Certification Practice Statement (CPS)

By NSDL e-Governance Infrastructure Limited (NSDL e-Gov)

Version 1.0

Contents

Definitions

Any terms not specifically defined below in this section of this CPS or in CPS but defined in IT Act 2000 or Rules, Regulations and Guidelines notified thereunder will carry the same meaning as given in the said IT Act 2000 or Rules, Regulations and Guidelines. Any definition which is defined in IT Act will prevail over the definition given in this document.

- **Aadhaar Biometric:** Aadhaar Biometric shall mean biometric information of Aadhaar holder's collected using the finger print scanner or IRIS scanner by UIDAI for the purpose of authentication.
- **Aadhaar KYC or eKYC**: Aadhaar KYC or eKYC shall mean the transfer of demographic data (such as Name, Address, Date of Birth, Gender, Mobile number, Email address, etc.) and photograph collected by UIDAI in the form of a digitally signed XML document to a KYC User Agency, through an KYC Service Agency, based on resident authorization received by UIDAI in the form of successful biometric or OTP-based Aadhaar authentication.
- **Aadhaar OTP or OTP:** Aadhaar OTP or OTP shall mean one-time password sent to the Aadhaar holder's registered cell phone by UIDAI for the purpose of authentication.
- **Access Control:** The process of limiting access to the resources of a computer system only to authorized users, programs or other computer systems.
- **Applicant:** Applicant means a person, entity or organization that has requested for a digital signature.
- **Archive:** Archive is the process to store records and associated journals for a given period of time for security, backup, or auditing purposes.
- **ASP or Application Service Provider:** ASP or Application Service Provider is an organization or an entity using eSign service as part of their application to electronically sign the content.
- **Audit:** A procedure used to validate that controls are in place and adequate for their purposes. Includes recording and analyzing activities to detect intrusions or abuses into an information system. Inadequacies found by an audit are reported to appropriate management personnel.
- **Audit Trail:** A chronological record of system activities providing documentary evidence of processing that enables management staff to reconstruct, review, and examine the sequence of states and activities surrounding or leading to each event in the path of a transaction from its inception to output of final results.

- **Authentication:** A process used to confirm the identity of a person or to prove the integrity of specific information. Message authentication involves determining its source and verifying that it has not been modified or replaced in transit.
- **Authorization:** The granting of rights, including the ability to access specific information or resources.
- **Backup:** The process of copying critical information, data and software for the purpose of recovering essential processing back to the time the backup was taken.
- **CA or Certifying Authority:** An organization or an entity licensed under CCA for issuance of Digital Signature Certificate and carrying out CA operations.
- **CCA:** Controller of Certifying Authorities (CCA) is the entity who provides licence to Certifying Authority and regulates the working of Certifying Authorities and also to ensure that none of the provisions of the IT Act are violated.
- **CIDR:** Central Identities Data Repository (CIDR) is an infrastructure set-up by Government of India that stores and manages data for the Aadhaar. CIDR, is under the control of Unique Identification Authority of India (UIDAI), which is responsible for administration of Aadhaar enrollment and issuance process. It also provides the Authentication and eKYC services based on data hosted in CIDR.
- **CPS:** A statement issued by a Certifying Authority to specify the practices that the Certifying Authority employs in issuing Digital signature certificates.
- **CRL or Certificate Revocation List or Certificate Revocation:** CRL or Certificate Revocation List or Certificate Revocation means that a periodically (or exigently) issued list, digitally signed by a Certifying Authority, of identified Digital signature certificates that have been suspended or revoked prior to their expiration dates. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the suspended or revoked Digital signature certificates' serial numbers, and the specific times and reasons for suspension and revocation.
- **Digital Certificate or Digital Signature Certificate or DSC:** Digital Certificate or Digital Signature Certificate or DSC Means a Digital signature certificate issued under sub-section (4) of section 35 of the Information Technology Act, 2000.
- **Digital Signature:** Digital Signature Means authentication of any electronic record by a Subscriber by means of an electronic method or procedure in accordance with the provisions of section 3 of the Information Technology Act, 2000.
- **ESP or eSign Service Provider:** ESP or eSign Service Provider is a Trusted Third Party as per definitions of Second Schedule of Information Technology Act to provide eSign service.
- **IRIS –** IRIS recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on image of one or both Iris of an individual's eyes, whose complex random patterns are unique and stable This biometric attribute provide huge number unique combinations making a popular mechanism for biometric authentication.

- **Public Key Infrastructure or PKI:** The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of a Certificate-based public key cryptographic system. It includes a set of policies, processes, server platforms, software and workstations, used for the purpose of administering Digital signature certificates and keys.
- **Private Key:** The key of a key pair used to create a Digital Signature.
- **Public Key:** The key of a key pair used to verify a Digital Signature and listed in the Digital signature certificate.
- **Relying Party:** An entity that relies on the information provided in a valid Digital Signature Certificate and/ or any other information to verify and identify the public key of the subscriber.
- **Repository:** A database of Digital signature certificates and other relevant information accessible on-line.
- **Subscriber:** Subscriber means a person, entity or organization in whose name the Digital Signature Certificate (Digital certificate) is issued. Applicant becomes subscriber once Digital signature certificate is issued.
- **UIDAI or Aadhaar Agency:** UIDAI or Aadhaar Agency shall mean Unique Identification Authority of India or any of its successors in office. UIDAI has been set up with the mandate of issuing unique identification numbers, i.e., "Aadhaar Numbers" to the residents of India, based on their biometric and demographic information.
- **X-509 Version 3 digital Certificate:** The ITU-T (International Telecommunications Union-T) standard for Digital signature certificates. X.509 v3 refers to Certificates containing or capable of containing extensions.

1. Introduction

Certification Practice Statement (CPS) of NSDL e-Governance Infrastructure Limited, Certifying Authority (NSDL e-Gov CA), has been drafted taking reference from (1) RFC 2527 - Internet X.509 PKI Certificate Policy (2) Certificate Practice Framework guidelines and (3) Guidelines for submission of application for license to operate as Certifying Authority (CA) under Indian IT Act 2000 as amended up-to-date and the accompanying Rules and Regulations, (hereinafter referred to as "IT Act"). This document adheres to the specific requirement as mentioned in the e-authentication/ e-signing technique using Aadhaar KYC Services in India. Controller of Certifying Authority issues licence to the entities applying to become Certifying Authority and grants permission to operate as per the published CPS.

1.1. Overview

NSDL e-Governance Infrastructure Limited (NSDL e-Gov) has achieved and delivered path breaking success in the area of e-Governance solutions and services, through automation of large government processes. The solutions are customised using appropriate technology so that the fundamental aim of governments i.e., of delivering benefits to the society at large is fulfilled efficiently while ensuring that the solution are cost effective, highly secure, scalable, requiring very minimal Time-to-market and efficient in terms of quality and performance. The services include Business Process (Re) Engineering, Solution Architecture, Designing, Developing and managing such System, Project and Change Management, Quality Management, User Enablement, Process training etc.

I. eSign service of ESP is legally acceptable under the provisions of Indian IT Act 2000 and various Rules and Regulations as amended from time to time.
II. 'NSDL e-Gov CA' will act as an eSign Service Provider (ESP) to entities registered as an ASP with NSDL e-Gov and the services that will be provided by NSDL e-Gov as an ESP is a part of the Certification Practice Statement (CPS) document.
III. NSDL e-Gov CA setup is to issue Aadhaar based Digital Signature Certificate (DSC) as per X.509 version 3 format in as per the Guidelines issued by CCA, for the limited purpose of eSign services to various users.
IV. NSDL e-Gov CA & ESP setup is complying with the below provisions;
    a. IT Act, Rules and Regulations including Schedule II & Schedule III of Rule 19(2) of IT Act
    b. Guidelines issued by CCA of India
    c. e-Authentication guidelines of the CCA as published at URL http://cca.gov.in/cca/sites/default/files/files/e-AuthenticationGuidelines.pdf

V. NSDL e-Gov, through its eSign services initiative will facilitate the valid Aadhaar holders to authenticate with Central Identities Data Repository (CIDR) through NSDL e-Gov or Application Service Provider's KUA and after successful authentication (OTP/ Biometric) will allow the user to ascribe Electronic Signature on the documents/ transaction on real time basis.

VI. This CPS document is intended to legally bind all the participating entities such as applicants, subscriber, Application Service Provider (ASP) and relying parties. This CPS details the rights and obligations of all entities participating in the issuance and usage of Aadhaar based DSC. This CPS also provides a detailed statement of operational procedures and guidelines of the NSDL e-Gov CA.

