e-authentication guidelines for

eSign- Online Electronic Signature Service

(Issued under Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015)

Version 1.7

27.01.2021

Controller of Certifying Authorities

Ministry of Electronics and Information Technology

Document Control

Document Name	e-authentication guidelines for eSign- Online Electronic Signature Service
Status	Release
Version	1.7
Last update	27 Jan 2021
Document Owner	Controller of Certifying Authorities, India

Table of contents

Terminologies

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

"eSign User or eKYC user or user or subscriber" is an Individual requesting for eSign online Electronic Signature Service of eSign Service provider

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

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

1. Introduction

Under the Information Technology Act, 2000 and Rules made thereunder, the Digital Signature Certificates (DSCs) are being issued by Certifying Authorities (CA) on successful verification of the identity and address credentials of the applicant. To begin with, these guidelines are intended to be operated by CAs for e-authentication service through e-KYC mentioned in the Second Schedule of Information Technology Act, 2000. CA may use the same physical infrastructure and manpower resources for e-authentication purposes. Security requirements for this service should be at the same level as being currently maintained by the CA. Further, the Audit of the e-authentication shall be included in the audit of CA facilities. The Trusted Third Party eSign-Online Electronic Signature Service of CA is referred as eSign Service Provider (ESP) in this document.

2. ESP Requirements

2.0 e-KYC Services Providers

The applicable e-KYC services provider for eSign are

1. UIDAI (Online Aadhaar e-KYC Services)
2. eSign User Account with CA (based on Offline Aadhaar e-KYC , Organisational KYC or Banking eKYC)

2.1 REQUIREMENTS FOR e-AUTHENTICATION USING e-KYC SERVICES

1) eSign user should have unique id
2) Application Service Provider should have gone through an approval process of ESP and should have agreement/undertaking with them.
3) ESP should adhere to e-KYC compliance requirements independently
4) eSign user Account with CA should be as per section 9

2.2 AUTHENTICATION AND DSC APPLICATION FORM

1) The mode of e-authentication should be biometric or OTP or PIN or combination of PIN and OTP in accordance with e-KYC Services

2) DSC application form is based on the digitally signed information received from e-KYC service provider. The digitally signed information from e-KYC services include name, address, email id, mobile phone number, photo etc of eSign user and response code.

3) The response code, should be recorded on the application form (Form C of Schedule IV) and included in the DSC as well.

4) The application form should programmatically be filled with the digitally signed information received from e-KYC services.

5) The filled-in application form should be preserved. The following events should be recorded
   - Authentication of user
   - Response received from e-KYC Services
   - Communication with CAs for Certificate issuance

6) The consent of the eSign user for getting a Digital Signature Certificate should be obtained electronically.

2.3 SECURITY PROCEDURE FOR KEY-PAIR GENERATION

1) ESP should facilitate generation of key pairs on their Hardware Security Module. The key pairs shall be unique to the eSign user. The private key will be destroyed after one time use

2) The private key of the eSign user shall be secured by Hardware security module (HSM) in accordance with FIPS 140-2 level 3 recommendations for Cryptographic Modules Validation List.

3) HSM of ESP should be separate from that of CAs for DSC issuance.

2.4 CERTIFICATE ISSUANCE

1) The validity of the certificate shall be not more than 30 minutes for one time use only so revocation and suspension services will not be applicable vis-à-vis such certificates.

2) On successful key generation (2.3 above), the Certificate Signing Request is sent to CA by ESP for issuing the DSC.

3) The DSC should be published in the Repository maintained

2.5 AUTHENTICATION OF ELECTRONIC RECORD BY APPLYING DIGITAL SIGNATURE

1) The consent of the eSign user for digital signing of electronic record would have already been obtained electronically. (ref 2.2(6) above)

2) eSign user should be given an option to reject the Digital Signature Certificate.

2.6 EVIDENCE REQUIREMENTS

1) Digital Signature Certificate issuance: Record all relevant information concerning the e-authentication of eSign user for generation of key pair and subsequent certification functions for a minimum period of 7 years (ref *The Information Technology (Certifying Authorities) Rules, 2000*, Rule 27), in particular for the purpose of providing evidence for certification purposes. Such electronic record should be preserved accordingly in secure environment.

2) Digital Signature creation: Record all relevant information concerning the e-authentication of eSign user for accessing the key pair for a minimum period of 7 years, in particular for the purpose of providing evidence of Digital signature creation. Such electronic record should be preserved accordingly in secure environment.

