eSign API Specifications

Version 3.3

09 Dec 2020

Controller of Certifying Authorities

Ministry of Electronics and Information Technology

Document Control

Document Name	eSign API Specifications
Status	Release
Version	3.3
Release date	09.12.2020
Last update	09.12.2020
Document Owner	Controller of Certifying Authorities, India

Table of Contents

1. Introduction

Information Technology Act, 2000 grants legal recognition to electronic records and electronic signatures. IT Act,2000 provides that where any law requires that information or any other matter shall be authenticated by affixing signature then notwithstanding anything contained in the law, such requirement shall be deemed to be fulfilled if such information is authenticated by means of electronic signatures affixed in a manner prescribed by the Central Government. Under the IT Act, 2000, 'Electronic signatures' means authentication of an electronic record by a subscriber by means of electronic technique specified in second schedule and includes Digital signatures. Digital Signature means authentication of any electronic record by a subscriber by means of procedure specified in Section 3 of the IT Act, 2000.

The Controller exercises supervision over activities of Certifying Authorities and certifies public keys of Certifying Authorities. The Certifying Authorities are granted licence under the IT Act, 2000 by the Controller to issue Digital Signature Certificates. Any person can make an application to Certifying Authority for issue of an Electronic signature Certificate in such form as may be prescribed by the Central Government. For issuance of Digital Signature Certificates, the applicant's Personal identity, address and other details to be included in the DSC need to be verified by CAs against an identity document. For class II & III certificates, physical presence of the individual is also required. Digital Signatures are widely used for authentication in the electronic environment. The cost of verification individual's identity and address and also the secure storage of private keys are the stumbling block in the widespread usage of Digital Signature in the electronic environment.

X.509 Certificate Policy for India PKI states that the certificates will confirm that the information in the application provided by the subscriber does not conflict with the information in well-recognized consumer databases. The database of individual's information maintained by e-KYC providers will be used for eSign . The accepted e-KYC providers are listed in the e-authentication guidelines.

Verification of the Proof of Identity (PoI) and Proof of Address (PoA) is a pre-requisite for issuance of Digital Signature Certificates by Certifying Authorities.

e-KYC Service providers can provide a paperless KYC experience by using e-KYC and avoid the cost of repeated KYC, the cost of paper handling and storage, and the risk of forged documents. The real-time e-KYC service makes it possible for service providers to provide instant service delivery to eSign Users which otherwise would have taken a few days for activation based on the verification of KYC documents, digitization, etc.

ESP and ASP have to make sure that mechanisms implemented for authentication of individuals adhere to the prescribed e-KYC guidelines

The Government has introduced ***Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015*** in which the technique known as "e-authentication technique using e-KYC services" has been introduced to eliminate stumbling block in the widespread usage of Digital Signature.

e-Sign facilitates digitally signing a document by an eSign user using an Online Service. While authentication of the signer is based on e-KYC response and a confirmation by CA, the signature on the document is carried out on a backend server, which is the e-Sign provider. The service shall be offered only by Certifying Authorities. The eSign is an integrated service that facilitates issuing a Signature Certificate and performing Signing of requested data on basis of authenticated e-KYC response. The eSign Service shall be implemented in line with e-authentication guidelines issued by Controller. The certificate issued through eSign service will have a limited validity period and is only for one-time signing of requested data.

The prescribed modes of user verification may be online or offline. The 3.x version will be for offline verification and 2.x version will be for online verification. In the case of offline user verification, the e-KYC service will be provided by CA and one time registration of user is required. Both 2.x and 3.x versions of API are designed for applying Digital Signature based on the response received from e-KYC service after online authentication of eSign user.

1.1. Target Audience

This is a technical document and is targeted at Application Service Providers who require signing of digital document(s) in their application.

1.2. Objective of the document

This document provides eSign Service API specification for offline verification. This includes 3.x API Data format, protocol and other related specifications.

1.3. Terminology

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

"eSign User or eKYC user or subscriber" is an individual requesting for eSign online Electronic Signature Service of eSign Service provider. This individual shall be using the application of ASP and represents himself/herself for signing the document under the legal framework. For the purposes of DSC by the CA, the eSign user shall also be the 'applicant/subscriber for digital certificate', under the scope of IT Act.

"e-KYC" means the transfer of digitally signed demographic data such as Name, Address, photograph etc of an individual collected and verified by e-KYC provider on successful authentication of same individual

"Response code" is the identification number maintained by e-KYC provider to identify the authentication and eSign

Application Service Provider (ASP): An organization or an entity using eSign service as part of their application to digitally sign the content. Examples include Government Departments, Banks and other public or private organizations. ASP may contact the ESP (eSign Service Provider) directly to avail the service within its framework.

eSign Service Provider (ESP): An organization or an entity providing eSign service. ESP is a "Trusted Third Party", as per the definitions of Second Schedule of Information Technology Act. ESP will facilitate subscriber's key pair-generation, storing of key pairs on hardware security module and creation of digital signature. ESP must be integrated with a CA for the purpose of obtaining Signature Certificate for the generated Key-pair.

Certifying Authority (CA): An organization or an entity licensed under CCA for issuance of Digital Certificate and carrying out allied CA operations.

e-KYC Number/eSign user id shall mean the unique identification such as username/number/id maintained by e-KYC provider to uniquely identify user;

e-KYC provider shall mean any e-KYC provider listed in e-Authentication Guidelines. eKYC provider is responsible for eKYC user management and authentication eSign user. In case CA maintains eSign User Accounts of subscribers/eSign user, the security and privacy will be applicable as per the provisions specified under IT Act.

'**OTP'** shall mean one-time password either sent to or generated on the eSign User's cell phone for the purpose of authentication, including SMS OTP, Time based OTP (TOTP), or any other secure OTP bound token generation methods;

UIDAI: An authority established by Government of India to provide unique identity to all Indian residents. It also runs the e-KYC authentication service for the registered KYC User Agency (KUA).

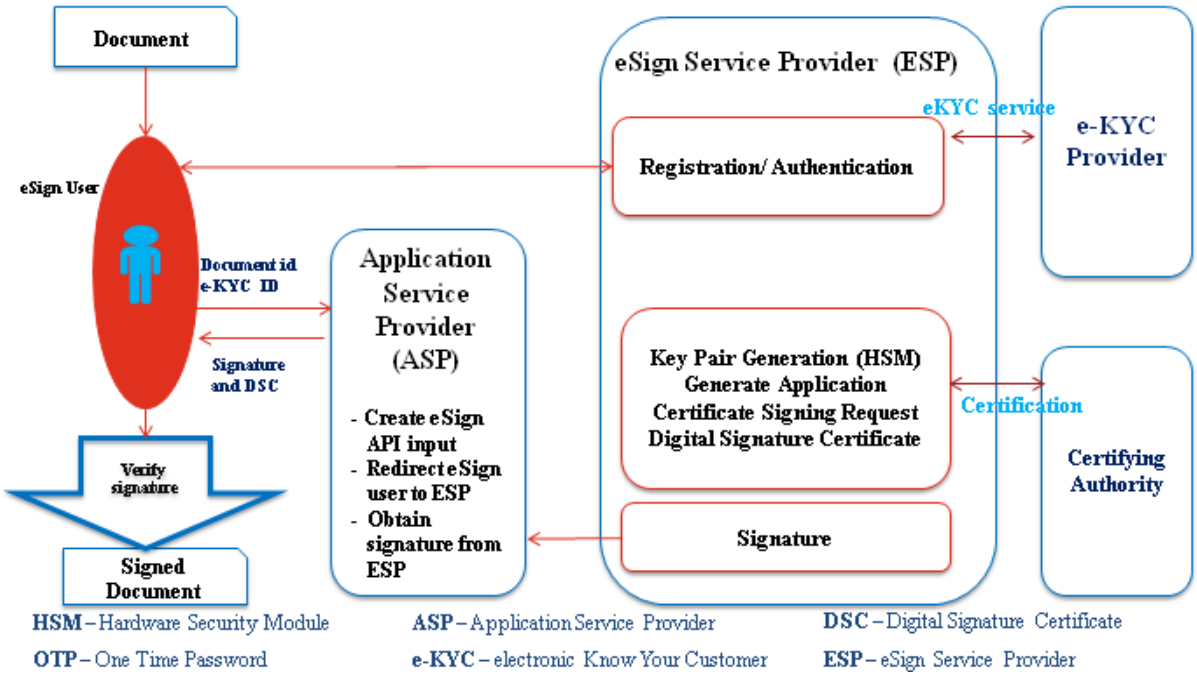
1.4. Legal Framework

eSign service will operate under the provisions of the Second Schedule of Information Technology Act, 2000 (e-authentication technique using Aadhaar and other e-KYC services) as notified vide (notification details)

2. Understanding eSign Service

This chapter describes eSign Service, some of the envisioned usage scenarios, and working details. Technical details follow in subsequent chapters.

2.1. eSign Service at a glance



3. eSign Service API

This chapter describes the API in detail including the service flow, communication protocol, and data formats.

This API expects that authentication of the individual has been carryout and the digitally signed e-KYC response is made available to ESP. The authentication needs to be carried out independent of section 3

The suggested method for obtaining authenticated e-KYC response is

ESP facilitates authentication of eSign user by calling authentication URL of eKYC provider. The e-KYC response will be received by ESP and performs eSign on the eSign request received from ASP within permissible time limit.

3.1. eSign - Usage scenarios

The API specifications remain common for all eSign Service provider. However, the parameter values that will vary for each ESP are ‘eSign Service URL’ and ‘ASP ID’ (Unique User ID provided by the ESP).