VII. This CPS explains the Certification process and Certificate life cycle of NSDL e-Gov CA as an eSign Service Provider (ESP) which starts with the process of application for the services, exchange of data between relying parties, and the treatment given to the Certificate after the limited validity is over.

VIII. NSDL e-Gov offers option of "eSigning" the transaction/ document, after successful e-KYC verification of the individual who is desirous to apply eSign. NSDL e-Gov will allow e-KYC using both the modalities i.e. Capturing Biometric Data (Fingerprint/ Iris scan) OR capturing OTP received by the end user on their Mobile Number linked to their Aadhaar.

IX. Adhering to the CCA e-authentication guidelines, Aadhaar based DSC will be generated and offered with limited time validity so as to be used for one time signing. As soon as the transaction is signed NSDL e-Gov ESP will delete/ destroy the Private Key. DSC can continue to be used for verification.

X. More information, related to PKI, DSC and e-signature can be obtained from NSDL e-Gov portal for eSign (https://egov-nsdl.co.in/eSign) as well as on the website of CCA (www.cca.gov.in).

XI. Electronic Copy of CPS document of NSDL e-Gov CA is available on NSDL e-Gov portal / websites for eSign (https://egov-nsdl.co.in/eSign/CPS).

1.2. Identification

This CPS is identified as NSDL e-Governance Infrastructure Limited – Certifying Authority Certification Practice Statement or NSDL e-Gov CA CPS document.

1.3. Community and Applicability

The CPS is applicable to all the entities / stake holders as given below:

1.3.1 NSDL e-Gov Certifying Authority (CA)

NSDL e-Gov CA is the licensed CA by CCA under the IT Act 2000 who shall provide Aadhaar based Digital Signature Certificate (DSC) as per X.509 version 3, for the limited purpose of eSign services to various users. Individuals applying to avail eSign services from NSDL e-Gov CA can digitally sign their electronic document after successful e-KYC authentication. NSDL e-Gov is trusted CA under Root Certifying Authority of India (RCAI) to issue the Aadhaar based DSC directly without any involvement of sub-CA or sub-RA.

1.3.2 End Entity

Details of the end entities are as mentioned below;

Sr. No.	End Entity	Details of the End Entity
1	Applicant	An entity with valid Aadhaar who applies for a Digital Signature Certificate by providing consent to NSDL e-Gov CA (e-Sign Service Provider (ESP)) for the facilitation of key pair generation
2	Subscriber	The applicant status is changed to Subscriber after receiving the Aadhaar based DSC and its acceptance of the contents of certificate constitutes acceptance of the certificate
3	Relying Party	An entity that relies either on the information provided in a valid Aadhaar based DSC issued by NSDL e-Gov CA and/ or any other information provided in the NSDL e-Gov CA Repository to verify and identify the public key of the subscriber

1.3.3 End-user Aadhaar

Aadhaar of the user will be authenticated based on the biometric information of the applicant or OTP (One Time Password) which is sent to the registered mobile number of the applicant. KYC of the Aadhaar holder shall be verified by UIDAI through e-KYC services for which explicit consent of the user shall be obtained and subsequently the Aadhaar based DSC will be issued by NSDL e-Gov CA. To substantiate, the application form will be attached with the unique transaction number received from UIDAI to suffice as proof of identity and address verification.

1.3.4 Application Service Provider

Application Service Provider (ASP), will facilitate the eSign modality of document/ form/ data signing to the end-user by integrating their Application with ESP application. This will be done based on the standard API / Web-services published by eSign application of NSDL e-Gov CA and in adherence to the standards notified by governing entities such as CCA or UIDAI. ASP will ensure that necessarily the request is sent and response received in a manner that is prescribed for this operation and necessary steps taken for the same will be in adherence to the "ASP On boarding Guidelines Document" (published by NSDL e-Gov CA. ASP will also obtain necessary consent from the end-user that it is obliged to provide before availing this service. ASP will provide facility to capture Biometric or OTP for Aadhaar authentication and e-KYC of the end-user. ASP will ensure the retention of the logs as per the provisions of IT-Act 2000 and amendments effected on it by Government of India.

1.4. Applicability

NSDL e-Gov CA CPS will be applicable to all the entities such as CA, Aadhaar, Subscriber, Application Service Provider and Relying Parties and it documents the lawful use of Aadhaar based DSC. The Aadhaar based DSC issued by NSDL e-Gov CA are intended to support the Assurance of the identity of Aadhaar holder and Message integrity.

NSDL e-Gov CA shall not be responsible for any liabilities howsoever arising from the use of any certificate unless NSDL e-Gov CA has expressly undertaken such liabilities in this CPS.

1.5. Contact Information

a. **CPS Administration** – This CPS is administered by NSDL e-Governance Infrastructure Ltd. – Certifying Authority. CPS shall be revised as and when needed and will be adopted only after the approval from NSDL e-Gov management and CCA.

b. NSDL e-Governance Infrastructure Limited – Certifying Authority can be contacted at the address as mentioned below;

NSDL e-Gov Infrastructure Limited (NSDL e-Gov),
1st Floor, Times Tower,
Kamala Mills Compound, Senapati Bapat Marg,
Lower Parel (West), Mumbai - 400013
Phone: (+91 22 40904200), Fax: (+91 22 24915217)
Email: esign@nsdl.co.in

c. For more information or for feedback:
   - Visit NSDL e-Gov CA portal at https://egov-nsdl.co.in/eSign
   - Contact eSign helpdesk at eSign-help@nsdl.co.in

2. General Provisions

This section sets forth the various obligations, liabilities, responsibilities, and financial and legal considerations associated with the use of NSDL e-Gov CA.

2.1 Obligations

2.1.1 CA Obligations

a) NSDL e-Gov CA shall act in accordance with the policies and procedures designed to safeguard the end-user and offer a secured Aadhaar based DSC generation and management process.

b) NSDL e-Gov CA shall secure and safeguard the PKI key (Public and Private Keys) infrastructure deployed for NSDL e-Gov CA operations and protect NSDL e-Gov CA private key from mis-use and any kind of compromise.

c) NSDL e-Gov CA, after completion of Aadhaar based authentication and e-KYC and generating key pair of public key and private key, will issue a corresponding DSC to ESP who, on behalf of the end-user, sign the document hash.

d) NSDL e-Gov CA shall not be responsible or liable for any loss, damage or penalty resulting from delay or failure in performance in resulting from events like but not limited to such as acts of God, strikes, or other labor disputes, riots, civil disturbances, Software/ Hardware/ equipment/ device/ communication failures/ malfunctioning/ bugs / viruses, actions or inactions of suppliers, war, fire, explosion, earthquake, flood or other catastrophes. In any of the aforementioned events, NSDL e-Gov CA shall for the duration of such event be relieved of any and all obligations, responsibilities, duties and liabilities covered in this CPS.

2.1.2 Obligations of Subscriber / end-user

The Subscriber/ end-user shall have the following obligations:

a) Provide Subscriber's/ end-user's own valid Aadhaar number without any errors, omissions or misrepresentations in the application.

b) Subscriber / end-user shall ensure that his mobile number and e-mail ID is registered with UIDAI to receive the OTP generated by UIDAI for successful OTP based authentication.

c) Subscriber/ end-user shall accept and abide by the policies and procedures as specified in this CPS.

d) Provide the consent directly or through ASP, to NSDL e-Gov, which is providing the eSign service of NSDL e-Gov CA:

   i. to generate the key pair on behalf of the end-user
   ii. to obtain eKYC details from Aadhaar holder,
   iii. use applicant's private key for signing of the applicant's document hash and
   iv. to include necessary information obtained from eKYC for inclusion in the Digital Signature Certificate.

e) Under the terms and provisions of this CPS which are binding on the Subscriber/ End-user, each of the certificates issued is personal to the respective Subscriber/ end-user.

2.1.3 Obligation of Registration Authority

The issuance of Aadhaar based DSC is subject to successful electronic authentication of applicant by Aadhaar eKYC service either using OTP or Biometric mode of authentication. No authorities are engaged by NSDL e-Gov CA for the registration of eSign service and therefore there shall be no entity acting in the capacity of Registration Authority (RA).

