ASP On-Boarding Guidelines

Version 1.2

April 2017

Controller of Certifying Authorities
Ministry of Communications and Information Technology

Document Control

Document Name	ASP On-Boarding Guidelines
Status	Release
Version	1.2
Last update	12.04.2017
Document Owner	Controller of Certifying Authorities, India

Table of Content

Contents

Executive Summary

The Information Technology Act, 2000 provides the required legal sanctity to Digital signatures based on asymmetric crypto systems. Digital signatures are accepted at par with handwritten signatures and the electronic documents that have been digitally signed are treated at par with paper documents signed in the traditional way. However the scheme of physical verification, document based identity validation, and issuance of cryptographic tokens does not scale to a billion people. The eSign online Electronic Signature Service allows anyone who can be authenticated through acceptable e-KYC services to be able to easily sign a document electronically

eSign Electronic Signature Service can be integrated with various service delivery applications to facilitate digitally signing a document by authenticated through e-KYC of eSign user. It is designed for applying Digital Signature based on authenticated responses received from e-KYC service pertaining to the eSign users demographics. The benefits that eSign provides includes convenience and security to the citizens while the organizations save on time, achieve streamlined processes and reduce the costs associated with handling and storage of paper.

The stakeholders involved in the process include the Application Service Provider (ASP), eSign Service Provider (ESP), the Certifying Authority (CA) and e-KYC Providers. All these players are instrumental in signing of a document through eSign. This document details out the entire process for eSign starting from eSign user initiating the process up to the ESP signing the hash of the document and sending it back to the ASP.

In order to become an eSign enabled Application Service Provider, the organization needs to first apply to a particular ESP by filling the form and submitting the required documents as prescribed. Once the ESP has satisfied itself, the two parties will (ESP and ASP) will enter into an agreement/undertaking to decide the scope of services, service level agreements and other terms of business. Once all these formalities have been completed, the ASP will be given an integration kit to start the pre-production work.

Once the ESP team is satisfied with the preparations of ASP regarding the environment that it has, it will give its approval for the pre-production testing. The ASP needs to generate a -pubic key certificate for mapping and authentication to access the pre-production environment and perform end to end testing. The testing phase lasts for usually 7-10 days during which the main thrust is on testing the domain application and connectivity with the ESP. Once it is complete, the ASP can send a request for approval to Go-Live. The ESP on its part performs tests or checks logs to satisfy itself about the readiness of the ASP to go live.

Once approval is received from the ESP, the ASP needs to obtain a public key certificate for mapping and authentication to access the production environment. The migration from pre-production to production stage is done and after due testing, the ASP can roll out the application to provide eSign service to various eSign users who want to avail it.

The objective of this document is to provide detailed guidelines and activities on how to onboard various organizations to become Application Service Providers (ASP) for the eSign Service. The document gives a brief overview of the eSign service and the process flow for the same. It details out the various stakeholders that are involved in this process and the prerequisites that an organization needs to fulfill. An organization will gain a complete understanding on the various steps that it needs to follow to integrate eSign service in its application. The document also will include the Application form, Agreement/undertaking that the ASP needs to enter into with the eSign Service Provider. Also included are the audits requirements which the ASP needs to fulfill in order to carry out its operations.

Terminologies

"eSign" or "eSign Service" is an online Electronic Signature Service in which the key pair generation, certification of the public key by the CA and digital signature creation for electronic document are facilitated by the eSign online Electronic Signature Service provider instantaneously within a single online service based on successful authentication of individual using e-KYC services

"eSign User" is an Individual requesting for eSign online Electronic Signature Service of eSign Service provider.

"e-KYC" mean the transfer of digitally signed demographic data such as Name, Address, Date of Birth, Gender, Mobile number, Email address, photograph etc of an individual collected and verified by e-KYC provider on successful authentication of same individual

"response code" is the identification number maintained by e-KYC provider to identify the authentication

1. Introduction

1.1. Information Technology Act and Digital Signatures

The Information Technology Act, 2000 provides that information or any other matter shall be authenticated by affixing signature then notwithstanding anything contained in the law, such requirement shall be deemed to be fulfilled if such information is authenticated by means of electronic signatures affixed in a manner prescribed by the Central Government.

Under the IT Act, 2000, 'Electronic signatures' means authentication of an electronic record by a subscriber by means of electronic technique specified in second schedule and includes Digital signatures. Digital Signature means authentication of any electronic record by a subscriber by means of procedure specified in Section 3 of the IT Act, 2000.

