ASP On-Boarding Guide

(Draft for discussion only)

Version 1.0
April 2015

Controller of Certifying Authorities
Department of Electronics and Information Technology
Ministry of Communications and Information Technology
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. Current scheme of physical verification, document based identity validation, and issuance of cryptographic tokens does not scale to a billion people. Current scheme requires issuance of millions of crypto tokens, people to keep track of the token and passwords, etc. For mass adoption of DSC, a simple online service must be designed that allows anyone in this country to have the ability to sign a document with no complexity. And hence, eSign is being developed.

eSign is an online service that can be integrated within various service delivery applications via an open API to facilitate digitally signing a document by an Aadhaar holder. It is designed for applying Digital Signature using authentication of consumer through Aadhaar authentication and e-KYC service. The various benefits that eSign provides include convenience and security to the citizens while the organizations will save on time, streamline the processes and reduce their costs which is associated with handling and storage of paper.

The various stakeholders involved in the process include the Application Service Provider (ASP), eSign Service Provider (ESP), the Certifying Authority (CA) and UIDAI. All these players together play a role in the Aadhaar holder signing a document through eSign. This document also details out the entire process for the eSign starting from an Aadhaar holder initiating the process to ESP signing the hash of the document and sending it back to the ASP.

In order to become 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 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 kick start the pre-production work.

Once the ESP team is satisfied with the preparations of ASP regarding the equipment and environment that it has, it will give its approval for the pre-production testing. The ASP needs to generate a public 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 generate 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 Aadhaar 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 an 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 and give convenience to the end user. This will include the Application form, Contract and Agreement that the ASP needs to enter with eSign Service Provider and adhere to. Also included is the audit requirements which the ASP needs to fulfill in order to carry out its operation.
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.


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 Aadhaar eKYC services, the key pairs generation, the certification( by the CA) of the public key based on authenticated response received from Aadhaar eKYC services, and digital signature of the electronic document are facilitated by the eSign online Electronic Signature Service provider instantaneously within a single online service.

1.2. eSign Service

eSign facilitates digitally signing a document by an Aadhaar holder using an Online Service. eSign is designed for applying Digital Signature using authentication of consumer through Aadhaar eKYC service. The eSign is an integrated service that facilitates issuing a Signature Certificate and performing Signing of requested data by authenticating AADHAAR holder. Aadhaar id is mandatory for availing eSign Service.

Sign is an online service that can be integrated within various service delivery applications via an open API to facilitate digitally signing a document by an Aadhaar holder. It is designed for applying Digital Signature using authentication of consumer through Aadhaar authentication and e-KYC service.
### 1.3. Types of Verification

Based on the verification of identity of the signer 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 in the following classes.

- **Aadhaar-eKYC – OTP**: This class of certificates shall be issued for individuals use based on **OTP authentication** of subscriber through Aadhaar e-KYC.

- **Aadhaar-eKYC – Biometric (FP/Iris)**: This class of certificate shall be issued based on **biometric authentication** of subscriber through Aadhaar e-KYC service.

These certificates will confirm that the information in Digital Signature certificate provided by the subscriber is same as information retained in the Aadhaar databases pertaining to the subscriber as Aadhaar holder.

### 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.

<table>
<thead>
<tr>
<th>S. N.</th>
<th>Stakeholders</th>
<th>Roles and Responsibilities</th>
</tr>
</thead>
</table>
| 1.   | Application Service Provider (ASP) | - Using eSign service as part of their application to digitally sign the content  
- Sign the contract with the ESP to provide eSign Service  
- Provide the required infrastructure (e.g. biometric scanners) to the end user  
- Make sure the application is properly integrated with ESP/ Gateway and the required infrastructure in place  
- 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  
- The end-user shall also be the ‘resident’ holding the Aadhaar number  
- For the purposes of DSC by the CA, the end-user shall also be the ‘applicant/subscriber for digital certificate’, under the scope of IT Act |
### 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
- Must be a registered KYC User Agency (KUA) with UIDAI
- Facilitates subscriber’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. Unique Identity Authority of India
- An authority established by Government of India to provide unique identity to all Indian residents
- Runs the eKYC authentication service for the registered KYC User Agency (KUA)

### 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 Aadhaar eKYC 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 Aadhaar number and authentication factor (OTP/Biometric)
4. Calls the e-Sign API of the eSign provider
5. Validates the calling application, input, and then creates the Aadhaar e-KYC input based on Aadhaar e-KYC API specification
6. Invokes the Aadhaar e-KYC API
7. On success, creates a new key pair for that Aadhaar holder
8. 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 Aadhaar e-KYC response
     - b. This is used for pricing and reporting
9. Sends the e-Sign API response back to the calling application
10. 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 straightforward 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.

