to use eSign?**

Application service providers can do a price discovery and get the best offer from any of the providers. Depending on the volume and usage, pricing may vary. CCA believes that with large scale adoption and multi-provider ecosystem, market forces will automatically provide the best price for the application providers. Considering physical paper handling costs, archival costs, audit costs, etc. are high, application providers can work out the return of investment easily.

**What are the requirements for enabling application with eSign Electronic Signature Service?**

* CA should be KUA to provide eKYC service
* ASP should be a sub-KUA of CA to integrate eKYC service
* ASP should Service Integrator of eSign online Electronic Signature Service of one or more CAs.(includes a contract between CA and ASP)
* Integrate eSign API and Aadhaar eKYC API in the application of ASP
* The Audit as per the guidelines of UIDAI and CCA
* 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
* ASP database should be seeded with Aadhaar number to ensure authenticity of the signer is verifiable by ASP.

**How do I know my signature and certificate is the one which applied to the document?**

The contents of DSC is shown to signatory prior to affixing the signature within the ASP application. The ASP need to provide necessary tool to verify the signature.

**What is the validity of Digital Signature Certificate?**

While signed document is valid for ever, the particular certificate used to sign will be invalidated after 30 minutes and the private key immediately deleted after signing. This eliminates any misuse of the certificate and simplifies the need for checking revocation list during signature verification.

**Whether 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.

**Whether providing my personal identity information like biometric is secure?**

The ASPs and eSign online service providers of CAs are bound by the agreement with UIDAI for the confidentiality of information in line with UIDAI agreement.

**Whether a complete paperless office can be setup using eSign Electronic Signature Service.**

Depending on the requirements, the ASP can use biometric or OTP based authentication for different class of DSCs.

**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 signature created.