# Certification Practice Statement (CPS)

## Version 1.0 June 04, 2015

## OID: 2.16.356.100.1.9.2

**Published by**

**Centre for Development of Advanced Computing (C-DAC)**

**Department of Electronics and Information Technology (DeitY)**

**Ministry of Communications & Information Technology**

**Government of India**

**Approved by**

**Controller of Certifying Authorities**

# Table of Contents


1. INTRODUCTION ..... 6
   1.1 Overview ..... 6
   1.2 Identification ..... 7
   1.3 Agencies and Applicability ..... 8
   1.4 End Entity ..... 8
   1.5 Applicability ..... 9
   1.6 Contact Details ..... 9
2. GENERAL PROVISIONS ..... 9
   2.1 Obligations ..... 10
   2.2 Liabilities ..... 13
   2.3 Financial Responsibility ..... 14
   2.4 Interpretation and Enforcement ..... 16
   2.5 Fees ..... 17
   2.6 Publication and Repositories ..... 18
   2.7 Compliance Audit ..... 19
   2.8 Confidentiality ..... 20
   2.9 Intellectual Property Rights ..... 21
3. IDENTIFICATION AND AUTHENTICATION ..... 22
   3.1 Initial Registration ..... 22
   3.2 Routine Re-Key ..... 23
4. OPERATIONAL REQUIREMENTS ..... 23
   4.1 Certificate Application ..... 23
   4.2 Certificate Issuance ..... 24
   4.3 Certificate Download and Acceptance ..... 26
   4.4 Certificate Revocation List (CRL) ..... 27
   4.5 System Security Audit Procedures ..... 27
   4.6 Archival and Retention period ..... 28
   4.7 Key Changeover ..... 29
   4.8 Compromise and Disaster Recovery ..... 29
   4.9 Termination ..... 30
5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS ..... 30

5.1 Physical Security Controls ..... 30
5.2 Procedural Controls ..... 31
5.3 Personnel Controls ..... 32
6. TECHNICAL SECURITY CONTROLS ..... 32
6.1 Key Pair Generation and Installation ..... 33
6.2 Private Key Protection ..... 34
6.3 Computer/Systems Security Controls ..... 35
6.4 Network Security Controls ..... 36
6.5 Cryptographic Module Engineering Controls ..... 36
7. CERTIFICATE AND CRL PROFILES ..... 36
7.1 Certificate Profile ..... 36
7.2 CRL Profile ..... 38
8. SPECIFICATION ADMINISTRATION ..... 38
8.1 Specification Change Procedure ..... 38
8.2 Publication and Notification Policies ..... 38
8.3 Approval Procedure ..... 38

## List of Acronyms & Abbreviations

| Sl. No | Term | Description |
|---|---|---|
| 1 | CA | Certifying Authority |
| 2 | CCA | Controller of Certifying Authority |
| 3 | C-DAC CA | C-DAC Certifying Authority |
| 4 | CPS | Certificate Practice Statement |
| 5 | CRL | Certificate Revocation List |
| 6 | CRL DP | CRL Distribution Point |
| 7 | CSR | Certificate Signing Request |
| 8 | DSC | Digital Signature Certificate |
| 9 | eKYC | Electronic Know Your Customer |
| 10 | POI | Proof of Identity |
| 11 | FIPS | Federal Information Processing Standard |
| 12 | HTTP | Hypertext Transfer Protocol |
| 13 | HTTPS | Hypertext Transfer Protocol with SSL |
| 14 | IETF | Internet Engineering Task Force |
| 15 | IT | Information Technology |
| 16 | ITU | International Telecommunications Union |
| 17 | LAN | Local Area Network |
| 18 | OID | Object Identifier |
| 19 | OTP | One Time PIN |
| 20 | PKI | Public Key Infrastructure |
| 21 | PKIX | Public Key Infrastructure X.509 |
| 22 | RFC | Request For Comments |
| 23 | SSL | Secure Socket Layer |
| 24 | UID | Unique Identifier |
| 25 | UIDAI | Unique Identification Authority of India |
| 26 | WWW | Wide World Web |
| 27 | X.509 | the ITU-T standard for Certificates and their corresponding authentication framework |

# Terminology

**“Applicant”** or “User” means a person who t has requested for a digital signature certificate to be issued by CDAC CA .

**“Auditor”** means an organisation empanelled by Controller of Certifying Authorities (CCA) for auditing of Licensed CA.

**"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 IT Act;

“**Digital Signature Certificate” or the “certificate” or DSC** means a digital signature certificate issued by CDAC CA to the applicant. It also means a Digital Signature Certificate issued under subsection (4) of Section 35 of IT act • “CA” refers to CDAC , as licensed by CCA to issue digital signature certificate

“**Controller”** means the Controller of Certifying Authorities appointed as per Section 17 subsection (1) of the Act.

**"CPS "** Unless otherwise specified, the word “CPS” used throughout this document refers to Certification Practice Statement of CDAC CA

**“Private Key”** means that part of cryptographic key pair generated for creating Digital Signature

**“Subscriber”** means a person whose name the Digital Signature Certificate is issued by CDAC CA .

**"eSign"** is an integrated service which facilitates issuing a Digital Signature Certificate and performing Signing of requested data by authenticating the Aadhaar holder

**Application Service Provider (ASP):** An organization or an entity using eSign service as part of their application to digitally sign the content.

**End-User:** An Individual using the application of ASP and represents himself/herself for signing the document under the legal framework. For the purposes of KYC with UIDAI, the end-user shall also be the ‘resident’ holding the AADHAAR number. For the purposes of DSC by the CA, the end-user shall also be the ‘applicant/subscriber for digital certificate’, under the scope of IT Act.

**eSign Service Provider (ESP):** An organization or an entity providing eSign service. ESP is a “Trusted Third Party”, as per the definitions of Second Schedule of Information Technology Act.

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

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

**"KUA "** is a registered e-KYC User Agency under UIDAI to provide e-KYC authentication service

# 1. INTRODUCTION

This document is the Certification Practice Statement (CPS) of C-DAC Certifying Authority (C-DAC CA), a Certifying Authority licensed under IT Act 2000 by the Controller of Certifying Authorities, (CCA.) India. It is assumed that the reader is generally familiar with Public Key Infrastructure (PKI) and networking technologies.

