1.7. 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.

1.8. 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

1.9. 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.

1.10. Supporting Documents Submission

ASP shall submit supporting documents towards KYC verification and other requirements of on-boarding. These documents should be duly attested & forwarded by the authorized signatory of the organization.

The list of documents to be submitted shall be as given at Annexure 2.2

1.11. 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.

Note : The sample agreement is available on the website. The eSign requirements in respect of security, consent, audit and communication shall be enforced through undertaking by ASP or an agreement between ESP and ASP

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.

1.12. 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.

1.13. 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

1.14. 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:

1. 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.
2. ASP shall appoint eligible auditor and perform the audit.

~~3.~~ 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,

4. 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.
5. ASP Audit report should be carried out by Auditor empanelled by Cert-in /IS Auditor
6. 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.
7. In special circumstances, ESP can initiate audit or seek audit report from ASP.
8. In respect of e-KYC compliance requirements, ESP shall carryout necessary auditing of ASP as applicable separately

1.15. 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.

1.16. 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.

2. Annexure

2.1. 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: _____________________

2.2. 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.

2.3. ASP Audit Checklist

Sl	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 empanelled 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	

2.4. Go Live Checklist

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 licence 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: _____________________

****