ASP On-Boarding Guidelines

eSign API Version 2.1

Centre for Development of Advanced Computing
(C-DAC)

Innovation Park, S. No. 34/B1, 4th Floor, Panchavati, Pashan
Pune - 411 008, Maharashtra (INDIA)
Telephone: +91-20-2550-3314
Website: https://esign.cdac.in
Email: ess@cdac.in

Contents

List of Figures

1 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 Digital Signature Certificate (DSC), a simple online service is desirable that allows one to have the ability to sign a document with ease. With that in consideration, an online scheme that uses the Electronic Know Your Customer (e-KYC) mechanisms from Aadhaar and provides the trust on documents in the form of digital signatures, eSign, is enabled by the Government of India.

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 signer through Aadhaar authentication and e-KYC service. The various benefits that eSign provides include convenience and ease of operations to the signer, streamlined processes and reduction in the costs of operations largely associated with handling and storage of paper.

Presently, C-DAC offers its eSign service, named e-Hastakshar, to Aadhaar holders with registered mobile numbers using Aadhaar OTP (One Time Password) or Biometric (Finger Minutiae) based e-KYC services to authenticate the document signer. The various stakeholders involved in the process include the Application Service Provider (ASP), eSign Service Provider (ESP), the Certifying Authority (CA) and Unique Identification Authority of India (UIDAI). All these stakeholders together ensure that an Aadhaar holder is enabled to sign a document through eSign services.

C-DAC is an ESP and offers services to various ASPs. In order to register as an ASP with C-DAC ESP (e-Hastakshar), the corresponding organization needs to carry out certain necessary steps including integration of their application(s) with e-Hastakshar. The integrations is based on the following four level of integration processes-

(1) Staging Level Integration,

(2) Pre-Production Level Integration,

(3) Production Level Integration and

(4) Release and Go-Live.

The objective of this document is to provide detailed guidelines on the activities that are required to be carried out for onboarding the organizations which intend to become an Application Service Provider to avail the e-Hastakshar service. An organization will gain complete understanding on various steps that are required while integrating their application(s) with the e-Hastakshar service. The document also provides prerequisites including the audit requirements which every ASP needs to fulfill in order to avail eSign service as per the Controller of Certifying Authorities (CCA) guidelines.

2 Background

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 Signature' 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. This mandates that the authentication issued by CCA must be followed for operating as ESP. These e-authentication guidelines are made available by CCA

In the traditional Digital Signature system, an individual is responsible for applying for a Digital Signature Certificate to a CA for key pair generation and for safe custody of the keys. The Certifying Authorities issue Digital Signature Certificate (DSC) to individuals after verification of credentials. Such Digital Signature Certificates are valid for a fixed duration, normally two to three years.

In the eSign online Electronic Signature Service, on successful authentication of individual using Aadhaar e-KYC services, the key pair generation, the certification(by the CA) based on the response received from Aadhaar e-KYC services, and digital signature of the electronic document are facilitated by the eSign online Electronic Signature Service provider instantaneously within a single online service.

As is necessary under the guidelines of CCA, an eSign service provider must also be a CA. C-DAC is a CA approved by CCA and is authorized to provide eSign services. To that extent, C-DAC issues digital signatures as well as digital signature certificates to verify the digital signatures.

3 Glossary of Terms and Abbreviations

Table 1. Terms and Abbreviations

Terms	Definition
Aadhaar Number	12 digit individual identification number issued by the Unique Identification Authority of India on behalf of the Government of India.
API	Application Program Interface
ASP	Application Service Provider
ASP-ID	User ID issued by ESP to the ASP
AUA	Authentication User Agency
CA	Certifying Authority
CCA	Controller of Certifying Authority
C-DAC	Centre for Development of Advanced Computing
CSR	Certificate Signing Request
Document Signer	Represents himself/herself for signing the document under the legal framework
DSC	Digital Signature Certificate (for the verification of the digital signatures by public-at-large)
e-Hastakshar	eSign Service from C-DAC
e-KYC	electronic Know Your Customer
ESP	eSign Service Provider
HSM	Hardware Security Module
ICERT	Indian Computer Emergency Response Team
IS	Information Security
Key-Pair	Pair of Private key and Public key as defined in PKI
KUA	KYC User Agency
KYC	Know Your Customer
OTP	One Time Password
PKCS7	Public-Key Cryptography Standards #7
PKI	Public Key Infrastructure
Signer Consent	Consent from the document signer to use the identity and address data obtained from Aadhaar system to generate and submit the request for issuance of DSC to CA after generating the key pair and to use the private key for computation of digital signature, to delete the key pair thereafter, and to specify what to include optionally in the DSC as subject's identity.
UI	User Interface
UIDAI	Unique Identity Authority of India
UID Token	Unique Identifier
W3C	World Wide Web Consortium

4 eSign Overview and Workflow

The workflow of eSign service is given in Figure 1.

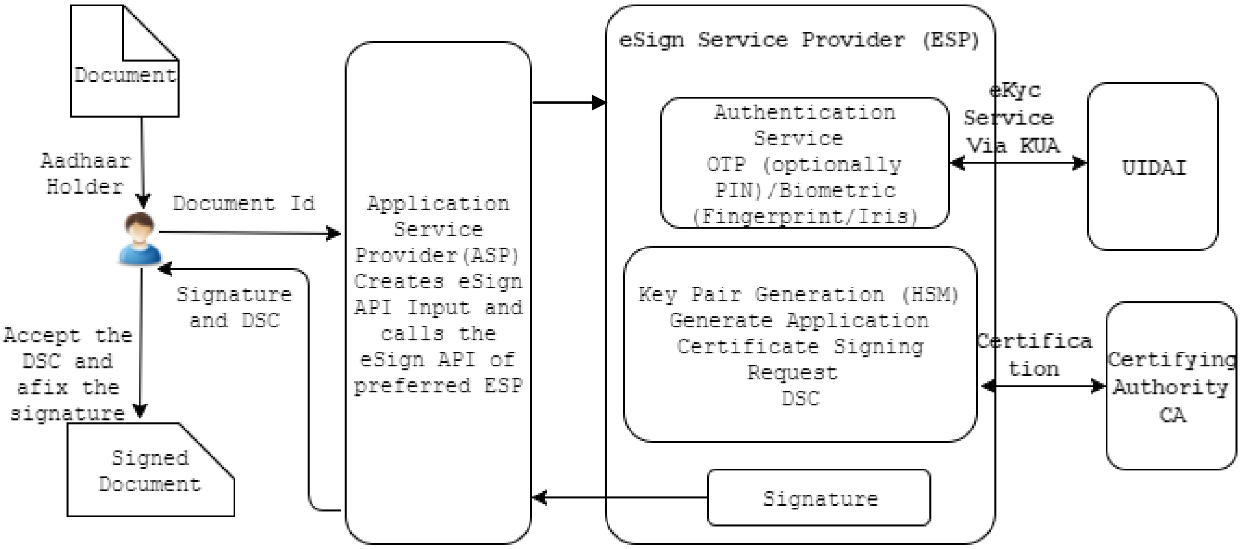

Document
Aadhaar Holder
Document Id
Signature and DSC
Accept the DSC and afix the signature
Signed Document
Application Service Provider(ASP) Creates eSign API Input and calls the eSign API of preferred ESP
eSign Service Provider (ESP)
Authentication Service OTP (optionally PIN)/Biometric (Fingerprint/Iris)
eKyc Service Via KUA
UIDAI
Key Pair Generation (HSM) Generate Application Certificate Signing Request DSC
Certification
Certifying Authority CA
Signature

Figure 1. eSignWorkflow

In the eSign workflow, there are three main entities -

- ASP – Application Service Provider
- ESP– eSign Service Provider. C-DAC is an ESP and its eSign services are known as e-Hastakshar
- UIDAI – Aadhaar Authentication and e-KYC interface

4.1 Flow-I at Application Service Provider (ASP)

- Compute the document hash (to be signed).
- Captures authentication mode
- Obtains the document signer's consentfor usingthe signatory's identity and address data received from e-KYC provider to, generate and submit the electronic DSC application form to CA, creation of key pairs by ESP for signatory, submission of certificate to CA for certification, one time creation of signature on the hash along with this request, deletion of key pairs after applying signature.
- Creates the request (in XML format) for eSign.
- Calls the eSign Service for computing digital signature.

4.2 Flow-II at eSign Service Provider (ESP)

- Validates the request received from ASP
- Responds ASP with C-DAC ESP Authentication Page URL

- ASP redirects signer to C-DAC ESP Authentication Page
- Signer enters Aadhaar ID/Virtual ID on ESP Authentication Page.In case of OTP authentication Virtual ID can be used while in case of Biometric Aadhaar ID/Virtual Id can be used.
- C-DAC ESP creates the OTP Request XML (In case authentication mode is OTP)
- C-DAC ESP sends the OTP request to Aadhaar through its AUA
- Upon success, creates the Aadhaar e-KYC request
- Obtains the document signer's consent for authenticating signer's identity and for obtaining e-KYC through Aadhaar e-KYC service only for the purpose ofeSigning
- Sends the e-KYC request to Aadhaar through its KUA.
- Upon success, creates a new key pair for the document signer.
- Sends public key and e-KYC information to the Certifying Authority as a certificate signing request (CSR).

4.3 Flow-III at Certifying Authority (CA)

- Based on the CSR received from ESP, DSC is issued and sent back to the ESP.
- C-DACCA offers the class of certificate as shown in Table 2.

Table 2: Certificate Class

Class	Assurance	Applicability	Suggested Use
Aadhaar-e-KYC–OTP	Aadhaar OTP class of certificates shall be issued for individual's use based on OTP authentication of subscriber through Aadhaar e-KYC. 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.	This level is relevant to environments where OTP based Aadhaar-e-KYC authentication is an acceptable method for credential verification prior to issuance of DSC. Certificate holder's private keys are created on hardware and destroyed immediately after one time use at this assurance level.	Document signing
Aadhaar-e-KYC–BIO	Aadhaar BIO class of certificates shall be issued for individual's use based on Biometric based authentication of subscriber through Aadhaar e-KYC. 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	This level is relevant to environments where Biometric based Aadhaar-e-KYC authentication is an acceptable method for credential verification prior to issuance of DSC. Certificate holder's private keys are created on hardware and destroyed immediately after one time	Document signing

	Aadhaar holder.	use at this assurance level.	

C-DAC CA supports this class of certificate within its Certification Practice Statement which is valid under the IT ACT 2000.

4.4 Flow-IV at eSign Service Provider (ESP)

- Signs the document hash using the private key (Note: the document is never made available to the ESP).
- Creates an audit trail for the transaction which includes the transaction details, timestamp, and Aadhaar e-KYC response.
- Sends the e-Sign response back to the calling application (ASP).

4.5 Flow-V at Application Service Provider (ASP)

- Receives the signature and DSC from the e-Sign provider (as PKCS7 packet).
- Attaches the signature to the corresponding document for which Hash was sent to ESP.

5 Stakeholders – Roles, Responsibilities and Interactions

The roles and responsibilities of various stakeholders involved in offering eSign Services to an ASP are detailed below in Table 3.

Table 3: Stakeholders' Roles and Responsibilities

S.No	Stakeholder	Roles and Responsibilities
1.	Document signer	• Represents himself/herself for signing the document under the legal framework • The document signer shall also be the 'resident' holding the Aadhaar number and should have a registered mobile number with Aadhaar • For the purposes of DSC by the CA, the document signer shall also be the 'applicant/subscriber for digital certificate', under the scope of IT Act • Provides the correct Aadhaar Number for eSign and will not impersonate anyone else
2.	Application Service Provider (ASP)	• Must ensure the security of the application as per the procedures defined by Controller of Certifying Authority (CCA) and Indian Computer Emergency Response Team (ICERT) • Facilitate and provide necessary Interface/Application and infrastructure to an applicant for eSign • Sign contract and integrate Application with ESP to use eSign service
3.	C-DAC eSign Service Provider (ESP)	• Provides the eSign service and is a "Trusted Third Party", as per the definitions of Second Schedule of Information Technology Act • Is a registered KYC User Agency (KUA) with UIDAI • Facilitates subscriber's authentication capturing, key pair-generation, storing of key pairs on hardware security module (HSM) and creation of digital signature • C-DAC is licensed Certifying Authority (CA).
4.	Certifying Authority (CA)	• Licensed by the CCA for issuance of Digital Signature Certificate • Carries out allied CA operations such as maintenance of CRL etc.
5.	Unique Identity Authority of India (UIDAI)	• Provides unique identity to residents as per the authority established by Government of India for that purpose. • Runs the e-KYC 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 their effective functioning.

The interactions among these stakeholders involved in usage of eSign Services are detailed below in 2.

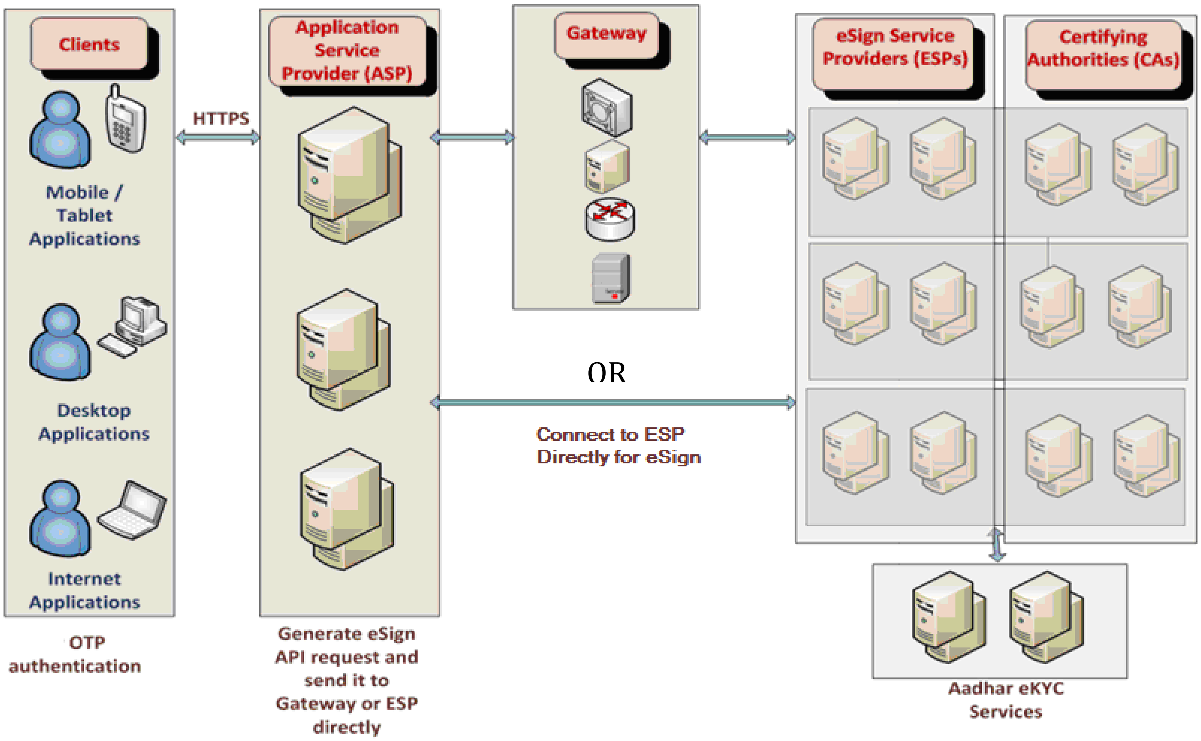

Clients
Mobile / Tablet Applications
Desktop Applications
Internet Applications
OTP authentication
HTTPS
Application Service Provider (ASP)
Generate eSign API request and send it to Gateway or ESP directly
Gateway
OR
Connect to ESP Directly for eSign
eSign Service Providers (ESPs)
Certifying Authorities (CAs)
Aadhar eKYC Services

Figure 2. Stakeholders' Interactions

6 Process for Integration of ASP with e-Hastakshar

6.1 Scope

The ASPs need to enter into an agreement with C-DAC and integrate their application(s) with e-Hastakshar to use the eSign services provided by C-DAC. The scope of this process includes the following.