1.6. Process flow diagram

The entire process flow starting from a request being raised by an Aadhaar holder to signing of the document with eSign is shown in the sequence diagram below. Each step is described detailing the various processes that are occurring.
OTP Based

1. Initiate eSign request process by giving Aadhaar
2. Forward OTP generation request to ESP
3. Invoke UIDAI’s OTP API
4. Append license key & forward to UIDAI
5. Generate OTP & send to resident mobile / email ID
6. Input OTP, complete ASP form, as required
7. Create eSign API input (doc hash, eSign API license key, Aadhaar PID etc.)
8. Wrap & forward eKYC request
9. Forward final eKYC XML input
10. Authenticate resident through OTP
11. Generate & send eKYC response XML
12. Forward eKYC response XML
13. Decode eKYC response, generate key pair and CSR
14. Sign doc hash & create eSign response
15. Attach signature to original document
16. Get informed of digital signature acceptance
17. Generate DSC
18. Forward & archive copy of DSC
19. Validate functioning key pair
20. Check authorization
21. Receive and Decode CSR

Certifying Authority Functions

ESP* is the AUARUA in this scenario

Biometric Based

1. Initiate eSign request process by giving Aadhaar & biometric; Complete ASP form, as required
2. Create eSign API input (doc hash, eSign API license key, Aadhaar PID etc.)
3. Wrap & forward eKYC request
4. Forward final eKYC XML input
5. Authenticate resident through biometric
6. Generate & send eKYC response XML
7. Forward eKYC response XML
8. Decode eKYC response, generate key pair and CSR
9. Sign doc hash & create eSign response
10. Attach signature to original document
11. Receive and Decode CSR
12. Generate DSC
13. Forward & archive copy of DSC
14. Validate functioning key pair
15. Check authorization
16. Get informed of digital signature acceptance

Certifying Authority Functions

ESP* is the AUARUA in this scenario
2. **ASP On Boarding Process for eSign**

2.1. **Scope**

Application Service Providers (ASP) are the entities which will offer the end users, that is, the citizens various services online. The ASPs need to enter into an agreement with the eSign Service Provider (ESPs) to provide the users the services of eSign. The scope of this process is:

- To define the protocol for engagement between ASP and ESP
- The legal framework between ASP and ESP for carrying eSign service
- To define various inputs that are critical for success of process / activities

2.2. **Prerequisites for Process**

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

B. Need is expressed by the probable agencies to avail eSign Online service through formal communication to ESP and application form is filled

C. Any legal entity registered in India should refer to the following guidelines before applying eSign Online Services

a) **Criteria for legal entities registered in India who are eligible to apply**

Legal entities eligible to apply to use eSign service, can be
   - Any 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;
     and
     The entity should not have been blacklisted by any State Government, Central Government, Statutory, Autonomous, or Regulatory body.

b) **Details regarding the profile of the entity**

The entities are required to provide the following details, along with application
   - Describe nature of business, along with key product and/or services with brief profile of customers and/or suppliers.
   - Financial and technical capability
   - The proposed model for integrating online eSign Signature service in their application

c) **Details regarding the benefits delivered by the entity as an eSign Service provider**
The entities are required to provide details on how the following stakeholders will be benefited if the entity integrating online eSign Signature service

- Customers/subscribers
- Government of India/State Government/UTs
- Benefit to any other stakeholder

d) List of documents to be submitted with the application form

- Annual Report of last financial year
- Audited Balance sheet and P/L account for last financial year
- 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
- List of names of CEO/CFO/directors/partners/trustees/person-in-charge of the agency along with the organization chart
- 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
- Letter of authority authorizing the signatory to sign documents on behalf of the organization

Agency should provide all the documents duly attested by the authorized signatory. A complete list of documents is given in the Annexure.

2.3. Process Outcome

The outcome of the entire process should be such that:

- Signed Addendum (to be part of ASP agreement) between ESP and ASP
- Aligned Processes followed by ASP with ESP

2.4. On Boarding Process

A number of steps need to be taken in order to successfully on board the Application Service Provider for eSign services.