2.1.4 Obligation of Relying Party

The relying party shall have following obligations:

a) Any Relying Party seeking to rely upon Aadhaar based DSC is solely responsible for deciding whether or not to rely upon the said Aadhaar based DSC.

b) The Relying Party should be aware that, the Aadhaar based DSC used for eSigning of Document or transaction was issued after successful electronic authentication of applicant by Aadhaar e-KYC service either using OTP or Biometric mode of authentication or adhering to the guidelines issued by UIDAI.

c) Relying Parties must verify the Aadhaar based DSC and its chain of trust and only on successful verification should rely on the certificate.

2.1.5 Obligation of Application Service Provider

Application Service Provider will integrate their Application Services with eSign Service offered by NSDL e-Gov CA, in accordance with the ASP Onboarding process which is formulated by NSDL e-Gov CA adhering the various guidelines and rules applicable for eSign & CA services.

Application Service Provider is obliged to obtain consent of the end-user before it subjects the transaction of end-user for eSignature process. This will include but not limited to consent for Aadhaar based authentication using Biometric or OTP, consent for using Aadhaar authentication for e-KYC purpose, consent for using e-KYC data for formation of CSR and generating DSC, consent for using DSC to sign the document/ form/ transaction hash on behalf of end-user, consent for accepting and adhering to all the rules and guidelines stated in CPS document.

2.1.6 Obligation of Repository

As a CA repository, NSDL e-Gov CA shall publish the NSDL-CA CPS. NSDL e-Gov CA will also publish the CRLs as per the requirement which would include the CRL with NIL records. NSDL e-Gov CA will also publish the changes / updates that may be effected in the CPS and also publish the updated consolidated version of the CPS as and when any such change is affected.

2.2 Liabilities

2.2.1 Liability of CA

a) NSDL e-Gov CA shall not be liable, for any certificates obtained from it, by representing any false or erroneous or misleading information and / or unauthorized use of the Aadhaar either through OTP or biometric authentication.

b) NSDL e-Gov CA will not be responsible for failures that may take place during the Aadhaar based authentication and eSign process, including but not limited to, failures as a result of, false reject, network, or connectivity failure, device failure, software failure, OTP not received by end-user, possible down time or rejection of Aadhaar authentication by UIDAI due to technical problem of CIDR.

c) Warranties and Limitations on Warranties – NSDL e-Gov does not give any kind of warranties about its CA services. NSDL e-Gov hereby disclaims all warranties and conditions, either express, implied or statutory, including, but not limited to, any (if any) implied warranties or conditions of merchantability of fitness for a particular purpose, of lack of viruses, of accuracy or completeness of responses, of results, and of lack of negligence or lack of reasonable care or workmanlike effort, all with regard to its services. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NON-INFRINGEMENT WITH REGARD TO THE SOFTWARE / SYSTEM/ SERVICES.

d) Services provided by NSDL e-Gov CA is based on reasonable effort basis. Unless otherwise specifically stated in this CPS, NSDL e-Gov including its affiliates, shareholders, officers, directors, employees, agents, representatives etc. shall not be responsible and liable under tort/ contract or any legal theory, to end-users/ subscriber or any other person who avail/ facilitate/ operate/ access or otherwise connect/ communicate for NSDL e-Gov CA services for any actual/ anticipated/ threatened direct, indirect, consequential, remote loss/ damage of any kind including but not limited to loss of data, loss of goodwill, loss of profits, loss of business, loss of opportunities, loss of reputation etc., caused by whatever acts/ omissions/ failures/ defaults/ negligence etc., of NSDL e-Gov including its affiliates, shareholders, officers, directors, employees, agents, representatives etc.

e) Loss Limitations – Notwithstanding anything contained herein, NSDL e-Gov CA's liability under any circumstances/ situations shall not exceed the net surplus generated by it out of the particular transaction resulting into alleged loss to claimant user of NSDL e-Gov CA service. Net Surplus will be the positive balance amount arrived at after deducting total expenditure from the fees collected in respect of the particular transaction.

f) Force Majeure – NSDL e-Gov shall not be liable for any loss, delay, damage or other casualty suffered or incurred by any person due to failure to perform/ delayed performance of obligations owing to earthquakes, floods, fires, explosions, acts of God, acts of State, war, terrorism, action of any governmental authority or any other cause, which is beyond the reasonable control of NSDL e-Gov.

g) NSDL e-Gov shall not responsible and liable for any errors/ mistakes in Aadhaar based DSC or other outputs/ documents, not attributable to NSDL e-Gov.

2.2.2 Liability of Subscriber

a) **End-user / Subscriber Warranties**

End-user / Subscribers warrant that:

- The End-user / Subscriber has provided true and accurate information about his/her Aadhaar.
- The Aadhaar based DSC obtained by the end-user / subscriber is only used for eSigning of the document/ transaction as permitted under applicable laws.
- The End-user/ Subscriber provided a free consent, without any external coercion, willfully and voluntarily, for using their Aadhaar, Biometric or OTP and eKYC information for the purpose of eSign services.

b) **Private Key Compromise (PKC) -** Not applicable

c) **End-user / Subscriber-** shall be liable for submission/ obtaining NSDL e-Gov CA service for any material/ contents/ documents which are wrong/ incomplete /incorrect /inaccurate /insufficient /inappropriate /illegal /immoral /unethical or infringing upon third person's intellectual property, for e-sign purposes.

2.2.3 Liability of Relying Party

Relying Parties are solely responsible for verifying, deciding and taking an informed decision with respect to the information in a certificate, and to rely or not to rely on such information, and that they shall bear all the consequences.

2.2.4 Liability of Application Service Provider

Application Service Provider will be solely responsible to ensure that end-user / subscriber of application services provides the consent for eSign process, as detailed in CPS. Application Service Provider will be liable for any mis-use or fraud happening due to any loopholes / application or infrastructure security lapses / unauthorised access happening in their Application. ASP shall be responsible and liable for all financial and other consequences arising out of or incidental to such actions/omissions by ASP and for breach of any of the obligations /responsibilities /duties /performance of ASP and NSDL e-Gov shall not be responsible and liable for the actions/ omissions/ performance/ non-performance/ under-performance/ part-performance/ defaults/ failures/ lapses etc. of ASP

2.3 Financial Responsibility

2.3.1 Financial Responsibility of NSDL e-Gov CA

a) NSDL e-Gov CA shall not be responsible and liable for any direct, indirect, consequential, remote loss/damage of any kind arising out of any contract/tort or under any legal theory, including but not limited to loss of data, loss of goodwill, loss of profits, loss of business, loss of opportunities, loss of health, loss of reputation etc., even if NSDL e-Gov CA has been advised of the possibility of such damages.

b) Any Limited Warranty, if any, referenced above is the only express warranty made to end-user / subscriber and Relying party and is provided in lieu of any other express /implied warranties (if any) created by any documentation. Except for such Limited Warranty, NSDL e-Gov CA hereby disclaims all other warranties and conditions, either express, implied or statutory, including, but not limited to, any (if any) implied warranties or conditions of merchantability of fitness for

a particular purpose, of lack of viruses, of accuracy or completeness of responses, of results, and of lack of negligence or lack of reasonable care or workmanlike effort, all with regard to its services. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NON-INFRINGEMENT WITH REGARD TO THE SERVICES Subject to the above exceptions, the entire risk as to the TRANSACATION of or arising out of the use or performance of the e-Sign/ CA services by NSDL e-Gov shall not remain with NSDL e-Gov CA.

c) NSDL e-Gov CA does not make any representation OR give any warranties on the financial transactions, which the end-users/ subscribers and the relying parties undergo using the e-sign obtained from the NSDL e-Gov CA using the e-authentication and e-signing techniques described in the CPS. The subscribers and the relying parties shall be solely and exclusively responsible and liable for any losses, damages or any consequences due to such transactions.

d) NSDL e-Gov CA cannot be held liable if the Application Service Provider or end-user/ subscriber use the eSign services after making false / incorrect declaration/ claims there by leading to financial losses for themselves or for other parties relying on the eSignature provided by NSDL e-Gov CA.

2.3.2 Independent Parties

NSDL e-Gov CA does not have any relation of agents or fiduciaries or trustees with the end-user / Subscriber / Relying Party. The relationship between NSDL e-Gov CA and end-user / Subscriber and that between NSDL e-Gov CA and Relying Party are not that of an agent and principal. Neither end-user nor Subscriber nor Relying Party have any authority to bind NSDL e-Gov CA, by contract or otherwise, to any obligation. NSDL e-Gov CA does not make any representations to the contrary, either expressly, implicitly, by appearance or otherwise. NSDL e-Gov CA, Aadhaar Subscriber and Relying Party are totally independent parties and not agent/representative/subcontractor of each other.