- To define the protocol for engagement between ASP and C-DAC including necessary documentation.
- To follow the four-level integration process as defined by C-DAC.
- To sign the framework of engagement between ASP and C-DAC for using e-Hastakshar.

6.2 Prerequisites for On-boarding Process

The Agency which desires to avail the eSign service shall submit the duly filled in request form to be the ASP as given in Annexure-1 , along with documents as necessary as per Annexure-2.

6.3 Integration Process

C-DAC offers a four level integration process for the seamless usage of e-Hastakshar service. The levels ensure the errors and gaps that may arise during the development and testing phases are removed and the ASP application that includes eSigning is effectively offered to the document signers in production environment.

The ASP must acquire the following inputs from the document signer in their application-

- UID Token (optional)
- Authentication Mode (OTP/Bio)
- Document to be signed
- Signer consent

Prior to integration it would be necessary to verify that the ASP takes such input. A visual check on the application interface shall be carried out by C-DAC prior to starting the integration. ASPs are to facilitate C-DAC to carry out the pre-check of their user interface. This could be carried out through desktop sharing/other methods.

The four levels of integration process with e-Hastakshar are-

(1) Staging Level Integration,

(2) Pre-Production Level Integration,

(3) Production Level Integration and

(4) Release and Go-Live.

The transition from one level to another is carried out as following –

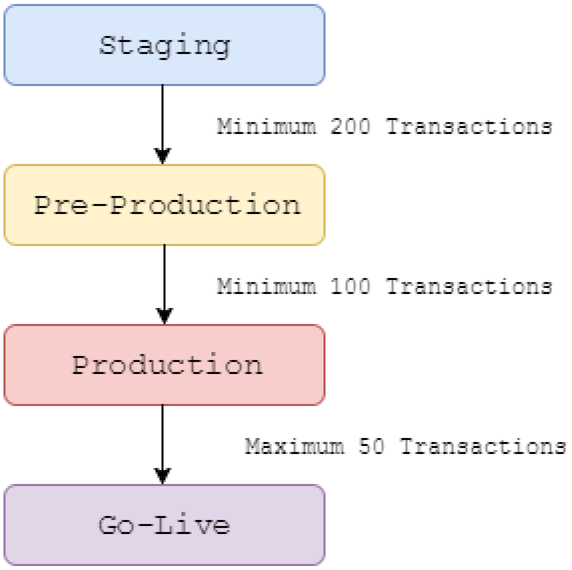


Figure 3. Levels of Integration with e-Hastakshar

6.3.1 Level I: Staging

Integration at this level is targeted towards conformity of ASP requests for eSign to API specifications as defined by CCA. This will include format checks on requests for (but not limited to)-

- Basic checks for HTTP header/protocol usage such as request method (Only POST allowed), Content-Type (Only application/xml allowed) and usage of SSL (i.e. HTTPS)
- Presence of all mandatory elements and attributes in the request XML
- Check for data type and values to be in specified range
- Checks that the request XML does not contain extra elements and/or attributes other than those which are mandatory and optional
- Checks for more than one occurrence of said attribute and element and data contained within to avoid conflict
- Presence of enveloped ASP signature on request XML and its verification

Staging level integration can be done as follows -

- ASP to submit the duly filled-in ASP Application Form (Annexure-1) to C-DAC along with documents as necessary as per Annexure-2.
- Upon verifying the same along with documents as necessary, C-DAC shall provide ASP with integration kit with details including API, URL, ASP-ID(Test), Digital Certificate of C-DAC etc.
- ASP to share digital certificate which will be used to verify signature in the request XMLs. The certificate can be a self-signed certificate (such a certificate shall not be

allowed in Production environment) or issued by a CCA empanelled Certifying Authority.

- The Digital Certificate of C-DAC corresponding to Level I/Level II integration must be used by ASP to verify the signature in the response XML from ESP.
- Subsequent to the integration at Staging level, successful processing of at least 200 transactions between ASP and e-Hastakshar shall be carried out.
- ASP shall provide an undertaking mentioning that the action performed for each of the response transactions are carried out as expected and Level II integration can be initiated.

The process flow for Level I, Staging, is shown in Figure 4

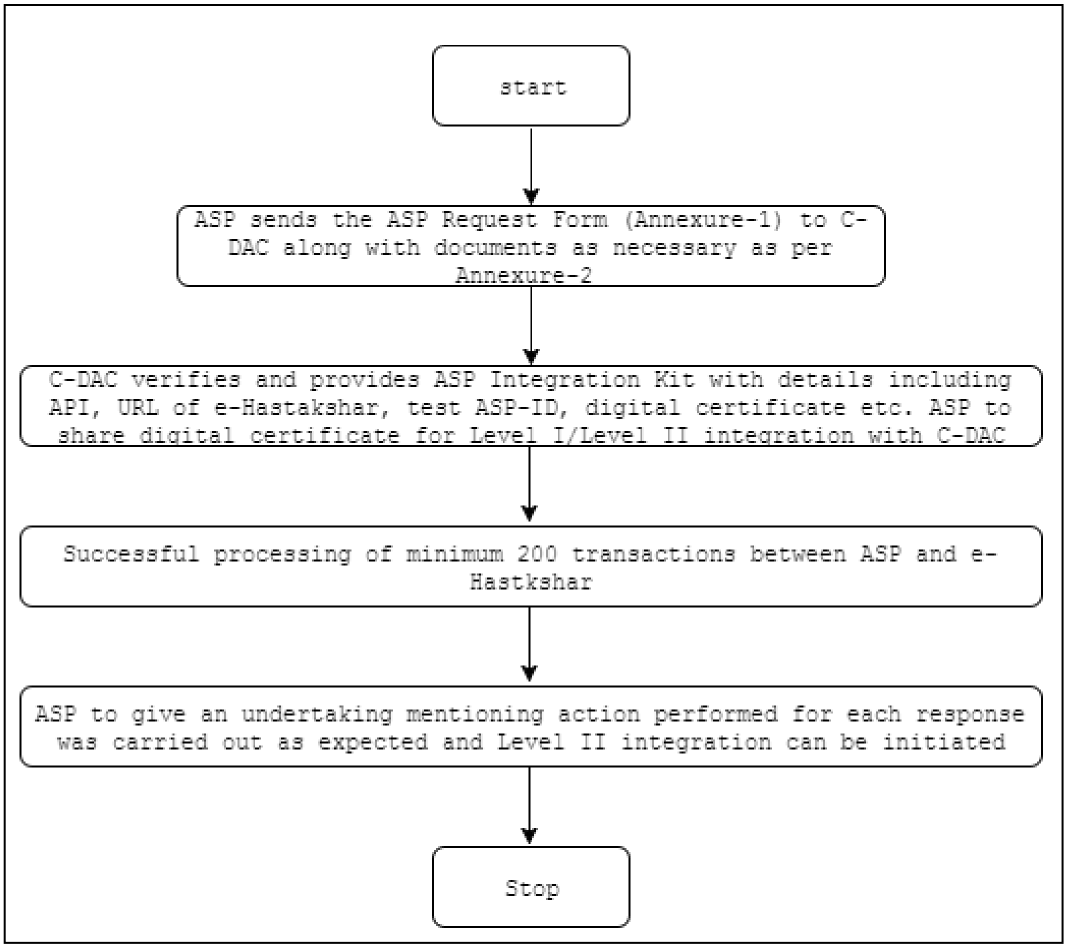

start
ASP sends the ASP Request Form (Annexure-1) to C-DAC along with documents as necessary as per Annexure-2
C-DAC verifies and provides ASP Integration Kit with details including API, URL of e-Hastakshar, test ASP-ID, digital certificate etc. ASP to share digital certificate for Level I/Level II integration with C-DAC
Successful processing of minimum 200 transactions between ASP and e-Hastkshar
ASP to give an undertaking mentioning action performed for each response was carried out as expected and Level II integration can be initiated
Stop

Figure 4. Flow Diagram for Level I: Staging

6.3.2 Level II: Pre-Production Level

Focus at this level of integration will be use of signer's e-KYC data as obtained from UIDAI for DSC generation. To enable this, ASP is expected to use Aadhaar numbers/Virtual IDs/UID Token of those individuals who have given written consent to take part in the integration by using their Aadhaar numbers/Virtual ID for at least 50% of transactions. For using such Aadhaar

Numbers/Virtual ID, it is necessary to obtain Aadhaar Holder's consent as given in Annexure-7. This level will also encompass all integration checks as there are in Level I. Among the requests received from ASP, only those requests for which written consent is obtained shall be sent to UIDAI for e-KYC.

Pre-production level integration can be done as follows -

- ASP to share Aadhaar holders' consent as given in Annexure-7. ASP is expected to use these Aadhaar numbers/Virtual IDs/UID token for about 50% of transactions at Level II integration.
- Subsequent to the integration at Pre-Production level, successful processing of at least 100 transactions between ASP and e-Hastakshar shall be carried out.
- ASP shall provide an undertaking mentioning that the action performed for each of the response transactions are carried out as expected and Level III integration can be initiated.

In parallel to the integration at this step, the ASP is strongly advised to initiate the production level documentation and processes as follows -

- ASP to initiate the Application Security Audit to be done by ICERT empanelled agency listed on www.cert-in.org.in/PDF/Empanel org.pdf (such as C-DAC, Hyderabad) that should be completed prior to the Production level integration.
- ASP to initiate audit of the application by IS certified auditor to carry out the audit as given in Annexure-11.
- ASP to take steps towards signing the ASP-ESP (C-DAC) agreement as given in Annexure-3.

The process flow for Level II, Pre-Production, is shown in Figure 5.

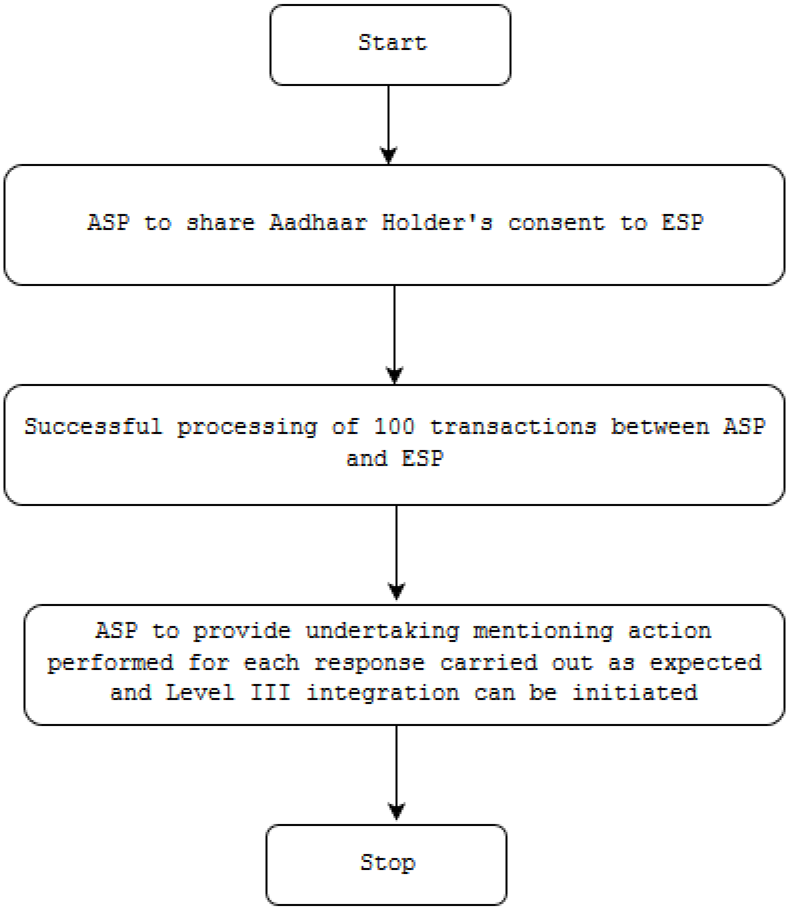

Start
ASP to share Aadhaar Holder's consent to ESP
Successful processing of 100 transactions between ASP and ESP
ASP to provide undertaking mentioning action performed for each response carried out as expected and Level III integration can be initiated
Stop

Figure 5. Flow Diagram for Level II: Pre-Production

6.3.3 Level III: Production Level

Production level integration shall be carried out after the integration with pre-production level is successful. This level aims to integrate ASP with the production environment of e-Hastakshar before the release and go-live of the ASP. The agreement between ASP and C-DAC is to be signed, prior to the carrying out of Production level integration.