Agreement with ESP

- Submit Application form to any of ESP
- ESP approval and agreement signing
- ESP pre-production environment Testing
- Pre-Production approval
- Go-Live Checklist and Audit Report
- Interoperability - Check list & Testing report
- Production Access & Testing
- Approval & Go Live
2.5. Process Description

2.5.1. Agreement with ESP

Registration

In order to register itself as an ASP, the agency must follow the following steps:

- An organization interested in becoming an Application Service Provider sends a request to eSign Service Provider to enquire about the eSign service and to understand the process for getting access to it.
The eSign Service Provider sends a suitable response to organization enquiry, share the ASP related documentation and proposes to conduct kick off session on the eSign services. ESP team shares the contact details of the team managing the organization engagement provides access to eSign Services knowledgebase which includes the documents listed below:

1. eSign Service Operating Model
2. ASP On-Boarding Guidebook
3. ASP Application form (Appendix 1)
4. Draft Structure of ASP-ESP Agreement (Appendix 3)
5. List of supporting documents and application process (Appendix 4)

Organization submits the application with supporting documents as per the eligibility criteria provided.

ESP engagement team scrutinizes the ASP application and supporting documents as per the guidelines and specifications, List of support documents and application process and other documents published from time to time. ESP team will approve the application and inform the entity.

Initiate the ASP On-Boarding Process to begin applicant’s engagement with ESP as ASP.

**Contract and Agreement Signing**

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.

- Once both ASP and ESP are satisfied, they proceed to sign an agreement
- ESP and ASP enter into an agreement as per the Draft structure of the agreement between ESP-ASP (Appendix 3)

**Integration Kit**

Once the contract and agreement have been signed, the ASP is provided with the integration kit which shall include, but not limited to, the following: API, URL, etc.

- Based on interaction during the previous steps of the process and inputs, an ASP assesses the level of support it requires for go live readiness
- If the ASP team feels that it requires assistance in setting up its services, it can take the needed help.
- ASP team engages with an ESP to define the schedule and agenda of on boarding process which provides access to preparation material on eSign services to better prepare an ASP for the process
- ASP builds the required infrastructure for adopting eSign service with support provided by the approved agency. Once the required infrastructure for eSign service is ready, ASP will request the ESP to send the request for pre-production environment access

**Pre-Production Testing:**

ESP support team provides access to pre-production environment and enables the ASP to establish end to end connectivity to carry out eSign services testing.
ESP support team responds to pre-production access request by sharing the ASP code to enable ASP to conduct end to end testing.

ASP performs end to end 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 following manner:

- ASP will test the domain application by transmitting transaction request on pre-production environment
- ASP is expected to test the connectivity on testing environment as it is critical for integration testing of transmitting end user request to ESP
- ASP should conduct at least 50 successful transactions in the pre-production stage

Post successful end to end testing ASP engages an Information Security Certified Auditor to conduct the compliance audit as per the specifications

**Audit Report Submission and Security Assessment**

- Audit report/ certificate duly signed by an IS certified auditor should be submitted to the ESP as per below schedule
  a. ASP should submit the report/ certificate to ESP prior to the commencement of operations
  b. ASP should submit annual compliance report, upon request by ESP, within 30 days of such request by ESP
- A complete detailed checklist for Audit has been provided in Appendix 5.
- The Application Service Provider is required to get a detailed security and risk assessment of its application before getting the final approval from the ESP.

**Go-Live – Readiness and Approval**

- ASP notifies ESP Business team about its readiness for migration to production environment
- Subsequently ASP completes the go live checklist and submits the request for go live with the following documents:
  - Go Live checklist (Appendix 6)
  - Audit certificate as proof of compliance to current standards and specifications
- ESP engagement team scrutinizes the ASP go live request as per the Go-Live checklist and supporting documentation and seeks internal approvals for Go Live

**Generate License for Production and Go-Live**

- ESP provides access to ASP admin portal for accessing ASP code and ASP generates the public key certificate for mapping and authentication
- Post migration & testing, ASP shall establish production release and operation management mechanism
- ASP goes live and updates status to ESP

This process ends when the ASP systems are aligned to ESP terms & condition and is ready for eSign service delivery
3. Annexure

