CVL eSign FAQs

1. 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 signer using aadhar e-KYC services. With this service, any eSign user can digitally sign an electronic document without having to obtain a physical digital signature dongle. Application Service Providers can integrate this service within their application to offer eSign user 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 aadhar e-KYC services. The interfaces are provided to users on a variety of devices such as computer, mobile phone etc. 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 document which will be applied to the document on acceptance by the user.

2. What is the online eSign service provided by CVL?

CVL provides an Online eSign service which is a paperless mode of signing electronic documents by authenticating signer using Aadhaar based e-KYC services.

3. 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 eSign user can electronically sign a form/document anytime, anywhere, and on any device. eSign service facilitates significant reduction in paper handling costs, improves efficiency, and offers convenience to customers. 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. ASPs who can be potential users of eSign include Government agencies, Banks and Financial Institutions, Educational Institutions etc.

4. Can you provide some use-cases of eSign online Electronic Signature Service?

eSign online Electronic Signature Service can be effectively used in scenarios where signed documents are required to be submitted to service providers – Government, Public or Private sector. The agencies which stand to benefit from offering eSign online electronic signature are those that accept large number of signed documents from users.

Some applications which can use eSign for enhancing for enhancing services delivery are the following:-

Digital Locker → Self attestation
Tax → Application for ID e-filing
Financial Sector → Application for account opening in banks and post office

Transport Department → Application for driving license renewal vehicle registration
Various Certificates → Application for birth, caste, marriage, income certificate etc
Passport → Application for issuance, reissue
Telecom → Application for new connection
Educational → Application forms for course enrollment and exams
Member of Parliament → Submission of parliament questions

5. 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.

6. 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 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, based on successful authentication of individual using e-KYC services, the key pairs generation, the certification of the public key based on authenticated response received from e-KYC 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 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 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.

7. 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 USB dongle to store private key. The access to private key is secured with a password/pin. The 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.

8. Who can use Aadhaar eSign?

Any Indian citizen with an Aadhaar number and a mobile number registered with Aadhaar can use eSign to sign documents through online mode.

9. Who can provide eSign Online Electronic Signature Service?

eSign Online Electronic Signature Service is offered by Certifying Authorities registered under Control of Certifying Authorities (CCA).

10. What is the role of eSign Service Provider (ESP) in eSign Online Electronic Signature Service?

ESP invokes the Aadhaar eKYC API and creates new key pair for the user for his/her Aadhaar. Once user is authenticated, ESP sends public key and eKYC information to the Certifying Authority for certification.

11. What is the role of Certifying Authority (CA) in eSign Online Electronic Signature Service?

Based on the eKYC authentication information received from UIDAI, electronic signature certificate is issued and sent to the ESP by CA.

12. Who can integrate eSign Online Electronic Signature Service in their application?

The agency who intends to integrate eSign service should be any of the following:

- A Central/ State Government Ministry / Department or an undertaking owned and managed by Central / State Government,
- An Authority constituted under the Central / State Act,
- A Not-for-profit company / Special Purpose organization of national importance,
- A bank / financial institution / telecom company, or
- A legal entity registered in India

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

13. What are the steps for onboarding an ASP?

An ASP must submit an application form, provide supporting documents and duly executed Agreement for onboarding as an ASP with CVL. For more details, please send an email to esign@cvlindia.com

14. What should the ASP do in order to integrate with eSign Online Electronic Signature Service of CVL?

CVL eSign FAQs

The ASP can apply to eSign Service Provider (i.e. CVL) for integrating with CVL's eSign Online Electronic Signature Service in their application. The ASP would be onboarded with CVL after fulfilling the criteria for On-Boarding.

15. What are the steps to go live?

Once ASP is onboarded, he would be provided UAT access. ASP will have to generate 50 successful cases in UAT and submit the audit compliance report to CVL. On receiving advance payment, live access would be provided.