Following steps are required to initiate Production level integration:

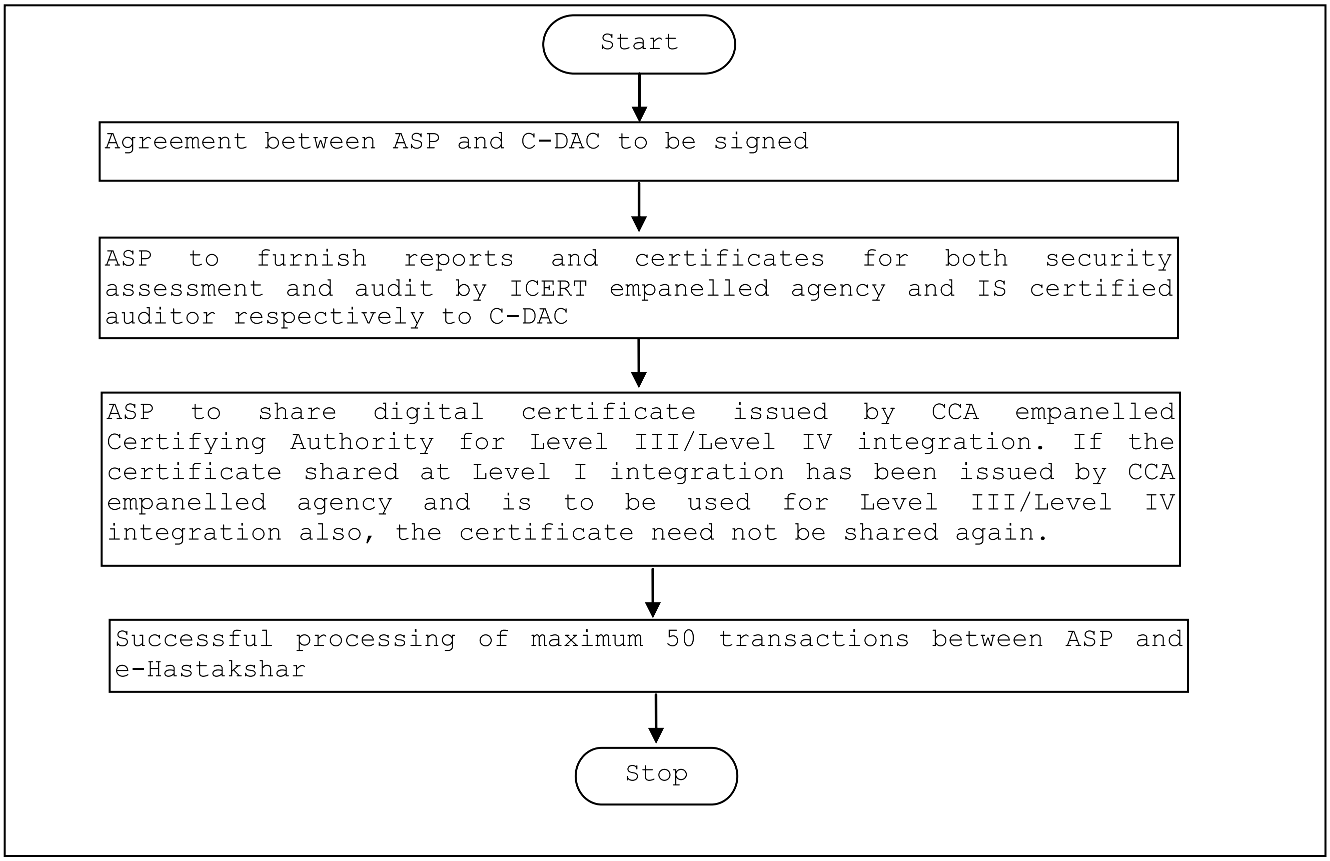
1. Agreement between ASP and C-DAC to be signed.
2. ASP to furnish the certificate and reports of the security assessment carried out by ICERT empanelled agency of the ASP application to C-DAC.
3. ASP to furnish audit report carried out by IS certified auditor. A complete detailed checklist for Audit has been provided in Annexure-11.
4. ASP incorporates process to obtain Resident consent for every transaction. (Refer sample given in Annexure-4).

5. ASP to share digital certificate which will be used to verify signature in the request XMLs. The certificate is required to be issued by a CCA empanelledCertifying Authority.

   In case the digital certificate shared by ASP during Level I integration has been issued by a CCA empanelled Certifying Authority and same has to be used in production environment also, the certificate need not be shared again.

6. Subsequent to the integration at Production level, successful processing of maximum 50 transactions between ASP and e-Hastakshar shall be carried out before Go-Live.

The process flow for level III, Production, is shown in Figure 6.



Start

Agreement between ASP and C-DAC to be signed

ASP to furnish reports and certificates for both security assessment and audit by ICERT empanelled agency and IS certified auditor respectively to C-DAC

ASP to share digital certificate issued by CCA empanelled Certifying Authority for Level III/Level IV integration. If the certificate shared at Level I integration has been issued by CCA empanelled agency and is to be used for Level III/Level IV integration also, the certificate need not be shared again.

Successful processing of maximum 50 transactions between ASP and e-Hastakshar

Stop

Figure 6. Flow Diagram for Level III: Production

6.3.4 Level IV: Release and Go-Live

At this level ASP notifies C-DAC about its readiness to offer eSign Services. The subsequent steps are:

- ASP to comply with the items in the go-live checklist (Annexure-12).
- C-DAC team to scrutinize the ASP go-live request as per the Go-Live checklist and supporting documentation and seek internal approvals for Go-Live.

- C-DAC to offer Production level ASP-ID to ASP.
- ASP goes live and updates status to C-DAC.

The process flow for Level IV, Release and Go-Live, is shown in Figure 7.

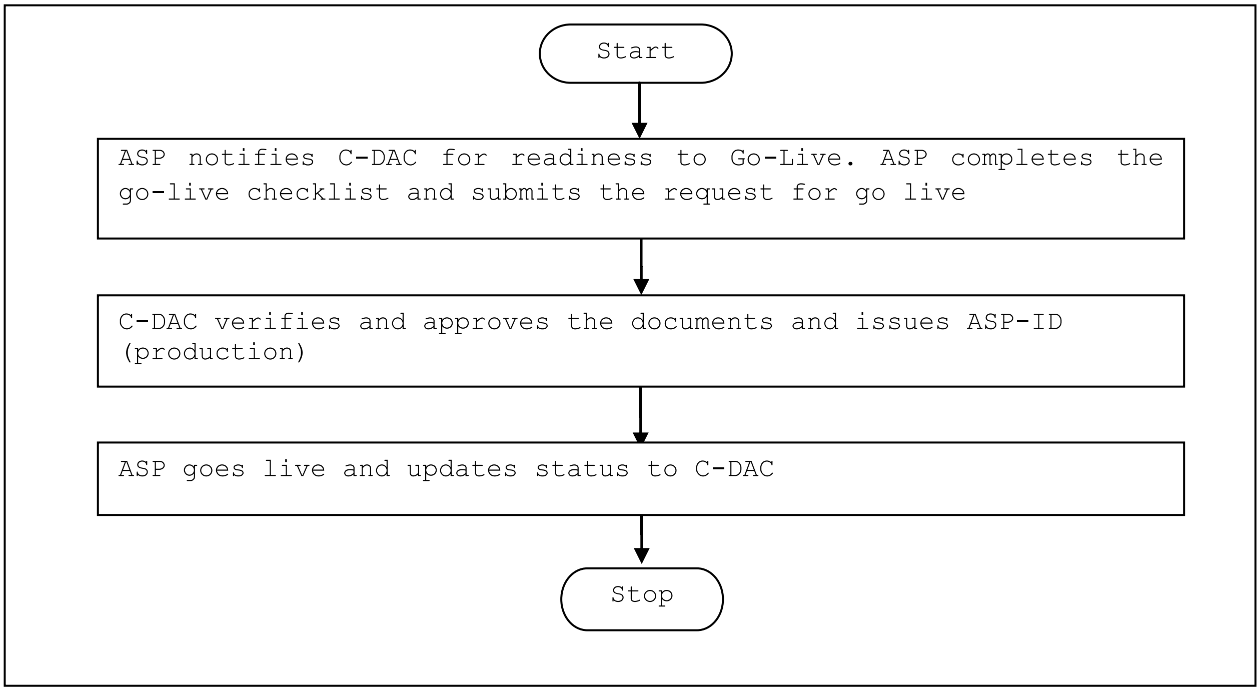

Start
ASP notifies C-DAC for readiness to Go-Live. ASP completes the go-live checklist and submits the request for go live
C-DAC verifies and approves the documents and issues ASP-ID (production)
ASP goes live and updates status to C-DAC
Stop

Figure 7. Flow Diagram for Level IV: Release and Go-Live

7 eSign API Specification Between ASP and e-Hastakshar

eSign service is exposed as stateless service over HTTPS. Usage of an open data format such as XML and widely used protocol such as HTTP allows easy adoption and deployment of this service. To support strong end-to-end security and to avoid request tampering and man-in-the-middle attacks, it is essential that encryption of data happens at the time of capture on the capture device.

7.1 Directly Connecting to e-Hastakshar

The API specifications are standard for all eSign Service providers. For connecting directly to e-Hastakshar, an ASP would require the following:

- e-Hastakshar Service URLs
- ASP-ID - Unique ID provided by C-DAC
- Public key certificate of e-Hastakshar service

7.2 Authentication API: Input Data Format - eSign Service

eSign Service uses XML as the data format for input and output.

7.2.1 eSignRequest XML structure

Following is the XML data format for eSign XML.

```
<Esignver="" sc="" ts="" txn="" ekycId="" ekycIdType="" aspId=""
AuthMode="" responseSigType=" responseUrl="">
<Docs>
<InputHash id="" hashAlgorithm="" docInfo="">Document Hash in
Hex</InputHash>
</Docs>
<Signature>Digital signature of ASP</Signature>
</Esign>
```

7.2.1.1 Element Details

Element Name: Esign

- Description: Root element of the eSign xml
- Requirement of tag: Mandatory
- Value: Sub-elements
- Attributes: Table below

Sr No	Attribute	Required?	Value
1	ver	Mandatory	eSign version. This is alphanumeric string with supported characters as 0-9 and period. Allowed value

			is **2.1**
2	sc	Mandatory	ASP should have taken a clear consent from 'document signer' to carry on eSign from their front ending application. This attribute represents signatory's explicit consent is obtained by ASP for using the signatory's identity and address data received from e-KYC provider to, generate and submit the electronic DSC application form to CA, creation of key pairs by ESP for signatory, submission of certificate to CA for certification, one time creation of signature on the hash along with this request, deletion of key pairs from the after applying signature. Please refer to Section 7.4 for details of value of "sc" field.
3	ts	Mandatory	Request timestamp in the format of "YYYY-MM-DDTHH:mm:ss.sss" (generated at ASP). 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
4	txn	Mandatory	Transaction ID of the ASP calling the API, this is logged and returned in the output for correlation. This is an alpha-numeric string of maximum length 50 (generated at ASP). Only supported characters are A-Z, a-z, 0-9, period, comma, hyphen, backward & forward slash, left & right parenthesis, and colon.
5	e- KYCIdType	Mandatory	This represents the type of e-KYC ID being used. The value can be any one out of below: 1. Aadhaar = A
6	ekycId	Optional	If present, the value must be UID TOKEN. ESP should process the request only if ekycId of input XML and e-KYC authentication response are same. ***Provided UID token will be used for authentication purpose.***
7	aspId	Mandatory	Organization ID issued by C-DAC ESP to the ASP. This is an alpha-numeric string. Only supported characters are A-Z, a-z, 0-9 and hyphen.

8	AuthMode	Mandatory	Mode of authentication being requested. Allowed values are:
			OTP = 1
			Fingerprint = 2
			IRIS = 3
			Class of eSign Certificate will be "OTP Class" for OTP based authentication. For Fingerprint and IRIS, the class will be "Biometric Class". These will be as per definitions of "Class of Certificate" in India PKI-CP.
			Currently, C-DAC ESP supports OTP, Finger Print and IRIS based Biometric mode only.

9	responseSigType	Mandatory	Response signature type, where ASP can request for specific type of signature, like Raw or PKCS7.

			Allowed Values are: 1. rawrsa 2. pkcs7 3. rawecdsa Examples: responseSigType="rawrsa" responseSigType="pkcs7" C-DAC ESP supports 'pkcs7' type response signature only
10	responseUrl	Mandatory	This is mandatory. This should contain a valid HTTPS URL of the ASP, to which ESP has to redirect back to ASP with response XML.

Element Name: Docs

- Description: Contains 1 sub-element with Document Hash
- Requirement of tag: Mandatory
- Value: Sub-elements
- Attributes: Not applicable

Element Name: InputHash

- Description: Contains the value of Document Hash, which has to be signed.
- Requirement of tag: Mandatory
- Value: SHA256 hash value of the document in Hex format

Sl No	Attribute	Required?	Value
1.	id	Mandatory	Contains serial number for document hash. This will be the key to correlate the response signature of each document.
2.	hashAlgorithm	Mandatory	Should be fixed to "SHA256"
3.	docInfo	Mandatory	Description for the respective document beingsigned, not more than 50 characters.

Element Name: Signature

- Description: Contains the signature of ASP.
- Requirement of tag: Mandatory
    - Value:Signed value of Input XML, as per the W3C recommendation on XML Signature Syntax and Processing (Second Edition)
    - Refer http://www.w3.org/TR/xmldsig-core/ for more information
- Attributes: Not applicable

7.3 eSign API: Response Data Format - eSign Service

7.3.1 eSignResponseXML structure

Below is the response format of eSign Service API. Note that, the API does not give any identity related data of the document signer.

```
<EsignResp status="" ts="" txn="" resCode="" errCode="" errMsg="">
      <UserX509Certificate>base64     value     of     eSign     user
      certificate(.cer)</UserX509Certificate>
      <Signatures>
            <DocSignature  id=""  sigHashAlgorithm="SHA256"  error="">
            Signature data in raw (PKCS#1) or PKCS7 (CMS) signature
            as requested
            </DocSignature>
      </Signatures>
      <Signature>Signature of ESP
      </Signature>
</EsignResp>
```

7.3.1.1 Element Details

Element Name: EsignResp

- Description: This element is the root element of the response and contains the meta values.
- Value: Sub-elements
- Attributes: Table below

S.No.	Attributes	Required?	Value
1.	status	Mandatory	In case of success, it will be “1” In case of failure, it will be “0”
2.	ts	Mandatory	Will contain the response timestamp in the format of “YYYY-MM-DDTHH:mm:ss.sss” (generated at C-DAC ESP).
3.	txn	Mandatory	The Transaction ID provided by ASP in the request.
4.	resCode	Mandatory	A unique response code provided by ESP. This is a unique id for the transaction provided by ESP. It shall make the transaction traceable, and ASP is expected to store this code in their audit log. This is an alpha-numeric string of maximum length 50. Only supported characters are A-Z, a-z, 0-9, period, comma, hyphen, backward & forward slash, left & right parenthesis, and colon.
5.	errCode	Optional	In case of failure, this will contain the failure error code.
6.	errMsg	Optional	In case of failure, this will contain a descriptive message against the error code.

Element Name: UserX509Certificate

- Description: This element will contain the Base 64 value of the Certificate. No private key information is shared. For manual verification, this value can be copied and saved as .cer file (With begin and end statements - PEM Format).
- Presence: Mandatory, if success.
- Value: Base 64 value of document signer certificate (public).
- Attributes: Not Applicable

Element Name: Signatures

- Description: This element contains the sub-elements of signatures corresponding to InputHash.
- Presence: Mandatory, if success.
- Value: Sub-elements.
- Attributes: Not Applicable

Element Name: DocSignature

- Description: This element will contain the signed value which will be verifiable against original document.
- Presence: Mandatory
- Value: Signed value in raw (PKCS#1) or PKCS7 (CMS) signature format as per the request XML.
- Attributes: Table Below

S.No.	Attributes	Required?	Value
1.	id	Mandatory	Contains the corresponding ID to the Input Hash received
2.	sigHashAlgorithm	Mandatory	Should be fixed to “SHA256”
3.	error	Optional	In case of failure, this will contain the corresponding error code

Element Name: Signature

- Description: This element will contain the signature of ESP, which can be used for verification by ASP and protect the response from any kind of tamper.
  - Value: Signed value of response XML, as per the W3C recommendation on XML Signature Syntax and Processing (Second Edition)
  - Refer http://www.w3.org/TR/xmldsig-core/ for more information
- Attributes: Not Applicable

7.4 String Format of Signatory Consent “sc”

The “sc” field in Esign request XML is used to indicate the document signer’s consent for inclusion of X.509 subject name fields from Aadhaare-KYC data. This enhanced format provides explicit consents for each field at higher granularity to be included in the X.509 certificate.