2.3.3 Administrative Processes

NSDL e-Gov CA has implemented and deployed the functional processes for its limited purpose CA functions which are reviewed, audited and approved periodically.

2.4 Interpretation and Enforcement

NSDL e-Gov CA has documented administrative, technical and physical security and operational policies, procedures and standards for the CA Operations as per IT

Act, 2000 as amended from time to time and Rules & Regulations notified thereunder as applicable.

2.4.1 Governing Laws

NSDL e-Gov CA will be governed by IT Act, 2000 and Rules & Regulations notified thereunder and the rules and regulations and guidelines specified by CCA from time to time.

2.4.2 Severability of Provisions, Survival, Merger & Notices

a) **Severability of Provisions:** While interpreting the clauses of this CPS, if any clause is found to be severable from the rest of the clauses in the document, the invalidity of such clause shall not affect the validity of the other clauses in the document.

b) **Survival:** Clauses of confidentiality obligations, Audit, Obligations of NSDL e-Gov CA, Subscriber and Relying party(ies) and limitations thereof, Liability of NSDL e-Gov CA, Subscriber and Relying party(ies) shall survive expiry/ termination of this CPS.

c) **Merger:** In the event of merger of NSDL e-Gov CA with any other entity, all rights and obligations of NSDL e-Gov CA shall vest in the acquiring or new entity created by merger.

d) **Notice:** Any notice or other communication which subscriber/ Relying Party is required under this CPS to serve on NSDL e-Gov CA shall be sufficiently served if sent to the address as specified in this CPS either;

- by hand;
- by applicable full postage paid courier/registered/speed post acknowledgement due or;
- by facsimile or electronic mail transmission confirmed by registered/speed post acknowledgement due within 48 hours of transmission.

Notices are deemed to have been served as follows:

- delivered by hand; on the day when they are actually received,
- sent by the registered post or sent by facsimile or electronic mail; on the day of transmission if transmitted before 17.00 hours on the working day, but otherwise 10.00 hours on the following working day, provided in each case that the required confirmation is sent as mentioned above.

  Address:

  NSDL e-Gov Infrastructure Limited (NSDL e-Gov),
  1st Floor, Times Tower, Kamala Mills Compound,
  Senapati Bapat Marg, Lower Parel (West), Mumbai - 400066
  Phone: (+91 22 40904200), Fax: (+91 22 24915217)
  Email: esign@nsdl.co.in

e) No waiver of any provisions of this CPS by either party shall be effective unless made in writing. Any waiver of any term or condition of this CPS shall not be deemed or construed to be a waiver of such term of condition for the future, or any subsequent breach thereof.

2.4.3 Dispute Resolution

a) For any disputes based on the contents of this CPS, the aggrieved party shall intimate NSDL e-Gov CA either through e-mail or post or officially registered courier who provides Proof of Delivery (POD) for the delivered packages. NSDL e-Gov will take necessary steps for resolution of dispute. If the dispute is not resolved within (30) business working days after initial notice as above, then aggrieved party shall have the right to ask for face to face meeting NSDL e-Gov CA officials at NSDL e-Gov CA registered office address indicated in this CPS or any other NSDL e-Gov office that is mutually agreed between the NSDL e-Gov CA and end-user / subscriber. NSDL e-Gov will not refuse or unreasonably delay meeting requested by the aggrieved party due to non-receipt of any response to its communication related to dispute about the contents of the CPS.

b) If the dispute cannot be amicably resolved by the parties as mentioned in point 2.4.3-a, then the matter will be referred to the Controller of Certifying Authorities (CCA). The CCA is competent under the IT Act, Section 18 (l), to resolve any dispute between Certifying Authorities and Subscribers.

c) This Agreement shall be governed by the laws of India and the parties hereby submit to the exclusive jurisdiction of the Indian courts in Mumbai.

2.5 Fees

2.5.1 Certificate Issuance

Services will be chargeable to End-user / Subscribers and all such other parties, either directly or to Application Service Provider on behalf of end-user / subscriber, for availing the NSDL e-Gov CA services. All End-user / Subscribers or the Application Service Provider and all such other parties shall be obliged to pay to NSDL e-Gov CA such charges in accordance with its Schedule of Fees and at such times as may be prescribed by NSDL e-Gov CA published on NSDL e-Gov CA website (https://egov-nsdl.co.in/eSign/) from time to time.

2.5.2 Certificate Access Fees

NSDL e-Gov CA reserves rights to apply slab based charges as well as block / mass discounted charges and change the charge for the service with immediate effect. Such charge structure arrived by NSDL e-Gov on case to case basis would not be necessarily published on its website, however the standard changes in charge structure for base / standard charges will be effected by notification on its website (https://egov-nsdl.co.in/eSign/).

2.5.3 Revocation or Status Information Access Fees

At present, this is not applicable as NSDL e-Gov CA will issue DSCs only through and for the purpose of its eSign service and such DSC will be issued with validity of not more than thirty (30) minutes from the time of its generation.

2.5.4 Fees for Other Services such as Policy Information

At present, online Access to CPS is given free of charge. However, NSDL e-Gov CA reserves right to charge this service with effect from the date of notification on its website (https://egov-nsdl.co.in/eSign/).

2.5.5 Refund Policy

No refund shall be given by NSDL e-Gov of any fees/ amounts paid to NSDL e-Gov towards Aadhaar based DSC or other services.

NSDL e-Gov CA has absolute right at its sole discretion to refuse to issue a certificate without assigning any reason. In such case, NSDL e-Gov shall not incur any responsibility/ liability arising out of or incidental to such refusal. However, in the event of such refusal, NSDL e-Gov CA will refund the fee received by it from any end-user / subscriber towards Aadhaar based DSC; provided that end-user / subscriber has not submitted any untrue / false / fraudulent / incorrect / misleading / misrepresenting / wrong / non-admissible / incomplete / insufficient information to UIDAI / NSDL e-Gov CA to complete the process of eSignature.

2.6 Publication and Repositories

NSDL e-Gov CA shall maintain the repository to store information relevant to the operations of the NSDL e-Gov CA Public Key infrastructure Services under the NSDL e-Gov CA. All information and modification are published in the repository to provide the updated information. This information is subject to changes and any such changes shall be published in the repository as detailed in this CPS. NSDL e-Gov CA reserves rights to not to publish any information that NSDL e-Gov CA considers as confidential or not to be disclosed due to the sensitivity of the information or as required under applicable law.

2.6.1 Publication of CA Information

a) All the information as mentioned below is published on NSDL e-Gov CA repository at (https://egov-nsdl.co.in/eSign/)

- The NSDL e-Gov CA Certification Practice Statement
- The Digital Signature Certificates and public keys of NSDL e-Gov CA
- Certification Revocation List - CRL will be published and updated periodically.
- Standard Fee structures of the various services

2.6.2 Frequency of Publication

NSDL e-Gov CA CPS is published as per the policy set forth in the Section 8 of this CPS.

2.6.3 Access Control

NSDL e-Gov CA CPS is published on NSDL e-Gov CA portal and is accessible to everyone. The CPS and CRLs in the electronic repository are restricted from unauthorized modification.

2.7 Compliance Audit

NSDL e-Gov CA shall be audited for compliance with the procedures specified in the NSDL e-Gov CPS and IT Act 2000 and its associated rules, regulations and amendments as applicable.

2.7.1 Frequency of Compliance Audit

The compliance audit of NSDL e-Gov CA Audit shall be performed on annual basis as per Rule 31 (1) of the IT (Certifying Authorities) Rules, 2000.
In addition, periodic internal audits shall be conducted every six months, to ensure the compliance.

2.7.2 Identity/ Qualifications of Auditor

Annual audit shall be performed by an external auditor who has been empanelled by the CCA.

2.7.3 Auditor's Relationship to Audited Party

The auditor or its audit firm involved in the audit process shall be independent of NSDL e-Gov and will not have other business dealings with NSDL e-Gov.