2.7 ESSENTIAL SECURITY REQUIREMENTS

1	**Identification and Authentication**
1.1	eSign xml request and response should be as per the eSign API specification.
	The communication between ASP and ESP should be secured (e.g. SSL, VPN, etc).
1.2	**eSign Request to ESP**
	The eSign xml request should be digitally signed prior to sending it to ESP.
	ESP should verify ASP's digital signature on each eSign xml request received
1.3	**e-KYC Request to** e-KYC provider
	The e-KYC request should be as per e-KYC provider's specifications
1.4	**e-KYC response to ESP**
	The e-KYC response shall be as per e-KYC provider's specifications
1.5	**Certification request to CA**
	ESP should form a digitally signed Certificate Generation Request with ESP's key prior to sending it to CA system.
	The CA system should accept only digitally signed Certificate Signing Request (CSR) from designated ESP systems over a secure link
1.6	**Certification response to ESP**
	CA system shall be configured to issue only e-KYC class end entity individual digital signature certificate(s).
1.7	**eSign Response**
	The eSign xml response formed by ESP should be digitally signed prior to sending it to ASP
1.8	**OTP request and Response**
	OTP request-should conform to e-KYC provider's OTP request API specifications.
2	**Domain Separation**
2.1	The ESP systems used for e-KYC service request and response should be different from ESP systems used to communicate with CA servers.
2.2	The eSign user key generation and management systems of ESP should be separate from CA systems in use for issuing end user certificate.
2.3	The CA system used for issuing e-KYC class based DSCs should be independent of CA systems used for other classes of DSCs.

3	Cryptographic Requirements
3.1	Key Generation for eSign user should happen on HSM and also should be secured by HSM
3.2	The private key of the user should be secured by Hardware security module (HSM) in accordance with FIPS 140-2 level 3 recommendations for Cryptographic Modules Validation List

2.8 PHYSICAL, PROCEDURAL AND PERSONNEL SECURITY

ESP should deploy trustworthy systems and employ trusted personal for eSign online electronic signature service.

3. Audit Logging Procedures

Audit log files shall be generated for all events relating to the security of the eSign-Online Electronic Signature Service. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with Section below.

3.1 Types of Events Recorded and Records Archival

All security auditing capabilities of the operating system and the applications required shall be enabled. As a result, most of the events identified in the table shall be automatically recorded. At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event):

1. The type of event,
2. The date and time the event occurred,
3. Success or failure where appropriate, and
4. The identity of the entity and/or operator that caused the event.

The following events shall be audited:

Auditable Event/Audit Criteria (ESP)
SECURITY AUDIT
Any changes to the Audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the Audit logs
LOGICAL ACCESS
Successful and unsuccessful attempts to assume a role
The value of *maximum number of authentication attempts* is changed
The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
An Administrator changes the type of authenticator, e.g., from a password to a biometric
KEY GENERATION
Generation of Signing Key Pair for eSign users
Deletion of key pair after signature
SECURING KEY

Auditable Event/Audit Criteria (ESP)
Securing eSign user Signing private key
Retrieval of eSign user Signing private key for usage
ESIGN ONLINE ELECTRONIC SIGNATURE SERVICES
All eSign Online Electronic Signature Signing requests received from ASP
All e-KYC response received from e-KYC Provider
All electronic DSC Application Form Generated
Proof of eSign user's consent for - key pair generation, - DSC application form submission to CA, -Generate CSR based on the digitally signed information received from e-KYC services -signature generation on the hash submitted
Mechanism Implemented for acceptance of DSC by eSign user
Communication to CA in respect of Certification.
Response sent to ASP
ESSENTIAL SECURITY REQUIREMENTS
Identification and Authentication as per 1 of 2.7
Domain Separation as per 2 of 2.7
Cryptographic Requirements 3. of 2.7
ACCOUNT ADMINISTRATION
Roles and users are added or deleted
The access control privileges of a user account or a role are modified
eSign Online Electronic Signature Service API
All changes to the eSign Online Electronic Signature Service API
MISCELLANEOUS
Appointment of an individual to a Trusted Role
Designation of personnel for multiparty control
Installation of the Operating System
Installation of the eSign Online Electronic Signature Service Application
Installation of hardware cryptographic modules
Removal of hardware cryptographic modules
Destruction of cryptographic modules
Zeroization of cryptographic modules
System Startup
Logon attempts to eSign Online Electronic Signature Service Application
Receipt of hardware / software
Attempts to set passwords
Attempts to modify passwords
Back up of the internal eSign Services database
Restoration from back up of the internal eSign Services database
File manipulation (e.g., creation, renaming, moving)
Access to the internal eSign Online Electronic Signature Service database
Re-key of the eSign Online Electronic Signature Service signing certificate
CONFIGURATION CHANGES
Hardware
Software
Operating System
Patches
Security Profiles
PHYSICAL ACCESS / SITE SECURITY