The structure of this document is generally in conformity to the RFC 2527 - Internet X.509 PKI Certificate Policy and Certificate Practice Framework guidelines wherever possible. There may be some variations in details and headings in order to meet the requirements of C-DAC CA as set forth by the Office of the CCA and Indian IT Act 2000 and the accompanying rules and regulations, which are specific to the requirements of e-authentication/e-signing technique using Aadhaar KYC Services in India.

## 1.1 Overview

i. Centre for Development of Advanced Computing (C-DAC) is a premier R&D organization of the Department of Electronics and Information Technology (DeitY), Ministry of Communications & Information Technology (MCIT). It carries out Research and Development activities in the ICT sector, Electronics and associated areas.

ii. CDAC CA is setup to cater the needs of issuing of Digital Certificates for eSign services. The CA is setup is adhering to the security requirements as mentioned in the information technology Act Schedule II. The Certifying Authorities functions are in accordance with Information technology Act, rules, regulations and guidelines issued by Controller where ever it is applicable. CA provides eSign online electronic signature service in accordance with e-Authentication guidelines (http://cca.gov.in/eauthentication.pdf)

iii. **Hastaksara - C-DAC's On-line Digital Signing Service:** C-DAC through its Hastaksara initiative, is setting up an eSign facility to enable on-line e-authentication and digital signing of documents using Aadhaar KYC Service.

iv. The Objective of C-DAC's On-line Digital Signing Service, Hastaksara is to offer an on-line platform to citizens of India for instant signing of their documents securely in a legally acceptable form, under the Indian IT Act 2000 and various rules and regulations therein.

v. As a provider of Digital Certificates and eSign services, 'C-DAC CA' will be playing the role of a Trusted Third Party eSign Provider (ESP).

vi. The Certification Practice Statement (CPS) of the CDAC CA states how the PKI component(s) meet the assurance requirements in conformity with India PKI CP and also security control and operational policy & procedures and other matters relevant to obligations and responsibilities in accordance with the IT Act, Rules, Guidelines and Regulations. The Services provided by CDAC CA are part of this CPS

vii. The 'C-DAC-CA' CPS as a document captures the rights and obligations of each and every entity participating in the issuance and usage of Digital Signature Certificate

viii. The 'C-DAC CA' CPS is a detailed statement of operational procedures and guidelines of the C-DAC CA. The 'C-DAC CA' CPS is intended to and is a legal document covering the

participating entities like the applicants, subscriber, Application Service Provider (ASP), and relying parties.

ix. The CPS lays down the entire Certification process and life cycle. It begins with the establishment of the CA and start up procedures, the application for the services, the process involved in exchange of data between the relying parties, the expiry and storage of certificates.

x. The 'C-DAC CA' provides eSign service to Individual applicant who has a valid Aadhaar ID and mobile number registered with Aadhaar for the purpose of digital signing of document hash. The digital certificate offered by C-DAC CA through the eSign service is for one-time signing usage and shall be of class "Aadhaar-eKYC – OTP" as per e-Authentication guidelines (http://cca.gov.in/eauthentication.pdf). The digital certificate is offered as part of the eSign service to the applicant. The one-time signing is already consumed to sign the applicant's document as part of availing the eSign service and therefore cannot be used further for any signing purpose.The DSC can continue be used for verification purposes.

xi. This document is meant to be reviewed and updated regularly and the current version is referred to as in the document title.

xii. This CPS assumes that the reader possesses basic knowledge and familiarity of the concepts of PKI, Digital Signatures, eSignatures and Indian IT Act. Readers are further suggested to acquire required knowledge and training before making use of these techniques. For further familiarity the reader may visit the website of C-DAC CA and the CCA (https://esign.cdac.in/ca and www.cca.gov.in). The reader can further get in touch with C-DAC CA helpdesk at ess@cdac.in.

xiii. The Digital Certificates issued by the CDAC CA will be as per X.509 version 3 format in conformity with Interoperability Guidelines

xiv. Electronic copy of this CPS is available at the C-DAC CA web-site https://esign.cdac.in/ca.

## 1.2 Identification

| Sr. No. | Product | OID |
|---|---|---|
| 1. | C-DAC CA | 2.16.356.100.1.9 |
| 2. | C-DAC CA CPS | 2.16.356.100.1.9.2 |

## 1.3 Agencies and Applicability

### 1.3.1 Certifying Authority (CA)

1.3.1.1 C-DAC CA is the CA licensed by CCA under the Indian Information Technology Act, 2000 that shall offer Digital Signature Certificate for eSign Service to sign the document of applicants. Each certificate shall bind the public key of each entity to its Digital Signature Certificate.

C-DAC CA comes under the Root Certifying Authority of India (RCAI) following the hierarchical implementation of the PKI. The DSC will be issued directly from the CA and there will not be any sub-CA.

### 1.3.2 Aadhaar

For the issuance of DSC to applicant, CADC CA relies only on the pre-verified information held by UIDAI's Central Identities Data Repository (CIDR) using OTP authentication. The DSC application of the applicant will be electronically generated based only on the demographic details received from CIDR data base. The format of the application form is given in annexure. The response id received from Aadhaar eKYC service will be a part of application form as a proof of identity verification.

1.3.2.1 Aadhaar offers authentication service based on biometric based authentication or non-biometric based one using OTP (One Time Password/PIN). C-DAC CA shall leverage Aadhaar OTP based service to authenticate the applicant for issuance of DSC and creation of signature for eSign purpose.

1.3.2.2 eSign facilitates Aadhaar ID holder to digitally sign a document. eSign uses authentication service of Aadhaar through Aadhaar e-KYC service, and the data/information provided by Aadhaar for authentication of the applicant.

1.3.2.3 Digital Signature Certificate issued by C-DAC CA shall be based on the information provided by Aadhaar e-KYC services and the electronic consent obtained from the applicants.