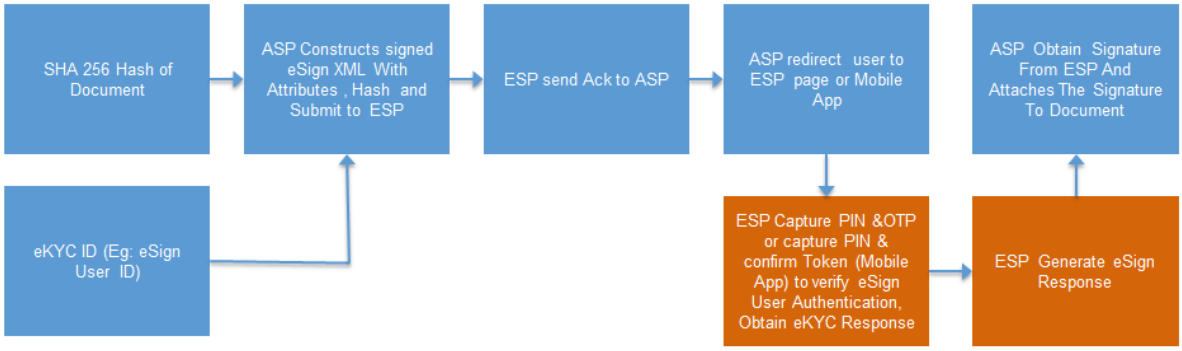
ASP provides eSign facility to public should integrate with all other ESPs within one month after on-boarding with first ESP.

The eSign service API can be used in the scenario where ASP initiates eSign request and ESP authenticates user for eKYC before eSign through eKYC provider.

3.1.1. eSign using e-KYC made by ESP

eSign 3.3 uses asynchronous API for request and response. ASP calls the ESP signing request API, later (post signature authorization by subscriber) ESP will call back ASP and provide the signature status and data.

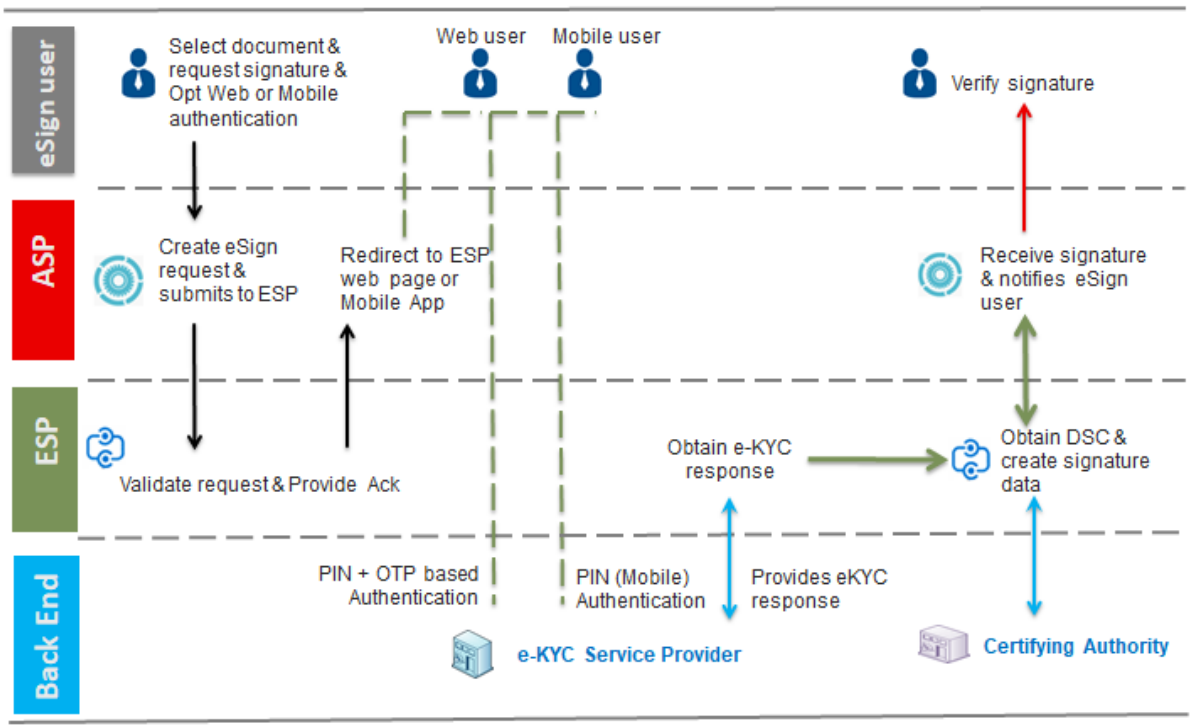
Flow of eSign process using this option:



In this scenario:

1. ASP client application asks eSign user to sign the document
2. ASP client application creates the document hash (to be signed) on the client side
3. ASP client application asks the eSign user id for certificate generation and signature.
4. ASP forms the input data for eSign API
5. ASP calls ESP's URL and submit request XML
    a. ESP validates the calling application and the input.
    b. ESP verifies the Digital signature of ASP for eSign XML received
    c. ESP logs the transaction
    d. ESP acknowledges the request back to ASP by providing an ack response with same txn ID. At this time ASP can close the connection to ESP.
6. ASP redirects the user to ESP's authentication page. Alternatively, User can use ESP's mobile app to authenticate. ASP shall suitably display necessary information.
    a. ESP displays e-authentication page (if web flow) or notifies on ESP mobile app to the eSign user.
    b. ESP performs authentication using OTP (SMS/TOTP for web flow or OTP bound token for ESP mobile app) along with PIN and get e-KYC information from e-KYC provider.
    c. ESP shows the document hash along with document information to eSign user.
    d. ESP creates a new key pair and CSR for eSign user.
    e. ESP calls the CA service and gets a Digital Signature Certificate for eSign user.
    f. ESP signs the 'document hash'
    g. ESP calls ASP's response URL or redirects to response URL (which was part of eSign request) with signed XML response.
    h. If ASP has provided 'redirectUrl', ESP redirects the user back to ASP's web page (web flow).
    i. In case response is not received by ASP or user session ends within ASP, ASP can check status of signing request using "checkStatus" API using the same txn ID of the request.
7. ASP receives the document signature and the eSign user's Digital Signature Certificate.
8. ASP client application attaches the signature to the document.
9. ASP shall provide a choice to user to obtain signed document via email, download, short URL sent via SMS, etc.

The web page flow for eSign using e-KYC made by ESP is as given below



3.2. API Protocol - eSign Service

eSign service is exposed as stateless service over HTTPS. Usage of open data format in XML and widely used protocol such as HTTPS allows easy adoption and deployment of this service. To support strong end to end security and avoid request tampering and man-in-the-middle attacks, it is essential that the requests and responses are digitally signed.

The usage of HTTPS shall ensure transport layer encryption, while digital signing of XML shall ensure integrity & authenticity of data.

Following is the URL format and the parameters for eSign service:

API URL	ESP shall expose URL as HTTPS endpoint
Protocol	HTTPS
Method	POST
Content-Type	application/xml
Post data	A well-formed XML, as per the specifications provided in this document.

ASP is required to collect the necessary API URL from the respective ESP.

3.3. eSign API: Input Data Format - eSign Service

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

3.3.1. eSign XML structure

Following is the XML data format for eSign XML.

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

3.3.1.1. Element Details

Element Name: Esign

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

Sl No	Attribute	Required?	Value
1.	Ver	Mandatory	eSign version (mandatory). ESP may host multiple versions for supporting gradual migration. As of this specification, API Version is "3.3".
2.	signerid	Optional	Format: id@id-type.esp-id ASP collects the ID of the signer, along with ID type and ESP Name. ASP may make it intuitive for user to select their required ID type and then specify the value. Allowed ID Types: username, Mobile, PAN If mobile is the id-type, then mobile number should be same as in the eKYC XML. Allowed ESP ID: Unique Identifiers specified by CCA for each empanelled ESP. ASP should construct the signerid based on ID given by user and selected ID type and ESP. This information shall be used by ESP to validate and then pre-populate the username for the convenience. ESP should not allow modification of the username in their screen.

			If signerid is not present, ESP may facilitate the new signer id creation through eKYC provider, however authentication of user should be carried out before signing.
3.	ts	Mandatory	Request timestamp in ISO format. The value should be in Indian Standard Time (IST), and should be within the range of maximum 30 minutes deviation to support out of sync server clocks.
4.	txn	Mandatory	Transaction ID of the ASP calling the API, this is logged and returned in the output for correlation. Should be unique for the given ASP-ESP combination for that calendar day.
5.	maxWaitPeriod	Mandatory	Expiry time in minutes. This is maximum wait time for the ESP to allow Signer to complete the signing. In case the user does not sign within ASP's expected duration, ESP should mark the transaction as error 'User timeout' error code. Default = 1440 minutes
6.	aspId	Mandatory	Organization ID of ASP
7.	responseUrl	Mandatory	ASP URL to receive the response from ESP. This should be a valid URI accessible from ESP system to make a call and submit the response XML packet using HTTP(S)-POST with Content-Type as application/xml. On success or failure including cancellation by user, ESP shall perform a background call to this response URL with 'eSign Response Format' which contains the status success/failure (status = 1/0).
8.	redirectUrl	Optional	ASP URL to redirect the user after completion of transaction. This is supported only in case where ASP uses redirection to ESP authentication page. If present, ESP shall redirect the user back to ASP's designated URL. Such redirection shall have a HTTP(S)-POST and Content-Type of 'application/x-www-form-urlencoded' with parameter of 'txnref' containing concatenated transaction ID and responseCode (separated with a pipe character) in base 64 encoding. txnref=Base64(transaction ID + "|" + responseCode)
9.	signingAlgorithm	Mandatory	This value represents the signature Algorithm. End user certificate generation (DSC) shall also be based on this algorithm. Allowed Values are: 1. ECDSA 2. RSA

Element Name: Docs

- Description: Contains one 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
- Attributes: Table below

