# e-authentication guidelines for

# eSign- Online Electronic Signature Service

Version 1.0

June 2015

Controller of Certifying Authorities

Department of Electronics and Information Technology

Ministry of Communications and Information Technology

## Document Control

| | |
|---|---|
| Document Name | e-authentication guidelines for eSign- Online Electronic Signature Service |
| Status | Release |
| Version | 1.0 |
| Last update | 24 June 2015 |
| Document Owner | Controller of Certifying Authorities, India |

# Table of contents

## 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

### 2.1 REQUIREMENTS FOR e-AUTHENTICATION USING AADHAAR E-KYC SERVICES

1) e-authentication user should have 12 digit Aadhaar Number

2) Application Service Provider should have gone through an approval process of ESP and should have agreement between them.

3) ESP should function as AUA and e-KYC agent of UIDAI

### 2.2 AUTHENTICATION AND DSC APPLICATION FORM

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

2) Aadhaar e-KYC service should provide digitally signed information that contains name, address, email id(optional), mobile phone number (optional), photo and response code to applicant and the same should be shared with ESPs with the consent of applicant.

3) The response code, which is preserved online for six months from the date of its generation and further two years offline by UIDAI, should be recorded on the application form (Form C of Schedule IV) and included in the DSC as well.

4) DSC application form is to be electronically generated after successful authentication of DSC applicant by Aadhaar e-KYC services.

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

6) The filled-in application form should be preserved. The following events should be recorded
   - Response code (e-KYC)
   - Authentication logs
   - Communication with CAs for Certificate issuance
   - Activation mechanism for Digital Signature

7) The consent of the subscriber 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 subscriber. The private key will be destroyed after one time use

2) The private key of the subscriber 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 (III above), the Certificate Signing Request is sent to CA by ESP for issuing the DSC.

3) The DSC is published in the Repository maintained by CA.

2.5 AUTHENTICATION OF ELECTRONIC RECORD BY APPLYING DIGITAL SIGNATURE

1) The consent of the applicant for digital signing of electronic record would have already been obtained electronically. (ref II (7) above)

2) Subscriber 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 DSC applicant 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 subscriber for accessing the key pair for a minimum period of 2 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 encrypted (e.g. SSL, VPN, etc). |
| | Aadhaar OTP request can be made directly by ASP to UIDAI or via ESP. OTP request must comply with Aadhaar Request OTP API specifications. |
| **1.2** | **eSign Request to ESP** |
| | The Aadhaar number + biometric/OTP should be captured and encrypted by ASP front-end application into PID block and Aadhaar Auth XML must be formed as per UIDAI specifications |

| | |
|---|---|
| | The eSign xml request formed by ASP using the PID block should be digitally signed prior to send it to ESP eSign API |
| | ESP should verify ASP's digital signature on each eSign xml request received |
| **1.3** | **eKYC Request to UIDAI** |
| | The eKYC XML should be formed by ESP as per UIDAI eKYC specifications prior to sending it to KSA |
| | KSA should validate input and ensure Aadhaar eKYC API structure compliance before forwarding the KYC XML to Aadhaar KYC API |
| **1.4** | **eKYC response to ESP** |
| | After successful authentication of the Aadhaar holder by Aadhaar KYC service, the response containing demographic details and photograph in XML format should be digitally signed and encrypted by UIDAI as per Aadhaar eKYC 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 Aadhaar eKYC class end entity individual digital signature certificates. |
| **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 through ESP** |
| | OTP request, either sent directly or sent via ESP, shall conform to Aadhaar OTP request API specifications. |
| **1.9** | **Gateway options** |
| **1.9.1** | **eSign Request- ASP to Gateway** |
| | When gateway is used, ASP should send eSign API request XML signed using ASP's key . |
| **1.9.2** | **eSign Request- ESP to Gateway** |
| | After processing, eSign XML, the Gateway should forward eSign XML to ESP without modifications. If pin is present, it should be in unintelligible form |
| **1.9.3** | **eSign response - ESP to Gateway** |
| | When request is sent to ESP via gateway, ESP should sign the response prior to sending the response back to Gateway |
| **1.9.4** | **eSign response - Gateway to ASP** |
| | Gateway should forward response to ASP without any modifications |
| **2** | **Domain Separation** |

| | |
|---|---|
| | The ESP systems used for Aadhaar KYC service request and response should be different from ESP systems used to communicate with CA servers. |
| | The end 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 Aadhaar eKYC class based DSCs should be independent of CA systems used for other classes of DSCs. |
| **3** | **Cryptographic Requirements** |
| | Key Generation of 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 |
| | |

## 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 | X |
| Any attempt to delete or modify the Audit logs | X |
| **LOGICAL ACCESS** | |
| Successful and unsuccessful attempts to assume a role | X |
| The value of *maximum number of authentication attempts* is changed | X |
| The number of unsuccessful authentication attempts exceeds the *maximum authentication attempts* during user login | X |
| An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts | X |