Auditable Event/Audit Criteria (ESP)
Personnel Access to room housing eSign- Online Electronic Signature Service
Access to the eSign- Online Electronic Signature Service
Known or suspected violations of physical security
ANOMALIES
Software error conditions
Software check integrity failures
Receipt of improper messages
Misrouted messages
Network attacks (suspected or confirmed)
Equipment failure
Electrical power outages
Uninterruptible Power Supply (UPS) failure
Obvious and significant network service or access failures
Violations of eSign- Online Electronic Signature Service

Auditable Event/ Audit Criteria(ESP)
REPORTS
Agreement between ESP e-KYC Provider and its Compliance audit report
Report of Vulnerability Assessment and Penetration Test
Agreement between ESP-ASP
Compliance audit report of ASP
Any other applicable agreements and its compliance reports

Apart from the auditing of CA in compliance with IT Act ,its rules, regulations and guidelines, the following events shall be audited in respect of eSign service:

Auditable Event/ Audit Criteria(CA)	
SECURITY AUDIT	
The isolation of CA system used for issuing e-KYC class from the CA system used for issuing other classes of DSCs as per 7(1)	
Digitally signed Certificate Signing Request (CSR) from ESP systems as mentioned as 7(2)	
Ensuring no DSCs other than e-KYC class of certificates are issued from ESP in accordance with 7(3)	
Secure communication between ESP and CA system as specified in 7(4)	

3.1.1 Frequency of Processing Audit Logs

Frequency of ESP audit log processing shall be in accordance with the requirements set for the CAs in Section 5.4.2 of the [CCACP].

3.1.2 Retention Period for Audit Logs

The minimum retention periods for archive data are listed below for the various assurance levels.

Assurance Level	Archive Retention Period
e-KYC Single Factor	7 Years
e-KYC Multi Factor	7 Years

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined. Applications required to process the archive data shall also be maintained for the minimum retention period specified above

3.1.3 Protection of Audit Logs

Protection of ESP audit log shall be in accordance with the requirements set for the CAs in Section 5.4.4 of the [CCA-CP].

3.1.4 Audit Log Backup Procedures

Audit logs and audit summaries shall be archived per Section 3.1.2

3.1.5 Audit Collection System (internal vs. external)

ESP audit collection requirements shall be in accordance with the requirements set for the CAs in Section 5.4.6 of the [CCA-CP].

3.2 Records Archival

3.2.1 Types of Records Archived

ESP's archival of records shall be sufficiently detailed to establish the proper operation of the ESP Service or the validity of any signature generated by ESP.

Data To Be Archived (CA Or ESP)
Contractual obligations
System and equipment configuration
Modifications and updates to system or configuration
eSign- Digital Signature signing requests
eSign user's Digital Signature and Certificate
Response received from e-KYC Services and DSC application form
Record of eSign- Digital Signature signing Re-key
All Audit Logs
All Audit Log Summaries
Other data or applications to verify archive contents
Compliance audit reports

3.2.2 Retention Period for Archive

The archive retention period for ESP Service shall be the same as those listed for CA in Section 5.5.2 of the [CCACP].

3.2.3 Protection of Archive

Protection of ESP Service archives shall be the same as those listed for CA in Section 5.5.3 of the [CCACP].

3.2.4 Archive Backup Procedures

No Stipulation.

3.2.5 Requirements for eSign- Online Electronic Signature Service records

Archived records shall be time stamped such that order of events can be determined.

3.2.6 Archive Collection System (internal or external)

No stipulation.