As per the Gazette notifications "Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015", Online Digital Signing through the eSign Service will be offered by Trusted Third Parties (TTP) or eSign Service Provider (ESP). Currently only licensed Certifying Authorities (CAs) can operate as ESP. The above mentioned rules states that the e-authentication issued by Controller must be followed for operating as ESP. These e-authentication guidelines, "e-authentication guidelines for eSign Online Electronic Signature Service", is available at www.cca.gov.in/esign

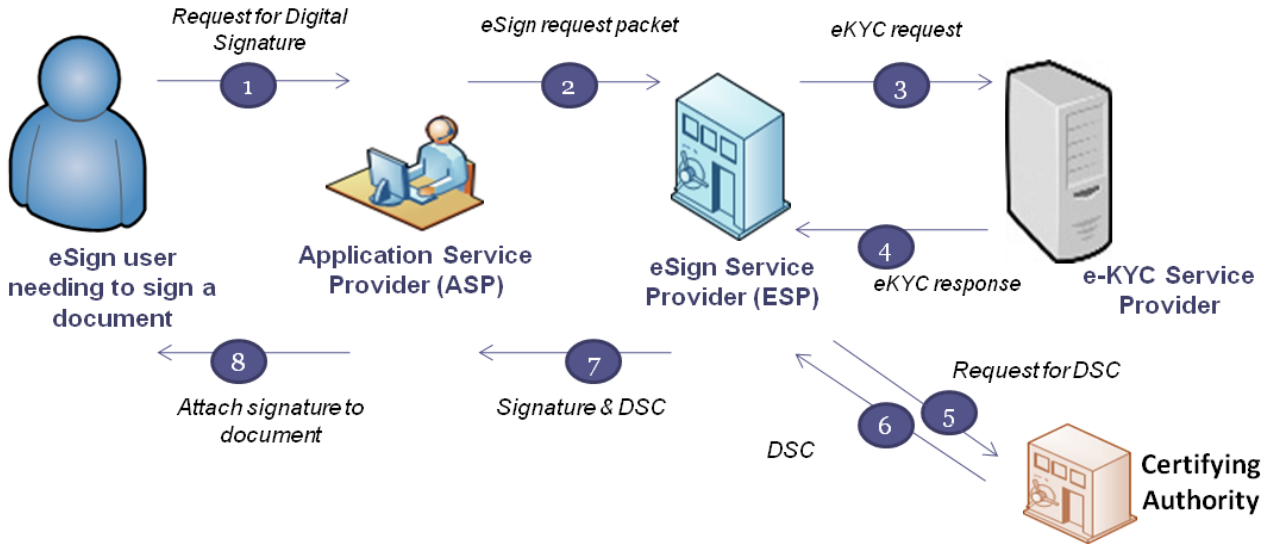
In the traditional Digital Signature system, an individual is responsible for applying for a Digital Signature Certificate to a CA, key pair generation and safe custody of keys. The Certifying Authorities issue Digital Signature Certificate to individuals after verification of credentials submitted in the application form. Such Digital Signature Certificates are valid for 2-3 years

In the eSign online Electronic Signature Service, on successful authentication of individual using e-KYC services, the key pairs generation, the certification (by the CA) of the public key based on authenticated response received and digital signature of the electronic document are facilitated by the eSign online Electronic Signature Service provider.

1.2. eSign Service

eSign facilitates digitally signing a document by an individual using an Online Service. eSign is designed for applying Digital Signature based on the response received from e-KYC service. eSign is an integrated service that facilitates issuing a Digital Signature Certificate and performing Signing of data. A unique e-KYC identifier based on response received from e-KYC services is mandatory for availing eSign Service.

Service delivery applications can integrate with eSign via an open API to facilitate digitally signing a document by an eSign user. It is designed for applying Digital Signature of eSign user who is issued a DSC based on e-KYC authentication.



eSign Process Flow

1.3. Types of Verification

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

1. **e-KYC Services**
   - **OTP**: based on ***OTP authentication*** of eSign user through e-KYC Service
   - **Biometric (FP/Iris)**: based on ***biometric authentication*** of eSign user through e-KYC service.

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.

1.4. 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 with the ESP • Provide the required infrastructure (e.g. biometric scanners) to the end user • Make sure the application is properly integrated with ESP and the required infrastructure in place • Make sure that consent is obtained for each transaction from the eSign to be used by an Application Service Provider (ASP). • Archive logs and carryout audit as per the guidelines of CCA • Examples include Government Departments, Banks and other public or private organizations

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 e-KYC identification Number while eSigning 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

1.5. eSign API

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. Capture e-KYC identification Number
4. Calls the e-Sign API of the eSign provider
5. eSign provider validates the calling application, obtain e-KYC response and validate the authenticity of the e-KYC response.
6. On success, creates a new key pair for that eSign user
7. 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
8. Sends the e-Sign API response back to the calling application
9. Attaches the signature to the document