| Auditable Event/Audit Criteria | ESP |
|---|---|
| An Administrator changes the type of authenticator, e.g., from a password to a biometric | X |
| **KEY GENERATION** | |
| Generation of Signing Key Pair for users | X |
| Deletion of key pair after signature | X |
| **SECURING KEY** | |
| Securing user Signing private key | X |
| Retrieval of user Signing private key for usage | X |
| **ESIGN- ONLINE ELECTRONIC SIGNATURE SERVICES** | |
| All eSign- Online Electronic Signature Signing requests received from ASP | X |
| All eSign- Online Electronic Signature Signing requests received from Gate way , if applicable | |
| All Biometric/OTP e-KYC response received from CIDR of UIDAI | X |
| All electronic DSC Application Form Generated | X |
| Proof of user's consent for<br>- Aadhaar authentication, key pair generation,<br>- DSC application form submission to CA,<br>-Generate CSR based on the digitally signed information received from Aadhaar e-KYC services<br>-signature generation on the hash submitted | X |
| - Mechanism Implemented for acceptance of DSC by subscriber | |
| - communication to CA in respect of Certification. | X |
| - response sent to ASP | X |
| - All response sent to Gateway if applicable | X |
| **ESSENTIAL SECURITY REQUIREMENTS** | |
| Identification and Authentication as per 1 of 2.7 | X |
| Domain Separation as per 2 of 2.7 | X |
| Cryptographic Requirements 3. of 2.7 | X |
| **ACCOUNT ADMINISTRATION** | |
| Roles and users are added or deleted | X |
| The access control privileges of a user account or a role are modified | X |
| eSign- Online Electronic Signature Service API | |
| All changes to the eSign- Online Electronic Signature Service API | X |
| **MISCELLANEOUS** | |
| Appointment of an individual to a Trusted Role | X |
| Designation of personnel for multiparty control | X |
| Installation of the Operating System | X |
| Installation of the eSign- Online Electronic Signature Service Application | X |
| Installation of hardware cryptographic modules | X |
| Removal of hardware cryptographic modules | X |
| Destruction of cryptographic modules | X |
| Zeroization of cryptographic modules | X |
| System Startup | X |
| Logon attempts to eSign- Online Electronic Signature Service Application | X |
| Receipt of hardware / software | X |
| Attempts to set passwords | X |
| Attempts to modify passwords | X |
| Back up of the internal eSign Services database | X |
| Restoration from back up of the internal eSign Services database | X |

| Auditable Event/Audit Criteria | ESP |
|---|---|
| File manipulation (e.g., creation, renaming, moving) | X |
| Access to the internal eSign- Online Electronic Signature Service database | X |
| Re-key of the eSign- Online Electronic Signature Service signing certificate | X |
| **CONFIGURATION CHANGES** | |
| Hardware | X |
| Software | X |
| Operating System | X |
| Patches | X |
| Security Profiles | X |
| **PHYSICAL ACCESS / SITE SECURITY** | |
| Personnel Access to room housing eSign- Online Electronic Signature Service | X |
| Access to the eSign- Online Electronic Signature Service | X |
| Known or suspected violations of physical security | X |
| **ANOMALIES** | |
| Software error conditions | X |
| Software check integrity failures | X |
| Receipt of improper messages | X |
| Misrouted messages | X |
| Network attacks (suspected or confirmed) | X |
| Equipment failure | X |
| Electrical power outages | X |
| Uninterruptible Power Supply (UPS) failure | X |
| Obvious and significant network service or access failures | X |
| Violations of eSign- Online Electronic Signature Service | X |

The audit carried out as a part of agreement between ESP and ASP & ESP and UIDAI should include all auditable events relating to ASP and Aadhaar eKYC . Compliance to the agreement between ESP and ASP & ESP and UIDAI should be verified as part of ESP audit.

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 Aadhaar eKYC class from the CA system used for issuing other classes of DSCs as per 7(1) | X |
| Digitally signed Certificate Signing Request (CSR) from ESP systems as mentioned as 7(2) | X |
| Ensuring no DSCs other than Aadhaar eKYC class of certificates are issued from ESP in accordance with 7(3) | X |
| Secure communication between ESP and CA system as specified in 7(4) | X |

### 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 |
|---|---|
| Aadhaar-eKYC - OTP | 7 Years |
| Aadhaar-eKYC - 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 [CCACP].

### 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 [CCACP].

## *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/ESP |
|---|---|
| Contractual obligations | X |
| System and equipment configuration | X |
| Modifications and updates to system or configuration | X |
| eSign- Digital Signature signing requests | X |
| User's Digital Signature and Certificate | X |
| Response received from Aadhaar e-KYC Services and DSC application form | X |
| Record of eSign- Digital Signature signing Re-key | X |
| All Audit Logs | X |
| All Audit Log Summaries | X |
| Other data or applications to verify archive contents | X |
| Compliance audit reports | X |

### 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>
   <EkycResponseCode></EkycResponseCode>
   <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>
```

## 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 Aadhaar e-KYC response " |
| 2. | Unique Identifier | This attribute shall be used for SHA 256 hash of Aadhaar ID for individuals |
| 3. | Pseudonym | Response code in the case of Aadhaar 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 on-boarding process manual 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 on-boarding process manual. The ESP should allow access to ASPs only after fulfilling the criteria mentioned in the on-boarding process manual. An agreement, as given in the on-boarding process manual, should be executed between ESP and ASP

**7. CA REQUIREMENTS**

1. The CA system used for issuing Aadhaar eKYC 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 Aadhaar eKYC class end entity individual digital signature certificates.
4. ESP shall be allowed access to CA systems only for submitting CSR for issuance of Aadhaar eKYC 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)<br>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 eKYC service is only for intended purpose and nothing else<br>Modified: CA system shall be configured to issue only Aadhaar eKYC class end entity individual digital signature certificates.<br>2.Existing: The CA system should accept only digitally signed Certificate Signing Request (CSR) from designated ESP systems over a dedicated link.<br>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<br>CA & ESP Auditable events are separated |
| 5 | 21.05.2015 | 2.6 | 2.6 EVIDENCE REQUIREMENTS<br>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 eKYC service is only for intended purpose and nothing else<br>Modified: CA system shall be configured to issue only Aadhaar eKYC class end entity individual digital signature certificates. |
| 7 | 23.06.2015 | 2.3 -1 | Existing: The key pairs are generated after Aadhaar eKYC based authentication which is unique to the subscriber.<br>Modified: The key pairs shall be unique to the subscriber. |