3.2.7 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby a ESP Service installation is physically damaged and all copies of the eSign-Online Electronic Signature Service Signing Key are destroyed as a result, the eSign- Online Electronic Signature Service shall reestablish services as soon as practical

3.2.8 Archival Format.

The Form C should be archived in machine readable or human readable format (XML or PDF) with a digital signature of ESP. The forms should be versioned and stored to provide a complete history of compliance.CA must have managed process for creating, maintaining, and verifying archive. The XML schema for archiving Form C is as given below

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<FormC>
   <ClassOfCertificate></ClassOfCertificate>
   <E-KYCResponseCode></E-KYCResponseCode>
   <ApplicationDate> </ApplicationDate>
   <ApplicantDetails>
      * <ApplicanteKYCID> </ApplicanteKYCID>
       <ApplicantName></ApplicantName>
       <ApplicantDOB></ApplicantDOB>
      <ApplicantGender></ApplicantGender>
       <ApplicantEmail> </ApplicantEmail>
       <ApplicantMobile> </ApplicantMobile>
       <ApplicantAddress> </ApplicantAddress>
       <ApplicantPhoto></ApplicantPhoto>
        <ApplicantPAN></ApplicantPAN>
   </ApplicantDetails>
   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
   </Signature>
</FormC>
```

- In case of Aadhaar , only Last four digit

4 eSign- Digital Signature Certificate and Profiles

4.1 eSign- Digital Signature Certificate Profile

eSign- Online Digital Signature Certificate profile is detailed in the CCA's Digital Signature Interoperability Guidelines document.

The end-user Digital Signature Certificates issued by CA should contain the following fields specific to eSign-Online Electronic Signature service along with other specified fields in IOG

Sn.	Attribute	Definition
1.	Common Name	"Name of the person as in e-KYC response "
2.	Pseudonym	Response code/e-KYC unique Number in the case of e-KYC Service (Mandatory) (2.5.4.65 - id-at-pseudonym)

5. eSign API

The communication between Application service provider and ESP should operate in accordance with eSign API Specifications to provide eSign- Online Electronic Signature Service

6. On-Boarding Process and Agreement

Any legal entity registered in India should refer to ASP On-Boarding Guidelines before applying to integrate eSign- Online Electronic Signature Service in their application. ASP should apply ESP for enabling online Electronic Signature on its application as per the application form mentioned in the ASP On-Boarding Guidelines. The ESP should allow access to ASPs only after fulfilling the criteria mentioned in the On-Boarding Guidelines. ESP should take an undertaking from ASP or an agreement should be executed between ESP and ASP. The template for the preparation of undertaking or agreement is available on the website.

7. CA REQUIREMENTS

1. The CA system used for issuing e-KYC class based DSCs should be independent of CA systems used for other classes of DSCs.
2. The CA system should accept only digitally signed Certificate Signing Request (CSR) from designated ESP systems over a secure link.
3. CA system shall be configured to issue only e-KYC class end entity individual digital signature certificates.
4. ESP shall be allowed access to CA systems only for submitting CSR for issuance of e-KYC classes of DSCs to be used for eSign.

8. eKYC Service modes

The eSign service will have two modes of verification of eSign user. Online Aadhaar eKYC authentication (API 2.x version) of eSign user is facilitated by CA. Offline Aadhaar eKYC authentication(API 3.x version) will be carried out by eSign user and authentication response will be submitted to CA. CA further confirm the submission and accept the same. Offline Aadhaar eKYC authentication of eSign user requires one time registration. The procedure to be followed for registration is given in the IVG section 5. The API specification for interface with ESP is specified under eSign API version 3.x. The eKYC accounts of registered and verified users are used for eSign.

9 CA eKYC Implementation Requirements

This section is applicable to CA that maintains eKYC accounts of registered users. ESP use registered & verified information of eSign user retained on eKYC system for eSign service. CA may also use the same verified user information for DSC issuance. In both cases, two factor authentications is required for CA or ESP to use the eKYC account holder's information retained in the eKYC account held by CA.

1	**Data Protection and Privacy**
1.1	**eKYC Data Protection**
	eKYC data protection should be part of the design and implementation of eKYC systems, services, products and practices.
1.2	**Privacy of eKYC Data**
	Ensure to process the data that is necessary to achieve specific eKYC user's account management & authentication. The eKYC user's account information should be used only for DSC issuance and authentication purpose only.
1.3	**Risk Assessment**
	Risk assessment of eKYC system should have carried out and security measures should be in place.