Based on the consent obtained for the individual components, the string is formed by separating the individual components using comma. An example of this format is "*cn:Y,x500UniqueIdentifier:N*" which refers to the document signer consent as "include commonName in the X.509 certificate and populate it using Aadhaare-KYC details".

A missing component in the list is treated as no consent for that attribute to be included in the X.509 certificate. In this regard, the following two examples are equivalent - "*cn:Y,x500UniqueIdentifier:N*" and "*cn:Y*".

The list of X.509 attributes for which the document signer consent can be explicitly provided is given in the following table. Each attribute consent will be either "Y" or "N". Missing attribute in the "sc" field is taken as no consent as described earlier.

Table 4. X.509 Attributes

Sl. No.	X509 Attribute (and OID)	Component name in sc	Rules to populate from e-KYC
1.	commonName (2.5.4.3)	cn	name in Poi from e-KYC is copied to cn in X.509
2.	uniqueIdentifier (2.5.4.45)	x500UniqueIdentifier	tkn in UidData is copied as x500UniqueIndentifier in X.509
3.	pseudonym (2.5.4.65)	pseudonym	code in AgentKycRes for e-KYC is copied as pseudonym in X.509
4.	localityName (2.5.4.7)	L	loc in Poa is copied as l in X.509
5.	stateOrProvinceName (2.5.4.8)	St	state in Poa is copied as st in X.509
6.	streetAddress (2.5.4.9)	street	(co, house, street, lm, loc, vtc, subdist, dist, state, pc, po) in Poa is copied as street in X.509
7.	postalAddress (2.5.4.16)	postalAddress	(co, house, street, lm, loc, vtc, subdist, dist, state, pc, po) in Poa is copied as postalAddressin X.509
8.	postalCode (2.5.4.17)	postalCode	pc in Poa is copied as postalCode in X.509

An example of "sc" string is following:

cn:Y,x500UniqueIdentifier:Y,pseudonym:Y,l:N,street:N,state:Y,postalAddress:Y,postalCode:Y

Correspondingly the DSC generated shall include *commonName, x500UniqueIndentifier, pseudonym, state, postalAddress, and postalCode* for the subject name populated appropriately from Aadhaare-KYC data.

Based on this enhanced format, “sc” as “Y” shall be treated equivalently as “*cn:Y,x500UniqueIdentifier:Y,pseudonym:Y,stateOrProvinceName:Y,postalCode:Y* .

Formation of streetAddress and postalAddress X.509 Attributes

The e-KYC data obtained from UIDAI has the following address related attributes –

- co (care of)
- house
- street
- lm (landmark)
- loc (location)
- po (post office)
- vtc (village/town/city)
- subdist (sub-district)
- dist (district)
- state
- pc (postal code)
- country

For X.509 attributes streetAddress and postalAddress, the above e-KYC data is concatenated using comma (‘,’) as the separator between the attributes. The order of concatenation is

```
co house street lm locpovtcsubdistdist state pc country
```

The po attribute if non-empty will be prefixed by a string “post office”. The comma separator will not be used between state and pc. In case any of the attribute is not present in e-KYC data, it is not included for concatenation.

For example, given the following as the response of e-KYC

```
<Poa co="S/O C.S. Karvade" lm="near rajkamal public school"
loc="102/AN -shakuntalanagarnayapurakolar road" vtc="BHOPAL"
dist="Bhopal" state="Madhya Pradesh" pc="462042" po="Kolar Road"
country=”IN”/>
```

The street address will look like this.

```
streetAddress = "S/O C.S. Karvade, near rajkamal public
school, 102/AN -shakuntalanagarnayapurakolar road, Kolar Road
post office, BHOPAL, Bhopal, Madhya Pradesh 462042 IN"
```

The postal address will look like this.

```
postalAddress = "S/O C.S. Karvade, near rajkamal public
school, 102/AN -shakuntalanagarnayapurakolar road, Kolar Road
post office, BHOPAL, Bhopal, Madhya Pradesh 462042 IN"
```

7.5 UsageScenario

The eSign service API can be used in as follows.

ASP initiates eSign request and ESP authenticates document signer for e-KYC before eSign.e-Hastakshar facilitates authentication of document signer by calling authentication URL of C-DAC ESP. The e-KYC response shall be received by e-Hastaksharand it shall performeSign on the eSign request received from ASP. Flow of eSign process using this option is shown in Figure 8.

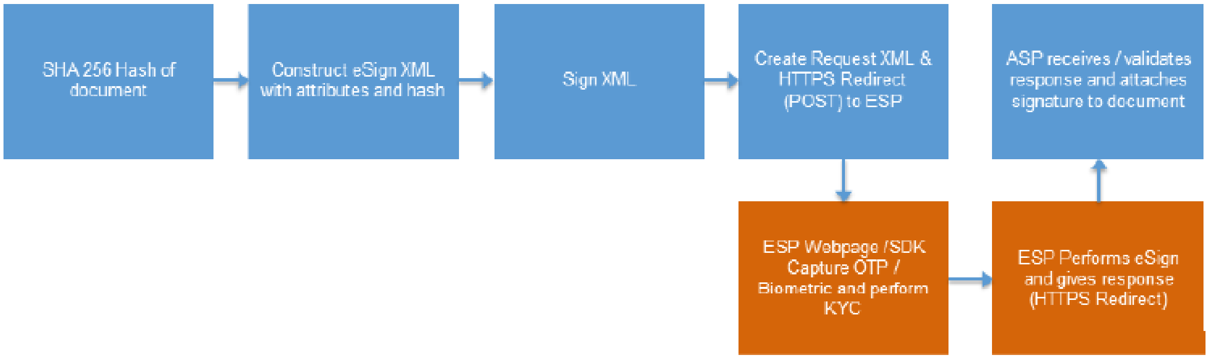

SHA 256 Hash of document
Construct eSign XML with attributes and hash
Sign XML
Create Request XML & HTTPS Redirect (POST) to ESP
ASP receives / validates response and attaches signature to document
ESP Webpage /SDK Capture OTP / Biometric and perform KYC
ESP Performs eSign and gives response (HTTPS Redirect)

Figure 8. eSign using e-KYC made by e-Hastakshar

Using web browser / APK based, the re-direction to ESP authentication page from ASP end can be achieved in one of the following 2 ways

1) Re-direction to ESP Authentication Page using HTML FORM data from signer's browser
2) On Android based application, the ASP APK can re-direct to ESP authentication page using eSign APK

7.5.1 Details of Re-Direction using Form Based Data

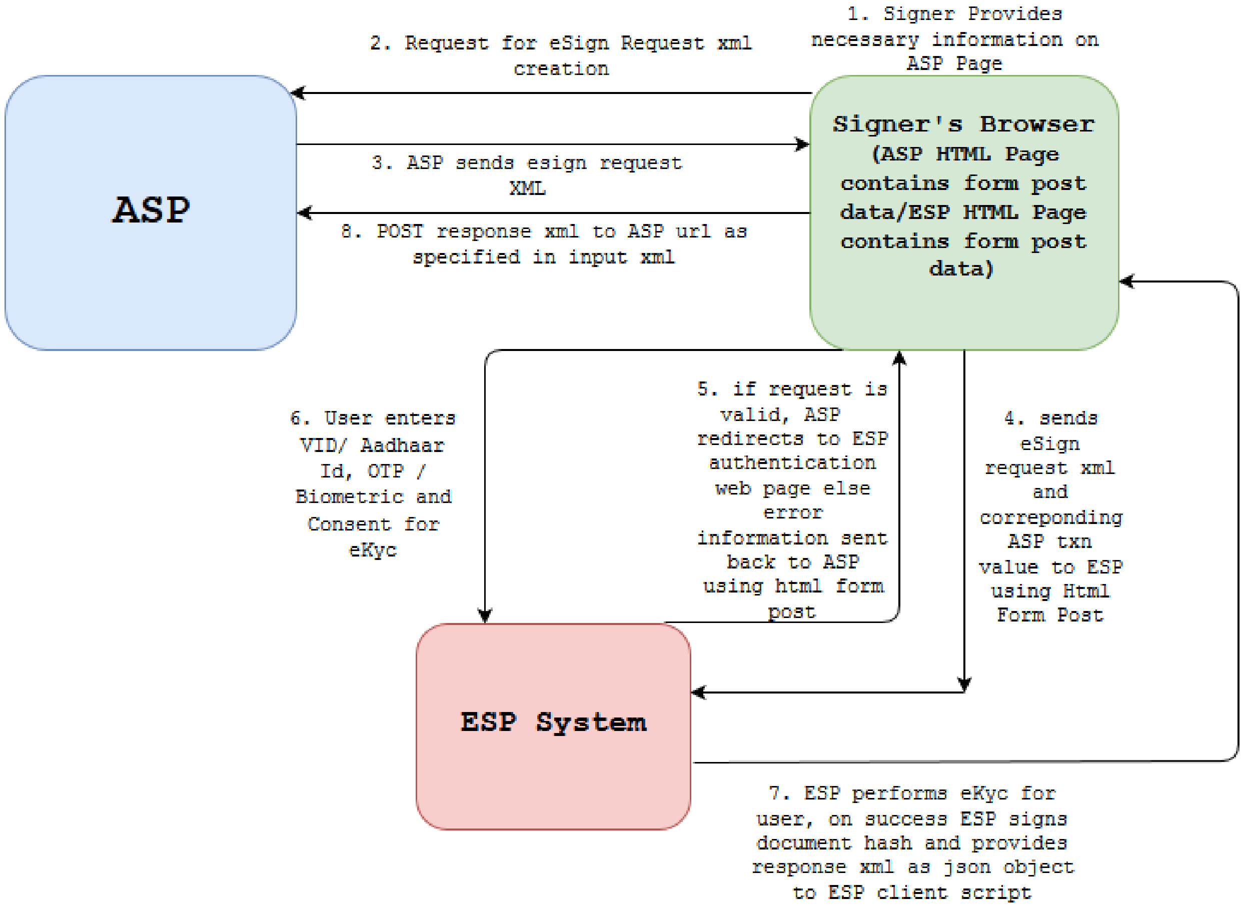

1. Signer Provides necessary information on ASP Page
2. Request for eSign Request xml creation
ASP
Signer's Browser (ASP HTML Page contains form post data/ESP HTML Page contains form post data)
3. ASP sends esign request XML
8. POST response xml to ASP url as specified in input xml
6. User enters VID/ Aadhaar Id, OTP / Biometric and Consent for eKyc
5. if request is valid, ASP redirects to ESP authentication web page else error information sent back to ASP using html form post
4. sends eSign request xml and correpending ASP txn value to ESP using Html Form Post
ESP System
7. ESP performs eKyc for user, on success ESP signs document hash and provides response xml as json object to ESP client script

Figure 9. Detailed Process Flow of HTML Form Data Based Redirection

The detailed process flow for eSign, using Re-direction using Form data, is shown in Figure 9.

Following is the sequential execution of the process:-

1. ASP captures document hash, Authentication Mode and obtains document signer consent for key-pair generation/computation of digital signature using the hashes provides/creation of Digital Signature Certificate
2. Based on the information received, ASP creates the signed eSign request XMLas per eSign API specification version 2.1.
3. The ASP application populates HTML Form with following Read Only Hidden input fields and Form "action" attribute should be set to "ESP redirection URL"

Input field ID	Input field type	Description
eSignRequest	Text Area	This will contain a valid signed eSign request XML
aspTxnID	Text Area	This should contain ASP transaction ID as in eSign request XML

Content-Type	Text Area	This attribute shall be set as `application/xml`

4. Upon receiving form data, ESP shall extract eSign request XML from “eSignRequest” input field, transaction ID from “aspTxnID” input field and content-type from “Content-Type” input field.
5. ESP shall validate the eSign request XML, match transaction ID obtained from “aspTxnID” input field, and upon successful validation, signer shall be redirected to ESP authentication page.
6. Signer shall provide his/her Aadhaar number/Virtual ID/UID token, authentication data (OTP or Biometric), consent on ESP authentication page and submit the request for eSigning.
7. Based on the information provided by the signer,
    a. C-DAC ESP system prepares e-KYC request XML for the signer.
    b. On successful response of e-KYC data, C-DAC ESP system performs signing on the document hash and generates DSC for the signer.
    c. C-DAC ESP system prepares response XML for the ASP containing PKCS7 packet (In case of any error, response XML shall contain appropriate error code and/or error message).
8. C-DAC ESP system populates HTML Form with following Read Only Hidden input fields and Form “action” attribute shall be set to “aspResponseURL”asspecified in eSign request XML

Input field ID	Input field type	Description
eSignResponse	Text area	This will contain a valid signed eSign response XML with PKCS#7 signature
espTxnID	Text area	This will contain ASP transaction ID as received “aspTxnID” input field

9. Signer browser shall POST HTML form to “aspResponseURL”
10. Upon receiving form data, ASP shall extract eSign response XML from “eSignResponse” input filed and transaction ID from “espTxnID” input field
11. ASP shall verify eSign response XML using ESP public certificate.