3.1. Application form

ASP Application Form

Organization Name: ____________________________________________

Category of Organization

☐ Government Organization

☐ Legal entity registered in India

☐ Private Sector Company

☐ Bank/ Financial Institution/ Telecom Company

☐ Not for Profit Organization/ Special Purpose

Address: ____________________________________________

________________________________________

________________________________________

Propose Business Scope
w.r.t. e-KYC Service:

________________________________________

________________________________________

Propose Business Scope
w.r.t. eSign Service:

________________________________________

________________________________________

Management Point of Contact
Nodal Person Name: ____________________________________________

Email-ID: ____________________________________________________

Mobile No.: __________________________________________________

Telephone No.: _______________________________________________

FAX: ________________________________________________________

Technical Point of Contact

Nodal Person Name: ____________________________________________

Email-ID: ____________________________________________________

Mobile No.: __________________________________________________

Telephone No.: _______________________________________________

FAX: ________________________________________________________

Submitted By (from ASP Organization)                           Approved By (from ESP)

Signature: ___________________________                           Signature: ___________________________

Name: ______________________________  Name: ______________________________

Designation: _________________________  Designation: _________________________

Organization: _________________________  Organization: _________________________

Date: _______________________________                           Date: _______________________________
3.2. Aadhaar Holder Consent Form

The below illustrative template for obtaining consent from the Aadhaar holder for using the Aadhaar number, Biometric information and/or One Time Pin (OTP) for providing the Aadhaar Authentication Service to be used by an Application Service Provider (ASP). ASP may customize the consent form as per their requirement.

<Name of Agency Providing the Service>

Consent for Authentication

Please check the box to provide your consent to the below option

I hereby state that I have no objection in authenticating myself with Aadhaar based authentication system and consent to providing my Aadhaar number, Biometric and/or One Time Pin (OTP) data for Aadhaar based authentication for the purposes of availing of the ______ from ______. I understand that the Biometrics and/or OTP I provide for authentication shall be used only for authenticating my identity through the Aadhaar Authentication system for that specific transaction and for no other purposes. I understand that ______ shall ensure security and confidentiality of my personal identity data provided for the purpose of Aadhaar based authentication.

OR

I do not wish to authenticate myself with the Aadhaar based Authentication system for Authentication of my identity. However, I do understand that if at any time I wish to authenticate myself with the Aadhaar based Authentication system I need to provide consent to ______ to provide my Aadhaar number, Biometric and/or OTP data.
3.3. *Contract and Agreement*
### 3.4. Supporting Documents accompanying the Application

<table>
<thead>
<tr>
<th>Organization Type</th>
<th>Supporting Documents required along with the Application</th>
</tr>
</thead>
</table>
| A Central/ State Government Ministry / Department or an undertaking owned and managed by Central / State Government | • Application should be signed by authorized signatory along with the seal of the official signing the document  
• No other supporting documents required |
| An Authority constituted under the Central / State Act                              | • Application should be signed by authorized signatory along with the seal of the official signing the document  
• Copy of the act under which the organization is constituted |
| A Not-for-profit company / Special Purpose organization of national importance      | • Application signed by Authorized signatory  
• Letter of authority, authorizing the signatory to sign documents on behalf of the organization  
• Documentary proof for Not-for-profit company/special purpose organization of National importance |
| A bank / financial institution / telecom company                                     | • Application signed by Authorized signatory  
• Letter of authority, authorizing the signatory to sign documents on behalf of the organization  
• License issued by competent authority to run a bank / financial institution / telecom company in India |

**Note:**

- *All the supporting documents should be self-attested with seal of authorized signatory*
- *The above list of supporting documents is indicative. ESP reserves right to call for any other document on case to case basis*
3.5. Audit Requirement

ASPs have to ensure that its operations and systems related to Aadhaar Authentication are audited by information systems auditor certified by a recognized body before commencement of its operations and it has to provide a certified audit report, to ESP, confirming its compliance with the standards, directions, specifications, as specified.