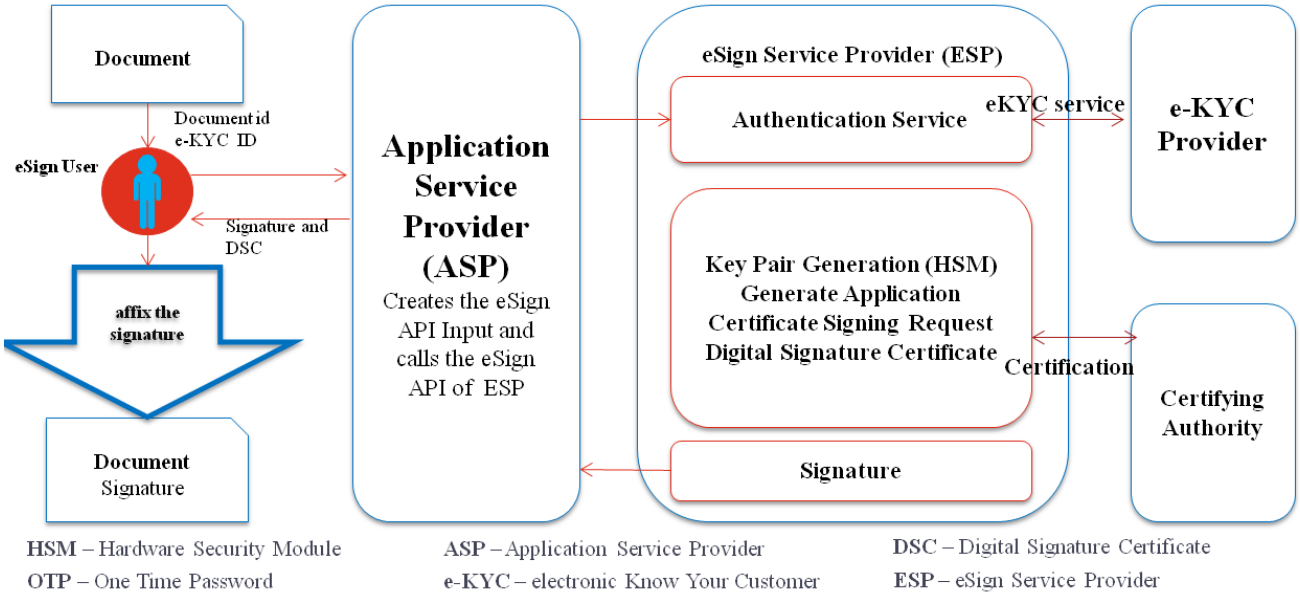
The API specifications remain common for all eSign Service providers. However, below are the things which will vary for each ESP.

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

The eSign service API can be used in different scenarios. ASPs may use:

- Single eSign Service Provider
- Multiple eSign Service Provider

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.



HSM – Hardware Security Module
OTP – One Time Password
ASP – Application Service Provider
e-KYC – electronic Know Your Customer
DSC – Digital Signature Certificate
ESP – eSign Service Provider

1.6. Scope

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.

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. Confirmation on readiness to Go Live by ASP
8. 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.

ESP provides pre-production access by sharing the ASP code to enable ASP to conduct end-to-end testing.

ASP performs end to end integration and 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 the following manner:

1. ASP will test the domain application by transmitting transaction request on pre-production environment. For the purpose of achieving minimum number of transactions ESP should confirm that all such transactions have been successful.

2. ASP is expected to test the connectivity on testing environment as it is critical for integration testing of end user request to ESP

3. ASP should conduct at least 50 successful transactions in the pre-production stage

It is mandatory that, ASP meets the technical requirements of eSign on-boarding during completion of such testing. This includes (but is not limited to) maintaining of logs, signing of transactions, capturing proper consent of end user, adherence to audit requirements and security.

ASP should carry on successful integration with ESP system (APIs) before gaining production access. For this purpose, ASP should carry on a minimum prescribed number of transactions in a testing / preproduction environment of ESP, and submit such transaction information to ESP.

ESP should validate such transaction being recorded and successful in their system.

Post successful end- to- end testing, ASP engages an Auditor empanelled by Cert-in to conduct the compliance audit as per the specifications.

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, Auditor shall consider the following matters mandatorily, in addition to their audit procedures:

    a. Refer the Stakeholders involved in eSign service like end-user, ASP, ESP, CA, e-KYC Provider, and CCA.

    b. Audit checklist provided under these guidelines.

c. Demonstration and analysis of the production-ready application, with regard to eSign.

d. Verification of Production environment for its security requirements, compliance and location.

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

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. If there is major modification, a fresh audit shall be conducted and report shall be submitted, before implementing those changes in production.

8. In special circumstances, ESP can initiate audit or seek audit report from ASP.

9. 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. Annual Report of last financial year b. Audited Balance sheet and P/L account for last financial year c. Memorandum and articles of association along with certificate of incorporation, partnership deed or any other document in support of the Agency being a legal entity registered in India d. List of names of CEO/CFO/directors/partners/trustees/person-in-charge of the agency along with the organization chart e. 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. b. Self-Declaration for Financial and Technical Capability, in company letter head. c. Description of nature of business, along with key product and/or services with brief profile of customers and/or suppliers. d. Proposed model for integrating online eSign service in their application e. Provide details on how the stakeholders (Customers/ eSign Users / Government of India/ State Government/ UTs /Any other Stake holder) will be benefited if the entity integrating eSign service 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	
10.	ASP data logging for audit purposes provisioned.	
11.	ASP should not delegate any obligation to external organizations or applications.	

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	☐
3.	Resident consent process to obtain consent for every transaction is ready & deployed	☐

**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: _____

****