CVL ASP Onboarding

CDSL VENTURES LIMITED

CVL ASP Onboarding procedure

Version: 1.2

Date: 27 August 2021

REVISION CONTROL

Revision	Revision Date	Type of changes	Author	Approved By
1.0	25.04.2019	Initial Document	Shrikrishna Koranne	Arun Narasimhan,
1.1	12.03.2021	Document review	Shrikrishna Koranne	Arun Narasimhan
1.2	27.08.2021	Document review	Shrikrishna Koranne	Arun Narasimhan

Contents

1 Introduction

This document contains all essential information for the ASP Onboarding.

2 Purpose

The purpose of this User manual is to provide the User a detailed and Step by Step guidance of the procedures to be followed for ASP onboarding.

3 Scope

The scope of this plan covers only ASP onboarding for utilising the eSign system.

4 Overview

CVL **offlineEsignWeb** application is developed to demonstrate **CVL ESP. offlineEsignWeb** facilitates the eSign user to initiate the esign sign request by providing / uploading PDF document and receive the response back from the ESP to with PKCS7PDFPDF data to sign the .pdf document.

5 ASP Onboarding steps in brief:

- Execute an agreement between ASP and ESP.
- ASP's public IP address and URL must be whitelisted at ESP. IP whitelisting will be done as per standard procedures of CVL i.e. by creating CR.
- CVL will provide UAT access to ASP first.
- On UAT, ASP must perform at least 50 transactions before moving to production.
- ASP application must be audited before moving to production.

6 e-KYC Services

- **OTP:** based on **OTP authentication** of eSign user through e-KYC Service
- **OTP & PIN** : based on ***OTP & PIN authentication*** of eSign user

These certificates will confirm that the information in the Digital Signature Certificate provided by the eSign user is same as information retained in the e-KYC service provider's databases pertaining to the eSign user.

7 Stakeholders – Roles and Responsibilities

The entire ecosystem for providing the eSign Services will include a number of stakeholders that will come together to provide eSign service to an applicant.

S. N.	Stakeholders	Roles and Responsibilities

1.	Application Service Provider (ASP)	• Using eSign service as part of their application to digitally sign the content • Sign the contract/agreement/undertaking with the ESP • Indemnify both ESP and CA for integrity related discrepancies arises at ASP end. • Archive logs and carryout audit as per the guidelines of CCA • *ASP integrate with ESPs through standard eSign APIs • *ASP provides eSign facility to public service should integrate with all other ESPs within one month after on-boarding with first ESP. • *ASP shall protect the document URL (available within eSign request) from anyone or any system accessing it using URL and also from virus, malware, etc.

		• *ASP shall display (and allow download/print) the document that is to be signed clearly for subscribers to read before signing. • *Provision for providing/accessing the copy of the signed document to the signer * *Applicable to ASP availing eKYC service provided by CA*
2.	End User	• Represents himself/herself for signing the document under the legal framework • For the purposes of DSC by the CA, the end-user shall also be the 'applicant/eSign User for digital certificate', under the scope of IT Act • Provide the correct eSign user id while signing and should not impersonate anyone else
3.	eSign Service Provider	• It provides the eSign service and is a "Trusted Third Party", as per the definitions of Second Schedule of Information Technology Act • Facilitates eSign User's key pair-generation, storing of key pairs on hardware security module and creation of digital signature • It can be a licensed Certifying Authority (CA), or must be having an arrangement / integration with a CA for the purpose of obtaining Signature Certificate for the generated key pair
4.	Certifying Authority	• Licensed by the CCA for issuance of Digital Certificate • Carries out allied CA operations
5.	e-KYC Provider	• As per the list of e-KYC providers are given in the e-authentication Guidelines.
6.	Controller of Certifying Authority (CCA)	• Licenses and regulates the working of Certifying Authorities • Ensures that none of the provisions of the Act are violated • Performs audits and keeps checks on the functioning of the CAs to ensure it functions effectively

eSign application programming interfaces (APIs) define the major architectural components and also describe the format and elements of communication among the stakeholders like Application Service Provider, Certifying Authorities and e-KYC service. This Standard eSign API enables Application Service Providers to integrate eSign API in their Application with minimum effort.