Sl No	Attribute	Required?	Value
1.	id	Mandatory	The index number of the document. Should start with one. Maximum 5. Should be sequential. Shall not repeat.
2.	hashAlgorithm	Mandatory	Should be fixed to "SHA256"
3.	docInfo	Mandatory	Description for the respective document being signed, not more than 50 characters. docInfo should be strictly adhere to the content of document. Multiple documents of same type or different types should not be included in a single file. ESP shall display this information against docUrl, so that user can identify the same.
4.	docUrl	Mandatory	URL of the document. Should be a HTTP / HTTPS URL for the document, accessible by the signer during the transaction permitted duration (maxUserWait Time). ESP shall display this URL with hyperlink, so that user can access the document to view.
5.	responseSigType	Mandatory	This value represents the response signature type, where ASP can request for a specific type of signature from one of the following Allowed Values are: 1. raw 2. PKCS7(with only the signer certificate in the certificate section and no revocation information) 3. PKCS7pdf(all issuer certificates up to and including root CA certificate and CRLs/OCSP responses of each issuer certificates should be included in the response. In case, the number CRL entries are more than 5, only OCSP responses are allowed. The revocation information should be included as a signed

			attribute under pdfRevocationInfoArchival (1.2.840.113583.1.1.8). The signature may also be optionally time stamped using the time stamping services of CA. 4. PKCS7complete(All issuer certificates & its revocation information in unsigned info)

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

3.4. eSign: User Authentication Page

Once ASP submits the Request XML, ESP provides a 'pending for completion' (status=2) response which will contain the response code (as an acknowledgement). At this stage, ASP is expected to guide the user with proper information as under:

1. Redirect the user to the authentication page of the ESP.
2. Provide information to the user to authenticate over ESP's mobile app. (ESP may also support push notification for mobile app users, and allowing to authenticate on mobile through eKYC provider)

In case of redirection (browser based flow), ESP shall expose a redirection URL with following specifications.

API URL	ESP shall expose URL as HTTPS redirection page.
Protocol	HTTPS
Method	POST
Content-Type	application/x-www-form-urlencoded
Parameter name	txnref
Parameter Value	Concatenated transaction ID and responseCode (separated with a pipe character) in base 64 encoding.
Example format	txnref=Base64(transaction ID + "|" + responseCode)

3.5. eSign API: Response Data Format - eSign Service

Below is the response format of eSign Service API. This response shall be used in following situations:

1. Once the subscriber authorizes (or cancels or expire), ESP shall provide a completed response to the ASP on the responseUrl (status = 1/0).
2. ESP shall also respond to 'Check Signing Status' API call with this response format including 'pending for completion' statuses.

Note that, the API does not give any identity related data of the eSign user.

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

3.5.1. 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

Sl No	Attribute	Presence	Value
1.	ver	Mandatory	Should be set to 3.3
2.	status	Mandatory	In case of success, it will be “1” In case of failure, it will be “0” In case of pending for completion, it will be “2”
3.	ts	Mandatory	Will contain the response timestamp in ISO format.
4.	txn	Mandatory	The Transaction ID provided by ASP in the request.
5.	resCode	Mandatory	A unique response code provided by ESP. This is a unique id for the transaction (eSign user authentication & eSign request) provided by ESP. It shall make the transaction traceable, and ASP is expected to store this code in their audit log. The response code shall be maintained same for particular transaction. Being asynchronous, there may be need for providing the response multiple times including the acknowledgement stage and final response stage. All the responses shall carry same response code for the particular transaction.
6.	error	Optional	In case of failure, this will contain an error code. OR blank, in case of success.

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 eSign user 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 raw(ECDSA) or PKCS7 (CMS) signature format as per the request XML.
- Attributes: Table Below

Sl No	Attribute	Presence	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 an error code. OR blank, in case of success. ESP shall provide necessary option for signer to uncheck any document hash. Such unchecked document hash shall not be signed and shall be returned with an error called “User Rejected”.

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

3.6. eSign API: Check Signing Status - Request

This is an additional option for ASP to check the status of the transaction, in case necessary.

On a successful & timely flow, ESP will automatically call back the ASP’s responseUrl with necessary eSign response. However, in case of any need, ASP can call the signing status API and receive the response again.

ESP shall provide this service for minimum of 30 days from the date of transaction, for the ASP.

3.6.1. Request XML format

```
<EsignStatus ver="" ts="" txn="" aspId="" >
        <Signature>Digital signature of ASP</Signature>
</EsignStatus>
```

3.6.1.1. Element Details

Element Name: Esign

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

	Attribute	Required?	Value
1.	ver	Mandatory	Should be set to 3.3
2.	ts	Mandatory	Request timestamp in ISO format. The value should be in Indian Standard Time (IST), and should be within the range of maximum 30 minutes deviation to support out of sync server clocks.
3.	txn	Mandatory	Transaction ID of the ASP provided in original request.
4.	aspId	Mandatory	Organization ID of the ASP

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

This will respond with an eSign response data as defined in this document. The status attribute of the response will indicate the success or pending for completion.

4. eKYC Service requirements

CA shall implement a comprehensive eKYC service to fulfil the KYC requirements of eSign user.

Important points to consider:

1. eKYC system shall be a protected and shall not be exposed to any external services directly.
2. The access of eKYC information shall be on need basis for the services prescribed.

3. The access to such information by other services shall be bound by authentication of eSign user by two factors, namely the PIN and a second factor as prescribed.
4. The information of PIN shall not be stored in plain text format. The authentication of PIN shall be always verified after comparing against the stored value.
5. The PIN information in plain text shall not be part of any logs or data monitoring systems. For this purpose, PIN shall undergo necessary hashing / encryption methods at the source of capture (user entry) during authentication.

4.1. Functions of eKYC Service

eKYC Service shall operate with the minimum required functions.

The functions shall include:

1. Creation of eSign user account
2. Fetch eSign / KYC user information by ESP / CA systems (with user authentication)
3. Perform user Authentication
4. eSign user functionalities

4.2. Creation of eSign user account

eKYC system shall provide provision for online enrolment to eSign users and the same should be able access through ESP page or ASP applications. Such enrolment is bound by procedures and requirements defined under Identity Verification Guidelines. Mobile number and PAN should be unique within Personal eKYC accounts.

On successful enrolment of an eKYC User, following data eSign user information is recorded in eKYC user account. These fields are subject to verification against the prescribed 'Verified Source'. (Aadhaar Offline XML, Bank eKYC, organisational KYC)

4.2.1. Aadhaar Offline XML

Aadhaar Offline XML shall be verified on its receipt for a valid digital signature by UIDAI.

Sl No	Field name	Description	Source	Additional Actions
1.	Username	eSign user Id in the format prescribed.	User entry	Should be Unique
2.	PIN	PIN of the user	User entry	Meet the requirements laid down in IVG
3.	Name	Name of the eKYC user	Aadhaar Offline XML	
4.	Mobile	Mobile Number of the user	User entry	This shall be checked with the Aadhaar Offline XML using the hashing process defined by UIDAI
5.	Email	Email ID of the user	User entry	If a value is present in Aadhaar Offline XML, the value entered by user shall be verified against it using hashing process defined by UIDAI. Else, ESP shall send an Email OTP and validate it for verification. This field is optional.

6.	Address	Address of the eKYC user	Aadhaar Offline XML	Shall be concatenated with the fields from Aadhaar Offline XML, to form an address, excluding State, Country and Postal Code.
7.	StateProvince	StateProvince of the eKYC user	Aadhaar Offline XML	
8.	Country	Country of the eKYC user	Aadhaar Offline XML	
9.	Postal Code	Postal Code of the eKYC user	Aadhaar Offline XML	
10.	Photograph	Photograph of the eKYC user	Aadhaar Offline XML	Shall be verified against Video, as prescribed under IVG
11.	DOB	DOB of the eKYC user	Aadhaar Offline XML	
12.	Gender	Gender of the eKYC user	Aadhaar Offline XML	
13.	PAN	PAN Number of eKYC user	User entry	CA should verify the PAN by the verification service provided by Income Tax. CA should preserve the evidence of verification with their digital signature. This field is optional.
14.	Aadhaar Number	Last Four digit of Aadhaar Number	Aadhaar Offline XML	
15.	eKYC Type	Offline Aadhaar	CA	

4.2.1.1. KYC Data Format and Verification Requirements

Aadhaar Offline XML data format shall meet the requirements of "Aadhaar Paperless Offline e-KYC" specified by UIDAI in https://www.uidai.gov.in/.

Towards the verification of such data, below minimum steps shall be implemented:

a. Validate the Digital Signature of the XML to avoid any tampering.
b. Validate that it is digitally signed using UIDAI public key certificate, as published by UIDAI. For this purpose, CA may maintain pre-mapped list of valid UIDAI certificates, and update it time-to-time.
c. The date of such XML shall be within the prescribed limits by Identity Verification Guidelines (If any).
d. Field level verifications as mentioned in above table.

4.2.2. Bank eKYC

Bank sends eKYC to CA directly up on authentication by user as a banking customer. Bank eKYC shall be verified on its receipt by CA for a valid digital signature by respective bank.

Sl No	Field name	Description	Source	Additional Actions
1.	Username	eSign user Id in the format prescribed.	User entry	Should be Unique
2.	PIN	PIN of the user	User entry	Meet the requirements laid down in IVG
3.	Name	Name of the eKYC user	Bank eKYC	
4.	Mobile	Mobile Number of	Bank eKYC	This shall be verified by sending

		the user		OTP to the mobile of user and validate it for verification.
5.	Email	Email ID of the user	Bank eKYC /User entry	If a value is not present in Bank eKYC XML, the value entered by user shall be verified by sending an Email OTP and validate it for verification. This field is optional.
6.	Address	Address of the eKYC user	Bank eKYC	
7.	StateProvince	StateProvince of the eKYC user	Bank eKYC	
8.	Country	Country of the eKYC user	Bank eKYC	
9.	Postal Code	Postal Code of the eKYC user	Bank eKYC	
10.	Photograph	Photograph of the eKYC user	Bank eKYC	
11.	DOB	DOB of the eKYC user	Bank eKYC	
12.	Gender	Gender of the eKYC user	Bank eKYC	
13.	PAN	PAN Number of eKYC user	Bank eKYC /user entry	In case of user entry , CA should verify the PAN by the verification service provided by Income Tax. CA should preserve the evidence of verification with their digital signature. This field is mandatory
14.	Aadhaar Number	Last Four digit of Aadhaar Number	Bank eKYC	
15.	Bank Account Number	Account Number of the account for which KYC was made by Bank.	Bank eKYC	
16.	Bank IFSC Code	IFSC code of the bank / branch associated with account	Bank eKYC	This field is Optional
17.	eKYC Type	BANK	CA	

4.2.2.1. KYC Data Format and Verification Requirements

Bank KYC information shall be shared with CA in a digitally signed format. For the uniformity and long-term retention purposes under the IT Act, a common specification shall be implemented, as provided below.