7.5.2 Details of Re-Direction using Android APK

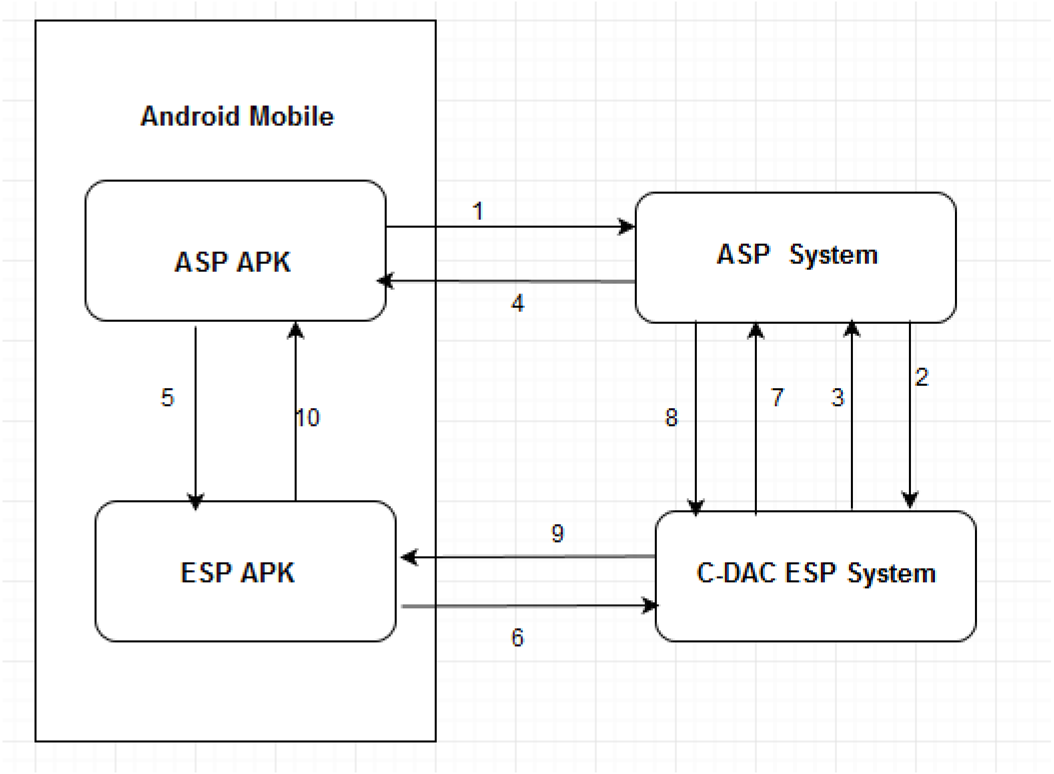


Figure 10. Detailed Process Flow of Android APK Based Redirection

1. ASP APK may provision uploadof document to be signed, authentication mode to be set and obtainsdocument signerconsent for key-pair generation/computation of digital signature using the hash provided/creation of Digital Signature Certificate
2. ASP ASK interacts with ASP application with the necessary information and ASP applicationgenerates eSign Request XML as per eSign API specification v2.1 and forwards the eSign Request XML to ESP System
3. ESP System validates the request XML and on Successful validation, generates a token which is unique identifier for the individual transaction and sends back to ASP System eSignResponse Info xml.

```
<EsignInfoResp status="1" ver="1.0" txn="" rescode=""
espToken=""><eSignResponse></eSignResponse></EsignInfoResp>
```

S. No.	Attribute	Mandatory/Optional	Allowed Values
1	status	Mandatory	0 or 1
2	ver	Mandatory	1.0

3	txn	Mandatory	same as in request XML
4	rescode	Mandatory	UUID generated at ESP
5	espToken	Mandatory	Unique id to maintain user identification
6	eSignResponse	Optional	Base64 encoded esign Response xml if there is any error otherwise the value will be null

4. On receipt of token, ASP system creates the eSign process info xml comprises the EPS token, ASP Transaction ID, bio environment (pp for preproduction/P for production)and forward as a response to ASP APK.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><EsignProcessInfo
bioMode="" espToken= "”
aspToken="NA" aspIdentifier="NA"
aspTxnId=""/>
```

S.No.	Attributes	Required?	Value
1.	bioMode	Optional	Mandatory in the case of Biometric based Authentication In case of Preproduction environment, value should be “PP” In case of Production environment, value should be “P”
3.	espToken	Mandatory	ESP Unique Identifier for ASP transaction.It will same as esptoken attribute in the EsignInfoResp xml
4.	aspToken	Optional	ASP Unique Token for ESP transaction. Currently the value should be “NA”
5.	aspIdentifier	Optional	ASP Unique Token for session management during the ESP transaction. Currently the value should be “NA”
6.	aspTxnId	Mandatory	The Transaction ID provided by ASP in the request.

5. The ASP APK invokes the ESP APK and sends the eSign process info xml as aninput to ESP APK.

```
Intent intentInfo = new
Intent("esign.cdac.in.ehashtakshar.SIGN_ACTIVITY");

intentInfo.putExtra("aspProcessInfo", eSignTxn);
startActivityForResult(intentInfo, 2);
```

6. ESP APK calls the Bio Device SDK/Activity (provided by Vendor) to capture and obtain the Authentication Data and sends the ASP transaction id, Authentication Data and ESP token using the rest client web service to ESP System (web service).
7. ESP System will initiate authentication of document signer using captured Biometric Data with UIDAI and upon success shall carry out generation of DSC and PKCS#7 signature.On

successful transaction, the ESP System shalluse Rest Client web service to send the eSign Response to ASP System.

8. On receipt of eSign response, the ASP System sends back the acknowledgementxml to ESP System.

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?><EsignAckResp
status="1"
ts="2018-08-27T18:30:05.059" txn="0185a675-611d-4d17-910c-cd53c9bd4fe5"
errCode="NA" errMsg="NA"/>
```

S. No.	Attribute	Mandatory/Optional	Allowed Values
1	status	Mandatory	0 or 1
2	ver	Mandatory	1.0
3	txn	Mandatory	same as in request XML
4	ts	Mandatory	Response received time stamp at the ASP Server
5	errCode	Mandatory	NA (receiving the response successfully) or Error code occurred during receiving the response at the ASP Server
6	errMsg	Mandatory	NA (receiving the response successfully) or Error Message occurred during receiving the response ASP Server

9. The ESP System receives the acknowledgementxml and sends back the response acknowledgement to ESP APK. Based on the response status ESP APK displays the corresponding message (“eSign Transaction is completed successfully”/“Invalid eSign Transaction. Please try Again!”)
10. ESP APK uses the call back to acknowledge the ASP APK with the corresponding status, error Code and Message.

```
protected void onActivityResult(intrequestCode, intresultCode, Intent
data)
{
super.onActivityResult(requestCode, resultCode, data);
// check if the request code is same as what is passed  here it is 2
if (resultCode == Activity.RESULT_OK) {
if(requestCode==2)
{
String code =data.getStringExtra("errorCode");
String msg = data.getStringExtra("info");
String status = data.getStringExtra("status");
String aspTxnId = data.getStringExtra("aspTxnId");

AlertDialog.BuilderconsentMsg = new
AlertDialog.Builder(MainActivity.this);
consentMsg.setMessage(code+status+aspTxnId+msg)
.setPositiveButton("CLOSE", new DialogInterface.OnClickListener() {
@Override
public void onClick(DialogInterface dialog, int which) {
dialog.dismiss();
}
}).setTitle("Device Status").create();
consentMsg.show();
}
}
}
```

8 Business Continuityfor C-DAC eSign Service

C-DAC shall manage and operate the ESP and CA services as given in the Certification Practice Statement (CPS), Version 1.0, June 2015 published by C-DAC based on the guidelines provided by CCA. The details of the same can be found at the following URL.

http://www.cca.gov.in/cca/sites/default/files/files/CADC-CA-CPSv10.pdf

Disaster Recovery site for C-DAC CA is set up for providing high availability and aligned for the business continuity process.

9 Procuring Digital Certificates

As per the e-Authentication guidelines by CCA, the XML from ASP to ESP should be digitally signed. For this, ASP needs to procure a Digital Signature Certificate. More information for procuring a digital certificate can be found on the website at http://www.cca.gov.in/cca/?q=faq-page#n39.

10 Frequently Asked Questions (FAQ)

1. **What are the main features of v2.1 eSign specifications?**

   eSign 2.1 facilitates capturing of Authentication ID and authentication data of the individual to be carried out by ESP. eHastakshar uses the service of UIDAI for authenticating the document signer through its e-KYC mechanism.

2. **Is it required for me to carry out testing at all the levels of integration to migrate to v2.1 of eSign specifications?**

   Yes

3. **Is bulk signing supported? If so details.**

   No

4. **What are the modes on which OTP shall be received by Aadhaar holder for authentication purpose?**

   e-Hastakshar enables Document signer to receive the OTP on registered Mobile number and email ID. In case both are not registered with Aadhaar, an error code of 112 will be returned.

5. **What are the technical challenges in implementation of eSign v2.1 APIs?**

- *e-Hastakshar supports redirection form based eSign 2.1 architecture.*
- *e-Hastakshar services are accessible over HTTPS. Therefore, SSL configuration needs to be incorporated.*
- *eSign 2.1 supports OTP/ Biometric based authentication using Virtual ID/ Aadhaar ID/UID Token and Biometric based authentication using Aadhaar ID/Virtual ID/UID Token. An Aadhaar holder needs to access UIDAI website for generation of Virtual ID.*

6. **What is licensing model of APIs?**

   Not Applicable

7. **What is eSign API license key?**

   It is the ASP-ID given by ESPs after sharing required details with ESPs. Refer http://www.cca.gov.in/cca/?q=eSign.html.

8. **How to ensure that the ASP-ID will remain unique?**

   C-DAC will allocate and will ensure the uniqueness.

9. **In the input data format for the eSign services the "sc" attribute is mandatory. But how does it represent the signatory's explicit consent?**

   This attribute ensures that document signer is providing the signer consent. This must be filled only after taking inputs from the document signer to that extent in the ASP application.

10. **ASP should make sure that the affixing of digital signature to document or storage of digital signature only after the signatory's approval of contents of certificate and signature.**

ESP will return the signed hash of the document along with the document signer's public certificate. ASP has to affix/store the digital signature after presenting the details to the signer and taking their explicit consent for the same.

11. For the routing of requests to each API is the gateway essential or the functionality can be built without the gateway? If it is so then what is the need of services of the gateway service provider. More over the additional validation process may increase the turnaround time.

ASP has a choice of routing the request via Gateway or directly to ESP. Gateway may provide pin management system which is an additional security system that ASP can avail.

ASP may also link with ESP directly for eSign service as per the specifications.

Presently, C-DAC ESP services can be accessed directly without gateway.

12. What are the different security and audit requirement to be carried out for the ASP application?

There are two aspects of security and audit assessment to be carried out:

a) Security assessment of the application by ICERTempanelled agency where the security threats, vulnerabilities etc. are carried out for the ASP application and its environment (OS, web server etc.)

b) Application audit to be carried by IS certified auditor to ensure the application data, logs etc. are maintained as per Annexure-11.

10. Whether eSign online Electronic Signature Service is a replacement for the existing Digital Signature?

No. The existing method of obtaining Digital Signature Certificate by submission of a paper application form to a Certifying Authority, key pair generation by applicant Certification of public key of applicant by a Certifying Authority, signature generation as and when required using signature generation tools/utilities , safe custody of key pairs on Crypto tokens by DSC holder till the expiry of Digital Signature Certificate, etc. will continue to exist along with eSign Online Electronic Signature Service .

The Application Service Provider determines the suitability of eSign Online Signature service in their application.

11. Is my privacy protected?

Yes. Document content that is being signed is not sent in the clear to eSign service provider. The privacy of signer's information is protected by sending only the one-way hash of the document to eSign online Electronic Signature Service provider. Each signature requires a new key-pair and certification of the new Public Key by a Certifying Authority. This back-end process is completely transparent to the signer. In addition, Aadhaare-KYC data is not sent back to the Application Service Provider and is retained only within the eSign provider as the e-KYC audit record.

12. How much doeles it cost to use eSign?

The payment model can be mailed to you upon request.

13. Can we control the e-signature appearance? Is that configurable? Can we use our own logo/font? Can we control the size and placement of the signature box on the document?

Yes, it is customizable.

14. Can the same document be signed by multiple people?

Yes, it can be signed by multiple people. It will involve multiple transactions, involving the same document.

15. What all different formats of documents are supported by C-DAC eSign services?

It is possible to digitally sign other formats, too. You may convert the file format to ASN.1 container file format and then attach the signature on the same. The extension of this format is custom-defined. You can define any extension you want. You will also have to create a reader to read that file just like Adobe Reader for pdf. C-DAC has already created a custom defined ASN.1 container format with the extension '.sig'.

16. Does C-DAC assist ASP application development?

The development of the ASP Application is beyond the scope of ASP - ESP Integration and related to ASP development. If required, C-DAC can do it based on the availability of developers at additional costs.

17. If the internet connection is lost during an eSign request process – Is the entire process re-initiated or does it resume from the point when the internet connection was lost, once the internet connection is available?

The transaction will have to be re-initiated.

11 Graphical User Interface Checklist for ASP

Sr. No.	Component Type	Label Name	Default value	Validation condition	Mandatory (Y/N)
1.	TextBox	UID Token	NA	Should accept UID Token value as received from UIDAI in previously done eKYC transaction with same AUA	N
2.	Input to be signed selection	Selection of the input which needs to be signed. It may be a file (selected by document signer or selected from workflow), text etc. based on application requirement.	NA	Input to be signed is being appropriately selected	Y
3.	CheckBox	Populate Common Name field in DSC from e-KYC data	Checked	Document signer should compulsory select the checkbox.	Required if explicit consent of document signer is to be taken for inclusion of subject name in the DSC from Aadhaar e-KYC data
4.	CheckBox	Populate Unique Identifier field in DSC from e-KYC data	Checked	Document signer should compulsory select the checkbox.	Required if explicit consent of document signer is to be taken for inclusion of subject name in the DSC from Aadhaar e-KYC data
5.	CheckBox	Populate Pseudonym field in DSC from e-KYC data	Checked	Document signer should compulsory select the checkbox.	Required if explicit consent of document signer is to be taken for inclusion of subject name in

					the DSC from Aadhaar e-KYC data
6.	CheckBox	Populate Locality Name field in DSC from e-KYC data	Unchecked	Optional for Document signer	Required if explicit consent of document signer is to be taken for inclusion of subject name in the DSC from Aadhaar e-KYC data
7.	CheckBox	Populate State or Province Name field in DSC from e-KYC data	Checked	Document signer should compulsory select the checkbox	Required if explicit consent of document signer is to be taken for inclusion of subject name in the DSC from Aadhaar e-KYC data
8.	CheckBox	Populate Street Address field in DSC from e-KYC data	Unchecked	Optional for Document signer	Required if explicit consent of document signer is to be taken for inclusion of subject name in the DSC from Aadhaar e-KYC data
9.	CheckBox	Populate Postal Address field in DSC from e-KYC data	Unchecked	Optional for Document signer	Required if explicit consent of document signer is to be taken for inclusion of subject name in the DSC from Aadhaar e-KYC data
10.	CheckBox	Populate PostalCodefield in DSC from e-KYC data	Checked	Document signer should compulsory select the checkbox	Required if explicit consent of document signer is to be taken for inclusion of subject name in

					the DSC from Aadhaar e-KYC data
11.	CheckBox	By pressing eSign button, I hereby give my consent for using e-KYC data from Aadhaar for the purpose of signing selected data and using e-KYC data for generating Digital Signature Certificate (DSC) as above	unchecked	Document signer should compulsorily select the checkbox	Y
12.	CheckBox	Authentication Mode	Unchecked	Should allow signer to select Authentication mode. Currently, C-DAC ESP supports OTP and Biometric (Fingerprint) based authentication.	Y
13.	Button	eSign	NA	Click event of this button invokes eSign Service of ESP.	Y

12 Integrating eSign Service of C-DAC ESP

Step 1-Invoke eSign Service API using Form Based Redirection

ASP sends the request xml for electronic signature with the inputs Authentication parameter (OTP/Biometric), Document Hash and signatory consentand obtains the response xml from C-DAC eSign Service which has PKCS7Response.eHastakshar services are accessible over HTTPS. Therefore, SSL configuration needs to be incorporated.

Sending Request XML to ESP System

Request XML is sent to ESP system using POST method by the ASP web pageusing HTML form post.

```
<form action="esp Request Url" method="post" id="formid">

<input type="hidden" id="eSignRequest" name="eSignRequest" value="">

<input type="hidden" id="aspTxnID" name="aspTxnID" value="">

<input type="hidden" id="Content-Type" name="Content-Type" value="">

</form>
```

ASP System Receive eSign Response

Response XML is sent to ESP system using POST method by the ESP System using the HTML form post.

The ESP form post attributes are eSignResponse and espTxnID. eSignResponse attribute contains the eSign Response xml and espTxnID will be the aspTxnID same as esign request xml txn.