2.7.4 Topics covered by Audit

The half yearly Internal audit and Annual audit shall include following;

- Security Policy and planning
- Physical & Environmental Security
- NSDL e-Gov CA PKI operations management
- Compliance to relevant CPS
- Regulations prescribed by Controller
- IT Act 2000 rules, regulations and guidelines
- Relevant Contracts/ Agreements

2.7.5 Actions taken as Result of Deficiency

On receipt of the audit findings reported by auditor, the NSDL e-Gov CA shall take preventive and corrective actions to correct the deficiency within reasonable timeframes. NSDL e-Gov CA officials identified to act on the auditor report shall record and report the action taken along with observation closure statement to NSDL e-Gov CA management. If necessary, a report will be submitted to NSDL e-Gov Board / Board appointed committee / Audit committee or Sr. Management highlighting the audit observations, Root Cause Analysis, Closure / Corrective action and preventive measures, where applicable.

2.7.6 Communication of Audit Results

NSDL e-Gov CA or Auditor shall submit compliance audit results to CCA office within four weeks of completion of audit.

NSDL e-Gov reserves the right to share the audit results as may be required by law or by a competent regulatory authority or to any party as deemed fit.

2.8 Confidentiality

2.8.1 Types of Information to be kept Confidential

The following records of Subscribers are kept confidential and private;

a) Agreements related to NSDL e-Gov CA
b) Information pertaining to NSDL e-Sign/ CA Application
c) Transactional records (Full or audit trail of it)
d) System/ Application/ Network Event Logs
e) Access details of end-user / subscriber
f) Access to Audit Report and any classified and sensitive information pertaining to NSDL e-Gov CA and the Subscriber
g) Business Contingency/ Disaster Recovery Plan
h) NSDL e-Gov eSign Infrastructure/ Application/ Administration & Management Information
i) Security measures controlling the operations of NSDL e-Gov eSign services hardware and software and the administration of eSign/ Certificate services
j) Any other records / data / information mandated to be kept confidential and private by the IT Act 2000, its associated Rules and Regulations
k) Confidential information such as classified and sensitive information and information provided by the Subscriber shall not be disclosed to any party, unless the information is required to be disclosed under the law or a court order or for audit purpose

2.8.2 Types of Information not Considered Confidential

The types of information that are not considered confidential include;

a) Information contained in Subscriber's Certificate
b) Information included in CRL
c) NSDL e-Gov CA CPS published on NSDL e-Gov CA Portal

2.8.3 Disclosure of Certificate Revocation Information

NSDL e-Gov CA shall publish the Certificate Revocation List (CRL) details in NSDL e-Gov CA website portal.

2.8.4 Release to Law Enforcement Officials

NSDL e-Gov CA shall release the confidential information to law enforcement officials in compliance to an order from a Court or Tribunal or any Government or public authority having the power to compel the disclosure and in this scenario, such action shall be without any liability on NSDL e-Gov and also shall not be treated/ considered/ deemed as breach of confidentiality obligations by NSDL e-Gov, its directors or officers.

2.8.5 Release as Part of Civil Discovery

NSDL e-Gov CA may disclose confidential information during any judicial, arbitration, litigation or administrative proceedings and in this scenario, such action shall be without any liability on NSDL e-Gov and also shall not be treated/ considered/ deemed as breach of confidentiality obligations.

2.8.6 Disclosure upon end-user / Subscriber's Request

NSDL e-Gov CA shall disclose to the end-user / Subscriber, any information pertaining only to the said end-user / Subscriber, and only on receiving such request from that end-user / Subscriber along with the reason and justification for seeking such information. NSDL e-Gov CA acknowledges that it is obliged to keep such information confidential and hence after disclosing such information to the end-user / subscriber on his request, NSDL e-Gov CA shall not be liable for any loss arising out of such disclosure. NSDL e-Gov CA also reserves the right to deny such information disclosure to end-user / Subscriber if it finds the cause / reason / justification sited by the end-user / Subscriber not adequate enough for such information disclosure. In such case the end-user / client may have to obtain appropriate order from competent authority and approach NSDL e-Gov CA for disclosure based on such Order.

2.8.7 Other Information Release Circumstances

NSDL e-Gov CA may at its sole discretion and on case to case basis, charge a fees towards disclosure service availed by end-user / subscriber. Information would be disclosed only after receiving such payment by NSDL e-Gov CA.

NSDL e-Gov CA shall release the confidential information in compliance to request or order from CCA. This may be performed without any prior permission of the end-user / subscriber to whom such confidential information refers and in such scenario NSDL e-Gov CA shall not be liable for any legal actions or any financial penalty.

2.9 Intellectual Property Rights

NSDL e-Gov CA reserves its intellectual property rights (IPR) of NSDL e-Gov CA processes, practices, methods deployed by it for operations of CA set-up, CPS and other documentation.

3 Identification & Authentication

3.1 Initial Registration

As a part of initial e-Signing process, the applicant shall submit his valid and correct Aadhaar number details in the application form provided by ASP and authenticate either through OTP or biometric authentication method.

3.1.1 Type of Names

All names issued by NSDL e-Gov CA, in the Aadhaar based DSC, shall follow X.500 Naming Conventions and guidelines published by CCA, if any. Aadhaar based DSC shall contain the Distinguished Names (DN) as available in CIDR shall be used in Aadhaar based DSC to facilitate the identities of subscribers.

The following fields in Distinguished Name are mandatory in the case of eSign Service of NSDL e-Gov CA:

X509 Attribute	Details
CommonName	Name of the person as in Aadhaar e-KYC response
Unique Identifier	SHA 256 Hash of Aadhaar ID for individuals
Pseudonym	Response code in the case of Aadhaar e-KYC Service

3.1.2 Need for names to be meaningful

The names used shall identify the applicant or Subscriber in a meaningful way as the KYC details of the subscriber is verified by CIDR through OTP or biometric authentication.

3.1.3 Rules for Interpreting Various Name Forms

As NSDL e-Gov CA is providing eSign services to Subscribers and issue Aadhaar based DSC which as per CCA e-authentication guidelines, mandates to use Aadhaar Identification Number as Unique Identifier, to make the subscriber name unambiguous and unique.

3.2 Routine Rekey and renewal process

As Aadhaar based DSC issued by NSDL e-Gov will be for short term validity of thirty minutes only hence there will not be any renewal process applicable for the subscriber. However, NSDL e-Gov CA shall renew its public and private key pairs within permissible time limits before the date of expiry.

4 Operational Requirements

4.1 Certificate Application

4.1.1 Classes of Certificate

NSDL e-Gov CA offers the following class of certificates for eSign Service purpose only within its Certification Practice Statement:

Class	Assurance	Applicability	Suggested Use
Aadhaar-eKYC – OTP	Aadhaar OTP class of DSC shall be issued to an individual based on successful OTP authentication of the subscriber through Aadhaar eKYC. This class of certificates confirms that Aadhaar information of the subscriber is same as that in Aadhaar database.	Applicable where Aadhaar based OTP authentication of e-KYC for authenticating Aadhaar id holder. DSC will be issued subject to successful verification of OTP authentication and private keys of Aadhaar based DSC will be destroyed immediately after usage by subscriber.	Document signing
Aadhaar-eKYC-Biometric	Aadhaar Biometric class of DSC shall be issued to an individual based on successful Biometric authentication of the subscriber through Aadhaar eKYC. These certificates will confirm that Aadhaar information of the subscriber is same as that in Aadhaar database.	Applicable where Aadhaar based Biometric authentication of e-KYC for authenticating Aadhaar id holder. DSC will be issued subject to successful verification of Biometric authentication and private keys of Aadhaar based DSC will be destroyed immediately after usage by subscriber.	Banking, , Capital Market, Financial transactions etc.

4.1.2 Certificate Application Process

Aadhaar based DSC can be requested to NSDL e-Gov eSign services through its registered Application Service Providers (ASP).

As a part of ASP onboarding process, ASP is required to submit the ESP application form and supporting documents and execute a bi-partite agreement with NSDL e-Gov for availing eSign service.

ASP will make request on behalf of the end-user / Subscriber using eSign API as published in http://cca.gov.in/eSign and the onboarding guidelines document provided by NSDL e-Gov ESP. As a part of eSign service, ASP shall capture the Aadhaar of the subscriber and authenticate the details with CIDR and shall forward the same to NSDL e-Gov ESP as a part of eSign API XML. Each eSign XML request coming from ASP is authenticated by ESP by using DSC of ASP.

The ASP shall also obtain the consent of end-user/ subscriber for facilitating key pair generation, generation of dynamic application form with the DSC applicant's demographic information received from Aadhaar eKYC service, request for DSC to NSDL e-Gov CA on the behalf of the end-user / subscriber. On successful authentication of the end-user / subscriber using Aadhaar eKYC services, the key pairs generation and populating demographic details into DSC application form, a CSR will be generated and send to NSDL e-Gov CA for certification.