1.4	**Operational Requirements**
	The eKYC system should have made operational only after Risk assessment, VA/PT and Audit.
2	**Identification**
2.1	**Transaction ID**
	Generated by ASP calling the API, this is logged and returned in the output for correlation. Should be unique for the given ASP-ESP combination
2.2	**Response Code**
	Generated by ESP on eKYC user authentication request and should be a part of DSC . The Response Code should be of length 32.
2.3	**eKYC user ID**
	eSign signer can have one or more eKYC user account
3	**eKYC System security**
3.1	**Network Security**
	The e-KYC services systems (database) must be configured as secure systems as per the definitions of IT Act and should not have direct interface with system other than eKYC Server. The communication between eKYC server and e-KYC service systems (database) should be in request response mode.
3.2	**Dedicated for the Purpose**
	The CA e-KYC service systems should be dedicated only for e-KYC service purpose
4	**eKYC Account Management**
4.1	**eKYC User authentication**
	The authentication should be carried out using OTP sent to registered mobile eSign user and PIN.
	Access Token registered for the mobile Application based on OTP and PIN
4.2	**ESP e-KYC Request to CA e-KYC System**
	The e-KYC request should be as per the format specified in eSign API specifications
	ESP should send digitally signed eKYC Request with ESP's key.
4.3	**e-KYC response to ESP**
	The e-KYC response should be as per the format specified in eSign API specifications

	The response should be digitally signed using a CA eKYC System key
4.4	**OTP or Mobile Token Authentication**
	Each OTP or Mobile Token Response should be sent with purpose and Request and Response should be preserved.
4.5	**PIN Management**
	For PIN management, do not allow clear text transmission, storage or capture of passwords, maintain audit trails, and lock the account after repeated unsuccessful attempts.
	CA should implement mechanism for eKYC user to set eKYC user id and PIN. PIN shall be 6 characters in length
4.6	**Consent**
	The OTP and Mobile Access token verified along with PURPOSE text is deemed as consent.
5	**Audit Requirements**
5.1	**Audit Trail of Account Creation and Maintenance**
	The audit trail of eKYC account creation, modification, suspension, deletion etc should be maintained by CA with the details of authorised individual who carried out the operation. The date/time stamp, requested source details etc. also should be accessible for audit.
	A monthly audit of ten percent (subjected to maximum of 5000) of the eKYC account creation & modification should be carried out by an IS Auditor in the following month and the report should be made available during Annual CA compliance Audit.
6	**Account Monitoring**
6.1	**Account Monitoring facility to eKYC user**
	The history of eKYC account changes should be made available to eKYC users
	ESP should provide access to the signed transaction details to eSign users
	ASP should provide mechanism for viewing the signed documents to eSign users.

10 e-Authentication & Electronic Signature Guidelines for Remote Key-Storage

In order to provide the assurance of sole control over the private key of subscriber in a remote secure device, the authentication for activating the private key for signature function shall be secure and reliable. The authentication data shall be communicated to the HSM managing the private key in a secure manner. The authentication software/firmware shall be executed in the area protected by HSM securing the subscriber private key.

The requirements for creation, management and authentication to eKYC account of subscribers and signature creation based on the one time key pair generation and short validity certificates are specified in the earlier sections. This section is intend to specify the requirements for ESPs to act as a trusted third party for keeping the subscriber private keys and associated public key certificate. The deviation and additional requirements of subscriber private key life cycle management are described in this section. All other aspects relating to empanelment, signature generation, certificate & signature standards, are the same as eSign service for short validity certificate based electronic signature.

The overall functionality of the remote key-storage based solution is similar to EU standards (eIDAS, QSCD), however the actual implementation is specific to India PKI based on the architecture & protocol level implementation detailed in the eSign Remote API 1.0.

As in the case of crypto token, HSM based remote key-storage also shall use PIN as primary authentication. The additional modes of authentication shall be used at eKYC account level by CAs. The ESP/TTP shall use additional modes of authentication at application level before redirecting user to HSM secure key access environment.

This section also defines the security objectives and requirements for a Subscriber Authentication Module (SAM) to allow the private key of a subscriber to be remotely used to sign documents upon proper subscriber authentication. The key requirements are given below