Step 2–Usage of PKCS7 Response as per application requirement

ASP can use PKCS7 Response based on its requirement. Here two scenarios of usage are being described -

1. **Embed PKCS7 Response into PDF**

For the details regarding the embedding of the digital signatures in a PDF document the following link can be referred: https://www.adobe.com/devnet-docs/acrobatetk/tools/DigSig/Acrobat_DigitalSignatures_in_PDF.pdf

One can use available libraries like ApachePdfBox, iText or Bouncy Castle Library in Java and .NET for attaching Pkcs7Response in PDF, after taking care of necessary licensing conditions.

2. **Signed document using PKCS7 Response for any format of file**

In case of digitally signing a file containing data with any arbitrary format of file, the signed document is defined as a container format, .SIG, based on ASN.1 specifications using the PKCS7 response obtained. The signed document encapsulates document content, signature, certificates and optional additional information regarding the document like document name etc.

Abstract syntax notation for SIG file is as follows -

```
SignedDocument DEFINITIONS AUTOMATIC TAGS::= BEGIN

sigFile::= SEQUENCE {

        documentName                [0] DocumentName OPTIONAL,

        documentType        [1] DocumentType OPTIONAL,

        documentContent             DocumentContent,

signatures               SET OF Signature

}

DocumentName::= UTF8STRING

DocumentType ::= UTF8STRING

DocumentContent ::= OCTET STRING

Signature ::= ContentInfo – as defined in RFC 2315
```

For creating SIGfile,thefour fields required in the sequence are described below:

Field Name	Description	Data Type	Default Value	Mandatory (Y/N)
DocumentName	Name of the document for which the .SIG file is to be generated	UTF8String	Name of the file to be signed	N
DocumentType	MIME-type of the such as text/plain ,text/html	UTF8String	application/octet-stream	N
DocumentContent	Content of the file to be signed	OCTECT STRING		Y
Signature	Value from **Pkcs7Response** - output from eSign Service	ASN1Encodable		Y

Table 5 : SIG File Fields

For creating SIG file, Bouncy Castle Library in Java and .NET can be used by using classes like ASN1Sequence, ASN1InputStream, DERTaggedObject, DEROctetString, DERSequence and DERUTF8String present in the respective jar and dlls.

13 References

[1] eSign API and other details by CCA - http://www.cca.gov.in/cca/?q=eSign.html

[2] CCA's Draft ASP On-boarding guidebook –Version 1.2, April 2017 http://www.cca.gov.in/cca/sites/default/files/files/ESIGN/CCA-ASP.pdf

[3] C-DAC Certification Practice Statement -https://esign.cdac.in/ca/CPS/CPS.pdf

[4] Aadhaar Authentication API Specification - Version 2.5, March 2018,https://uidai.gov.in/images/resource/aadhaar_authentication_api_2_5.pdf

[5] Aadhaare-KYC 2.5 Specification – Version 2.5, March 2018, https://uidai.gov.in/images/resource/aadhaar_ekyc_api_2_5.pdf

[6] Aadhaar OTP 2.5 Specification – Version 2.5, March 2018, https://uidai.gov.in/images/resource/aadhaar_otp_request_api_2_5.pdf

[7] e-authentication guidelines for eSign- Online Electronic Signature Service - Version 1.3, April 2017, http://www.cca.gov.in/cca/sites/default/files/files/ESIGN/CCA-EAUTH.pdf

14 Annexure-1: ASP Request Form

Organization Name ________________________________

Category of Organization(Tick the most appropriate one)

⌗ Central Government

⌗ State Government

⌗ Academia

⌗ R&D Organization

⌗ Company

⌗ NGO / Charitable Institution

⌗ Others (Specify) __________________________

Substantially Funded by

⌗ Government

⌗ Private

Address ________________________________

____

____

____

The Project/Product details where e-Sign service shall be used and how it shall be beneficial to the organization.

____

____

____

____

____

____

____

Total expected daily signatures __________________________

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)

Signature: ____________

Name: ____________

Designation: ____________

Organization: ____________

Date: ____________

To be filled by C-DAC

Test ASP-ID: ____________

ASP-ID: ____________

Processed by: ____________

Signature: ____________

Name: ____________

Designation: ____________

Date: ____________

15 Annexure-2: List of Supporting Documents to be Submitted by ASP along with ASP Request Form

Organization Type	Supporting Documents required along with the Application
A Central/ State Government Ministry / Department or an undertaking owned and managed by Central / State Government	• ASP Request Form 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	• ASP Request Form 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	• ASP Request Form 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	• ASP Request Form 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
Any other Organization	• ASP Request Form signed by Authorized signatory • Letter of authority, authorizing the signatory to sign documents on behalf of the organization • Document proof of incorporation of the organization

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.

16 Annexure-3: Contract and Agreement

Agreement between C-DAC e-Sign Service Provider (ESP)

and

Application Service Provider (ASP)

AGREEMENT

BETWEEN

CENTRE FOR DEVELOPMENT OF ADVANCE COMPUTING (ESP)

AND

Application Service Provider (ASP)

This Agreement is made and executed on _______ day of _____________, 21_ _ at ______, by and

BETWEEN

Centre for Development of Advanced Computing, a Scientific Society of the Ministry of Electronics and Information Technology, Government of India; registered under the Societies Registration Act, 1860 and Bombay Public Trusts Act, 1950 and having its registered office at Savitribai Phule Pune University Campus, Ganeshkhind, Pune – 411007, India (hereinafter referred to as 'e-signature Service Provider' or 'ESP') which expression shall mean and includes its successors, permitted assigns **PARTY OF THE FIRST PART**

AND

____________________, department of ----- of Govt. of ------/established under -----Act----/an autonomous organization under ------and registered under the Societies Registration Act 1860/Bombay Public Trust Act 1950/Companies Act, 1956,/Companies Act 2013/Indian Partnership Act/Limited Liability Partnership Act having its registered office at _______________________________ (hereinafter referred to as 'Application Service Provider' or 'ASP' which expression shall unless repugnant to the context or meaning thereof mean and be deemed to include its authorized representatives, agents and permitted assigns) **PARTY OF THE SECOND PART**

Whereas C-DAC is set up to emerge as the premier R&D institution for the design, development and deployment of electronic and IT solutions for economic and human advancement, with the mission to expand the frontiers of electronics and IT, evolve technology solutions, architectures, systems and standards for nationally important problems, achieve rapid and effective spread of knowledge by overcoming language barriers through application of technologies, share experience and know-how to help build advanced competence in the areas of electronics and IT, bring benefits of electronics and IT to society, and utilize the Intellectual Property generated by converting it to business opportunities.

A. ASP wishes to obtain certain services as more specifically defined in this Agreement from ESP;

B. ESP is willing to provide such services in accordance with the terms and conditions of this Agreement;

Now therefore, inconsideration of the foregoing and mutual covenants and promises contained herein and other good and valuable Considerations, the receipt and adequacy of which is hereby acknowledged, the parties hereby covenant and agree and this agreement witness as follows:

1. Definitions and Interpretations

a. '**Aadhaar Authentication Services**' shall mean the authentication services provided by

i. UIDAI and used by ASP where the personal identity information of/data of an Aadhaar-holder (who is a beneficiary, customer, employee or associate of the ASP) is matched with their personal identity information/data that is stored in the UIDAI's Central Identity Data. Repository in order to provide Aadhaar enabled services to such Aadhaar holder.

ii. The ASP shall avail Aadhaar authentication service by establishing a connection with UIDAI's Central Identity Data Repository, through the ESP.

b. "**Aadhaar Enabled Services**" shall mean services provided by the ASP to Aadhaar Holder who is having a valid and registered mobile number with Aadhar (UIDAI), using the Aadhaar Authentication Services of UIDAI.

c. '**Aadhaar Holder**' shall mean an individual who holds an Aadhaar Number;

d. '**Aadhaar Number**' shall mean the unique identification number issued to a resident byUIDAI;

e. 'Contract/**Agreement**' shall mean this Contract/agreement executed between the Parties, along with its schedules, annexures and exhibits, if any, and all instruments supplemental to or amending, modifying or confirming this agreement in accordance with the provisions of this agreement, if any, in each case as they may be supplemented or amended from time to time;

f. '**Authentication Data Packet**' shall mean a data packet which has been created based on pre-defined protocol (data elements, order of data elements, etc.), prescribed by UIDAI from time to time and which contains Personal Identity Data (PID) collected from Aadhaar Holders for the purpose of Aadhaar Authentication;

g. '**Authentication Device**' shall mean a terminal or device from where the ASP carries out its service/business functions and interacts with Aadhaar Holders, by seeking authentication of Aadhaar Holders identity to enable the ASP's business function;

h. '**Authentication Service Agency (ASA)**' shall mean an entity providing compliant secured network connectivity to the UIDAI and the Authentication User Agency for enabling Aadhaar Authentication Services as separate agreements entered into between the entity and UIDAI and Authentication User Agency respectively;

i. '**Authentication User Agency**' shall mean an entity engaged in providing Aadhaar Enabled Services to Aadhaar Holder, using the Aadhaar Authentication Services of UIDAI, as facilitated by the Authentication Service Agency, in accordance with the terms and conditions of the relevant agreements that may be entered into between the Authentication Service Agency and an Authentication User Agency and between UIDAI and the Authentication User Agency, from time to time;

j. '**Biometric Information**' shall mean ten finger prints and iris image of a resident, captured by UIDAI, as a part of the enrolment process for issuance of Aadhaar Number;

k. '**Business Day**' shall mean any day other than a Saturday, Sunday or official public holiday in India;

l. '**Controller of Certifying Authorities (CCA)**' shall have the same meaning as such term is defined in Information Technology Act, 2000 and rules and regulations made thereunder as amended from time to time.

m. '**Central Identity Data Repository (CIDR)**' means a centralized database in one or more locations containing all Aadhaar numbers issued to Aadhaar number holders along with the corresponding demographic information and biometric information of such individuals and other information related thereto;

n. '**Confidential Information**' shall mean any information which is considered confidential in terms of Clause 13 of this Agreement and shall include, but not limited to, information such as Aadhaar

Number, name, address, age, date of birth, relationships and other demographic information, as also, biometric information such as finger print and iris scan of a resident;

o. '**Digital Signature Certificate (DSC)**' shall have the same meaning as defined under the Information Technology Act, 2000 and rules and regulations made thereunder as amended from time to time;

p. '**e-KYC**' shall mean the transfer of demographic data (such as Name, Address, Date of Birth,

Gender, Mobile number, Email address, etc.) and photograph collected by UIDAI in the form of a digitally signed XML document to an Authentication User Agency, through an Authentication Service Agency, based on resident authorization received by UIDAI in the form of successful biometric or OTP-based Aadhaar authentication;

q. '**e-signature**' shall mean an online electronic signature service which can be integrated with service delivery applications via an open API to facilitate an Aadhaar holder to digitally sign a document;

r. '**False Accept**' shall be referred to a accept transaction where a system identifies a biometric as genuine (while, in reality it belongs to some other individual) or will fail to reject an impostor biometric. Imposter can be defined as someone who intentionally or unintentionally is presenting his/her biometric against someone else's Aadhaar number;

s. '**KYC Service Agency (KSA)**' shall mean Authentication Service Agency that is eligible to provide access to the e-KYC service through their network;

t. '**KYC User Agency (KUA)**' shall mean Authentication User Agency that is eligible for the e-KYC service;

u. '**Laws**' shall mean all applicable laws, by-laws, rules, regulations, orders, ordinances, protocols, codes, guidelines, policies, notices, directions, judgments, decrees or other requirements or official directive of any governmental authority or person acting under the authority of any governmental authority, whether in effect or which may come into effect in the future;

v. '**OTP**' shall mean one time password sent to the Aadhaar holder's cell phone for the purpose of authentication;

w. '**Party**' refers to individually to ASP and the ESP;

x. '**Parties**' refer collectively to ASP and ESP;

y. '**Personal Identity Data (PID)**' refers to Aadhaar-based Personal Identity Data/ Information including biometric and demographic information as well as the OTP used for Authentication;

z. '**Services**' shall mean the services to be provided by ESP to ASP as agreed in this Agreement;

aa. '**Standards**' shall mean the standards issued by UIDAI with regard to Services covered by this Agreement and the standards issued by ASP from time to time for performance of Services;

bb. '**Successful Transaction**' means the event of receipt of a DSC by ASP from ESP for a particular Document in the case of ASP and the event of dispatch of a DSC to ASP by ESP for a particular Document ;

cc. '**Third Party**' shall mean any party who is not a Party to this Agreement;

dd. '**UIDAI**' shall mean Unique Identification Authority of India or any of its successors in office.

2. Interpretations

a. In this Agreement, unless the context requires otherwise:

   i. reference to singular includes a reference to the plural and vice versa;

   ii. reference to any gender includes a reference to all other genders;

   iii. reference to an individual shall include his legal representative, successor, legal heir, executor and administrator;

iv. reference to statutory provisions shall be construed as meaning and including references also to any amendment or re-enactment (whether before or after the date of this Agreement) for the time being in force and to all statutory instruments or orders made pursuant to statutory provisions;

v. references to any statute or regulation made using a commonly used abbreviation, shall be construed as a reference to the title of the statute or regulation;

vi. references to any Article, Clause, Section, Schedule or Annexure, if any, shall be deemed to be a reference to an Article, Clause, Section, Schedule or Annexure of or to this Agreement.

b. Clause headings in this Agreement are inserted for convenience only and shall not be used in its interpretation.

c. When any number of days is prescribed in this Agreement, the same shall be reckoned exclusively of the first and inclusively of the last day unless the last day does not fall on a Business Day, in which case the last day shall be the next succeeding day which is a Business Day.

d. If any provision in this Agreement is a substantive provision conferring rights or imposing obligations on anyone, effect shall be given to it as if it were a substantive provision in the body of this Agreement.

e. Any word or phrase defined in the body of this Agreement shall have the meaning assigned to it in such definition throughout this Agreement unless the contrary is expressly stated or the contrary clearly appears from the context.

f. The rule of construction, if any, that a contract shall be interpreted against the party responsible for the drafting and preparation thereof shall not apply.

g. Reference to days, months or years in this Agreement shall be a reference to calendar days, months or years, as the case may be, unless the contrary is expressly stated or clearly appears from the context.

h. Reference to any agreement, deed, document, instrument, rule, regulation, notification, statute or the like shall mean a reference to the same, as may have been duly amended, modified or replaced. For the avoidance of doubt, a document shall be construed as amended, modified or replaced only if such amendment, modification or replacement is executed in compliance with the provisions of such document(s).

3. Agreement

ASP agrees to avail Services from ESP and ESP agrees to provide Services to ASP, on nonexclusive, revocable and limited basis in accordance with the terms and conditions of this Agreement.

4. Scope of Services

C-DAC shall offer e-Sign service using which any valid Aadhaar holder with registered mobile numbers using Aadhaar OTP (One Time Password) or Biometric (Finger Minutiae) based e-KYC services, shall be able to get his document digitally signed. C-DAC has become a CA under the Controller of Certifying Authorities and has been empanelled as ESP to offer the eSign services.

eSign service can be integrated within various service delivery applications to facilitate digitally signing a document by an Aadhaar holder. It is designed for applying Digital Signature using authentication of the subscriber through Aadhaar authentication and e-KYC service. ESP shall enable ASP application to leverage the eSign service.