Towards the verification of such data, below minimum steps shall be implemented:

a. Validate the Digital Signature of the XML to avoid any tampering.

b. Validate that it is digitally signed using Bank's public key certificate, as provided by respective Bank. For this purpose, CA shall maintain pre-mapped list of valid Bank certificates, and update it time-to-time.
c. The date of such XML shall be within the prescribed limits by Identity Verification Guidelines (If any).
d. Field level verifications as mentioned in above table.

4.2.2.2. KYC Request XML Structure:

```
<BankKYC ver="" ts="" txn="" bankIfscCode="" bankName="" accountNumber="">
    <KYCInfo name="" mobile="" email="" address="" stateProvince="" country="" postalCode="" dateOfBirth="" gender="" pan="" Aadhaar="" />
    <Photo format="">Base 64 encoded photograph</Photo>
    <Signature>Digital signature of the Bank</Signature>
</BankKYC>
```

Element Details:

Element Name: BankKYC

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

Sl No	Attribute	Required?	Value
1.	ver	Mandatory	Shall be set to 1.0
2.	ts	Mandatory	Timestamp in ISO format. The value should be in Indian Standard Time (IST). Bank shall provide the time on which they generated and signed this KYC information
3.	txn	Mandatory	A Unique Transaction ID given by the Bank. (The uniqueness can be limited to a particular calendar day.) Bank should be able to identify the transaction based on this transaction ID, in case of any need.
4.	bankIfscCode	Optional	11 character alpha-numeric code of Bank associated with account
5.	bankName	Mandatory	Name of the Bank providing the KYC data. This information is provided for long term reference of the data. The name shall be the legal name of the Bank, and is expected to match the name provided in RBI website (https://m.rbi.org.in/CommonPerson/english/scripts/banksinindia.aspx).
6.	accountNumber	Mandatory	Bank Account Number of the KYC User.

Element Name: KYCInfo

- Description: Contains KYC Information
- Requirement of tag: Mandatory
- Value: Not Applicable
- Attributes: Table below

Sl No	Attribute	Required?	Value
1.	name	Mandatory	Name as per the Bank Records

2.	mobile	Mandatory	Mobile Number as per the Bank Records
3.	email	Optional	Email as per the Bank Records
4.	address	Mandatory	Address as per the Bank Records
5.	stateProvince	Mandatory	State as per the Bank Records
6.	country	Mandatory	Country as per the Bank Records. This shall be a 2-character representation of country based on ISO 3166 Example: IN: India
7.	postalCode	Mandatory	PIN Code as per the Bank Records
8.	dateOfBirth	Mandatory	Date of Birth as per the Bank Records. (in YYYY-MM-DD format)
9.	gender	Mandatory	Gender as per the Bank Records. This shall be 1-character representation as under: M: Male F: Female O: Others
10.	pan	Optional	Income Tax Permanent Account Number as per the Bank Records
11.	aadhaar	Optional	Last Four digit of Aadhaar Number as per bank records

Element Name: KYCInfo

- Description: Contains Photograph of corresponding KYC Information
- Requirement of tag: Mandatory
- Value: Base 64 Formatted (encoded) photograph of the user.
- Attributes: Table below

Sl No	Attribute	Required?	Value
1.	format	Mandatory	The format of the photograph represented in 3-character alphabets. Allowed values are: BMP: Windows Bitmap Format JPG: Joint Photographic Experts Group Format PNG: Portable Network Graphics Format

Element Name: Signature

- Description: Contains the signature of Bank.
- 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

4.2.2.3. KYC Response XML Structure

<BankKYCResp ver="" ts="" txn="" status="" resCode="" error="" />

Element Details:

Element Name: BankKYCResp

- Description: Root element of the Bank KYC response XML
- Requirement of tag: Mandatory
- Value: Not Applicable

- Attributes: Table below

Sl No	Attribute	Required?	Value
1.	ver	Mandatory	Shall be set to 1.0
2.	ts	Mandatory	Timestamp in ISO format. The value should be in Indian Standard Time (IST).
3.	txn	Mandatory	Transaction ID as in the request XML.
4.	status	Mandatory	In case of success, it will be "1" In case of failure, it will be "0"
5.	resCode	Mandatory	Unique Response Code from the CA for traceability.
6.	errorCode	Optional	In case of error, respective error code shall be provided here.
7.	errorMessage	Optional	In case of error, respective error code shall be provided here.

4.2.3. Organisational KYC

The eKYC account for the authorised signatory of the organisation as per IVG is a prerequisite. This option does not require the organisation to be an ASP of ESP.

CA shall verify the existence of organisation and organisational person as per 4.2.4. Upon successful verification, CA issues an organisational certificate to organisational person or accepts DSC issued by other CA. CA should map the certificate in their application to verify the digitally signed DSC application forms and documents to be received from the applicants of that organisation.

This option requires PAN, Aadhaar video, email, mobile and supporting digital document verification by CA prior to create and activate eKYC account for organisational person. CA shall log necessary audit logs as per the requirements laid down. The particulars includes the following

Sl No	Field name	Description	Source	Additional Actions
1.	Username	eSign user Id in the format prescribed.	User entry	Should be Unique
2.	PIN	PIN of the user	User entry	Meet the requirements laid down in IVG
3.	Name	Name of the organisational person	User entry	This name should match with the name certified by the authorised signatory of organisation.
4.	Mobile	Mobile Number of the user	User entry	CA should send a mobile OTP through SMS and validate it for verification.
5.	Email	Email ID of the user	User entry	CA should send an email OTP and validate it for verification. This field is optional.
6.	Address	Address of the eKYC user	User entry	CA should match the address against the address document displayed in the video by the user. CA shall also verify against the digital document proof provided by the user.
7.	StateProvince	StateProvince of the eKYC user	User entry	CA should match the address against the address document displayed in the video by the user. CA shall also verify against the digital

				document proof provided by the user.
8.	Country	Country of the eKYC user	User entry	CA should match the address against the address document displayed in the video by the user. CA shall also verify against the digital document proof provided by the user.
9.	Postal Code	Postal Code of the eKYC user	User entry	CA should match the address against the address document displayed in the video by the user. CA shall also verify against the digital document proof provided by the user.
10.	Photograph	Photograph of the eKYC user	User entry	CA s should verify the photo against Video, as prescribed under IVG.
11.	DOB	DOB of the eKYC user	User entry	Self-declaration by the user
12.	Gender	Gender of the eKYC user	User entry	Self-declaration by the user
13.	PAN	PAN Number of eKYC user	User entry	CA should verify the PAN Number and Name by the verification service provided by Income Tax Department. This field is optional; however either PAN or Aadhaar Number is required.
14.	Aadhaar Number	Last Four digit of Aadhaar Number	User entry	This field is optional. Aadhaar Number & photo should match against the Aadhaar document displayed in the video by the user.
15.	Organisational ID	Unique id of eKYC user in the organisation	User entry	CA should verify & match the organisational id proof submitted by the user with original displayed in the video by the user. This field is optional
16.	ORGSIGID	Unique id of authorised signatory who authorised the request	CA	
17.	Authorised Signatory of Organisation	The name of authorised of organisation	CA	As verified under the section 4.2.4
18.	Organisation Name	Legal name of the organization	CA	As verified under the section 4.2.4
19.	Organisation Unit	Organisational unit	User entry	As verified under the section 4.2.4 This field is optional
20.	eKYC Type	Organisational KYC Option 2	CA	eKYC Type
21.	CA Officer	CA Officer approved the KYC	CA	Name and identity of CA officer approved the eKYC account

4.2.4. KYC for Organisation and Authorised Signatory

The verification of existence of organisation and authorised signatory are covered under this section.

For the organisation KYC, the organisation should submit scanned copy of the proof of existence of organisation or GST as per IVG. In the case of scanned copy of the proof of existence of organisation the originals of proof documents submitted as per IVG should be verified by CA during the video verification.

For the KYC of the authorised signatory of the organisation, the scanned copy documents (authorization to authorized signatories) as per IVG should be submitted apart from the particulars 1-15 mentioned in 4.2.3

4.2.4.1. Organisation

The particulars includes the following for organisation

Sl No	Field name	Description	Source	Additional Actions
1.	Organisation Name	Legal name of the organization	User entry	In the case of scanned copies, CA should verify & match the proof submitted by the user with original displayed in the video by the user Or organisation name as in GST verification details
2.	Organisation address	Address of the Organisation	User entry	CA should verify & match the proof submitted by the user with original displayed in the video by the user or GST verification
3.	ORGID	Unique id allocated to organisation by CA	CA	
4.	eKYC Type	KYC organisation	CA	eKYC Type
5.	CA Officer	CA Officer approved the KYC	CA	Name and identity of CA officer approved the eKYC account

4.2.4.2. Authorised signatory

The particulars include the following for authorised signatory of organisation

Sl No	Field name	Description	Source	Additional Actions
1.	Name of Authorised Signatory	The name of authorised signatory of organisation	User entry	CA should verify & match the proof of authorization to authorized signatory submitted with the originals displayed in the video verification CA should also carry out a secondary verification as per 2.3.1(3) of IVG
2.	ORGSIGID	Unique id allocated for authorised signatory	CA	
3.	Organisation Unit	Organisational unit	User entry	CA should verify & match the proof submitted by the user with original displayed in the video by the user
4.	Fields 1-15 of 4.2.4	The fields required for the verification of authorised signatory	As per 4.2.4	As per the verification requirements for the fields 1-15 of 4.2.3

5.	Certid	Serial number of certificate issued to authorised signatory and issuer	CA	Certificate issued after successful verification
6.	ORGID	Organisation id	CA	
7.	Organisation Name	Legal name of the organization	CA	Verification as per 4.2.4.1
8.	eKYC Type	KYC authorised signatory	CA	eKYC Type
9.	CA Officer	CA Officer approved the KYC	CA	Name and identity of CA officer approved the eKYC account

4.2.5. PAN KYC

Under the provisions of IVG, CA can perform KYC of the user using PAN verification mechanism. This is achieved by performing electronic PAN verification along with Video and digital document verification mechanisms. CA shall log necessary audit logs as per the requirements laid down.