The various steps that are involved in the signing of document using eSign are:

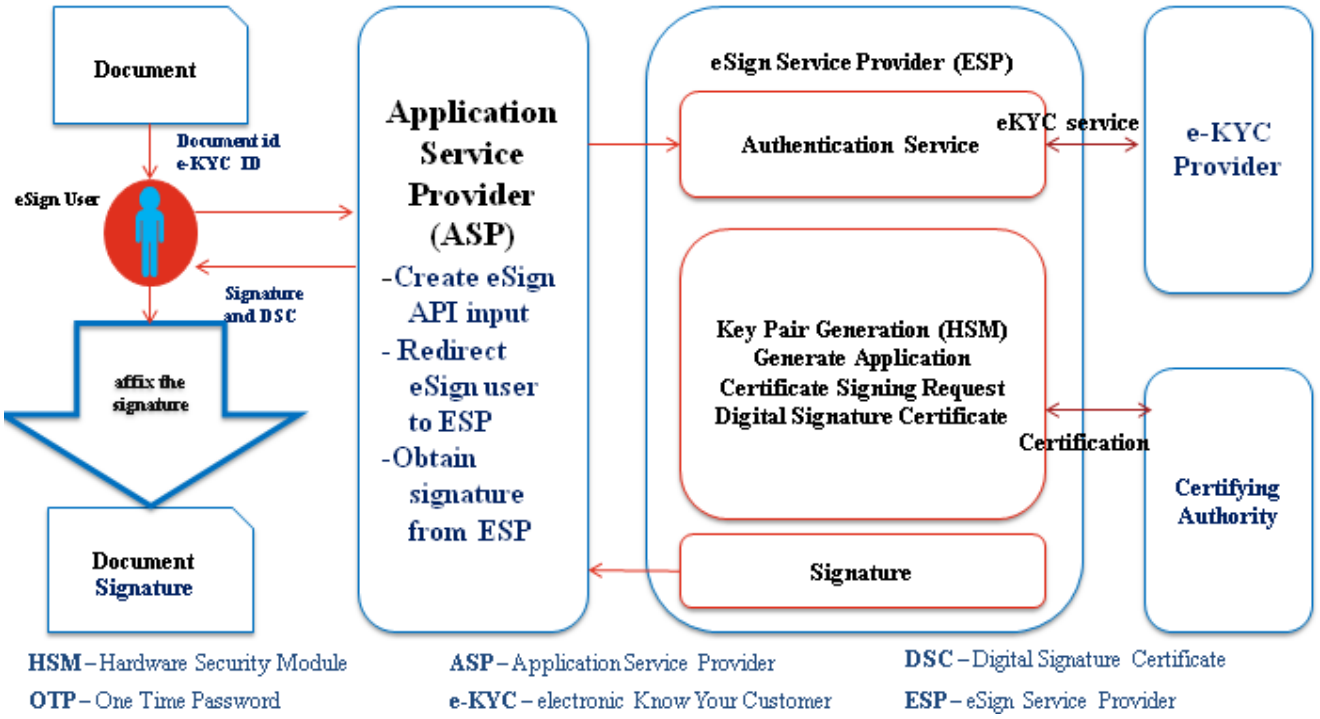
1. Asks the end user to sign the document
2. Creates the document hash (to be signed) on the client side
3. Calls the e-Sign API of the eSign provider
4. eSign provider validates the calling application, obtain e-KYC response
5. Redirect eSign user to ESP for authentication by eKYC provider
6. eKYC provider validate the information obtained from eSign user and on success, provide eKYC response
7. ESP validate the authenticity of the e-KYC response.
8. On success, creates a new key pair for that eSign user
9. Signs the input document hash using the private key (The original document is not sent to eSign service provider)
   Creates an audit trail for the transaction
   a. Audit includes the transaction details, timestamp, and e-KYC response
   b. This is used for pricing and reporting
10. Sends the e-Sign API response back to the calling application

11. Attaches the signature to the document

The API specifications remain common for all eSign Service providers. However, below are the things which will vary for each ESP.