C-DAC ESP shall offer the following services

- Shall offer e-Sign service through ASP using which any valid Aadhaar holder with a registered mobile number, shall be able to get his document digitally signed

- Shall offer Aadhaar-eKYC – OTP/BIO type class of certificates
- Shall manage and operate the ESP and CA services as given in the CPS and as per the guidelines of CCA
- Shall during the term of this agreement, maintain its empanelment / agreement with UIDAI

5. Obligations of ESP

5.1 The ESP shall, during the Term of this Agreement, maintain necessary licenses with CCA or Certifying Authority (as the case may be) as required for issuance of DSC.

5.2 The ESP shall, during the Term of this Agreement, maintain its empanelment / agreement with UIDAI enabling ESP to provide e-sign services to ASP.

5.3 ESP shall provide services in conformity with CDAC CA CPS available at www.esign.cdac.in.

5.4 The obligations/responsibilities/duties of ESP are subject to limitations/restrictions/constraints mentioned in this document.

5.5 ESP shall take consent from Aadhaar Holder(s) to use their Aadhaar Number/VID/UID Token /Biometeric Information/OTP for the services applied for by such Aadhaar Holder(s).

6. Obligations of ASP

6.1 ASP warrants and represents to ESP that-

i. ASP is an entity legally constituted and validly existing under the laws of India;

ii. ASP has all requisite powers and authority and has taken all actions necessary to execute, deliver, and perform its obligations under this Agreement;

iii. This Agreement has been validly executed by ASP and constitutes a valid agreement binding on ASP and enforceable in accordance with the laws of India.

iv. ASP is aware of the fact that online Aadhar based eKYC Authentication facility has been limited to specific services.

6.2 ASP, who is seeking to use Aadhaar Authentication to enable a specific service/business functions, is solely responsible for the choice of authentication type(s). The choice of the Authentication type shall be the sole decision of the ASP, and no other entity, including UIDAI, ESP and Aadhaar Holder shall have any role in this decision of ASP.

6.3 ASP shall undertake that "Services provided by C-DAC shall be exclusively in accordance with the guidelines provided in judgment delivered by the Supreme Court of India, on September 26, 2018, in writ petition (Civil) No.494 of 2012 – Justice K.S. Puttaswamy (Retd.) and Anr. Vs. Union of India and Ors."

6.4 ASP shall undertake to C-DAC for use of online services using the process of eKYC for limited purposes, based on the judgment delivered by Hon'ble Supreme Court of India, dt. September 26, 2018.

6.5 ASP hereby covenant and take full responsibility henceforth for providing eSign services of C-DAC, only for Non-commercial purposes and for Direct Benefit Transfer (DBT) purposes.

6.6 ASP shall undertake to indemnify and keep indemnified and harmless C-DAC, its Directors and employees, from and against any and all liability resulting from claims, demands, penalties, suits and judgments and all costs, charges and expenses relating thereto as a result of a breach by ASP of its covenants as stated hereinabove.

6.7 ASP assumes complete responsibility with regard to its network connectivity with ESP.

6.8 ASP shall establish and maintain necessary authentication related operations, including systems, processes, infrastructure, technology, security, etc., which may be necessary for using Aadhaar Authentication Service, in compliance with Aadhar Act, standards and specifications, issued by UIDAI from time to time.

6.9 ASP shall only employ the Authentication Devices and associated application components (such as sensor and extractor pairs for fingerprint and iris scanners) which are duly registered with/ approved/ certified by UIDAI or an agency appointed by UIDAI for this purpose. ASP understands and agrees that the authentication type to be employed by it in providing Aadhaar Enabled Services and shall employ the Authentication Devices which conform to the authentication type adopted by ASP, and ESP/UIDAI shall have no role to play in this regard, and shall have no liability or responsibility in this respect.

6.10 ASP shall ensure that the persons employed by it for providing Aadhaar Enabled Services and for maintaining necessary systems, infrastructure, processes, etc. in this regard, possess requisite qualifications for undertaking such works. The ASP shall be responsible for ensuring that such personnel are suitably and adequately trained to conduct Aadhaar Enabled Services, in compliance with specifications and standards prescribed by UIDAI from time to time.

6.11 ASP shall, at all times, comply with the provisions contained in the Information Technology Act, 2000 and the statutory rules framed there under, from time to time, in so far as the same has application to its operations in accordance with this Agreement, and also with all other Laws, rules and regulations, whether already in force or which may be enacted anytime in the future, pertaining to data security and management, data storage, sharing and data protection, as also with the National Identification Authority of India Bill, as and when the same in enacted into a law and comes into force, and shall ensure the same level of compliance by its Authentication Device.

6.12 ASP shall maintain logs of all authentication transactions processed by it, capturing the complete details of the authentication transaction and shall retain the same for a duration as prescribed by UIDAI from time to time but shall not, in any event, store the Aadhaar Personal Identity Data of the Aadhaar Holder (PID). The ASP understands and agrees that the logs maintained by it shall not be shared with any individual or entity, and that the storage of the logs maintained by it shall comply with all the relevant laws, rules and regulations, including, but not limited to, the Information Technology Act, 2000 and the Evidence Act, 1872.

6.13 In case of any investigations around authentication related fraud(s) or dispute (s), the ASP shall extend full cooperation to UIDAI, and/or any agency appointed/authorized by it and/or any other authorized investigation agency, including, but not limited to, providing access to their premises, records, personnel and any other relevant resource / information, etc. of or pertaining to its Authentication Device.

6.14 ASP shall carry out the integration process as outlined by ESP along with necessary documents, consents and undertakings.

6.15 ASP assures/declares/ conforms that all the documents/information/data etc.. given to /shared with/submitted to ESP shall be correct, genuine, true and ESP shall be entitled to terminate this contract with immediate effect and without notice to ASP; in the event of any information/documents/data given/shared/submitted by ASP is found wrong/false/missing/suppressed/misleading etc.. and ASP shall be responsible and liable for all financial and other consequences arising out of or incidental to such actions/omissions by ASP/termination of this contract

6.16 ASP shall send the document hash and other details to ESP in encrypted format for authentication by UIDAI as per the stipulation of UIDAI

6.17 The e-KYC data shall not be used by ASP for purposes other than that for which the resident has explicitly given his/ her consent.

6.18 ASP shall not share the e-KYC data with any other agency for whatsoever purposes except and to the extent provided under this Agreement.

6.19 ASP shall physically and virtually locate/install/keep/maintain/upgrade/operate all its infrastructure from within India only. ASP shall ensure that all its actions/omissions etc. shall be used for lawful purposes only and shall not be against/anti/detrimental to India’s security/safety/image/reputation and other interests.

6.20 ASP shall be responsible and liable for any claims/actions/demands/effects/consequences etc. arising out of/incidental to any information/documents/data etc. given to ESP by ASP.

6.21 ASP agrees that C-DAC shall neither be liable nor responsible for the actions/ omissions/ performance/ non-under-part performance/ defaults/ failures/ lapses etc of ASP.

6.22 ASP shall be responsible and liable for breach of any of the obligations / responsibilities / duties / performance (part-under-non-performance) arising out of the Supreme Court judgment.

6.23 ASP agrees and accepts that ESP shall have no responsibility in relation to failures that may take place during the Aadhaar based authentication process, including but not limited to, failures as a result of, false reject, network, or connectivity failure, device failure, software failure, possible down time and central identities data repository, etc.

6.24 ASP agrees and accepts that ESP shall have no responsibility in relation to failures that may take place during the eSign process, including but not limited to, failures as a result of, reject, network, or connectivity failure, device failure, software failure, possible down time and central identities data repository, etc.

6.25 ASP agrees and accepts that services offered by ESP are on the Best Effort basis and are dependent upon third parties actions/performance/availability/responses etc.

6.26 ASP agrees and accepts to pay the amount as per Tax invoice generated by ESP based on the successful transaction log generated at ESP end.

6.27 ASP shall carryout security audit of its application by ICERT empanelled agency and application audit as per CCA guidelines by IS certified auditor and submit the certificates along with auditors' reports to ESP along with request to act as ASP and also as and when and software application is changed or one year from the issuance of the Audit Certificate, whichever is earlier.

6.28 ASP acknowledges, agrees and accepts that ESP shall provide separate ASP-ID for each software application through which ASP will avail ESP services. Each new software application of ASP shall be audited and certified as mentioned in this document.

6.29 ASP shall ensure that all its actions shall be in conformity with CDAC CA CPS available on www.esign.cdac.in

6.30 ASP shall not use/publicize/print/emboss/circulate or otherwise associates itself with trademarks/logos/symbols of ESP without prior written permission of ESP. Any continued use of logos/names/marks/symbols of ESP by ASP upon expiry/termination of this contract or in violation of the permission given; shall make ASP responsible and liable to all legal/financial consequences/damages etc.

6.31 ASP shall save and indemnify ESP from/against any claims/demands/actions/suits etc. arising out of/incidental to this contract or any infringement of Intellectual property of C-DAC. ASP shall be liable to pay for all costs and expenses including but not limited to attorney's fees, travel, accommodation, lodging, boarding, transport etc.. claimed from/borne/incurred/paid by ESP.

6.32 ASP agrees and accepts entire responsibility and liability for breach of any of the obligations/responsibilities/duties/performance (part/under/non-performance) of ASP and ESP shall not be responsible and liable for the actions/omissions/performance/non-under-part performance/defaults/failures/lapses etc. of ASP.

7. Fees

As on the date of signing this agreement following will be applicable:

7.1 E-sign services shall be provided by ESP to ASP, as per following:

S. No.	Particulars	Price Per Signature(in ₹)
1.	e-Sign	

7.2 E-sign services shall be provided by ESP to ASP on Payment of advance amount of ____________ (Rupees ____________________________ only) as refundable non-interest bearing security deposit.

7.3 Invoices will be raised monthly/quarterly for the successful number of e-Signs logged at ESP server in that month/quarter.

7.4 GST as applicable at the time of billing shall be charged extra on price quoted above.

8. Force Majeure

8.1 The Parties agree that neither of them shall be liable to the other for any loss, delay, damage or other casualty suffered or incurred by the other owing to earthquakes, floods, fires, explosions, acts of God, war, terrorism, court orders, epidemics, pandemics, quarantines or any other such cause, which is beyond the reasonable control of the Party and any failure or delay by any other Party in the Performance of any of its obligations under this Agreement owing to one or more of the foregoing causes shall not be considered as a breach of any of its obligations under this Agreement. The Parties however agree that any financial failure or non-performance of any financial obligations or covenants of the Parties shall not constitute Force Majeure.

8.2 The Party claiming benefit of Force Majeure shall however not be entitled to the same unless it has intimated the other Party of the occurrence of such an event within a period of seventy hours from the occurrence of such Force Majeure event indicating therein the steps that it is taking or intending to take to mitigate the effect of such Force Majeure on the performance of his obligations under this Agreement.

9. Confidentiality and data protection

9.1 Each Party shall treat all information, which is disclosed to it as a result of the operation of this Agreement, as Confidential Information, and shall keep the same confidential, maintain secrecy of all such information of confidential nature and shall not, at any time, divulge such or any part thereof to any third party except as may be compelled by any court or agency of competent jurisdiction, or as otherwise required by law, and shall also ensure that same is not disclosed to any person voluntarily, accidentally or by mistake.

9.2 Parties shall use the Confidential Information strictly for the purposes of authentication of the Aadhaar Holder, and for providing Aadhaar Enabled Services, in accordance with this Agreement. Parties shall ensure compliance with all applicable laws and regulations including but not limited to regulations on data protection under the Information Technology Act, 2002 when collecting information from residents for their business purposes.

9.3 Parties shall scrutinize the data collected by it, while processing authentication requests, on a periodic basis, and shall preserve such data collected in relation to an authentication request until such time as may be prescribed by UIDAI from time to time.

9.4 Parties are prohibited from storing any PID in their data base or in any storage device of any nature whatsoever including Authentication Device or in any machine, device or instrument of any kind whatsoever, removable storage devices or in physical form, at point in time.

9.5 Parties hereby unequivocally agrees to undertake all measures, including security safeguards, to ensure that the information in the possession or control of the Parties, as a result of operation of this Agreement, is secured and protected against any loss or unauthorized access or use or unauthorized disclosure thereof.

9.6 Any and all Intellectual property arising out of or incidental to this contract shall be exclusively owned by C-DAC/ESP. ASP agrees to sign and execute all applications/affidavits/deeds/assignments/ documents etc. in favour of C-DAC/ESP to register/protect IP in the name of C-DAC.

9.7 It is hereby mutually agreed that this Clause shall survive the termination of this Agreement.

10. Disclaimer of Warranties and Limitation of Liability

C-DAC does not give any kind of warranties about its ESP services. ESP does not warrant that its services will be error/defect free. C-DAC hereby disclaims all guarantees, warranties and conditions, either express, implied or statutory, including, but not limited to, any (if any) implied warranties or conditions of merchantability of fitness for a particular purpose, of lack of viruses, of accuracy or completeness of responses, of results, and of lack of negligence or lack of reasonable care or workmanlike effort, all with regard to its services. Also, there is no warranty or condition of title, quiet enjoyment, quiet possession, correspondence to description, or non-infringement with regard to the software/system/services.

In no event ESP shall be liable to ASP/its clients/customers/users /employees/agents/associates /beneficiaries /citizens and any other persons for any incidental, consequential, special, and exemplary or direct or indirect damages, or for lost profits, lost revenues, or loss of business, loss of opportunities, loss of reputation etc.. arising out of or incidental to use of Services offered by CDAC/ESP, regardless of the cause of action, even if the C-DAC has been advised of the likelihood of damages. The entire risk as to the quality of or arising out of the use or performance of the ESP services remains with ASP.

11. Audit rights

The ASP unequivocally agrees to provide full co-operation to UIDAI/ESP/CCA or any agency approved and/or appointed by UIDAI/ESP/CCA in the audit process, and to provide to UIDAI/ESP/CCA or any agency approved and/or appointed by UIDAI/ESP/CCA, complete access to its procedures, records and information pertaining to services availed.

12. Term

12.1 This Agreement shall come into force and effect on the date first written above ('Effective Date').

12.2 Unless terminated earlier in accordance with the terms of this Agreement, this Agreement shall remain in force and effect for a period of _____ years from the Effective Date ('Term'). The Term of the Agreement may be extended by the Parties with mutual agreement.

13. Termination

13.1 This Agreement shall be deemed to be automatically terminated (without any notice) if and when:

(a) The term expires

(b) the agreement between ESP and ASA is terminated;

(c) the agreement between ESP and UIDAI is terminated;

(d) the license/authority provided by CCA/Certifying Authority to ESP for providing DSC related services is revoked/cancelled/suspended.

13.2 Either Party may terminate this Agreement by giving 30 days prior written notice to the other Party sent by Regd./Speed Post AD.

14. Consequences of termination

14.1 In case of termination of this Agreement due to any reason, ASP shall pay ESP all due and payable amounts of Fees for the Successful Transactions completed till the effective date of termination.

14.2 In case of termination of this Agreement due to any reason or upon expiry of this Agreement, the ESP shall retain a copy of all logs, documents, artifacts etc. for a period of 2 years thereafter and shall share with ASP such logs, documents, artifacts etc. promptly upon receipt of request from ASP.