## 1.4 End Entity

### 1.4.1 Subscriber

Digital Certificate registration procedure clearly differentiates the term “Applicant” and “Subscriber”. A person is termed as an Applicant who applies for a Digital Certificate having a valid Aadhaar ID and also provide consent to ESP for the facilitation of key pair generation, applying for a DSC to CA, electronic application form generation . The applicant status is changed to “Subscriber” after receiving the DSC and its acceptance. The acceptance of contents of certificate constitutes acceptance of the certificate

### 1.4.2 Relying Party

It is an entity that relies on the information provided in a valid Digital Signature Certificate (Aadhaar-eKYC – OTP class) issued by C-DAC CA and/or any other information provided in the C-DAC CA Repository to verify and identify the public key of the subscriber.

## 1.5 Applicability

**a.** The DSC issued by C-DAC CA are intended to support the following needs:

- Assurance of the identity of the applicant based on;
- Message integrity for verification purposes to check that the content of a message is intact, and has not been altered

b. Digital Signature – Facilitates non repudiation by providing assurance to the Relying Party against denial from a subscriber that, the subscriber has not authorized any particular transaction, if the transaction has been digitally signed by the subscriber.

c. C-DAC CA has been designed to issue Digital Signature Certificate and offer eSign service to valid Aadhaar users based on OTP authentication. Independent risk assessment and determining the appropriateness of certificate for any purpose is the responsibility of the subscribers and relying party.

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

## 1.6 Contact Details

### 1.6.1 Specification Administration Organization

This C-DAC CA CPS is published and administered by the C-DAC CA management.

### 1.6.2 Contact Person

Project Manager/Site Coordinator, C-DAC CA
Centre for Development of Advanced Computing (C-DAC)
Pune University Campus
Ganesh Khind
Pune - 411 007
Email: esign@cdac.in
Phone: +91-20-2570-4100
Fax: +91-20-2569-4004

### 1.6.3 Person Determining CPS Suitability for the Policy

The suitability of the CPS is determined by the management of C-DAC CA and acceptance of CCA.

# 2. GENERAL PROVISIONS

This section provides an insight to the various obligations, liabilities, responsibilities, and financial and legal considerations associated with the use of C-DAC CA.

## 2.1 Obligations

### 2.1.1 CA Obligations

2.1.1.1 C-DAC CA has been designed to offer Aadhaar OTP based DSC and eSign service to valid Aadhaar users. C-DAC CA will publish or make publicly available the CPS describing the practices employed in issuing the Digital Signature Certificates for the purpose of offering eSigning service. The CA operates in accordance with this CPS, and the Information Technology ACT 2000 and its subsequent amendments, if any.

2.1.1.2 C-DAC CA shall perform services and operations, and maintain the infrastructure related to certificates issued under this CPS, in substantial conformity with the requirements of the Information Technology Act, 2000.

2.1.1.3 That the public key algorithm employed by C-DAC CA and C-DAC CA's private signing key will be reasonably secured and safeguarded within the C-DAC CA. In conformity with Information Technology Act, 2000.

2.1.1.4 To act in accordance with policies and procedures designed to safeguard the Digital Signature Certificate life cycle management process (including Digital Signature Certificate issuance, revocation, archival and audit trails) and protect C-DAC CA private key from compromise.

For issuance of Digital signature certificate to DSC applicants through CDAC CA's eSign service , CDAC CA will operate in conformity with IT Act.

For providing eSign online service , CDAC CA will operate In accordance with Electronic Signature or Electronic Authentication Technique and Procedure Rules, 2015 and its subsequent amendments under second schedule of IT Act.

2.1.1.5 eSign Service of C-DAC CA will comply with the requirements of this CPS and its applicable Certificate policies (a) for e-authenticating the applicant using Aadhaar e-KYC, while issuing the Digital Certificate and while carrying out e-signing of the digital document hash provided by the applicant, using the issued Digital Signature Certificate (DSC) on behalf of subscriber.

eSign Service of C-DAC obtains applicant's information based on the Aadhaar identification Information upon the consent provided by the applicant, for inclusion in the Certificate, and such information will be accurately transcribed to the Certificate.

2.1.1.6 eSign Service of C-DAC CA relies upon the eKYC information provided by Aadhaar for processing/ issuing the DSC for the e-signing purpose and therefore correctness/accuracy/sufficiency of eKYC information provided by Aadhaar shall not be the responsibility of eSign Service of C-DAC CA

eSign Service of C-DAC CA shall generate public-private key pair on behalf of the applicant and create the corresponding digital signature certificate. eSign applicant's document's hash will be signed using the private key (one-time usage).

2.1.1.7 Certificate Signing Request (CSR) generated by ESP shall be signed by C-DAC CA which shall use the system consisting of computer hardware, software, firmware and security procedures that are reasonably secured/protected from intrusion and misuse; provide a reasonable level of reliability, and correct operation; are configured only for the issuance of Aadhaar eKYC OTP class of individual DSCs and enforce the applicable security policy.

2.1.1.8 C-DAC CA shall not be responsible and liable or any loss, damage or penalty resulting from delays or failures in performance in resulting from acts of God or other causes beyond control. For purposes of clarity, such events shall include, but without limitation to, strikes, or other labour disputes, riots, civil disturbances, Software/Hardware/equipment/device/communication failures / malfunctioning /bugs / viruses, actions or inactions of suppliers, acts of God, war, fire, explosion, earthquake, flood or other catastrophes.

2.1.1.9 In any of the events mentioned in Section 2.1.1.12 hereof, the C-DAC 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 Subscriber Obligation

The Subscriber shall have the following obligations:

1. To ensure that the information/data provided is sufficient, accurate, current and without errors, omissions or misrepresentations.

2. Applicant shall not submit any material/contents which are illegal/immoral or infringing upon third person's intellectual property, for e-sign

3. Carefully read, understand and accept the policies and procedures as specified in this CPS.

4. Comply with the e-authentication verification using e-KYC by providing the required information and consent.

5. Provide the consent to eSign service of C-DAC CA (a) to generate the key pair on behalf of the Applicant, (b) to obtain eKYC details about the applicant from Aadhaar, (c) use applicant's private key for signing of the applicant's document hash and (d) to include necessary information obtained from eKYC for inclusion in the Digital Signature Certificate.