4.2 Certificate Issuance

4.2.1 Certificate issuance process

NSDL e-Gov is providing eSign services anyone eligible of availing this service as per the e-authentication guidelines of CCA. Certificate issuance process involves e-authentication and Aadhaar e-KYC verification of end-user / subscriber though CIDR. The following process will be followed for issuance of Aadhaar based DSC by NSDL e-Gov CA:

(a) End-user will visit the portal of ASP and provide his Aadhaar number and the document/ transaction that needs to be signed
(b) ASP offers the applicant the option of eSigning their transaction/ document.
(c) If applicant accepts this offer, ASP will ask the applicant to provide consent for Certificate generation and eSigning their document / transaction.
(d) Based on the online consent from end-user, ASP will securely log the same and create the document/ transaction hash (to be signed) on behalf of the end-user.
(e) Verification (Aadhaar based) can be done either by capturing Biometric Data (Fingerprint/ IRIS) through a device approved by UIDAI and obtaining authentication through UIDAI (through their ASP) or capture the OTP received by the end-user from UIDAI if their mobile number is registered with their Aadhaar in CIDR.
(f) ASP will generate the input data string, Digitally Sign using its DSC and provide to NSDL e-Gov ESP.
(g) NSDL e-Gov ESP will authenticate the ASP application, performs validation and performs e-KYC through CIDR for successful e-KYC of the applicant.

(h) On successful verification from CIDR, NSDL e-Gov ESP will generate creates a fresh key pair and CSR for applicant and using NSDL e-Gov CA service issue Aadhaar based DSC which is valid for limited time and of a Special Class Signature Certificate, which has embedded within it, AADHAAR number, Name of the Aadhaar holder, eKYC response code, Authentication Type, and Time Stamp.

(i) NSDL e-Gov ESP signs the 'document hash' and provides Document Signature and the end-users Public Key to the ASP. On receipt of Aadhaar based DSC, ASP shall offer the end user to accept the transaction.

(j) On acceptance by end-user, ASP attaches the signature to the document

Note: NSDL e-Gov ESP will delete/ destroy the Private Key as soon as the transaction is signed. For any reason, if there is a need to re-sign the same transaction, separate request would be initiated by ASP and fresh key pair would be used.

4.2.2 Approval / Rejection of Certificate Application

(a) After the successful validation of applicant's Aadhaar through CIDR, key pair generation and DSC application form generation, the DSC application is deemed as approved and the CSR is submitted to issue DSC.

(b) NSDL e-Gov reserves the right to reject the application where the Aadhaar authentication has failed or where vital information of applicant is not available in CIDR. Corresponding notification will be informed to the applicant through eSign application response.

4.2.3 CA's representations to Subscriber

NSDL e-Gov CA warrants to the subscriber named in the certificate that unless otherwise expressly provided in this CPS or mutually agreed upon–

(a) Name in Aadhaar based DSC is same as received through CIDR

(b) No misrepresentations of fact in the certificate known to or originated from NSDL e-Gov CA have been made at the time of certificate issuance

(c) Reasonable care has been taken in creation of Aadhaar based DSC by means of reliable processes and as per requirements of this CPS and any amendments made thereto are compiled with by NSDL e-Gov CA. Aadhaar based DSC complies with requirements of the IT Act 2000.

(d) After signing of the document/ transaction hash, NSDL e-Gov shall delete the key pair immediately. The logs for the DSC issuance process shall be kept for a period of seven years.

(e) NSDL e-Gov CA has no knowledge of any material fact, which had it been included in the digital signature certificate would adversely affect the reliability of the above-mentioned representations.

4.2.4 CA's representations to Relying Parties

(a) NSDL e-Gov CA warrants to all who reasonably rely as mentioned in this CPS on Aadhaar based DSC verifiable by the public key listed in the certificate that it is consistent with this CPS.

(b) The accuracy of verified information in or incorporated by reference within the certificate is assured, and NSDL e-Gov CA has complied with the CPS and IT Act 2000 when issuing the certificate.

4.2.5 Limitations on NSDL e-Gov CA Representations

NSDL e-Gov CA expressly prohibits any user, certificate applicant, subscriber, relying party, Aadhaar or any other party to monitor, interfere, with or reverse engineer the technical implementation of NSDL e-Gov CA eSign service except as explicitly permitted by this CPS or upon prior written approval from NSDL e-Gov CA. Any act in contravention of above will be subject to punitive action under the Indian Laws.

4.2.6 Right to Investigate Compromises

NSDL e-Gov CA may, but is not obligated to, investigate all compromises arising from use of Aadhaar based DSC provided that such investigations will comply with all applicable privacy and data protection laws of the Republic of India.

4.3 Certificate Download and Acceptance

Aadhaar based DSC is deemed to be accepted by the subscriber once;

- Subscriber provides the consent for use of Aadhaar details for eKYC
- Submit the request for eSigning of Aadhaar based DSC
- Receipt of certificate and agreeing on the contents of DSC

4.4 Certificate Revocation List (CRL)

NSDL e-Gov CA does not revoke any Aadhaar based DSCs issued through NSDL e-Gov eSign service as they are having thirty minutes validity. However, NSDL e-Gov CA publishes CRLs on their portal and as per the requirement of IT Act 2000.

4.5 System Security Audit Procedures

4.5.1 Types of Event Recorded (Audit)

NSDL e-Gov CA shall maintain the security events manually or electronically for audit trail as per the requirements in compliance with IT Act 2000. These events include, but are not limited to:

No	Type	Details
1	Security Audit	• Any changes to the audit parameters, e.g., audit frequency, type of events audited • Any attempt to delete or modify the audit logs
2	Identity proofing	• User provisioning
3	Key generation	• All certificate creation parameters
4	Certificate signing	• All certificate PKCS#10 requests signing
5	Account administration	• Roles and users are added, disabled and deleted • The access control privileges of user account or a role are modified
6	Configuration changes	• Hardware • Software • Firmware • Operating System • Patches • Security profiles • Network level Changes
7	Physical security/ Site security	• Personnel Access to room housing component • Access to the CA component • Known or suspected violations of physical security • Temperature and Humidity • Application/ System crash events

4.5.2 Frequency of Audit Log processing

NSDL e-Gov CA ensures that its audit logs are reviewed by authorized official periodically and all significant events are captured in an audit log summary and required action is taken and documented.

4.5.3 Retention Period for Audit Log

NSDL e-Gov CA shall retain its audit logs for at least seven years. However, NSDL e-Gov CA may also retain logs for longer duration depending on the prevailing legal requirements, customer request or for any other consideration which will be non-obligatory on NSDL e-Gov.

4.5.4 Protection of Audit Logs

Audit logs can only be viewed or deleted by the designated trusted administrators of the system. The administrator will also do the needful only based on approval which will have to be obtained for each activity and every time. Audit logs will be stored in a manner that it will not be tampered. Unauthorized access to the audit logs are restricted by physical and logical access control systems.

4.5.5 Audit Log Backup Procedures

NSDL e-Gov CA shall take backup of audit files on periodic basis on physical removable media as per the backup policy and stored at secured location with access is limited to restricted authorized trusted personal only. The control measures of backup processes are audited as per this CPS.

4.5.6 Vulnerability Assessments

Vulnerability assessments shall be performed, reviewed on half yearly basis to identify internal and external threats. NSDL e-Gov CA authorized trusted administrator shall be taking required action to mitigate and close the vulnerability reported.

4.6 Records Archival and Retention period

NSDL e-Gov CA shall record and archive "Audit Event Logs" as per the provisions of IT Act 2000, Rules and Regulations.

4.6.1 Protection of Archive

NSDL e-Gov CA shall protect archive which contains the critical "Audit Events logs" and access to such data is restricted to trusted administrator officials only.

4.6.2 Archive Backup

NSDL e-Gov CA shall keep the copy of all archive records and critical audit logs in backup media as per the backup policy. Such logs shall be kept at at-least three different locations in fire proof cabinet. NSDL e-Gov CA shall verify the integrity of the archive backups at least every six months and record for such verification will be maintained.

4.7 Key Changeover

The NSDL e-Gov CA, keys and certificate shall be changed at the time of expiry/ renewal as stipulated by the IT Act 2000 and the Key change shall be processed as per Key Generation specified in this CPS.