15. Dispute resolution / Arbitration

15.1 In the case of any dispute arising upon or in relation to or in connection with this Agreement between the Parties, the disputes shall at the first instance be resolved through good faith negotiations, which negotiations shall begin promptly after a Party has delivered to the other Party a written request for such consultation.

15.2 If the dispute or difference is not resolved within 30 days as per the above clause, it shall be taken up by either party for resolution through AMRCD as mentioned in DPE OM No. 4(1)/2013 – DPE (GM)/ FTS – 1835 dt. 22/05/2018. The common cost of the arbitration proceedings shall initially be borne equally by the Parties and finally by the Party against whom the award is passed. Any other costs or expenses incurred by a Party in relation to the arbitration proceedings shall ultimately be borne by the Party as the arbitrator may decide.

15.3The parties shall opt for the arbitration as per provisions of Arbitration and Conciliation Act, 1996 and as amended from time to time, if the mandate of above-mentioned arbitration by AMRCD/PMA is not in existence at the time of occurrence of dispute or the same is not applicable to the dispute.

15.4 The Parties shall continue to perform their respective obligations under this Agreement, despite the continuance of the arbitration proceedings, except for the disputed part under arbitration.

15.5 The Parties shall use their best endeavors to procure that the decision of the Arbitrators shall be given within a period of six (6) months or soon thereafter as is possible after it has been demanded.

16. Other

16.1 Applicable law and jurisdiction

This Agreement shall, in all respects, be governed by, and construed in accordance with the laws of India. The Courts in Pune, India shall have exclusive jurisdiction in relation to this Agreement, to try, entertain and decide the matters which are not covered under the ambit of Arbitration.

16.2 Waiver

No failure by a Party to take any action with respect to a breach of this Agreement or a default by any other Party shall constitute a waiver of the former Party's right to enforce any provision of this Agreement or to take action with respect to such breach or default or any subsequent breach or default. Waiver by any Party of any breach or failure to comply with any provision of this Agreement by a Party shall not be construed as, or constitute, a continuing waiver of such provision, or a waiver of any other breach of or failure to comply with any other provision of this Agreement, unless any such waiver has been consented to by the other Party in writing.

17. Severability

If any Clause or part thereof, of this Agreement or any agreement or document appended hereto or made a part hereof is rendered invalid, ruled illegal by any court of competent jurisdiction, or unenforceable under present or future Laws effective during the term of this Agreement, then it is the intention of the Parties that the remainder of the Agreement, or any agreement or document appended hereto or made a part hereof, shall not be affected thereby unless the deletion of such provision shall cause this Agreement to become materially adverse to any Party in which case the Parties shall negotiate in good faith such changes to the Agreement, or enter into suitable amendatory or supplementary agreements, as will best preserve for the Parties the benefits and obligations under such provision.

18. Notices

Any notice, direction or other documentation required or remitted to be given hereunder shall be in writing and may only be given by personal delivery, international courier, electronic mail or facsimile (with confirmation received) at the addresses hereinafter set forth:

a. **For ASP**:

Address: ____

Attention: ____

Phone Numbers: ____

Fax No. : ____

e-mail: ____

b. **For ESP**:

Address: Centre for Development of Advanced Computing (C-DAC)
Innovation Park 34, B/1,
Panchawati Rd, Panchawati, Pashan,
Pune, Maharashtra 411008

Attention: ____

Phone Numbers: ____

Fax No. : ____

e-mail: ____

19. Enurement

This Agreement will ensure to the benefit of and be binding upon the Parties hereto and their respective successors and assigns.

20. Expenses

Each of the Parties shall bear the fees and expenses of their respective counsels, accountants and experts and all other costs and expenses as may be incurred by them incidental to the negotiation, preparation, execution and delivery of this Agreement.

21. Surviving provisions

The provisions of this Agreement, which are intended to survive the term of this Agreement by their very nature, shall survive the termination of this Agreement. Notwithstanding the generality of the above, clauses related to indemnity, confidentiality, arbitration and applicable law and jurisdiction shall survive the termination/expiration of this Agreement.

22. Assignment

This Agreement shall not be assigned by either Party without obtaining a prior written consent from the other.

23. Independent Parties and Non-Solicitation

Parties shall be independent parties and the relationship arising out of/incidental to this contract shall not mean or construed/deemed as any kind of partnership/joint venture/agency etc..

Further, ASP shall not solicit/induce/attract/engage/employ directly or indirectly any employees/members/staff/associates/consultants without written consent of ESP.

24. Entire Agreement

This Agreement and its schedules/annexures/appendices constitutes the entire agreement between the Parties. There are not and will not be any verbal statements, agreements, assurances, representations and warranties or undertakings among the Parties and this Agreement may not be amended or modified in any respect except by written instrument signed by the Parties.

25. Counterparts

This Agreement is executed in one original and one copy. Original is kept with ESP and copy with ASP.

IN WITNESS WHEREOF the parties have each executed this Agreement by its duly authorized officer as of the day and year first above written

SIGNED AND DELIVERED FOR AND ON BEHALF OF ASP:

Title& Name: ______________________________________

Designation: ______________________________

Signature: ________________________________

SIGNED AND DELIVERED FOR AND ON BEHALF OF ESP:

Title& Name: ______________________________________

Designation: ______________________________

Signature: ________________________________

17 Annexure-4: Aadhaar-Holder Consent Format to be used in the ASP Application

Signatory's explicit consent is mandatory for using the signatory's identity and address data from Aadhaarsystem to generate DSC. ASP should ensure to obtain the consent in their user interface which can have values as "Y", "N". C-DAC provides an additional feature that enables users to choose details at higher granularity from Aadhaar e-KYC data in to be incorporated their DSC.

The following template is an illustration for obtaining consent from an Aadhaar holder to be used by an Application Service Provider (ASP) in their user interface.

ASP may customize the consent form as per their requirement.

Consent for Authentication

<<Name of Agency Providing the Service>>

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

I hereby give my consent for using my identity and address data received from e-KYC provider to generate and submit the electronic DSC application form to CA, creation of key pairs by ESP on my behalf, submission of certificate to CA for certification, one time creation of signature on the hash along with this request, deletion of key pairs after applyingsignature(s). I have noobjection in the use of my ID for authenticating myself with Aadhaar based authentication system for the purposes of availing of the _____*<<Name of the Application/Service>>*____ from ____*<<Name of* ASP>>____. 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 obtaining my e-KYC through Aadhaar e-KYC service and for the issuance of Digital Signature Certificate (DSC) for this specific transaction and for no other purposes.For the creation of DSC, I understand that the options that I have chosen are the ones that shall be populated in the DSC generated by the CA and I provide my consent for the same. I also understand that the following fields in the DSC generated by the CA are mandatory and I give my consent for using the Aadhaar provided e-KYC information to populate the corresponding fields in the DSC.

- Common Name (name as obtained from e-KYC)
- Unique Identifier (UID Token)
- Pseudonym (unique code sent by UIDAI in e-KYC response)
- State or Province (state as obtained from e-KYC)
- Postal Code (postal code as obtained from e-KYC)

I understand that ____<<Name of ASP>>____ 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 _____*<<Name of ASP>>*____ to provide my Aadhaar number, and Authentication Mode (Biometric and/or OTP).

18 Annexure-5: Staging Level Integration Checklist

Staging Level Integration Checklist *		
1.	Annexure -1 ASP Request Form	□
2.	Annexure-2 Supporting documents based on the category of organization	□
3.	Self-signed digital certificate or digital certificate issued by CCA empanelled Certifying Authority for Level I/Level II integration purposes	□
4.	Payment terms have been agreed upon and payment is carried out	□

*All the above items are mandatory and need to be submitted prior to Staging Level integration.

19 Annexure-6: Pre-Production Level Integration Checklist

Pre-Production Level Integration Checklist *		
1.	Annexure-8Letter of undertaking from ASP mentioning action performed for each of the response transaction have been carried out in Level I integration as expected and Level II integration can be initiated	□
2.	List of Aadhaar numbers to be used for pre-production level integration. It is expected that nearly 50% of transactions at this level will be done using these Aadhaar numbers. The DSC issued will be based on e-KYC received from UIDAI in these transactions.	□
3.	Annexure-7Aadhaar Holder Consent forms for Pre-Production Integration from the holder of such Aadhaar numbers which are provided for pre-production level integration	□

*All the above items are mandatory and need to be submitted prior to Pre-Production Level integration.

20 Annexure-7: Aadhaar Holder Consent Form for Pre-Production Level Integration

Consent for Authentication

<<Name of Agency Providing the Service>>

I hereby give my consent for using my identity and address data received from e-KYC provider to generate and submit the electronic DSC application form to CA, creation of key pairs by ESP on my behalf, submission of certificate to CA for certification, one time creation of signature on the hash along with this request, deletion of key pairs after applying signature(s). I have no objection in the use of my IDfor authenticating myself with Aadhaar based authentication system for the purposes of availing of the _____*<<Name of the Application/Service>>*____ from ____*<<Name of ASP>>*____ with e-Hastakshar (C-DAC's eSign Service) during ____*<<Start Date>>*_____ and ____*<<End Date>>*_____. 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 and for obtaining my e-KYC through Aadhaar e-KYC service and for the issuance of Digital Signature Certificate (DSC) for integration purposes and for no other purposes. I understand that C-DAC shall ensure security and confidentiality of my personal identity data provided for the purpose of Aadhaar based authentication. I also understand that subsequent to the completion of integration, ASP shall not use my Aadhaar ID for integration with C-DAC ESP.

Signature of Aadhaar holder ______________________________ **Date**________________

Name of Aadhaar holder ______________________________

Signature of ASP Authorized Person __________________

Name of ASP Authorized Person______________________

21 Annexure-8: Letter of Undertaking for Staging Level Completion

<<Name of Agency Providing the Service>>

We ___________*<<Name of ASP>>*________ have completed Staging Level integration for ____________*<<Name of ASP application>>*_____________________________ with e-Hastakshar (C-DAC's eSign Service) during ____*<<Start Date>>*____ and ___<<End Date>>______________. The action performed for each of the 200 response transactions have been carried out as expected. The following checks were carried out during the integration of our application with e-Hastakshar:

- Conformity of ASP requests for eSign to API specifications as defined by CCA
- Basic checks for HTTP header, content type and usage of SSL
- Presence of mandatory elements and attributes in the request XML
- Checks for data type and values in specified range
- Checks that the request XML does not contain extra elements and/or attributes other than those which are mandatory and optional
- Checks for more than one occurrence of said attribute and elements and data contained within to avoid conflict
- Presence of enveloped ASP signature on request XML and its verification

We are ready to initiate the Pre-Production Level integration.

Signature of ASP Authorized Person ____________________ **Date** __________________

Name of ASP Authorized Person _________________________

22 Annexure-9: Production Level Integration Checklist

Production Level Integration Checklist *		
1.	Annexure-10 Letter of undertaking from ASP mentioning action performed for each of the response transaction have been carried out in Level II integration as expected and Level III integration can be initiated.	□
2.	Certificate and reports of security assessment carried out by ICERT empanelled agency	□
3.	Certificate and reports of security assessment carried out by IS Certified Auditor based on the checklist given in Annexure-11	□
4.	Annexure-3Contract and Agreement between ASP and C-DAC	□
5.	Digital certificate issued by CCA empanelled Certifying Authority for production level integration. In case the certificate shared for Level I integration has been issued by a CCA empanelled CA and is to be used for production level integration as well, the certificate need not be shared again.	□

*All the above items are mandatory and need to be submitted prior to Production Level integration.

23 Annexure-10: Letter of Undertaking for Pre-Production Level Integration Completion

<<Name of Agency Providing the Service>>

We ___________*<<Name of ASP>>*________ have completed Pre-Production Level integration for ____________*<<Name of ASP application>>*____________________________ with e-Hastakshar (C-DAC's eSign Service) during ____*<<Start Date>>*____ and ___<<End Date>>______________. The action performed for each of the 100 response transactions have been carried out as expected. The following checks were carried out during the integration of our application with e-Hastakshar:

- Conformity of ASP requests eSign to API specifications as defined by CCA
- Basic checks for HTTP header, content type and usage of SSL
- Presence of mandatory elements and attributes in the request XML
- Checks for data type and values in specified range
- Checks that the request XML does not contain extra elements and/or attributes other than those which are mandatory and optional
- Checks for more than one occurrence of said attribute and elements and data contained within to avoid conflict
- Presence of enveloped ASP signature on request XML and its verification
- Approximately 50% of transactions done using the Aadhaar numbers shared with C-DAC prior to Pre-Production level integration and DSC generated contained e-KYC information of the respective Aadhaar holders

We are ready to initiate the Production Level integration.

Signature of ASP Authorized Person ___________________ **Date** _________________

Name of ASP Authorized Person _______________________

24 Annexure-11: Audit Requirements

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

#	Name of the Standard and Specification Document	Link/ Reference to the Document
1.	Aadhaar Authentication API Specification 2.5	https://uidai.gov.in/images/resource/aadhaar_authentication_api_2_5.pdf
2.	Aadhaar OTP Request API Specification 2.5	https://uidai.gov.in/images/resource/aadhaar_otp_request_api_2_5.pdf
3.	Demographic Data Standards	http://uidai.gov.in/UID_PDF/Committees/UID_DDSVP_Committee_Report_v1.0.pdf
4.	Date and Time format Standard	ISO_8601
5.	XML Signature	http://www.w3.org/TR/xmldsig-core/
6.	Audit logging requirements	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.
7.	UIDAI Guidelines including Compendium Of Regulations, Circulars & Guidelines For (Authentication User Agency (Aua)/E-Kyc User Agency (Kua), Authentication Service Agency (Asa) And Biometric Device Provider) *User should also follow required guidelines of UIDAI that are being announced from time to time as applicable	https://uidai.gov.in/images/resource/Compendium_of_Regulations_Circulars_Guidelines_for_AUA_KUA_ASA_05102017.pdf
8.	System Security and Data Security	As per Table given below

ASP Audit Checklist

SI	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 empanelledauditor
10	ASP data logging for audit purposes provisioned.
11	ASP should not delegate any obligation to external organizations or applications

25Annexure-12: ASP Go-Live Checklist

Go Live Checklist *		
1.	Staging Level integration carried out successfully and undertaking provided for the same	□
2.	Pre-Production Level integration carried out successfully and undertaking provided for the same	□
3.	ASP application audit by ICERT empanelled agency is completed and certificate and report provided to that effect	□
4.	ASP application audit by IS certified auditor is completed and certificate and report provided to that effect	□
5.	Agreement signed between ASP and C-DAC	□
6.	Payment terms have been agreed upon and payment is carried out as per the agreement	□
7.	ASP data logging for audit purposes provisioned	□
8.	ASP has conducted end-to-end testing for 50 number of successful transactions in Production environment	□
9.	Resident consent process to obtain consent for every transaction is ready and deployed	□

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

Please note that production ASP license will be provided post C-DAC 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 C-DAC*)

Signature: ____________________

Name: ____________________

Designation: ____________________

Organization: ____________________

Date: ____________________