10. 1 Security Procedure For Protection Of Subscriber's Key

1.	**HSM functionality**
1.	A Hardware Security Module (HSM) to ensure the security and subscriber control of private key. The HSM used for securing private keys of subscribers shall be at least FIPS 140-2 Level 3 validated/certified. In addition to generation, authentication, and usage of subscriber private keys, the HSM shall support SAM for secure execution of code .
2.	HSM shall be capable of implementing a secure channel establishment protocol stack for secure subscriber authentication data using secure communication protocol stacks like: TLS 1.2, TLS 1.3 or others offering similar or higher security.
3.	The HSM shall not permit export or output of subscriber private keys in any form except for the backup of the entire HSM.
4.	For synchronization of keys in HSM between Main and DR site, FIPS certified synchronization features of HSM shall be used.
2	**Subscriber Authentication Module (SAM)**
1.	Subscriber Authentication Module (SAM) is software which shall reside in the tamper proof environment protected by HSM. SAM shall utilize the secure channel interface through KMS to securely communicate with the subscribers, including the subscriber authentication.
2.	In the SAM, the software functions such as creation, destruction, signing, authentication shall be implemented as independent modules under an integrated module.
3.	The verification of authentication code must not be executed by any application other than that reside in SAM
4.	CA shall provide access to subscriber for key generation & setting Authpin only after the satisfactory completion of identity verification as per IVG.
5.	SAM shall verify the authentication of subscriber before facilitating any subscriber bound functions
6.	Subscriber actions such as communicating with the HSM for PKCS-10 request generation, obtaining the PKCS-10 from the HSM, and setting the Authpin shall be implemented in a single secure session thus providing binding among the subscriber, subscriber's key pair, and Authpin.
7.	HSM shall receive the authentication code submitted by subscribers in an encrypted form by the public key corresponding to the private key generated in the HSM.
8.	CA/ESP shall not deploy any software code components in the SAM which are not assessed by the empaneled experts.
9.	SAM shall perform authentication of end user using SHA-256 hash of Authpin and a random number of 128 bits or longer in accordance with RFC 2104. Alternative authentication protocols shall offer at least as much security

10.	The code to be deployed in the SAM shall be digitally signed by CA after security and software code level auditing to ensure security and reliability. The software testing shall be carried out by authorized cert-in empanelled experts. If the SAM functions are natively build in the HSM and certified , the same need not to be examined and tested by the empanelled experts.
11.	The logs of software changes / installations made in the SAM shall be archived.
12.	CA/ESP shall have dedicated Key Management Server (KMS) to interface with HSM/ SAM and the software module interfacing directly with HSM/SAM should host in KMS. All the communication to KMS server shall be in a request/response format.
3.0	**Key generation & management**
1.	The CA shall facilitate key pair generation by the subscriber under subscriber's direct control after successful authentication to eKYC account. The Authpin for subsequent successful authorization should be set by the subscriber.
2.	The HSM securing the private keys of subscribers shall be physically hosted in the CA premises or application owners premises however it should be under the sole administrative control of CA.
3.	The key generation shall be in the FIPS 140-2 Level 3 validated/certified HSM. Private keys shall always be secured by HSM.
4.	The HSM administrator of the hosting environment shall not be able to perform the subscriber's key authentication function.
5.	For any key management functions eKYC account id, eKYC account PIN and Authpin authentications shall be required.
6.	To ensure the centrally stored private key is bound to the subscriber, implement all subscriber actions such as communicating with the HSM for PKCS-10 generation, obtaining PKCS-10 from the HSM, and setting the Authpin in a single secure session. This secure session shall be available to the subscriber for key generation & setting Authpin only after the satisfactory completion of identity verification as per IVG
7.	The key management function by CA is limited only to deletion backup and restore
8.	The private key can be deleted by the subscriber directly or by CA as per the scenarios mentioned under CPS. i.e the private key shall be deleted after revocation.
9.	The private key shall not be retained by the HSM beyond the certificate validity period.
10.	The certificate renewal, re-key suspension etc., are not allowed under this scheme
4.0	**Authpin Authentication**
1.	SAM shall perform subscriber authentication related functions.