4.8 Compromise and Disaster Recovery

NSDL e-Gov CA maintains the offsite data backup of data and information and has implemented detailed disaster recovery plans and procedures. In event of NSDL e-Gov CA key compromise, authorized trusted administrator and NSDL e-Gov management will act as per the business continuity and disaster recovery plan which has been approved by NSDL e-Gov Management.

4.8.1 Recovery Procedures used if CA Certificate is revoked

As NSDL e-Gov is providing the CA services for the purpose of providing eSign services, hence revocation of subscriber certificate is not applicable as the Aadhaar based DSC has the short time validity of thirty minutes only.

However, NSDL e-Gov CA will provide prior notice in case of its own CA certificate is revoked and the notice will be posted on NSDL e-Gov eSign Service portal (www.esign-nsdl.com). Root cause analysis for such incidence will be done and recorded. After the investigation and analysis of root cause analysis, remediation steps shall be taken and recorded, to avoid the similar incidences in the future.

In case of the NSDL e-Gov CA's private key being compromised, NSDL e-Gov CA shall immediately inform the CCA and shall obtain new certificate from CCA.

4.8.2 Business Continuity and Disaster Recovery

NSDL e-Gov CA has established and implemented the Disaster Recovery and Business Continuity Plan. And as per the plan, all business critical data and information is sent to Disaster Recovery Site.

In an event of disaster at primary site, NSDL e-Gov authorized trusted personal and management shall invoke the plan and operate as per this plan.

4.9 CA Services Termination

NSDL e-Gov CA shall reserve right to terminate the CA operations and in such scenario, NSDL e-Gov CA shall ensure safe keeping of archival of its records and Certificates as per provisions of IT Act 2000, Rules, Regulations and Guidelines as may be applicable. NSDL e-Gov CA shall ensure following;

(a) Shall provide advance notice of ninety days to CCA with its reason to stop acting as a Certifying Authority.
(b) Shall provide notice of ninety days to all ASPs intimating them that NSDL e-Gov will not be acting as Certifying Authority.
(c) Shall make best effort before discontinuing its CA services to ensure minimal disruption to its subscribers and relying parties.
(d) Shall preserve records related to NSDL e-Gov CA for the period of seven years after discontinuing its CA services.
(e) Shall destroy its own CA Certificate signing private key after the date of expiry mentioned in the license or intimation and confirm the date and time of destruction of the private key to the CCA.

4.10 Residual clause:

Any terms not specifically defined in this CPS but defined in IT Act 2000 or Rules, Regulations and Guidelines notified thereunder will carry the same meaning as given in the said IT Act 2000 or Rules, Regulations and Guidelines.

5 Physical, Procedural, and Personnel Security Controls

NSDL e-Gov CA has implemented physical, environmental and personnel security controls in order to perform secure operations of certificate operations like authentication, key generation, certificate issuance, certificate revocation, audit and archival.

NSDL e-Gov shall ensure that it's Physical Infrastructure used for CA at Primary site and disaster recovery site and its repository is fully secured as per requirements stipulated under the provisions of IT Act 2000, Rules, Regulations and Guidelines.

5.1 Physical Security Controls

5.1.1 Site Location and Construction

NSDL e-Gov CA shall provide its CA services from their datacenter which is physically secured to prevent unauthorized handling of sensitive personal data. The physical security standards are designed as per physical and operational security guidelines mentioned in the Information Technology Act, 2000 and IT (CA) Rules, 2000 (Schedule II).

5.1.2 Physical access

Necessary physical security controls to restrict access to physical premises, relevant network, hardware and Software of NSDL e-Gov CA setup, has been implemented by and is being actively monitored on 24x7 basis and reviewed (by audit process) on periodic basis. Physical security is enforced in the facility by putting in place a set of controls through implementation of policies administrative procedures, use of biometric systems, access cards etc.

Access to the site is restricted to authorized officials only on need basis and the same is logged and reviewed. Further, Persons visiting the NSDL e-Gov data center facility are always escorted by authorized official after requisite approval and the same is recorded.

5.1.3 Power Supply and Air Conditioning

NSDL e-Gov datacenter facility has Primary and backup power systems/ sources with UPS system with adequate backup for power are deployed for protection against power outages. Further the datacenter temperature and relative humidity is monitored and controlled on a regular basis by using the HVAC equipment.

5.1.4 Water exposures

NSDL e-Gov datacenter facility has been constructed to minimize the risk of the threats related to water. Datacenter facility of NSDL e-Gov CA/ eSign services has the raised floor within entire datacenter area. Further the Water leakage sensors are placed below the floor to detect the water leakage. Any water leakage incident will be sensed by these sensors and they will raise an alarm to provide the warning to Datacenter operations staff.

Further to address water flood situation at their primary datacenter location, the NSDL e-Gov CA/ eSign operations can be shifted to disaster recovery site.

5.1.5 Fire prevention and protection

NSDL e-Gov datacenter facility has been constructed to minimize the risk of the threats related to Fire and adequate fire detection equipment like Smoke Detectors, Very Early Smoke Detection Alarm (VESDA) system is in place. Further, for Fire Protection Fire extinguishers, FM 200 Gas protection system has been implemented.

5.1.6 Media storage

NSDL e-Gov CA has implemented the controls as per the provisions of IT Act 2000, Rules, Regulations and Guidelines as applicable that their critical backup media of data and information related to NSDL e-Gov CA Services are secured at Primary and disaster recovery site from environment threats such as temperature, humidity and magnetic and electrostatic interference and from any unauthorized access. As per the policy access to this backup media is limited to authorized personal only.

5.1.7 Waste disposal

NSDL e-Gov CA shall perform the secured transfer & disposal of media as per its Policy for Electronic waste (e-Waste) Management & Policy for Media Handling & Security, NSDL e-Gov has documented guidelines for secure transfer & disposal of media. Media tapes, floppies, CDs & removable media are physically destroyed before disposal. Hard disk of desktops/ servers is de-magnetized to destroy the content & necessary records are maintained while disposal of assets are as per e-waste policy. Classified paper documents are shredded if not in use. Further, Cryptographic modules will pass through the process of Zeroisation and they will be physically destroyed to make it unreadable.

5.1.8 Off-Site Backup

NSDL e-Gov CA Services shall backup all critical data on periodic basis and backup copies shall be stored securely at Primary as well as at disaster recovery site.

5.2 Procedural Controls

5.2.1 Trusted roles

Identified Officials of NSDL e-Gov who have an access to NSDL e-Gov CA facility or control the operations of NSDL e-Gov CA are considered as "Trusted Officials". NSDL e-Gov shall prepare the document of roles and responsibility. Trusted Officials include, but are not limited to:

- Authorized officials of PKI business operations
- Authorized officials from System/ Database & Cryptographic administration
- Authorized officials that are assigned responsibility for managing the infrastructure

5.2.2 Number of persons required per task

NSDL e-Gov CA shall employ at least two CA administrators and two system administrators for performing and handling sensitive functions in order to protect the integrity of CA activities. Further NSDL e-Gov CA shall review this on annual basis and make the changes as needed for satisfying operational and administrative needs.

5.2.3 Identification and authentication for each role

NSDL e-Gov shall perform complete background check as per procedure prior to assigning the role of authorized trusted personal or trusted official. NSDL e-Gov CA shall ensure that each trusted officials performing this role shall;

- Be restricted to actions authorized for their role
- Role is Not shared with anyone

5.3 Personnel Controls

5.3.1 Background, qualifications, experience and clearance requirements

Officials being considered for trusted official/ roles shall possess the required background, qualifications and professional experience necessary to perform the roles ably and satisfactorily.

NSDL e-Gov CA shall authorize any official as trusted official after he has acquired the required skills and qualification to perform the trusted role.

5.3.2 Background Check Procedures

NSDL e-Gov as per their Human Resource policy performs following Background checks with the help of services of private or government agency, for trusted personnel, but not limited to:

- Check of previous employment
- Check for permanent and present address
- Check for educational qualifications

The personnel shall be rejected for the trusted role if any of the above checks reveals misrepresentation or indicates that the concerned individual is not suitable for the corresponding trusted role.

5.3.3 Training Requirements

NSDL e-Gov CA shall provide adequate training to personnel designated for each trusted role to perform their job responsibilities ably and satisfactorily.

This includes;

- Broad training with respect to duties to be performed
- Awareness of relevant features of IT Security policy of NSDL e-Gov CA
- Awareness of relevant features Disaster Recovery and Business Continuity Plan
- Incident handling and reporting Process

The adequacy of such training will be determined from time to time.