16. How can one generate virtual id?

Virtual id can be generated by accessing the below link.
https://resident.uidai.gov.in/web/resident/vidgeneration

17. 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 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.

- e-KYC – OTP : class of certificates is issued to individuals use based on OTP authentication of subscriber through e-KYC Service.

- e-KYC – Biometric : Biometric class of certificate is issued based on biometric authentication of subscriber through e-KYC service.

18. 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 be used to 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 option provided by ASPs.

19. 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 e-KYC provider, key pairs are generated and public key along with information received from e-KYC provider are submitted to CA for certification. Immediately after signature is generated with the private key of individual, the key pairs are deleted. 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 Electronic Signature Service. 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. The eSign service is governed by

e-authentication guidelines issued by CCA. While authentication of the signer is carried out using e-KYC services, the signature on the document is carried out on a backend server of the e-Sign provider (CVL eSign). To enhance security and prevent misuse, eSign user's private keys are created on Hardware Security Module (HSM) and destroyed immediately after one time use.

20. How to generate Offline Aadhaar?

The process of generating Aadhaar Offline e-KYC is explained below:
Go to URL **https://resident.uidai.gov.in/offlineaadhaar**
Enter 'Aadhaar Number' or 'VID' and mentioned 'Security Code' in screen, then click on 'Send OTP'. The OTP will be sent to the registered Mobile Number for the given Aadhaar number or VID. Enter the OTP received. Enter a Share Code which would be the password for the ZIP file and click on 'Download' button. The Zip file containing the digitally signed XML will be downloaded to device wherein the above-mentioned steps have been performed.

21. Who are the users of this Aadhaar Paperless Offline eKYC?

Any Aadhaar number holder who desires to establish his/her identity to any service provider (OVSE) using digitally signed XML downloaded from UIDAI website can be a user of this service. The service provider should have this provision in their application to enable offline verification.

22. How to share this Paperless Offline eKYC document with the service provider?

Residents can share the XML ZIP file along with the Share Code to the service provider as per their mutual convenience through the application.

23. What is the validity of Digital Signature Certificate created through online electronic signature service?

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

24. Is it safe to share Offline Paperless eKYC document with the Service Provider?

Yes, it is safe to share details with Service Providers as the Service Providers are bound by the regulations of the Aadhaar and are not allowed to share, publish or display either Share Code or XML file or its contents with anyone else and hence the privacy of the user sharing the Offline Paperless eKYC document is safeguarded.

25. If my question is not answered in the FAQs, how can I contact CVL?

Please send an email to esign@cvlindia.com

26. Does CVL eSign application require eSign user consent at the time of data processing?

Yes, CVL eSign application relies on the consent provided by eSign user at the point of data collection or disclosure in order to process data for activities relating to eSign.

CVL eSign FAQs

27. Is data shared on CVL eSign portal confidential?

In accordance with CCA guidelines, data shared is completely confidential. CVL 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. Yes. Document content that is being signed is not sent in the clear to eSign service provider. The privacy of signer's information is protected by sending only the one-way hash of the document to eSign online Electronic Signature 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.

28. How do I lodge the grievance/query?

The grievance/query can be lodged online on (eSign URL) grievance section. In cases where internet facility is not available or even otherwise, the citizen is free to send her/his grievance by Post. The grievance may be sent, addressed to the eSign department on address below: CDSL Ventures Ltd., A/401-409, Mahavir Icon, Plot number 89 & 90, Sector 15, CBD Belapur, Navi Mumbai – 400614

29. After redress, can the grievance be re-opened for further correspondence?

No. In such situations, fresh grievance will have to be lodged drawing reference to the closed grievance and call for details.

30. What is the time limit for redress of grievance?

Seven (7) days. In case of delay an interim reply with reasons for delay will be provided.

31. Does CVL eSign require eSign user consent during the time of data processing?

Yes, CVL eSign relies on the consent that eSign user you provides to us at the point of data collection or disclosure to us in order to process data for activities relating to eSign.