2.	Authpin for activation of the private key shall be stored along with eKYC id
3.	Authpin shall be 6 characters in length
4.	To protect the Authpin from exposure & binding to data to be signed, HSM shall use a secure session for submission of the data to be signed, once the Authpin authentication succeeds.
5.	The maximum number of consecutive Authpin retries shall be 10 after which the account shall be temporarily locked out for a period of no less than one hour or until HSM Trusted Administrator takes action. Upon three consecutive lockouts, the account shall be permanently locked out.
6.	Upon permanent locked out of account, CA should provide mechanism for resetting Authpin by the subscriber after a successful video verification of the subscriber
5	**Roles, privileges and access control**
1.	The following human users or IT entity with designated roles & privileges interact with SAM
2.	**Users** - the authorised and registered subscribers

3.	**HSM Administrator:** Handling software code, initialization of subscriber
4.	**Administrator** -security, user management and other administrative functions
5.	**Verification agent** - establishing the identity of the signatory, providing this data to the SAM ensuring it's integrity and initiating the lifecycle of the signatory account. Signatory account creation and initialization shall not allow without verification agent's authentication.
6.	**Auditor** -The auditor is in charge of performing the audit functions
6	**Software Modules**
1.	CA shall implement the following two software components in the CA systems for interfacing with HSM for management of eKYC account synchronization, key management, certificate management, Authpin management , and signature as per eSign Remote API 1.X
2.	**CHI-** eKYC account synchronization, key management, certificate management, Authpin management shall be managed by **CA-HSM Interface (CHI)** software module.
3.	**SHI-** The **Signing-HSM interface (SHI**) module shall interface with HSM for signature functionalities. The **SHI** module may be hosted in the CA or at trusted third party site.
4.	**AI-** CA shall implement **Authentication Interface(AI)** software component as per eSign API 1.x for interfacing with subscriber and HSM for authentication.
5.	All communication between CHI, SHI and AI shall be signed & encrypted through secure channel.
6.	CHI, SHI and AI modules shall be digitally signed by CA.

10.2 CA Requirements

The procedure to be followed for issuance of crypto token based certificates and eSign services are described/referred in the CPS. The following section will be used as a reference point in the CPS for certificate life cycle & signature service based on remote-key storage

1	**CA INFRASTRUCTURE**
	The CA system used for issuance of crypto token based DSC can be integrated with remote-key storage based DSC issuance .
2	**DSC Application Form**
2.1	**eKYC account**
	eKYC account maintained at CA/ESP is a prerequisite for remote key-storage of a subscriber.
2.2	**The DSC application form**
	The DSC application form for long term validity DSC issuance on remote key-storage of a subscriber shall be as per the CPS and Schedule IV of IT Act
2.3	**Response Code**
	Response code shall be generated by ESP on eKYC user authentication request for certificate generation and should be a part of DSC & DSC application form. The Response Code should be of length 32.
2.4	**eKYC user ID**
	eSign signer can have one or more eKYC user account
3	**Key Life cycle & Signature requirements**
	The key life cycle should be able to handle the following functions : 1. Creation of account in the protected storage area of HSM 2. Enrolment for authentication and signature service

	3. Key pair and certificate generation 4. Activation of signature service 5. Use of signature service 6. Deactivation of signature service 7. Deletion of the account created in the SAM
	For the certificate life cycle functions which involve HSM interaction, upon successful authentication to eKYC account by subscriber, CA redirect subscriber to HSM environment through CHI.
	The request/response between CA system and HSM environment shall be as per the eSign Remote API 1.X
3.1	**Certificate Issuance**
	eKYC account is pre-requisite for remote key storage. After success authentication to eKYC account by subscriber, CA redirect user to HSM environment for key generation, setting of Authpin, CSR generation, and verification of certificate details and download of certificate through CHI. CA shall ensure that all these actions are happening in a single secure session.
3.2	**Certificate Revocation**
	Subscriber requesting for revocation of shall be redirected to HSM environment through CHI for revocation of certificate. For self-revocation, the authentication to eKYC account is mandatory.
	The CA trusted persons are also be allowed to revoke after due verification of the as per the conditions and procedure specified under CPS
3.3	**Subscriber Signing**
	The Signing HSM Interface (SHI) module for subscriber signature function can reside at CA premises or trusted third party premises.