### 2.1.3 Registration Authority Obligation (Aadhaar)

The issuance of DSC is based only on the electronic authentication of applicant by Aadhaar eKYC service OTP. No registration authorities are engaged by CDAC CA for the eSign service.

### 2.1.4 Relying party obligation

A relying party may rely on a Digital Signature Certificate that references this CPS only if the Certificate is used and relied upon for usage in e-signing of the digital document and under the circumstances where the following occur.

1. The relying party should have the knowledge of Indian IT ACT 2000 including its amendments, IT rules and regulations.

2. Any relying party seeking to rely upon a Digital Signature Certificate is solely responsible for deciding whether or not to rely upon the said Digital Signature Certificate.

3. The relying party should have the knowledge that, the Digital Signature Certificate was issued after the e-authentication using OTP based Aadhaar authentication.

4. The Digital Signature Certificate is used exclusively for the e-Signing of the Digital Document.

5. Relying parties must use appropriate utilities or tools to perform digital signature verification or other operations. The utilities/ tools should be able to identify the certificate chain and verifying the digital signature on all certificates in the chain and only on successful verification should rely on the certificate.

### 2.1.5 Repositories Obligations

C-DAC CA shall maintain the repository to store information relevant to the operations of the C-DAC CA Public Key Infrastructure Services. C-DAC shall maintain the CPS and CRL(if any) in its repository as given in Section 2.6. All the information and modifications are published in the repository to provide access to the updated information. This information is subject to changes and any such change shall be published in the C-DAC CA repository as detailed in other relevant sections of this CPS.

## 2.2 Liabilities

### 2.2.1 CA Liability

2.2.1.1 C-DAC CA shall have no responsibility in relation to failures that may take place during the Aadhaar based authentication process, including but not limited to, failures as a result of, false reject, network, or connectivity failure, device failure, software failure, possible down time and central identities data repository, etc.

2.2.1.2 C-DAC CA shall have no responsibility in relation to failures that may take place during the eSign process, including but not limited to, failures as a result of, reject, network, or connectivity failure, device failure, software failure, possible down time and central identities data repository, etc.

2.2.1.3 Warranties and Limitations on Warranties

C-DAC does not give any kind of warranties about its CA services. C-DAC 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 SW/SYSTEM/SERVICES.

2.2.1.4 Kinds of damages covered

Unless otherwise specifically stated in this CPS, C-DAC including its affiliates, shareholders, officers, directors, employees, agents, representatives etc.. shall not be responsible and liable under tort/contract or any legal theory, to users/citizens or any other person who avail/facilitate/operate/access or otherwise connect/communicate for CDAC 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 C-DAC including its affiliates, shareholders, officers, directors, employees, agents, representatives etc..

2.2.1.5 Loss Limitations

C-DAC 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 CDAC 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.

2.2.1.6 Other Exclusions

CDAC shall not be responsible and liable for use/disposal/distribution/circulation of the DSC by the subscriber/relying authority. Subscribers and Relying authority are duty bound to use the DSC only for legal/lawful/moral/ethical/harmless purposes. CDAC disclaims any liability/damage/loss arising out of /due to any circumstances/situations beyond the control of C-DAC. Such situations/circumstances include but not limited to natural calamities, Acts of GOD, flood, earthquakes, explosions, fire, accident, cyclones, tempests, wars, terrorist actions, strikes, lockouts, bandhs, gheros, communication/power failures/shortages etc..

CDAC shall not responsible and liable for any errors/mistakes in DSC or other outputs/documents, not attributable to C-DAC.

### 2.2.2 Subscriber Liability

a. All information provided by Applicant/Subscriber shall be true, correct and valid at (i) while applying for DSC through eSign service, (ii) while the certificate is being used.

b. Applicant/Subscriber shall be liable for submission/obtaining CDAC 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 Relying Party Liability

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.

## 2.3 Financial Responsibility

2.3.1.1 C-DAC 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 C-DAC has been advised of the possibility of such damages.

2.3.1.2 Any Limited Warranty, if any, referenced above is the only express warranty made to 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, C-DAC 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 TRANSCATION of or arising out of the use or performance of the e-Sign/CA services by C-DAC shall not remain with CDAC CA.

2.3.1.3 The C-DAC CA further does not make any representation and does not give any warranties on the financial transactions, which the subscribers and the relying parties undergo using the e-signed Digital Document obtained from the C-DAC CA using the e-authentication and e-signing techniques described in this 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.

### 2.3.2 Indemnification by Relying Party and Subscriber

2.3.2.1 Subscriber or/and Relying Party shall jointly and severally save and indemnify and at all times keep CDAC saved/indemnified, against any and all liability, damages, claims, loss, legal fees/expenses, proceedings arising out of or in connection with use of or reliance upon DSC by way of any action/omission/default/breach of any of the terms and conditions of the CPS/Agreement by Subscriber or/and Relying Party its agents and employees or its agents, representatives, employees, consultants etc..

2.3.2.2 Subscribers are liable for any misrepresentations or any other statements made with fraudulent intent, negligence or error in their applications for Certificate to relying parties, who reasonably rely on the representations contained therein.

### 2.3.3 Independent Parties

C-DAC CA and subscriber/Relying party are not the agents, fiduciaries, trustees or other representatives of Subscriber or Relying Party. The relationship between C-DAC CA and Subscriber and that between C-DAC CA and Relying Party are not that of agent and principal. Neither Subscriber not Relying Party have any authority to bind the C-DAC CA, by contract or otherwise, to any obligation. C-DAC CA does not make any representations to the contrary, either expressly, implicitly, by appearance or otherwise. CDAC CA, Aadhaar, Subscriber and Relying Party are totally independent parties and not agent/representative/subcontractor of each other.

### 2.3.4 Administrative Processes

CDAC CA has its internal procedures for CA functioning. These procedures will be reviewed periodically.

## 2.4 Interpretation and Enforcement

C-DAC CA has framed administrative, technical and physical security and operational policies, procedures and standards for the CA Operations in line with the applicable sections of IT ACT, 2000 and subsequent amendments and guidelines.