Based on successful validation and verification of the user, CA shall create and activate the KYC account with below particulars:

Sl No	Field name	Description	Source	Additional Actions
1.	Username	eSign user Id in the format prescribed.	User entry	Should be Unique
2.	PIN	PIN of the user	User entry	Meet the requirements laid down in IVG
3.	Name	Name of the eKYC user	User entry	This name should exactly match as per the PAN database of Income Tax Department. CA should not auto populate to the user (based on PAN entered). CA should necessarily match the user entry, towards security and validation purposes.
4.	Mobile	Mobile Number of the user	User entry	CA shall send a mobile OTP and validate it for verification. This shall be different from email OTP, if any. And shall be delivered only to the given mobile through SMS message.
5.	Email	Email ID of the user	User entry	CA shall send an email OTP and validate it for verification. This shall be different from mobile OTP. And shall be delivered only to the given email ID. This field is optional.
6.	Address	Address of the eKYC user	User entry	CA should match the address against the address document displayed in the video by the user.

				CA shall also verify against the digital document proof provided by the user.
7.	StateProvince	StateProvince of the eKYC user	User entry	CA should match the address against the address document displayed in the video by the user. CA shall also verify against the digital document proof provided by the user.
8.	Country	Country of the eKYC user	User entry	CA should match the address against the address document displayed in the video by the user. CA shall also verify against the digital document proof provided by the user.
9.	Postal Code	Postal Code of the eKYC user	User entry	CA should match the address against the address document displayed in the video by the user. CA shall also verify against the digital document proof provided by the user.
10.	Photograph	Photograph of the eKYC user	User entry	Shall be verified against Video, as prescribed under IVG
11.	DOB	DOB of the eKYC user	User entry	Self-declaration by the user
12.	Gender	Gender of the eKYC user	User entry	Self-declaration by the user
13.	PAN	PAN of eKYC user	User entry	CA should verify PAN number against the digital document submitted by the user and also PAN document displayed in the video by the user. CA should verify Photo in the PAN card against the photo provided by the user CA should also verify Photo in the PAN card against the video by the user. CA should also verify the PAN number and Name by the verification service provided by Income Tax Department. CA should preserve the evidence of verification details received from Income Tax Department, with CA's digital signature.
14.	Aadhaar Number	Last Four digit of Aadhaar Number	User entry	This field is optional. CA should also match Aadhaar no and photo against the Aadhaar document displayed in the video by the user.
15.	eKYC Type	PAN KYC	CA	
16.	CA Officer	CA Officer	CA	Name and identity of CA officer

		approved the KYC		approved the eKYC account

4.2.5.1. KYC Data Format and Verification Requirements

PAN KYC based user account creation shall undergo necessary verification requirements as laid down in IVG. The field level verification requirements are also provided in the previous section of this document.

4.2.6. eKYC for foreign Nationals

This section is applicable for applicants who are falling under the category of foreign nationals as mentioned in IVG. The identity and address verification for personal and organisational certificates have to be carried out by CA directly. CA can perform KYC of the user based on the identity and address verification as provided eKYC user. For organisational person certificate, the proof of existence of organisation and organisational identity of the applicant are required.

Based on successful validation and verification of the user, CA shall create and activate the KYC account with below particulars:

Sl No	Field name	Description	Source	Additional Actions
1.	Username	eSign user Id in the format prescribed.	User entry	Should be Unique
2.	PIN	PIN of the user	User entry	Meet the requirements laid down in IVG
3.	Name	Name of the eKYC user	User entry	This name should exactly match as per the identity document.
4.	Mobile	Mobile Number of the user	User entry	CA shall send a mobile OTP and validate it for verification. This shall be different from email OTP, if any. And shall be delivered only to the given mobile through SMS message.
5.	Email	Email ID of the user	User entry	CA shall send an email OTP and validate it for verification. This shall be different from mobile OTP. And shall be delivered only to the given email ID. This field is optional.
6.	Address	Address of the eKYC user	User entry	CA should match the address against the address document displayed in the video by the user. CA shall also verify against the digital document proof provided by the user.
7.	StateProvince	StateProvince of the eKYC user	User entry	CA should match the address against the address document displayed in the video by the user. CA shall also verify against the digital document proof provided by the user.
8.	Country	Country of the eKYC user	User entry	CA should match the address against the address document displayed in the video

				by the user. CA shall also verify against the digital document proof provided by the user.
9.	Postal Code	Postal Code of the eKYC user	User entry	CA should match the address against the address document displayed in the video by the user. CA shall also verify against the digital document proof provided by the user.
10.	Photograph	Photograph of the eKYC user	User entry	Shall be verified against Video, as prescribed under IVG
11.	DOB	DOB of the eKYC user	User entry	Self-declaration by the user
12.	Gender	Gender of the eKYC user	User entry	Self-declaration by the user
13.	PAN	PAN of eKYC user	User entry	This field is optional CA should verify PAN number/Photo against the digital document submitted by the user, online PAN verification service provided by Income Tax Department and also PAN document displayed in the video by the user.
14.	Organisational ID	Unique id in the organisation	User entry	This field is optional CA should verify & match the organisational id proof submitted by the user with original displayed in the video by the user.
15.	Organisation Name	Legal name of the organization	CA	This field is mandatory in the case of organisational person reference Video verification of documents, verification of reference of listing by government, and website reference
16.	Organisation Unit	Organisational unit	User entry	This field is optional
17.	eKYC Type	Foreign National KYC	CA	
18.	CA Officer	CA Officer approved the KYC	CA	Name and identity of CA officer approved the eKYC account

4.3. User Authentication Types

CAs implements a comprehensive eKYC Service to fulfil the access to KYC information of eSign users as well as issuance of token-based DSC with longer validity period. The access to this eKYC information is bound by authentication of user by multiple factors.

4.3.1. Authentication Factors

The primary factor (first factor) for the user authentication will be the PIN of the user ("something that the user knows"). The second factor of authentication relies on "something that the user has"

(example: random OTP, etc) OR “something the user is” (example: trusted device, assertion of local authentication, etc).

The allowed ways of second factor authentication are:

1. SMS-OTP
2. T-OTP
3. Mobile access token
4. FIDO2 over mobile
5. Public Key Authentication

The mandatory FIRST FACTOR of user authentication is the PIN. CA shall secure the PIN storage at their end through one-way hashing function (that is secure as on date), and shall not store in any kind of reversible mechanism. The PIN shall always be entered in an interface facilitated by CA, and shall ensure confidentiality throughout any channel or application layers where it flows. It is recommended that, PIN shall be hashed or encrypted at first possible layer (like user interface).

The DEFAULT SECOND FACTOR is the SMS-OTP, to perform eKYC account creation, maintenance, etc. The user provides his/her mobile number as a pre-requisite for creation of eKYC account by CA, which is a verified attribute as per the verification guidelines. SMS-OTP is sent to such verified mobile number.

The authentication models extend the second factor to other authentication like T-OTP, Mobile access token, FIDO2 and public key authentication. In the absence of alternate second factor authentication SMS-OTP will become default choice for second authentication. CA shall ensure that SMS-OTP authentication shall be used as a fallback option for a second factor other than OTP during the life time of eKYC account.

Every CA/ESP shall offer PIN + SMS-OTP as a default authentication model and one or more of the aforesaid authentication models as the choice to the user. User shall be able to choose these authentication modes during the registration process, or at a later time. It shall be ensures that any change to enablement / disablement / migration of second factor authentication mode shall undergo necessary 2-factor authentication before making such change.

The second factor authentication of eKYC user shall be implemented in integration with eKYC servers. The authentication modes can be independent or along with eKYC request(composite). If the registered second factor authentication like FIDO, T-OTP,PUBLICKEY, or MAT is absent in the eKYC request, then eKYC server shall initiate the authentication of user using the mode registered in eKYC database.

Subsequent sections describe the process to be followed for each type of second factor authentication.

4.3.2. SMS-OTP Functionality

CA/ESP shall implement the process to authenticate user using SMS-OTP, as a second factor. For this purpose, user’s verified mobile number (verified as part of user registration) shall be used.

4.3.2.1. Implementation Requirements

1. The architecture requires ESP system to request KYC system for sending OTP to requesting user.
2. Such communication shall include minimum of the user name in the request, and provide an acknowledgement to ESP system on successful trigger.
3. CA/ESP shall use an internal secure API communication, in order to send OTP to the user.
4. The response to ESP system shall not share the OTP.
5. The OTP shall be valid for maximum of 15 minutes, and shall not be logged in any place other than for validation of OTP in authentication request.
6. ESP shall implement necessary process to avoid more than one OTP trigger within a span of one minute, unless last OTP was successfully consumed.
7. OTP shall be sent with purpose and the purpose should be part of audit logs.
8. OTP authentication shall be activated till the life period of eKYC account.

4.3.2.2. Initial registration for this second factor

1. SMS-OTP shall be sent only to verified mobile number as per KYC information of the user.
2. There are no other initial registration requirements.