	The user shall authenticate to eKYC account in the case of SHI is hosted at CA and trusted third party application access account if it is hosted at trusted third party premises
	The SHI software component shall redirect subscriber to HSM environment as per the eSign API .0
4	**Audit Trail of Account Creation and Maintenance**
	The audit trail of certificate issuance, key generation, Authpin setting/reset , signature request/response etc should be maintained by CA. The date/time stamp, requested source details etc. also should be accessible for audit.
	A monthly audit of ten percent (subjected to maximum of 5000) of the certificate issuance, signature functions shall be carried out by an IS Auditor in the following month and the report shall be made available during Annual CA compliance Audit.
5	**Account Monitoring facility to eKYC user**
	The history of certificate issuance, setting PIN, & signature of documents shall be made available to subscribers.
	CA shall provide access to the signed transaction details to subscribers
	ASP should provide mechanism for viewing the signed documents to eSign users.

****

Change History

SL	DATE	SECTION	MODIFICATION
1	09.04.2015	2.3(2)	Existing: The private key of the subscriber shall be stored in Hardware security module (HSM) Modified: The private key of the subscriber shall be secured by Hardware security module (HSM)
2.	21.05.2015	7.	1.Existing: Prior to DSC issuance, CA systems should programmatically verify to confirm the DSC issued through Aadhaar e-KYC service is only for intended purpose and nothing else Modified: CA system shall be configured to issue only Aadhaar e-KYC class end entity individual digital signature certificates. 2.Existing: The CA system should accept only digitally signed Certificate Signing Request (CSR) from designated ESP systems over a dedicated link. Modified: The CA system should accept only digitally signed Certificate Signing Request (CSR) from designated ESP systems over a secure link.
3.	21.05.2015	2.7	Addition: 2.7 ESSENTIAL SECURITY REQUIREMENTS
4	21.05.2015	3.1	3.1 Types of Events Recorded CA & ESP Auditable events are separated
5	21.05.2015	2.6	2.6 EVIDENCE REQUIREMENTS Heading added
6	23.06.2015	2.7 - 1.6	Existing : Prior to DSC issuance and sending response to ESP, CA systems should programmatically verify to confirm the DSC issued through Aadhaar e-KYC service is only for intended purpose and nothing else Modified: CA system shall be configured to issue only Aadhaar e-KYC class end entity individual digital signature certificates.
7	23.06.2015	2.3 -1	Existing: The key pairs are generated after Aadhaar e-KYC based authentication which is unique to the subscriber. Modified: The key pairs shall be unique to the subscriber.
Version 1.0 to 1.2 –Modifications			
8	07.06.2016	3.1	In auditable events, the applicability columns have been deleted.
9	07.06.2016	3.1	Auditable Event/ Audit Criteria(ESP) reports added
10	07.06.2016	8	section 8 added
11	07.06.2016	2..7	ESSENTIAL SECURITY REQUIREMENTS 1.9.2, 1.9.3 deleted
12	07.06.2016	2.7	In 1.1, "The communication between ASP and ESP should be encrypted " modified to "The communication between ASP and

			ESP should be secured"
Version 1.2 to 1.3 –Modifications			
13	12.04.2017	Entire document	The reference to Aadhaar e-KYC provider has been generalized to e-KYC provider.
14	12.04.2017	Before Introduction	The terms "eSign", "eSign Service", "eSign User", "eKYC" and "response Code" have been introduced for uniform representations
15	12.04.2017	Entire document	The scope of on-boarding Guidelines and Agreement between ASP-ESP has been restricted only to the requirements of eSign online Electronic Signature Service
16	12.04.2017	2.0	The acceptable mode of e-KYC for eSign purpose has been mentioned in the e-Authentication Guidelines.
Version 1.3 to 1.4 –Modifications			
17	22.06.2018		3.2.8 Archival Format *<ApplicantAadhaar> </ApplicantAadhaar> * UID Token
18	22.06.2018	Version 1.4, 4.1	Added dnqualifier 4.1 eSign- Digital Signature Certificate Profile
19	22.06.2018	Version 1.4, Section 8.0	Removed 8.0 additional requirements for eSign service with organizational identity
Version 1.4 to 1.5–Modifications			
20	26.12.2018	Version 1.5, Section 8,0 & 9.0	Added 8.0 eKYC Service modes 9.0 CA eKYC Implementation Requirements Modified 4.1 eSign- Digital Signature Certificate Profile
Version 1.5 to 1.6 –Modifications			
21	03.05.2019	Section 2.0	Organisational KYC or Banking eKYC have been added
22	03.05.2019	Section 2.2	Generalized the requirements with respect to eKYC Modes
23	03.05.2019	Section 3.1.2	e-KYC – OTP & e-KYC – biometric has been modified to e-KYC Single Factor e-KYC – Multi Factor
24	03.05.2019	Section 3.2.8	<ApplicantAadhaarID> has been modified to </ApplicanteKYCID> DOB and PAN included
25	03.05.2019	Section 9 , 3.1	The text have been to modified for clarity
26	03.05.2019	Section 9 , 5.1	For the monthly audit of ten percent the maximum limit has been added (subjected to maximum of 5000)
Version 1.6 to 1.7 –Modifications			
27	27.01.2021	Section 10	New