### 2.4.1 Governing Laws

- Information Technology Act, 2000, rules regulations and guidelines issued thereunder

### 2.4.2 Severability of Provisions, Survival, Merger & Notices

2.4.2.1 Severability of Provisions

While interpreting the clauses of this CPS, if any clause is found to be severable from the rest of the Agreement, the invalidity of such clause shall not affect the validity of the other clauses in the agreement.

2.4.2.2 Survival

Clauses of confidentiality obligations, Audit, Obligations of C-DAC CA, Subscriber and Relying party(ies) and limitations thereof, Liability of CDAC CA, Subscriber and Relying party(ies) shall survive expiry/termination of this CPS.

2.4.2.3 Merger

In the event of merger of C-DAC CA with any other entity, all rights and obligations of C-DAC CA shall vest in the acquiring or new entity created by merger.

2.4.2.4 Notice

Any notice or other communication which subscriber/Relying Party is required under this CPS to serve on C-DAC CA shall be sufficiently served if sent to the address as specified in this CPS either

(a) by hand

(b) by applicable full postage paid courier/registered/speed post acknowledgement due or

(c) 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.

**Address:**
Project Manager/Site Coordinator, C-DAC CA
Centre for Development of Advanced Computing
Pune University Campus
Ganesh Khind
Pune - 411 007
Maharashtra (India)
Phones: +91-20-2570-4100
Fax: +91-20-2569 4004

Each of the Certificate and all the terms and provisions of this CPS are personal to each of the Subscriber and the Subscriber shall not assign their Certificate to any other parties.

### 2.4.3 Dispute Resolution Procedures

2.4.3.1 For any disputes in CPS, the aggrieved party shall first intimate the C-DAC CA either through e-mail or fax or post for the purpose of dispute resolution. If the dispute is not resolved within (30) business working days after initial notice as above, then aggrieved party shall submit the dispute in writing to C-DAC management.

2.4.3.2 If the dispute cannot be amicably resolved by the parties as per section 2.4.3.1, then the matter will be referred to the Controller of Certifying Authorities (CCA). The CCA is competent under the IT Act, clause 18(I), to resolve any dispute between Certifying Authorities and Subscribers. However, Cyber Appellate Tribunal, under the IT Act, 2000 is the competent court to appeal against any order passed by the CCA. All arbitration proceedings shall be in the English language and judgement upon the award so rendered may be entered in the courts of Pune only.

## 2.5 Fees

### 2.5.1 Certificate Issuance

C-DAC CA may or may not charge Applicant/Subscribers and all such other parties for their use of the C-DAC CA services. If charged, all Applicant/Subscribers and all such other parties shall be obliged to pay to C-DAC CA such charges in accordance with its Schedule of Fees and at such times as may be prescribed by the C-DAC CA published on C-DAC CA website https://esign.cdac.in/ca

### 2.5.2 Certificate Access Fees

At present, certificate Access Fee is given free of charge. However, C-DAC CA reserves right to charge this service any time with immediate effect by notification on its website.

### 2.5.3 Revocation or Status Information Access Fees

At present, Revocation or Status Information Access Fee is given free of charge. However, C-DAC CA reserves right to charge this service any time with immediate effect by notification on its website
Not applicable as CDAC CA will issue DSCs only through eSign service with max of 30 mts validity.

### 2.5.4 Fees for Other Services such as Policy Information

At present, online Access to CPS is given free of charge. However, C-DAC CA reserves right to charge this service any time with immediate effect by notification on its website.

### 2.5.5 Refund Policy

No refund shall be given by C-DAC of any fees/amounts paid to C-DAC towards DSC or other services, if any.

C-DAC CA has absolute right at its sole discretion to refuse to issue a certificate without assigning any reason. In such case, C-DAC shall not incur any responsibility/liability arising out of or incidental to such refusal. However, in the event of such refusal, C-DAC CA will refund the fee received by it from any applicant/subscriber towards DSC; provided applicant has not submitted any untrue/false/fraudulent/incorrect/misleading/misrepresenting/wrong etc., information to ADHAR /UIDAI /CDAC.

## 2.6 Publication and Repositories

Vital Information related to CDAC CA Public Key infrastructure Services/Operations will be stored in the form of repository. The information is subject to changes which will be published and stored as mentioned in this CPS. The repository will be updated from time to time as and when new or modified information is received/stored. Subscriber can online access the repository on payment of prescribed fees, if any.

### 2.6.1 Publication of CA Information

2.6.1.1 The following information is published in C-DAC CA repository at https://esign.cdac.in/ca

a. The C-DAC CA CPS
b. The Certificate of the C-DAC CA corresponding to its private key
c. The CRL for the Certificates revoked by C-DAC CA. The CRL shall be updated as mentioned in this CPS and updated in the Repository.

2.6.1.2 The following information is published on C-DAC CA website at https://esign.cdac.in/ca

a. Fee structures of the various services
b. CRL

### 2.6.2 Frequency of Publication

This shall be done in accordance with the policy set forth in the Section 8 of this CPS.
The following information is published in the C-DAC CA repository at https://esign.cdac.in/ca.

a. The certificate of C-DAC CA corresponding to its private key.
C-DAC CA maintains a repository of certificates it issues and Certificate Revocation Lists (CRLs). The CRL (and the repository) for the certificates revoked by C-DAC CA shall be updated as mentioned in this CPS.

Frequency of Publication: C-DAC CA shall publish the C-DAC CA CPS and its CA certificate in its repository which shall be updated whenever there is any change in

them. The CRLs shall be published and updated in the C-DAC CA Repository, once a year. This Repository is made available at C-DAC CA website.

b. Certification Revocation list of the revoked or suspended certificates shall also be send the CCA's national repository as per the guidelines.

### 2.6.3 Access Control

There is no access control restriction for read/downloading the CPS, CRL's and Digital Certificates from the published public repository. The CPS, CRLs and Digital Certificates in the electronic repository are restricted from unauthorized modification.

## 2.7 Compliance Audit

### 2.7.1 Frequency of Entity Compliance Audit

An auditor empanelled by the CCA shall audit C-DAC CA PKI operations annually as per Rule 31 of the IT, 2000.