4.3.2.3. Authentication Value for this second factor

Authentication value in this factor will be the "OTP Value" received from user's SMS. This is read by the user and keyed in in the ESP/CA application interface. ESP/CA Server then matches the SMS-OTP value based on the original value generated by the server.

4.3.3. T-OTP Functionality

eKYC system of CA/ESP may implement Time Based OTP (TOTP) functionality using compliant T-OTP authenticators and/or ESPs own authenticator app through eKYC provider.

4.3.3.1. Implementation Requirements

1. The implementation of T-OTP shall be in compliance with RFC 6238.
2. The number of steps to support client clock drifts shall not exceed + or – 1 step.
3. It shall also support the time step of either 30 or 60 seconds only.

4.3.3.2. Initial registration for this second factor

1. Enrolment for T-OTP shall be made during registration process, or at a later stage.
2. If the enrolment or changes for T-OTP is made post registration, the user shall be successfully authenticated using 2 factors before permitting such change.
3. The enrolment for T-OTP can be made in any supporting device or application. Such enrolment shall be made using QR codes or any other secure means complaint to T-OTP requirements.

4.3.3.3. Authentication Value for this second factor

Authentication value in this factor will be the "OTP Value" received from user's T-OTP Authenticator. This is read by the user and keyed in the ESP/CA application interface. ESP/CA eKYC Server then matches the T-OTP value based on the secret value registered in the server.

4.3.4. Mobile Access Tokens

Towards an improved user experience, eKYC system of CA/ESP may offer mobile based authentication. In such a case, Mobile Access Token, that meets the requirements of this section, shall fulfil the need for second factor authentication.

4.3.4.1. Implementation Requirements

1. Mobile app shall be owned and operated by CA/ESP with complete control on its code, architecture, security and publishing requirements.
2. Mobile app shall support largely used Mobile operating systems. However, it shall not support any operating systems or its versions, which are known to have security issue or under deprecation.
3. Mobile app shall have a secure architecture and undergo vulnerability assessments to avoid any exploitation.
4. Mobile Access Token shall be created as per the Initial registration requirements specified here.
5. Mobile Access Token shall be marked for expiry in maximum of 3 months from its last successful usage. In case of expired Mobile Access Token, mobile app shall clear the local Mobile Access Token and force the user for fresh enrolment/registration to the mobile app.
6. eKYC server of CA/ESP shall support single Mobile Access Token against one eKYC user, towards supporting registered mobile devices.
7. Subscriber portal shall provide necessary option for Mobile Access Token history and revocation of Mobile Access Token.
8. Any signing transaction 'waiting for user authentication' shall be queued and shown separately on the mobile app. It is also recommended to show new signing transactions as a push notification.
9. User shall be able to open the mobile app (with or without a local sign in functionality) and confirm the signature with PIN authentication.
10. Mobile app may also support additional eSign user functions using same level of security required for eSign Subscriber portal.
11. Mobile app should be secure enough to avoid any kind of access breach, or any kind of hacks to gain direct access to the token and the eKYC server endpoint consumed by such mobile app.

4.3.4.2. Initial registration for this second factor

1. The registration starts with the PIN & OTP authentication eKYC user using the CA client APP installed on the mobile of eKYC user registered with CA eKYC database
2. This first-time usage shall have a secure layer/channel to create and make a handshake with KYC server with generation of a unique Access Token (MAT).
3. MAT shall be generated in the mobile device in a secure area (device's embedded Secure Element/Enclave) supported by the platform, and shared with eKYC server for enrolment of the device against that of eKYC user.

4.3.4.3. Authentication Value for this second factor

Authentication value in this factor will be the "access token" received from user's mobile device. This access token is protected by the mobile application, and will be transmitted using the encrypted channel as part of Second Factor Authentication. For security purposes, the device may ask for additional local authentication for the device before it can retrieve the access token from secure storage.

4.3.5. FIDO

Fast Identity Online (FIDO) is widely used as Universal Second Factor (U2F) authentication. FIDO2 enables users to leverage common devices to easily authenticate to online services in both mobile and desktop environments. FIDO2 may be used as a second factor authentication in the scope of this document.

4.3.5.1. Implementation Requirements

1. The FIDO2 protocols can be used as a second factor of authentication. The FIDO2 components include FIDO2 authenticator & FIDO2 Server. The FIDO2 authenticator & FIDO2 Server must conform to FIDO2 specification of standard to ensure interoperability.
2. The FIDO2 authenticator shall be local to subscriber and the FIDO2 server shall be hosted by CA/ESP at their premises with their exclusive control.
3. Using FIDO2, the local authentication can be accomplished by a user-friendly and secure action such as biometric authentication, entering a PIN, speaking into a microphone, inserting a second–factor device or pressing a button.
4. In the scope of this document, FIDO2 authentication is limited to user's mobile device installed with mobile app of Certifying Authority. CA application shall limit the number of mobile devices per user to one, which is registered in the eKYC database by the user
5. The FIDO2 registration shall be carried out through the software (Mobile App) provided by CA and shall be ensured to store the key pair in Trusted Platform Module (TPM) hardware of the registered mobile.
6. The maximum validity for the FIDO2 credentials of subscriber shall not be more than one year.
7. The digitally signed logs of the FIDO2 authentication, enrolment, updation and termination shall be achieved. The archival period for the logs shall be 7 years after the deactivation of eKYC account.
8. Vulnerability assessments shall be carried out on FIDO2 components and mobile app to avoid any exploitation.
9. The security strength of the asymmetric keys to be used for authentication shall be greater then or equal to 112.
10. The Web Authentication API (WebAuthn) is a specification written by the W3C and FIDO, with the participation of Google, Mozilla, Microsoft, Yubico, and others. The API allows servers to register and authenticate users using public key cryptography. The Web Authentication API has two main calls
    a) navigator.credentials.create-can be used to perform the registration step.
    b) navigator.credentials.get-can be used to perform the authentication step.

4.3.5.2. Initial registration for this second factor for registered eKYC users

1. To perform the FIDO registration the eKYC user shall install CA client APP integrated with FIDO API in the mobile of eKYC user. The API call navigator.credentials.create for registration of eKYC user to FIDO server of CA .
2. The registration starts with the PIN & OTP authentication eKYC user using the CA client APP installed on the mobile of eKYC user registered with CA eKYC database.
3. In registration, a server must provide data that binds a user to a credential i,e a private-public key pair, identifiers for the user and organization . The CA Mobile APP prompt the user to provide information and create a new key pair using FIDO API
4. The registration starts with CA APP sending a request for a randomly generated string from the server to be used as a challenge to prevent replay attacks.
5. CA APP calls navigatotor.credentials.create with challenge and new credential command. The users credentials include, user id, organisation name, public key (types are acceptable to a server).
6. Registration makes the mobile device to create a new set of public-key credentials that can be used to sign a challenge generated by the CA.
7. The public part of these new credentials, along with the signed challenge, shall be sent back to the CA
8. CA verifies the signature of the signed registration response and then stores the publicKeyBytes and credential Id in a database, associated with the user. The validation shall include two factor authentication of the user.

9. CA provide registration confirmation to the user through push notification.

4.3.5.3. Authentication Value for this second factor for registered eKYC users

During authentication an assertion is created, which is proof that the user has possession of the private key. This assertion contains a signature created using the private key. The server uses the public key retrieved during registration to verify this signature.

1. The authentication starts with CA client APP running on the mobile of eKYC user sending a request for a randomly generated string from the server to be used as a challenge to prevent replay attacks.
2. To perform the authentication step, the CA client APP integrated with FIDO API call navigator.credentials.get -.This will retrieve the credential generated during registration with a signature included. For the authentication, the user proves that they own the private key they registered with by providing an assertion, which is generated on the client.
3. After the assertion has been obtained, include it in the eKYC request and sent to CA for verification along with document signature data. .
4. The authentication data is verified by eKYC system of CA/ESP using the public key stored in the database during registration

4.3.6. Public Key Authentication

CA may offer the public Key authentication as a second factor authentication in the scope of this document. This section describes the public Key authentication requirements, registration and authentication process to be followed for public key authentication.

4.3.6.1. Implementation Requirements

1. This shall use Public Key Cryptography (or asymmetric cryptography). The permitted algorithms and Key Sizes include RSA 2048 or higher, ECC-P256 or higher.
2. Public Key uniqueness to eKYC account holder shall be ensured by the CA/ESP. No two users shall have the same public key.
3. ESP shall enforce a lifetime for the public key of user not exceeding 3 years.
4. eKYC applicant shall be able to change his key at any time before the expiry of such key. During key modification, public key registration process described shall be followed before a new key is mapped to the existing user. OR, shall be permitted through any permitted two factor authentication under this document.
5. The audit trail of public key enrolments and public key-based authentications shall be maintained by the CA with the details of signer id, the date/time stamp, requested source details, etc., and should be accessible for audit. All registration and authentication details should be available for audit.
6. eKYC applicant shall provide consent to use public key registered with eKYC application for further authentication process in the system. Consent text shall be part of the signed data in both registration and authentication.
7. The private key shall be stored securely by the eKYC applicant and shall always be in his physical and tangible possession and control. The access to such key shall be protected by a PIN / Password / biometric.
8. The key pair generation and storage shall be carried out through the software provided by CA and shall be ensured to store the key pair a secure storage. Such storage shall be compliant to one or more requirements including Trusted Platform Module (TPM), Trusted Execution Environment (TEE), FIPS 140-2 certified, Common Criteria certified key storage,

and/or Hardware backed key assertion provided by platform. (Example: cryptographic token, smartcard, secure element, secure enclave in a mobile phone/personal computer).

9. The digitally signed logs of the registration, authentication, enrolment, updation and termination shall be achieved. The archival period for the logs shall be 7 years after the deactivation of eKYC account.