5.3.4 Re-training frequency and requirements

NSDL e-Gov CA shall provide its personnel ongoing training to update their skills and knowledge to perform their job responsibilities ably and satisfactorily. Refresher training for the personnel in all the trusted roles shall be given by the NSDL e-Gov CA either on annual basis or as and when, if required.

5.3.5 Job Rotation Frequency and Sequence

Not Stipulated

5.3.6 Sanctions for unauthorized actions

In case if trusted personnel found guilty or an attempt for an unauthorized action, then his/ her access to facility and operations system would be immediately suspended or revoked and investigation would be made. Any violations or unauthorized actions of NSDL e-Gov policies and procedures will invite disciplinary actions. Such disciplinary actions may include without limitation termination of employment.

5.3.7 Contracting personnel requirements

Independent contractors and consultants are permitted access to NSDL e-Gov CA/ eSign secure facilities only; (a) after the approval from management and (b) if they are escorted and directly supervised by trusted personnel.

5.3.8 Documentation supplied to personnel

All the personnel involved in NSDL e-Gov CA services shall be required to read this CPS and other policy documents related to NSDL e-Gov CA services. Adequate training materials and relevant documents shall be provided to all the personnel in trusted roles to perform their job responsibilities ably and satisfactorily.

6 Technical security controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

NSDL e-Gov CA shall ensure following for key generation process;

- Key pairs shall be generated in presence of multiple trusted personnel in pre-planned key generation activity.
- Key generation activity shall be conducted in a secure and trustworthy environment as per standards specified in the IT Act, 2000 and Interoperability Guidelines published by CCA.
- Key generation activity shall be recorded, internally audited and signed by all trusted personnel involved in the key generation activity.
- Key pairs for NSDL e-Gov CAs shall be generated in a hardware security module (HSM) certified to meet the requirements of FIPS 140-2 level 3.
- Subscribers, key pairs shall be generated by NSDL e-Gov eSign Service and shall have the maximum validity of thirty minutes as per the e-authentication guidelines as published by CCA.

6.1.2 Private Key Delivery to Entity

The NSDL e-Gov CA shall generate the key pair for the Subscriber, and using the private key the document/ transaction is signed. And as documented in e-authentication guidelines published by CCA, the private key is destroyed and an audit log is generated for this transaction. Hence there is no private key delivery to subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

NSDL e-Gov CA shall ensure that their own public key shall be delivered to root CA in PKCS#10 request and it is delivered to Root CA in secure medium along with an authorization letter from NSDL e-Gov CA authorized trusted personnel.

As per e-Authentication guidelines, for subscribers, the public key is delivered via a secure channel to Application Service Providers and a copy of public key is maintained for Audit & Logging purposes.

6.1.4 CA Public Key Delivery to Users

NSDL e-Gov shall publish its own CA public key for relying parties at its repository on NSDL e-Gov portal (at https://egov-nsdl.co.in/eSign/).

6.1.5 Key Sizes

The key length size of the NSDL e-Gov CA shall be 2048-bit RSA key pair and Subscribers shall have keys which are 2048 bits long.

6.1.6 CA Public Key Parameters Generation

NSDL e-Gov CA shall ensure that its CA application is configured to set parameters for CA and Subscriber public key generation.

6.1.7 Hardware/ Software Key Generation

Key pairs of NSDL e-Gov CA shall be generated using trustworthy hardware cryptographic module in secured environment.

6.1.8 Key Usage Purposes (as per X.509 v3 key usage field)

Key usage purposes are incorporated in NSDL e-Gov CA as detailed in Section 7-Certificate and CRL profiles in this CPS document. NSDL e-Gov CA shall ensures that CA signing key is the only key permitted to be used for signing Aadhaar based DSC and CRLs.

6.1.9 Time Stamp

NSDL e-Gov CA shall ensure that all servers used for NSDL e-Gov CA are synchronized as per Indian Standard Time.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

NSDL e-Gov CA shall ensure that cryptographic module used by NSDL e-Gov CA system to generate CA keys is designed to comply with FIPS 140-2 level 3. And NSDL e-Gov CA shall ensure that necessary measures are taken to ensure that key pairs generated for eSign Service of NSDL e-Gov CA is secured by HSM.

6.2.2 CA Private Key (m out of n) Multi-Person Control

NSDL e-Gov CA has implemented control that multiple trusted personnel are required to activate the NSDL e-Gov CA private key, requires the presence of two persons to complete activity. No single NSDL e-Gov CA trusted personnel is allowed to generate the CA private key.

6.2.3 Private Key Backup

NSDL e-Gov creates backup of private keys and stored in strong encrypted form in Hardware Security Module/ cryptographic module.

6.3 Computer/ Systems Security Controls

6.3.1 Specific computer security technical requirements

NSDL e-Gov CA ensures that its CA services generation system provides reasonable assurance that the system software and the data files used to issue Aadhaar based DSC are kept in secured environment and secured from unauthorized access. NSDL e-Gov CA shall ensure that following are implemented on it;

- Access to its CA application is restricted to authorized CA personnel only
- Its CA application shall run from secured and hardened computer system
- No remote access on Certificate generation module
- Use of proper network security controls for protection against internal and external intrusion
- Access for management is provided only to CA trusted personnel after authorization
- Access to database is provided only to CA trusted personnel after authorization

6.4 Network Security Controls

NSDL e-Gov CA has deployed the network and related controls and NSDL e-Gov CA network is logically separated from other components using network devices and firewalls. All communication of sensitive information is secured by NSDL e-Gov, through encryption techniques and digital signatures.

6.5 Cryptographic Module Engineering Controls

The NSDL e-Gov CA shall utilize hardware cryptographic modules to perform all Digital signing operations that are rated FIPS 140-2 level 3 of security.

7 Certificate and CRL profiles

7.1 Certificate Profile

NSDL e-Go CA shall ensure that Aadhaar based DSC issued by the NSDL e-Gov CA under this CPS.

Certificates produced under this CPS shall contain the field and indicated prescribed values or constraints described by CCA in their Interoperability Guidelines, published on the CCA website (https://www.cca.gov.in). Certificates produced under this CPS shall contain following field as described below;

- Serial number - Unique Integer Value and Unique for each certificate
- Signature Algorithm - Algorithm used to sign certificate
- Issuer DN - X.500 Distinguished Name of the issuing CA
- Validity - Validity defined in UTC time format
- Subject DN - X.500 Distinguished Name of the associated entity
- Signature - Issuer CA's signature

7.1.1 Version Number

All NSDL e-Gov CA Certificates are complying Interoperability Guidelines, published on the CCA website (https://www.cca.gov.in) which is X.509 version 3 standards Certificates.

7.1.2 Certificate Extensions Populated

Minimum extensions for CA Certificates issued by NSDL e-Gov CA is as mentioned below:

- Authority Key Identifier – Identifies CA certificate that must be used to verify CA certificate
- Subject Key Identifier – It is Unique Value of Public Key
- Basic Constraints – Number that limit path length for certificate chain
- Key Usage - Defines Usage for Certificate key
- CRL Distribution Points – Location of CRL Information

Minimum extensions for subscriber Certificates issued by NSDL e-Gov CA is as mentioned below:

- Authority Key Identifier – Identifies CA certificate that must be used to verify CA certificate
- Subject Key Identifier – It is Unique Value of Public Key
- Key Usage - Defines Usage for Certificate key
- CRL Distribution Points – Location of CRL Information

7.2 CRL Profile

NSDL e-Gov CA publishes Certificate Revocation List under this CPS shall contain the list of revoked certificates.

7.2.1 Version Number

All NSDL e-Gov CA CRLs are X.509 version 2 CRLs and complying to Interoperability Guidelines, published on the CCA website (https://www.cca.gov.in)

8 Specification Administration

8.1 Specification Change Procedure

The details in the NSDL e-Gov CA CPS may be changed periodically with the approval of the NSDL e-Gov management and CCA. The updated CPS along with new version number and date of publication shall be published as specified in the Section 8.2 of this CPS.

8.2 Publication and Notification Policies

(a) All items in this CPS are subject to the publication and notification requirement.
(b) Latest version of CPS will be published via NSDL e-Gov CA website.

8.3 Approval Procedure

NSDL e-Gov shall ensure that whenever the CPS document needs to be revised, the revised CPS document shall be submitted along with proposed changes to the CCA for approval. The changes shall be adopted only after due approval from the CCA for its publication on NSDL e-Gov CA web site.