### 2.7.2 Identity/Qualifications of Auditor

The auditor, empanelled by the Controller of Certifying Authorities, shall do the audit.

### 2.7.3 Auditor's Relationship to Audited Party

The auditor will be one from list of CCA empanelled list

### 2.7.4 Topics covered by Audit

Annual audit shall include inter alia,

- Security policy and planning;
- Physical security;
- Technology evaluation;
- C-DAC CA's services administration;
- Compliance to relevant CPS
- Contracts/agreements:
- Regulations prescribed by the Controller;
- Policy requirements of IT (Certifying Authorities) Rules, 2000.
- Guidelines issued by Controller

### 2.7.5 Action Taken as a Result of Deficiency

If irregularities are found, C-DAC CA will prepare a report as to the action it will take in response to the audit report. Based on the severity of the irregularities, C-DAC CA will carry out corrections of problems in a most expeditious manner and in accordance with the Governing Law. If C-DAC CA determines that such exceptions or deficiencies pose an immediate threat to the security or integrity of C-DAC CA, a corrective action plan will be developed and implemented within a commercially reasonable period of time. For less serious exceptions or deficiencies, C-DAC CA management will evaluate the significance of such issues and determine the appropriate course of action.

### 2.7.6 Compliance Audit Results

2.7.6.1 C-DAC CA compliance audit results will not be made public unless required by law. Where appropriate, the method and detail of notification of audit results to C-DAC CA partners will be defined within respective agreements between C-DAC CA and the other party.

2.7.6.2 The results of the audit along with the actions taken on the non-conformities will be communicated to the Controller of Certifying Authorities within a period of four weeks of the completion of the audit. The frequency of the audit will be as per the requirements laid down on the IT Act.

## 2.8 Confidentiality

### 2.8.1 Types of Information to be Kept Confidential

2.8.1.1 The types of information C-DAC CA will keep confidential include agreements, transactional records, logs including system and network events, applicant access details, classified and sensitive information, pertaining to C-DAC CA and the Subscriber.

2.8.1.2 Confidential information including 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 information contained in Subscriber's Certificate, CRL-and C-DAC CA CPS that appear in C-DAC CA web site.

### 2.8.3 Disclosure of Certificate Revocation Information

C-DAC CA shall publish the Certificate revocation details(if any) in C-DAC CA website.

### 2.8.4 Release to Law Enforcement Officials

C-DAC CA's confidentiality obligations are subject to orders of courts/statutory authorities/statutory provisions/rules/regulations, by virtue of which, if C-DAC is required ( and also C-DAC CA has a liberty) to release/share/disclose/reveal/circulate/distribute etc. any confidential information then such release/sharing/disclosure/revelation/circulation/distribution shall be without any liability on C-DAC and also shall not be treated/considered/deemed as breach of confidentiality obligations.

### 2.8.5 Release as Part of Civil Discovery

If C-DAC as a party to any suit or otherwise, is required **(**and also C-DAC CA has a liberty) to release /share /disclose /reveal /circulate /distribute etc. any confidential information; under orders of courts /statutory authorities /statutory provisions /rules /regulations then such release/sharing /disclosure /revelation /circulation /distribution shall be without any liability on C-DAC and also shall not be treated/considered/deemed as breach of confidentiality obligations.

### 2.8.6 Disclosure upon Subscriber's Request

C-DAC may, on the request of owner of confidential information, consider to disclose/share/release/reveal/circulate/distribute the confidential information owned by the said owner, provided: (a) C-DAC CA in its judgement forms an opinion that the release/disclosure/revelation/sharing/circulation/distribution of any such information will not attract/result in any liability upon C-DAC CA or on any other party (b) C-DAC CA shall not be responsible and liable for any loss /damage /deficit/claim /demands/actions arising out of or incidental to such release /disclosure /revelation/sharing/circulation/distribution (c) Owner saves and indemnifies C-DAC CA against any and all liabilities /compensations /losses/damages arising out of or incidental to or pursuant to such release/disclosure /revelation /sharing /circulation /distribution.

### 2.8.7 Other Information Release Circumstances

C-DAC CA may at its option/in its sole discretion, on the reasonable and specific written request of a person to whom C-DAC CA is duty bound to keep the information confidential, consider to disclose/share/release/reveal/circulate/distribute the confidential information; provided he pays fees charged by C-DAC CA in this regard.

Also, CDAC CA, when ordered/requested/permitted by CCA, shall also have liberty (without any prior permission of owner of confidential information or any other person and without any financial liability/implications) to disclose/share/release/reveal/circulate/distribute the confidential information. C-DAC CA will determine the time/circumstances of such release /disclosure /revelation /sharing /circulation/distribution of the confidential information.

## 2.9 Intellectual Property Rights

C-DAC reserves rights over its intellectual property (IP) developed by CDAC, such as software, firmware, hardware, CPS, C-DAC CA documentation.

### 2.9.1 Subscribers

2.9.1.1 C-DAC CA shall comply with Applicant/Subscriber's information protection as per the Act. The information supplied by the Applicant/Subscriber is the property of the respective Applicant/ Subscriber. All Applicants/Subscribers shall grant to the C-DAC CA a non-exclusive, world-wide, paid-up, royalty-free, perpetual license to use, copy, modify, publish and distribute such information subject to Applicant/Subscriber's information protection as per the Act.

2.9.1.2 C-DAC CA shall grant to the Subscribers and the Relying Parties a non-exclusive, nontransferable license to use, copy and distribute the C-DAC CA Digital Signature Certificates provided that the Digital Signature Certificates are represented fully and accurately.