- eSign Service URL
- ASP ID - Unique User ID provided by the ESP

The usage of single eSign Service Provider is a straight forward case. However, in case of multiple eSign service provider ASP shall have parameters configurable for each request. The routing of requests to each API can be a round-robin, a failure switchover, an end-user selection basis, or any other manner implemented by ASP.



Request XML

<Esign ver="" signerid="" ts="" txn="" maxWaitPeriod="" aspId="" responseUrl="" redirectUrl="" signingAlgorithm="">
<Docs>
<InputHash id="" hashAlgorithm="" docInfo="" docUrl="" responseSigType="">Document Hash in Hex</InputHash>
</Docs>
<Signature>Digital signature of ASP</Signature>
</Esign>

Client will call the service URL with the request XML

Attribute	Required ?	Value
Ver	Mandatory	eSign version (mandatory). ESP may host multiple versions for supporting gradual migration. As of this specification, API Version is “3.0”.
signerid	Optional	Format: id@id-type.esp-id ASP collects the ID of the signer, along with ID type and ESP Name. ASP may make it intuitive for user to select their required ID type and then specify the value. Allowed ID Types: username, Mobile, PAN If mobile is the id-type, then mobile number should be same as in the eKYC XML. Allowed ESP ID: Unique Identifiers specified by CCA for each empanelled ESP. ASP should construct the signerid based on ID given by user and selected ID type and ESP. This information shall be used by ESP to validate and

		then prepopulate the username for the convenience. ESP should not allow modification of the username in their screen. If signerid is not present, ESP may facilitate the new signer id creation through eKYC provider, however authentication of user should be carried out before signing.
ts	Mandatory	Request timestamp in ISO format. The value should be in Indian Standard Time (IST), and should be within the range of maximum 30 minutes deviation to support out of sync server clocks.
txn	Mandatory	Transaction ID of the ASP calling the API, this is logged and returned in the output for correlation. Should be unique for the given ASP-ESP combination for that calendar day.

maxWaitPeriod	Mandatory	Expiry time in minutes. This is maximum wait time for the ESP to allow Signer to complete the signing. In case the user does not sign within ASP's expected duration, ESP should mark the transaction as error 'User timeout' error code. Default = 1440 minutes
aspId	Mandatory	Organization ID of ASP
responseUrl	Mandatory	ASP URL to receive the response from ESP. This should be a valid URI accessible from ESP system to make a call and submit the response XML packet using HTTP(S)-POST with Content-Type as application/xml. On success or failure including cancellation by user, ESP shall perform a background call to this response URL with 'eSign Response Format' which contains the status success/failure (status = 1/0).

redirectUrl	Optional	ASP URL to redirect the user after completion of transaction. This is supported only in case where ASP uses redirection to ESP authentication page. If present, ESP shall redirect the user back to ASP's designated URL. Such redirection shall have a HTTP(S)-POST and Content-Type of 'application/xwww- form-urlencoded' with parameter of 'txnref' containing concatenated transaction ID and responseCode (separated with a pipe character) in base 64 encoding. txnref=Base64(transaction ID + "|" + responseCode)
signingAlgorithm	Mandatory	This value represents the signature Algorithm. End user certificate generation (DSC) shall also be based on this algorithm. Allowed Values are: 1. ECDSA 2. RSA

Response will be forwarded to the response url provided in the request.