4.3.6.2. Initial registration for this second factor

1. This mode shall offer one or more of the permitted asymmetric cryptographic algorithms and the user may choose one of them.
2. The registration of the user for this mode shall include following steps:
    a. User initiates the registration process using the interface / application provided by CA (CA application).
    b. CA application generates the key pair using secure algorithm chosen by the user. User may not be technically savvy to select the algorithm, in which case, CA may choose one of the permitted algorithms as per CA's configuration.
    c. At this stage, CA application ensures the compliance of the key storage requirements for this mode. If the device does not support required key storage, CA application shall reject the request and show necessary message to the user.
    d. CA application transmits the public key activation data (containing minimum of public key, user identifier, device information, key storage information, consent, time stamp) of the user through an encrypted channel to the CA server. Public key activation data shall contain the signature through the private key of such user's key, conforming the integrity and authenticity of the request.
    e. CA server receives the public key activation data, validates it, and registers the public key against the user. The public key activation data is also logged by the server.
    f. User shall be provided relevant message up on successful registration of the Public Key.

4.3.6.3. Public Key Activation Data format

Towards uniformity across the providers, Public Key Activation Data shall conform to below structure.

```
<PublicKeyRegistration>
    <PublicKeyData SignerId="" TimeStamp="" Algorithm="" Consent="">Base64 encoded value of public key</PublicKeyData>
    <Signature>Digital signature of the subscriber using his private key as per XML Signature standards</Signature>
</PublicKeyRegistration>
```

Element Details

Element Name: PublicKeyRegistration

- Description: This element is the root element of the request.
- Value: Sub-elements
- Attributes: Not Applicable

Element Name: PublicKeyData

- Description: This element will contain Public Key related information
- Presence: Mandatory
- Value: base64 encoded value of 'Subject Public Key Info' as defined in RFC 5280.
- Attributes: As below

#	Attribute	Requirement	Value
	SignerId	Mandatory	Signer ID of the user
	TimeStamp	Mandatory	Will contain the request timestamp in ISO format.
	Algorithm	Mandatory	Shall include corresponding algorithm of Public Key, including its Key Length. Permitted values are: • RSA2048 • RSA4096 • ECC-P256 • ECC-P384 • ECC-P521
	Consent	Mandatory	The text as displayed to the user. This should be set to "I hereby agree that this public key be registered against my signer id and used during all subsequent authentications."

Element Name: Signature

- Description: This element will contain the signature value applied by user, which can be used for verification by ESP.
- 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

4.3.6.4. Authentication Value for this second factor

Authentication value in this factor will be the "signature" performed by the private key of the user, which will be verified by the corresponding public key stored at ESP/CA. The signature will be based on transaction reference sent by the ESP/CA server to the user's device, where the CA application (with the consent of the user) performs signature by accessing corresponding private key in the device. For security purposes, the device may ask for additional local authentication for the device before activating the private key to sign such data.

4.4. Access to eKYC data

The eKYC user information shall be allowed to access for eSign process and DSC issuance. For access of such data for eSign process, ESP shall implement necessary rest API based eKYC request, as per the formats provided under this section.

The audit logs (both success & Failure) of eKYC user authentications shall be maintained by eKYC Provider with timestamp and user id. The maximum retries with failed authentication by a user (for specific transaction) shall be limited to 5 attempts.

eKYC user shall be successfully authenticated as per the multi factor requirements, before accessing KYC information for transactional purposes.

The Authentication of the user can happen in one of the following manners:

1. **Composite**: In this case, the user will be performing first and second factor authentication as a single transaction. For example, the SMS-OTP is received and entered by the user while initiating the authentication, which means both PIN and SMS-OTP are part of one authentication request. Similarly, for other second factors as well, the second factor data will be part of initial authentication request.

2. **Independent**: In this case, the user will be performing first factor authentication and then proceeding for second factor. ESP/CA validates both independent requests based on common transaction ID & Signer ID combinations in the requests. For example, user first performs PIN authentication. Then triggers an SMS-OTP and submits it as next step. The KYC response in first step will provide a pending status, and will give full KYC response only after successfully receiving second factor authentication request.

The choice of whether composite or independent authentication manner will be based on the ESP/CA's system design, and can be implemented based on user experience and security considerations.

4.4.1. eKYC endpoint

Following is the URL format and the parameters for eKYC access:

API URL	ESP shall consume an URL for requests where ESP has to perform electronic KYC of eSign user.
Protocol	HTTPS
Method	POST
Content-Type	"application/xml"
Post data	A well-formed XML, as per the specifications provided in this document.

4.4.2. eKYC request format

```
<eKycReq ver="" signerid="" ts="" txn="" pinhash="">
        <SecondFactor>Base 64 encoded Second Factor Auth XML</SecondFactor>
        <Signature>Digital signature of ESP</Signature>
</eKycReq>
```

4.4.2.1. Element Details

Element Name: eKycReq

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

#	Attribute	Requirement	Value
1	ver	Mandatory	Should be set to 3.3
2	signerid	Mandatory	Signer ID entered by the user
3	ts	Mandatory	Will contain the request timestamp in ISO format.
4	txn	Mandatory	A unique transaction ID created by ESP system to request respective KYC data
5	pinhash	Mandatory	PIN entered by the user. This shall be the hash of the PIN, further hashed after prefixing the txn value. pinhash = hash(txn + hash(pin))

Element Name: SecondFactor

- Description: This element will contain the information for second factor authentication.
- Presence: Optional.
- Value: Base 64 encoded Second Factor Authentication XML

- Attributes: Not Applicable

Element Name: Signature

- Description: This element will contain the signature of ESP, which can be used for verification by eKYC system.
- Presence: Mandatory.
- 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

4.4.3. Second Factor Authentication format

```
<SecondFactorRequest ver="" signerid="" ts="" txn="" authenticationType="" consent="">
        <SMSOTP>OTP Value</SMSOTP>
        <TOTP>OTP Value</TOTP>
        <MAT>Mobile Access Token Value</MAT>
        <FIDO> Assertion received from the FIDO server against this user</FIDO>
        <PUBSIGN>signed data of the transaction reference value</PUBSIGN>
        <Signature>Digital signature of ESP</Signature>
</SecondFactorRequest>
```

4.4.3.1. Element Details

Element Name: SecondFactorRequest

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

#	Attribute	Requirement	Value
1	ver	Mandatory	Should be set to 1.0
2	signerid	Mandatory	Signer ID of the user
3	ts	Mandatory	Will contain the request timestamp in ISO format.
4	txn	Mandatory	This should be the transaction ID as per main eKYC authentication request. If the transaction is already successful, system should not accept this second factor request.
5	authenticationType	Mandatory	This shall indicate the type of Second Factor Authentication being performed. The allowed values are: • SMSOTP • TOTP • MAT • FIDO • PUBSIGN
6	consent	Mandatory	The text as displayed to the user. This should be set to "I hereby authorize this KYC Information authentication."

Element Name: SMSOTP

- Description: This element will contain information about SMS OTP authentication.

- Presence: Mandatory if type is SMSOTP.
- Value: OTP entered by the user. This should NOT be in a plain text. ESP shall implement any methods to replace plain text with encryption/hashing techniques. Shall be blank in case of mobile based authentication
- Attributes: Not Applicable

Element Name: TOTP

- Description: This element will contain information about T-OTP authentication.
- Presence: Mandatory if type is TOTP.
- Value: OTP entered by the user. This should NOT be in a plain text. ESP shall implement any methods to replace plain text with encryption/hashing techniques. Shall be blank in case of mobile based authentication
- Attributes: Not Applicable

Element Name: MAT

- Description: This element will contain information about Mobile Access Token authentication.
- Presence: Mandatory if type is MAT.
- Value: Access Token registered for the mobile App.
- Attributes: Not Applicable

Element Name: FIDO

- Description: This element will contain information about FIDO authentication.
- Presence: Mandatory if type is FIDO.
- Value: Assertion received from the FIDO server against this user.
- Attributes: Not Applicable

Element Name: PUBSIGN

- Description: This element will contain information about Public Key authentication.
- Presence: Mandatory if type is PUBSIGN.
- Value: Signature of the signed data of the transaction reference value as per the algorithm applicable (based on key type).
- Attributes: Not Applicable

Element Name: Signature

- Description: This element will contain the signature of ESP, which can be used for verification by eKYC system.
- Presence: optional if it is to be included in the eKYC request(composite).
- 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

4.4.4. eKYC response format

```
<eKycResp ver="" status="" signerid="" ts="" txn="" error="" respCode="" >
    <kycData name="" mobile="" email="" address="" stateProvince="" country=""
    postalCode=""  PAN=""  DOB="" Gender="" Aadhaar=""   eKYCtype=""/>
    <Photo>base64 encoded photo of the eKYC account holder</Photo>
```

```
<OrganisationDetails txn="" OrgName="" Orgunit="" KycOrgId="" orgSigName="" orgSigCertId=""/>
<Bankdetails txn="" bankIfscCode="" bankName="" accountNumber="" />
  <Signature>Digital signature</Signature>
</eKycResp >
```

Element Details

Element Name: eKycResp

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

#	Attribute	Value
1	ver	Should be set to 3.3
2	status	In case of success, it will be “1” In case of failure, it will be “0” In case of pending for second factor, it will be “2”
3	signerid	Signer ID sent in the request.
4	ts	Will contain the response timestamp in ISO format.
5	txn	The Transaction ID provided in the request.
6	error	In case of failure, this will contain a descriptive error message. OR blank, in case of success.
7	respCode	Unique eKYC response code given by KYC system. This shall form as a permanent reference to the log towards traceability of the transaction.

Element Name: kycData

- Description: This element contains the KYC information.
- Presence: Mandatory in case of Success. Not present in other cases.
- Value: Not Applicable
- Attributes: Table below

#	Attribute	Presence	Value
1.	name	Mandatory	Name of the eKYC account holder.
2.	mobile	Mandatory	Mobile Number of the eKYC account holder
3.	email	Optional	Email ID of the eKYC account holder
4.	address	Mandatory	Address of the eKYC account holder
5.	stateProvince	Mandatory	State or the Province of the address
6.	country	Mandatory	Two-character ISO representation of the country. Eg: IN=India
7.	postalCode	Mandatory	Postal code of the address
8.	PAN	Optional	PAN Number of eKYC account holder
9.	DOB	Optional	DOB Number of eKYC account holder. (in YYYY-MM-DD format)
10.	Gender	Optional	Gender of eKYC account holder
11.	Aadhaar	Optional	Last four digit of Aadhaar Number
12.	eKYC Type	Mandatory	Type of eKYC used for account creation

Element Name: Organisationdetails

- Description: This element contains the details of organisation.
- Presence: Mandatory in case of Success and user is an Organizational KYC user. Not present in other cases.