# 3. IDENTIFICATION AND AUTHENTICATION

## 3.1 Initial Registration

### 3.1.1 Type of Names

a. The names in the Digital Signature Certificates issued under the C-DAC CA Trust Network shall comply with the X.500 naming conventions and Interoperability Guidelines published by CCA.

b. Digital signature certificates issued C-DAC CA shall use Distinguished Names (DN) to facilitate the identities to subscribers. The Digital Signature Certificate issued in incompliance with the certificate profiles (personal use) specified in the "Interoperability Guidelines for Digital Signature Certificates"(http://cca.gov.in). The following fields in dDistinguished Name are mandatory in the case of eSign Service of CDAC CA:

| X509 Attribute (and OID) | Details |
|---|---|
| CommonName (2.5.4.3) | Name in POI from eKYC is copied to CN in X.509 |
| UniqueIdentifier (2.5.4.45) | Hash of UID (uid in UidData) is copied as x500UniqueIndentifier in X.509 |
| Pseudonym (2.5.4.65) | Code in AgentKycRes for eKYC is copied as pseudonym in X.509 |

### 3.1.2 Need for names to be meaningful

All names must be meaningful using commonly understood semantics to determine the identity of the Subscriber. The Common Name DN attribute contains the legal name as presented in Government issued Aadhaar Unique Identification Document. Each C-DAC CA issued Digital Certificate is with a unique DN, which is inclusive of Common name, SHA256 hash of Aadhaar Number attribute and pseudonym response code of Aadhaar eKYC service for each Subscriber.

### 3.1.3 Rules for Interpreting Various Name Forms

C-DAC CA mandates the inclusion of Unique Identifier, Aadhaar Identification Number, as a mandatory attribute to make the subscriber name unambiguous and unique.

## 3.2 Routine Re-Key

C-DAC CA's public-private key pair shall be changed at the expiry.

# 4. OPERATIONAL REQUIREMENTS

## 4.1 Certificate Application

### 4.1.1 Classes of Certificate

C-DAC CA offers the following class of certificates

| Class | Assurance | Applicability | Suggested Use |
|---|---|---|---|
| **Aadhaar-eKYC – OTP** | Aadhaar OTP class of certificates shall be issued for individuals use based on OTP authentication of subscriber through Aadhaar eKyc. These certificates will confirm that the information in Digital Signature certificate provided by the subscriber is same as information retained in the Aadhaar databases pertaining to the subscriber as Aadhaar holder. | This level is relevant to environments where OTP based Aadhaar-eKyc authentication is acceptable method for credential verification prior to issuance of DSC. Certificate holder's private keys are created on hardware and destroyed immediately after one time usage at this assurance level. | Document signing |

C-DAC CA supports the above listed class of certificates within its Certification Practice Statement. All the classes of the certificates offered for specification by C-DAC CA are valid under the IT ACT 2000.

### 4.1.2 Certificate Application Process

The request for DSC and signature creation is only through registered application service providers using eSign API as published in http://cca.gov.in/eSign. An ESP authenticates each eSign XML request coming from Application service providers by using Digital Signature. The certificate to be used for authenticating the ASP is registered with ESP as a part of on-boarding process. Each ASP has to undergo an on-boarding process and sign an agreement with ESP prior to becoming eligible for availing eSign service from ESP .

As a part of eSign service that includes both DSC issuance and signature creation, ASP capture the Aadhaar authentication details from DSC applicant as per the security specification of Aadhaar eKYC service and forward the same to ESP as a part of eSign API XML. The ASP also obtain the consent 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 CA on the behalf of DSC applicant. On successful authentication of DSC applicant using Aadhaar eKYC services, the key pairs generation and populating demographic details into DSC application form, a CSR will be generated and send to CA for certification.

## 4.2 Certificate Issuance

### 4.2.1 Certificate issuance process

Certificate issuance process involves e-authentication based on Aadhaar service. The information required to provide digital signature certificate is obtained from UIDAI based on subscriber's Aadhaar ID and his consent. The following process is involved.

4.2.1.1 Applicant to visit the specific URL of ASP

4.2.1.2 Applicant to provide his Aadhaar ID and the document that needs to be signed

4.2.1.3 Applicant to provide his/her OTP value received from Aadhaar on his/her mobile number.

4.2.1.4 Applicant to provide consent for a) UIDAI to provide Applicant/'s information/data to C-DAC CA, b) for C-DAC CA to generate key pairs on applicant's behalf for one-time usage, c) eSign service of C-DAC CA to carryout digital signing of Applicant's document hash using his/her private key on Applicant's behalf and d) to incorporate subscriber's information/data obtained from Aadhaar in the digital signature certificate.

4.2.1.5 eSign service of C-DAC CA shall carryout e-authentication based on Aadhaar eKYC service to identify and authenticate the Applicant.

4.2.1.6 eSign service of C-DAC CA generate key pairs on behalf of the Applicant and eSign Applicant's document hash using the private key (one-time usage) and send to the CA systems for the creation of corresponding digital signature certificate. The DSC will be sent to applicant along with signature.

4.2.1.7 Upon receiving the DSC and signature , subscriber examine the contents of the DSC and either accepts or rejects the DSC.

### 4.2.2 Approval / Rejection of Certificate Application

4.2.2.1 Upon the successful validation of DSC applicant through Aadhaar eKYC service, key pair generation and DSC application form generation , the DSC application is deemed as approved and the CSR is submitted to issue DSC in auto issuance mode.

4.2.2.2 C-DAC CA reserves the right to reject the certificate application in cases where details of the applicant fail validation check/necessary information not available. The applicant will be notified regarding the same through eSign API response

### 4.2.3 C-DAC CA's representations to Subscriber

4.2.3.1 C-DAC CA warrants to the subscriber named in the certificate that unless otherwise expressly provided in this CPS or mutually agreed upon–

a. It has complied with the provisions of the IT Act 2000 and rules and regulations made there under
b. Information contained in the digital signature certificate is same as the information received through Aadhaar eKYC service
c. No misrepresentations of fact in the certificate known to C-DAC CA or originating from C-DAC CA have been made at the time of certificate issuance
d. Reasonable care has been taken in creation of certificate using uniform and fail-safe procedures, and all requirements of this CPS and any amendments made

thereto are compiled with by C-DAC CA. The certificate complies with requirements of the IT Act 2000

e. C-DAC CA has published the digital signature certificate or otherwise made it available to such person relying on it and the subscriber has accepted it
   The key pair shall be deleted immediately after the DSC issuance and Signature creation
   The logs for the DSC issuance process shall be kept for a period of 7 years.
f. C-DAC 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 C-DAC CA's representations to Relying parties

4.2.4.1 C-DAC CA warrants to all who reasonably rely as mentioned in this CPS on a digital signature verifiable by the public key listed in the certificate that it is consistent with this CPS.