Response XML:

<EsignResp ver="" status="" ts="" txn="" resCode=" " error="">
<UserX509Certificate>base64 value of eSign user certificate (.cer)</UserX509Certificate>
<Signatures>
<DocSignature id="" sigHashAlgorithm="SHA256" error="">
Signature data in raw (PKCS#1) or raw (ECDSA) or PKCS7PDF (CMS) signature as requested
</DocSignature>
</Signatures>
<Signature>Signature of ESP</Signature>
</EsignResp>

Attribute	Presence	Value
ver	Mandatory	Should be set to 3.0
status	Mandatory	In case of success, it will be “1” In case of failure, it will be “0” In case of pending for completion, it will be “2”
ts	Mandatory	Will contain the response timestamp in ISO format.
txn	Mandatory	The Transaction ID provided by ASP in the request.
resCode	Mandatory	A unique response code provided by ESP. This is a unique id for the transaction (eSign user authentication & eSign request) provided by ESP. It shall make the transaction traceable, and ASP is expected to store this code in their audit log. The response code shall be maintained same for particular transaction. Being asynchronous, there may be need for providing the response multiple times including the acknowledgement stage

		and final response stage. All the responses shall carry same response code for the particular transaction.
error	Optional	In case of failure, this will contain an error code. OR blank, in case of success.

Based on the verification of identity of the eSign user 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 based the following verification methods

8 ASP On Boarding Process for eSign

Application Service Providers (ASP) are the entities which will offer the end users, various online services through owned or operated application. However, in the case of Central or State Government, its IT department can facilitate eSign service for other departmental applications.

ASP needs to complete the on-boarding procedure with desired eSign Service Provider. On successful completion of on-boarding procedure, ESP shall grant the access to ASP for the production environment of eSign.

9 ASP Eligibility Criteria

A. The agency which desires 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

Any legal entity registered in India shall be eligible subject to fulfillment of the criteria given below:

a. Should be an organization incorporated under Companies Act, 1956, Registrar of Firms, LLP Registered; OR An association of persons or a body of individuals, in India, whether incorporated or not

b. Should not have been blacklisted by any State Government, Central Government, Statutory, Autonomous, or Regulatory body.

10 Overview of on-boarding process

Below is the overview of the process, to be carried out by ASP in order to integrate eSign.

1. Application form submission by ASP.
2. Submission of supporting documents by ASP

3. Acceptance / agreement to terms of eSign service by ASP.
4. Submission of Digital Signature Certificate (public key) by ASP
5. Integration of API in ASP application in testing / preproduction environment of ESP.
6. Conducting audit and submission of Audit report by ASP
7. Grant of production access by ESP

11 Application form Submission

Organization intending to avail eSign service shall make a formal request to one or more ESP. Following points shall be kept in view while making an application:

1. Application form should be made specific to particular ESP. For this purpose, each ESP may share a format of application form, or ASP shall use the format in the annexure of this document by addressing it to specific ESP.

2. Application form should be submitted in original, and bear the signature / attestation of Authorized signatory of the organization.

3. In case of application form being submitted through paperless mode (email, etc), it shall be digitally / electronically signed by authorized signatory of the organization.

4. ESP shall grant the access to eSign only after receiving completed application form from ASP.

5. ESP may seek additional information over and above that already included in the application form.

12 Acceptance / agreement to terms of eSign service

The ASP should enter / agree to the terms of service with the eSign Service Provider (ESPs) to enable eSign in their application / software. The scope of this process is:

1. To define the terms of service between ASP and ESP.
2. To define scope and obligation of ASP.
3. The terms and conditions for integration and termination of eSign service .
4. To define various inputs that are critical for success of process / activities.

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.

ASP is also expected to understand that eSign service is a regulated service under the provisions of Information Technology Act.

13 Digital Signature Certificate (public key) Submission by ASP

eSign is an online service provided over API. Each transaction is carried out in XML format. For the authenticity and binding of the transaction, each XML request/response Form (request / response) need to be digitally signed.