<table>
<thead>
<tr>
<th>#</th>
<th>Name of the Standard and Specification Document</th>
<th>Link/ Reference to the Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Aadhaar OTP Request API Specification 1.5</td>
<td><a href="https://authportal.uidai.gov.in/static/aadhaar_otp_request_api_1_5.pdf">https://authportal.uidai.gov.in/static/aadhaar_otp_request_api_1_5.pdf</a></td>
</tr>
<tr>
<td>7.</td>
<td>Date and Time format Standard</td>
<td>ISO_8601</td>
</tr>
<tr>
<td>8.</td>
<td>XML Signature</td>
<td><a href="http://www.w3.org/TR/xmldsig-core/">http://www.w3.org/TR/xmldsig-core/</a></td>
</tr>
<tr>
<td>9.</td>
<td>Audit logging requirements</td>
<td>Authentication audit trail should be for a minimum of 6 months. Auditable fields - API Name, ASP Code, Transaction Id, Timestamp, Response Code, Response Timestamp, and any other non-PII data.</td>
</tr>
<tr>
<td>11.</td>
<td>System Security and Data Security</td>
<td>As per Table given below</td>
</tr>
</tbody>
</table>

### Audit Parameters

<table>
<thead>
<tr>
<th>SI</th>
<th>Audit parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>End to end encryption of personal identity data (PID block) is necessary to ensure that data is not read, stored, or tampered with for malicious purposes</td>
</tr>
<tr>
<td>2.</td>
<td>Aadhaar number should not be used as a domain specific identifier</td>
</tr>
<tr>
<td>3.</td>
<td>PID block captured for Aadhaar authentication must be encrypted during capture and should never be sent in the clear over a network</td>
</tr>
<tr>
<td>4.</td>
<td>The encrypted PID clock should not be stored unless it is for buffered authentication for a short period of time and after transmission, it should be deleted</td>
</tr>
<tr>
<td>5.</td>
<td>Biometric and OTP data captured for the purposes of Aadhaar authentication should not be stored on any permanent storage or database</td>
</tr>
<tr>
<td>6.</td>
<td>The meta data and the responses shall be stored for audit purposes for a period of minimum 6 months.</td>
</tr>
<tr>
<td>7.</td>
<td>The communication between ASP and ESP should be Digitally Signed and encrypted using mutually shared asymmetric keys.</td>
</tr>
<tr>
<td>8.</td>
<td>Communication line between ASP and ESP should be secured. It is strongly recommended to</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>9.</td>
<td>ASP should have a documented Information Security policy in line with security standards such as ISO 27001.</td>
</tr>
<tr>
<td>10.</td>
<td>Compliance review of controls as per Information security policy</td>
</tr>
<tr>
<td>11.</td>
<td>ASPs should follow standards such as ISO 27000 to maintain Information Security</td>
</tr>
<tr>
<td>12.</td>
<td>Compliance to prevailing laws such as IT Act 2000 should be ensured</td>
</tr>
<tr>
<td>13.</td>
<td>Software to prevent malware/virus attacks may be put in place and anti-virus software installed to protect against viruses. Additional networks security controls and end point authentication schemes may be put in place</td>
</tr>
<tr>
<td>14.</td>
<td>A two level authentication needs to be followed for all the applicants</td>
</tr>
<tr>
<td>15.</td>
<td>The user must be asked for his willingness to sign it and consent form be stored</td>
</tr>
<tr>
<td>16.</td>
<td>Storage of the authentication and hash of document be performed in a secure manner</td>
</tr>
<tr>
<td>17.</td>
<td>Application Security Assessment of the ASP</td>
</tr>
</tbody>
</table>

### 3.6. Go Live Checklist

**ASP Go live Checklist**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Go Live Checklist</strong></td>
<td></td>
</tr>
<tr>
<td>1.</td>
<td>ASP data logging for audit purposes provisioned</td>
</tr>
<tr>
<td>2.</td>
<td>ASP has conducted end-to-end testing for 50 no of successful transactions in Pre-production environment</td>
</tr>
<tr>
<td>3.</td>
<td>Resident consent process to obtain consent for every transaction is ready &amp; deployed</td>
</tr>
</tbody>
</table>

*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*

Please note 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)*

<table>
<thead>
<tr>
<th>Signature:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Designation:</td>
<td></td>
</tr>
<tr>
<td>Organization:</td>
<td></td>
</tr>
<tr>
<td>Date:</td>
<td></td>
</tr>
</tbody>
</table>

**Approved By** *(from ESP)*

<table>
<thead>
<tr>
<th>Signature:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Designation:</td>
<td></td>
</tr>
<tr>
<td>Organization:</td>
<td></td>
</tr>
<tr>
<td>Date:</td>
<td></td>
</tr>
</tbody>
</table>