- Value: Not Applicable
- Attributes: Table below

#	Attribute	Presence	Value
1.	txn	Mandatory	A Unique Transaction ID given by the Organization.
2.	OrgName	Mandatory	Name of the Organization
3.	OrgUnit	Mandatory	Organization Unit
4.	KycOrgId	Mandatory	Organization ID allocated by CA
5.	orgSigName	Mandatory	Designated authorised signatory of organisation
6.	orgSigCertId	Mandatory	the certificate identifier / serial number

Element Name: Bankdetails

- Description: This element contains the details of Bank.
- Presence: Mandatory in case of Success and user is a Bank KYC user. Not present in other cases.
- Value: Not Applicable
- Attributes: Table below

#	Attribute	Presence	Value
1.	txn	Mandatory	A Unique Transaction ID given by the bank.
2.	bankIfscCode	Optional	IFSC code of Bank associated with account
3.	bankName	Mandatory	Name of the Bank providing the KYC data
4.	accountNumber	Mandatory	Bank Account Number of the KYC User.

Element Name: Photo

- Description: This element will contain the Photo of eKYC account holder.
- Presence: Mandatory in case of Success. Not present in other cases.
- Value: Base 64 encoded photograph of the eKYC account holder.
- Attributes: Not Applicable

Element Name: Signature

- Description: This element will contain the signature of eKYC system, which can be used for verification by ESP 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

4.5. Subscriber Functionalities

ESP shall offer a subscriber portal to meet the following requirements through eKYC provider.

1. PIN change functionality
2. Signing History
3. Other modifications to user data

This portal shall implement single factor authentication including either PIN, or OTP, or Mobile app to login to the system.

The portal shall be secured and permit minimum of the requirements stated in this section. Any request for modifications to KYC data shall undergo necessary verification procedures laid down by CCA.

5. Error Codes

Below are the standard error codes for various types of failures. ASP application shall use the error codes to identity the cause of failure and display / take necessary action.

5.1. eSign Response

Error Code	Error Message
101	Invalid Request Format
102	Invalid Signer ID
103	Invalid Version
104	XML Signature validation failed
105	Invalid transaction ID
106	Invalid ASP ID
107	Invalid Digital Signature
108	Minimum one document is required
109	Request exceeds Maximum number of documents allowed
110	Invalid Timestamp
111	Invalid Maximum Wait Period
112	Duplicate Transaction ID
113	User Timeout. Maximum Wait Time expired.
114	Authentication failed. User credentials invalid.
199	Unknown error / Custom error from ESP

5.2. eSign Document Level Response

Error Code	Error Message
201	Invalid Document Hash
202	Invalid response signature type
203	Invalid document URL
204	Invalid document information
205	Invalid hash algorithm
206	Document cancelled by user
299	Unknown error / Custom error from ESP

5.3. eSign Status Check Response

Error Code	Error Message
301	Invalid Request Format
302	Transaction number not found
303	Invalid Version
399	Unknown error / Custom error from ESP

5.4. Bank KYC XML

Error Code	Error Message
401	Invalid Bank KYC Request XML
402	Invalid Bank Digital Signature or Bank is not registered entity in the eKYC application
403	Invalid Version Number
404	Invalid Transaction Id (Either empty or size not acceptable by the application)
405	Duplicate Transaction Id
406	Invalid Bank IFSC Code (Empty or invalid format)
407	Invalid Bank Name (Not a registered bank or the bank name is not as per the RBI specifications)
408	KYC Information Missing
409	Invalid Common Name
410	Invalid Mobile Number
411	Invalid Email Id
412	Invalid Address
413	Invalid State/Province
414	Invalid Country
415	Invalid Postal Code
416	Invalid Date of Birth
417	Invalid PAN
418	Invalid Aadhaar
419	Invalid Photo Format provided
420	Invalid Photo (Either Missing or photo not as per the defined format in the request)
499	Unknown error / Custom error from eKYC Service Provider

5.5. Organization KYC XML

Error Code	Error Message
501	Invalid Org KYC Request XML
502	Invalid Organizational Digital Signature or Org is not registered entity in the eKYC application
503	Invalid Version Number
504	Invalid Transaction Id (Either empty or size not acceptable by the application)
505	Duplicate Transaction Id
506	Invalid KYC Org Id (either NULL or the Id is not valid in the application)
507	Invalid Organization Name
508	Invalid Organization Signatory Name
509	Invalid Organizational Signatory Certificate Identifier
510	KYC Information is Missing
511	Invalid Employee Id
512	Invalid Name
513	Invalid Mobile Number
514	Invalid Email Id
515	Invalid Date of Birth
516	Invalid Gender

517	Invalid PAN
518	Invalid Aadhaar
519	Invalid Photo Format
520	Invalid Photo (Either Missing or photo not as per the defined format in the request)
521	Invalid Physical Verification Tag or The Name mentioned in this text and the name provided in the tag doesn't match
599	Unknown error / Custom error from eKYC Service Provider

6. Change History

Change History			
Section	**Ver**	**Date**	**Modification**
3.3.1	3.0	18.01.2019	Request XML => "Signing Algorithm" parameter added
3.3.1.1	3.0	18.01.2019	Definition for " Signing Algorithm" added Definition change for "Response Signature Type"
4.3	3.0	18.01.2019	Maximum failed attempts specified (The audit logs ....limited to 5 attempts.)
5.1	3.0	18.01.2019	error message
3.3.1	3.0	22.02.2019	signerid row, under value Coloum, the following is inserted *"If mobile is the id-type, then mobile number should be same as in the eKYC XML"*
3.5	3.0	22.02.2019	In the XML Header, status="" is added and "err" replaced with "error
4.2	3.0	22.02.2019	In the eKYC response format, PAN="" DOB="" and Gender="" included
4.3.2	3.0	22.02.2019	In the response format description table (Element Name: kycData) PAN, DOB and Gender added
4.2.	3.1	03.05.2019	The Verified Source has been specified as Aadhaar Offline XML, Bank eKYC, organisational KYC Two additional fields Aadhaar number and eKYCtype have been added in Aadhaar Offline XML Two sections Bank eKYC and Organisational KYC have been added. The field name, description, source additional actions required for each field have been specified
4.3.2	3.1	03.05.2019	To record last four digit of Aadhaar number the parameter Aadhaar added To distinguish the type of eKYC , eKYCtype has been added
4.2	3.1	21.06.2019	Added the following sections to include the XML KYC Data Format for Aadhaar Offline XML, Bank eKYC and Organizational KYC 4.2.1.1. KYC Data Format and Verification Requirements for Aadhaar Offline XML 4.2.2.1. KYC Data Format and Verification Requirements for Bank eKYC 4.2.3.1. KYC Data Format and Verification Requirements for Organizational KYC
4.2.2 , 4.2.2.2	3.1	12.07.2019	Aadhaar Number, Bank Account Number and Bank IFSC Code have been included
4.2.2.3.	3.1	12.07.2019	A new section "KYC Response XML Structure" has been included

			for intermediate response
4.2.3	3.1	12.07.2019	Physical verification requirements have been specified. The fields Aadhaar Number, authorised signatory and certificate ID of designated authorised signatory of organization have been added
4.2.3.2.	3.1	12.07.2019	modified to include the new fields and physical verification requirements
4.2.3.3			A new section "KYC Response XML Structure" have been included for intermediate response
4.3.2.	3.1	12.07.2019	Included Organisation details XML, Bank details XML in the section "4.3.2. eKYC response format"
5.4, 5.5	3.1	12.07.2019	Error codes for the sections "5.4. Bank KYC XML & 5.5. Organization KYC XML" have been included.
4.2.4,4.2.5,4.2.6 & 4.2.6	3.2	05.09.2019	Added the following sections 4.2.4. Organisational KYC Option 2 (new) 4.2.5. KYC for Organisation and Authorised Signatory (new) 4.2.6. PAN KYC (new) 4.2.6. KYC for Foreign Applicants (new)
4.2.3	3.2	05.09.2019	Organisational KYC OPTION 1 Para 1 - included reference to the verification of existence of organisation and authorised signatory.
4.2	3.2	03.02.2020	Mobile number and PAN should be unique within Personal eKYC accounts.
3.3.1.1.	3.2	10.08.2020	In the value field of "responseSigType", added PKCS7pdf & PKCS7complete
3.3.1.1.	3.3	09.12.2020	InputHash- 5.responseSigType The signature should also be optionally time stamped ...
4.2.2.	3.3	09.12.2020	The Bank IFSC code has been made it as optional
4.2.3	3.3	09.12.2020	Deleted Organisational KYC OPTION 1(4.2.3 of eSign API 3.2)
4.2.4	3.3	09.12.2020	Renamed Organisational KYC OPTION 2 (4.2.4 of eSign API 3.2) to Organisational KYC(4.2.3)
4.2.4.3	3.3	09.12.2020	The section “Requirement of accepting external certificate for authorised signatory(4.2.4.3 of eSign API 3.2)” relating to Organisational KYC OPTION 1 has been deleted.
4.3 & 4.4	3.3	09.12.2020	4.3. Access to eKYC data(eSign API 3.2) has been moved to 4.4. Access to eKYC data (eSign 3.3)
4.3	3.3	09.12.2020	A new section "4.3. User Authentication Types" included and existing authentication types SMS-OTP, T-OTP and Mobile access token have been included as sub-sections. In the section 4.3, the options FIDO and Public Key Authentication are new.