Hence, every request XML transaction needs to be digitally signed by the ASP before sending it to ESP

ASP has to submit the Digital Signature Certificate to ESP, so that ESP can configure it in their system and validate/verify each transaction received from the ASP.

Such Digital Signature Certificate should fulfill the criteria given below:

1. Should be a valid certificate issued by a CA licensed under Information technology (IT) Act.
2. Should be either an Organizational Person Digital Signature Certificate or an Organizational Document Signer Certificate. The O value in the certificate should be the legal entity name of the ASP organization.
3. Should be either Class 2 or Class 3 certificate.
4. Should be valid for at least six months from date of submission

ESP should implement necessary mechanism for mapping and carrying above validations for ASP's Digital Signature Certificate.

14 Integration of API in ASP application in testing / preproduction environment of ESP.

ASP builds the required infrastructure for adopting eSign service. ESP provides access to pre-production environment and enables the ASP to establish end- to -end connectivity to carry out eSign services testing and integration

15 Audit: Conducting and submission of Audit report by ASP

ESP shall ensure that the ASP application is compliant to the requirement mentioned in e-authentication guidelines and all other applicable regulations. For this purpose:

- ASP should submit the report/ certificate to ESP prior to gaining production access. The audit report shall be examined prior to completion of on-boarding.
- ASP shall appoint eligible auditor and perform the audit.
- ASP shall submit the audit report in original to the ESP. Such audit report should not be older than 3 months. In case, ASP is taking service from multiple ESPs, common audit report can be submitted,
- Audit report should comply positively to all Audit requirements. No open comments / objections should be reported by the auditor. A complete detailed checklist for Audit has been provided in Annexure 2.3.
- ASP Audit report should be carried out by Auditor empanelled by Cert-in /IS Auditor
- ASP should carry out the audit prior to the completion of one year from the date of completion of last audit. Audit report shall also be examined on a yearly basis by ESP by requesting a fresh audit report. ASP should submit annual compliance report with the same audit requirements and procedures provided here, upon request by ESP, within 30 days.
- In special circumstances, ESP can initiate audit or seek audit report from ASP.
- In respect of e-KYC compliance requirements, ESP shall carryout necessary auditing of ASP as applicable separately

16 Confirmation on readiness to Go Live by ASP

ASP shall notify ESP about its readiness for migration to production environment. Subsequently ASP completes the go live checklist and submits the request for Go Live checklist as provided in Annexure 2.4

ESP shall scrutinize the ASP go live request as per the Go-Live checklist and supporting documentation, before moving forward to production access.

17 Grant of production access by ESP

ESP shall ensure successful scrutiny of the following before granting production access:

1. Application form
2. Supporting documents
3. Acceptance of terms of service
4. Digital Signature Certificate submission
5. Integration / testing completion in preproduction / testing environment
6. Audit report
7. Go Live checklist
8. Internal approvals and clearance within ESP organization

On successful completion, ESP grants the access to production environment in the form of necessary URLs and ASP code. ESP shall ensure that such information is securely shared with the relevant person in ASP organization.

18 Application form

ASP Application Form

Organization Name: _____

Category of Organization _____

□ Government Organization	□ Bank/ Financial Institution/ Telecom Company
□ Legal entity registered in India	□ Not for Profit Organization/ Special Purpose
□ Authority Constituted under Central Act	

Address:

_____

Propose Business Scope _____

w.r.t. eSign Service: _____

Management Point of Contact

Nodal Person Name: _____ Mobile No.: _____

Email-ID: _____ Telephone No _____

Technical Point of Contact

Nodal Person Name: _____ Mobile No.: _____

Email-ID: _____ Telephone No _____

Submitted By (*from ASP Organization*)

Signature: _____

Name: _____

Designation: _____

Organization: _____

Date: _____

Approved By (*from ESP*)

