e-authentication guidelines for

eSign- Online Electronic Signature Service

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

Version 1.4

22 June 2018

Controller of Certifying Authorities

Ministry of Communications and Information Technology

Document Control

Document Name	e-authentication guidelines for eSign- Online Electronic Signature Service
Status	Release
Version	1.4
Last update	22 June 2018
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" 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 is UIDAI (Aadhaar e-KYC Services)

2.1 REQUIREMENTS FOR e-AUTHENTICATION USING e-KYC SERVICES

1) eSign user should have unique e-KYC Number
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

2.2 AUTHENTICATION AND DSC APPLICATION FORM

1) The mode of e-authentication should be biometric or 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 contains name, address, email id(optional), mobile phone number (optional), 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
   - Response code
   - Authentication logs
   - 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 by CA.

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 request will 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**
	The ESP systems used for e-KYC service request and response should be different from ESP systems used to communicate with CA servers.
	The eSign user key generation and management systems of ESP should be separate from CA systems in use for issuing end user certificate.
	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**

	Key Generation for eSign user should happen on HSM and also should be secured by HSM
	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

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

Auditable Event/Audit Criteria (ESP)
Generation of Signing Key Pair for eSign users
Deletion of key pair after signature
SECURING KEY
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 Biometric/OTP 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

Auditable Event/Audit Criteria (ESP)
Patches
Security Profiles
PHYSICAL ACCESS / SITE SECURITY
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 - OTP	7 Years
e-KYC - biometric	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 3.2.1.

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>
     * <ApplicantAadhaar> </ApplicantAadhaar>
      <ApplicantName></ApplicantName>
      <ApplicantEmail> </ApplicantEmail>
      <ApplicantMobile> </ApplicantMobile>
      <ApplicantAddress> </ApplicantAddress>
      <ApplicantPhoto></ApplicantPhoto>
   </ApplicantDetails>
   <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
   </Signature>
</FormC>

*UID Token
```

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

Sn.	Attribute	Definition
1.	Common Name	"Name of the person as in e-KYC response "
2.	Unique Identifier	This attribute shall be used for SHA 256 hash of e-KYC ID for individuals
3.	Pseudonym	Response code/e-KYC unique Number in the case of e-KYC Service (Mandatory) (2.5.4.65 - id-at-pseudonym)
4.	DnQualifier	YOB+Gender+Hash of photograph (Mandatory) (2.5.4.46- id-at-dnQualifier)

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.

****

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.
17	22.06.2018	3.2.8 Archival Format	*<ApplicantAadhaar> </ApplicantAadhaar> * UID Token
18	22.06.2018	4.1 eSign- Digital Signature Certificate Profile	Added dnqualifier
19	22.06.2018	8.0 additional requirements for eSign service with organizational identity	Removed