Signature: _____

Name: _____

Designation: _____

Organization: _____

Date: _____

19 Supporting Documents accompanying the Application

Category	Documents to be submitted
Government Organization	1. Application form. 2. KYC documents: No documents are required. 3. Audit report. 4. Go Live checklist.
Authority Constituted under Central Act	1. Application form. 2. KYC documents a. Copy of the act under which the organization is constituted. 3. Audit report. 4. Go Live checklist.
Not for Profit Organization/ Special Purpose	1. Application form. 2. KYC documents a. Letter of authority, authorizing the signatory to sign documents on behalf of the organization. b. Documentary proof for Not-for-profit company/ special purpose organization of National importance. 3. Audit report. 4. Go Live checklist.
Bank/ Financial Institution/ Telecom Company	1. Application form. 2. KYC documents a. Letter of authority, authorizing the signatory to sign documents on behalf of the organization. b. License issued by competent authority to run a bank / financial institution / telecom company in India. 3. Audit report. 4. Go Live checklist.
Legal entity registered in India	1. Application form. 2. KYC documents a. certificate of incorporation, partnership deed or any other document in support of the Agency being a legal entity registered in India b. List of names of CEO/CFO/directors/partners/trustees/person-in-charge of the agency along with the organization chart c. Letter of authority authorizing the signatory to sign documents on behalf of the organization 3. Additional documents a. Self-declaration stating that the entity has not been blacklisted by any State Government, Central Government, PSUs, Statutory, Autonomous, or Regulatory body in last five years. 4. Audit report. 5. Go Live checklist.

20 ASP Audit Checklist

Sr no	Audit parameters
1.	The communication between ASP and ESP should be Digitally Signed and encrypted
2.	Communication line between ASP and ESP should be secured. It is strongly recommended to have leased lines or similar secure private lines between ASP and ESP. If a public network is used, a secure channel such as SSL should be deployed
3.	ASP should have a documented Information Security policy in line with security standards such as ISO 27001.
4.	Compliance review of controls as per Information security policy
5.	ASPs should follow standards such as ISO 27000 to maintain Information Security
6.	Compliance to prevailing laws such as IT Act 2000 should be ensured
7.	Software to prevent malware/virus attacks may be put in place and anti-virus software installed to protect against viruses. Additional network security controls and end point authentication schemes may be put in place.
8.	Resident consent process must be implemented to obtain consent for every transaction carried out. The user must be asked for willingness to sign it and consent form should be stored.
9.	Application Security Assessment of the ASP by Cert-in empaneled auditor /IS Auditor
10.	ASP data logging for audit purposes provisioned.
11.	ASP should not delegate any obligation to external organizations or applications.
12.	ASP integrate with ESPs through standard eSign APIs only
13.	Provision for providing/accessing the copy of the signed document to the signer
14.	ASP shall display (and allow download/print) the document that is to be signed clearly for subscribers to read before signing.
15.	ASP shall protect the document URL (available within eSign request) from anyone or any system accessing it using URL and also from virus, malware, etc.
16.	Indemnify both ESP and CA for integrity related discrepancies arises at ASP end

21 ASP Go live Checklist

Go Live Checklist *		
1.	ASP data logging for audit purposes provisioned	☐
2.	ASP has conducted end-to-end testing for 50 no of successful transactions in Pre- production environment	☐

**All the above items are mandatory and need to be completed before submitting for go live approval to ESP. For additional information on the above checklist items please contact the corresponding ESP*

We understand that production ASP license will be provided post ESP approval of this checklist. ASP hereby confirms compliance to the current standards and specifications as published.

Submitted By (*from ASP Organization*)

Signature: _____

Name: _____

Designation: _____

Organization: _____

Date: _____

Approved By (*from ESP*)

Signature: _____

Name: _____

Designation: _____

Organization: _____

Date: _____

22 Reference

http://cca.gov.in/sites/files/pdf/ACT/eSign-APIv3.0.pdf