4.2.4.2 The accuracy of verified information in or incorporated by reference within the certificate is assured, and C-DAC CA has complied with the CPS and IT Act 2000 when issuing the certificate.

#### 4.2.5 Limitations on C-DAC CA Representations

C-DAC 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 C-DAC CA eSign service except as explicitly permitted by this CPS or upon prior written approval from C-DAC CA. Any act in contravention of above will be subject to punitive action under the Indian Laws.

#### 4.2.6 Right to Investigate Compromises

C-DAC CA may, but is not obligated to, investigate all compromises to the farthest extent of the law. By submitting a request for facilitating certificate application, all applicants authorize the undertaking and scope of such investigations and agree to assist in determining all facts, circumstances, causes/reasons and other pertinent information that C-DAC CA deems appropriate and consistent with the CPS, provided that such investigations comply with all applicable privacy and data protection laws of the Republic of India. Investigations of C-DAC CA may include but are not necessarily limited to interviews, the review of applicable books, records, and procedures, and the examination and inspection of relevant facilities. Investigations of certificate applicants and subscribers may include but are not limited to interviews and requests for and evaluation of documents.

### 4.3 Certificate Download and Acceptance

Once a subscriber has completed request for facilitating certificate application and issuance procedures, receipt of certificate and agreeing on the contents of DSC in single round-trip-process powered by eSign API , the DSC is deemed as accepted by subscriber

## 4.4 Certificate Revocation List (CRL)

a. The relying party is strongly advised to a) check the class of certificate and the status of certificate prior to its use; In the case of eSign aadhar eKYC class of DSCs , CRL checking is not required and b) verify the authenticity and integrity DSC to ensure that it is issued and digitally signed by C-DAC CA.

b. CDAC CA does not revoke any DSCs issued through eSign service as the DSC is of 30 minutes validity. However CDAC CA publishes NULL CRLs for relying party tools which mandatorily check CRL as a part of their verification.

## 4.5 System Security Audit Procedures

### 4.5.1 Types of Event Recorded (Audit)

CDAC-CA would record security events manually or electronically for audit trail as per the requirements in compliance with IT Act. These events include, but not limited to:

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

IDENTITY PROOFING

- User provisioning

KEY GENERATION

- All certificate creation parameters

CERTIFICATE SIGNING

- All certificate PKCS#10 requests signing

ACCOUNT ADMINISTRATION

- Roles and users are added, disabled and deleted
- The access control privileges of user account or a role are modified

CONFIGURATION CHANGES

- Hardware
- Software
- Firmware
- Operating System
- Patches
- Security profiles

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

### 4.5.2 Frequency of Audit Log processing

C-DAC CA ensures that its audit logs are reviewed by its trusted member's at least once in two weeks and all significant events are detailed in an audit log summary. Such reviews also involve verifying that these logs are not tampered with, and then briefly inspecting all the log entries, with a more thorough investigation of any alerts or irregularities in the logs. Action taken following these reviews is documented.

### 4.5.3 Retention Period for Audit Log

C-DAC CA shall retain its audit logs in the manner described in para 10 of the Information Technology Security Guidelines as given in Schedule-II of IT(CA) Rules, 2000.

### 4.5.4 Protection of Audit Logs

Audit logs can only be viewed, by the designated trusted administrators of the system. They cannot be viewed, modified or deleted. Un-authorized access to the audit logs is restricted by logical access control systems. Manual audit information will be protected from unauthorized viewing, modification and destruction.

### 4.5.5 Audit Log Backup Procedures

Audit logs and audit summaries are backed up or copied if in manual form.

Audit log collection / accumulation system is internal to C-DAC CA which have multilevel secure system to maintain the integrity of its electronic audit logs over time and has established a series of security procedures regarding their storage, access and backup.

CDAC-CA audit collection system is a combination of automated and manual processes. The system is maintained through access control mechanisms and role separations with regard to the software and hardware and through documented operational procedures know and followed by C-DAC CA personnel. The control measures of both automated and the manual processes are audited in accordance with of this CPS.

### 4.5.6 Vulnerability Assessments

CDAC-CA shall perform regular security assessment to identify internal and external threats, which could result in unauthorized access, disclosure, misuse, modification, or destruction of any certificate data or other classified sensitive data.

CDAC-CA shall review:

- Administrative Controls
- Technical Controls
- Physical Controls

## 4.6 Archival and Retention period

"Types of Event Recorded (Audit)" will be archived and retained as per IT ACT 2000.

### 4.6.1 Protection of Archive

C-DAC CA protects the archive so that only trusted personnel can obtain access. The electronic archive is restricted from unauthorized viewing, modification, and deletion by physical and logical controls.

Manual archive records will be protected from unauthorized viewing, modification and destruction.

### 4.6.2 Archive Backup Procedures

C-DAC CA periodically backs up electronic and manual archives as and when they are created. Copies of the archive shall be stored at the protected disaster recovery site.

### 4.6.3 Procedure to Obtain and Verify Archive Information

The CDAC CA shall verify the integrity of the backups at least once every six months. Information stored off-site shall be periodically verified for data integrity. Only authenticated and authorized personnel are allowed to handle the archive as per the procedure.

## 4.7 Key Changeover

a. The C-DAC CA keys shall be changed periodically as per IT Act.
b. Certifying Authority's keys and associated Certificates – ten years

## 4.8 Compromise and Disaster Recovery

C-DAC CA supports detailed Disaster Recovery Procedures.

### 4.8.1 Recovery Procedures used if CA Certificate is revoked

In case the C-DAC CA certificate is revoked a notice will be posted on the https://esign.cdac.in/ca website. Incident will be recorded investigated and remedial measures will be taken to avoid similar risk. Recovery Procedures shall be used if the Private Key is damaged. Subsequently, C-DAC CA shall obtain a new certificate from the CCA.

### 4.8.2 Secure Facility after a Natural or Other Type of Disaster

C-DAC CA shall operate as per its disaster recovery plan.

### 4.8.3 Incident Management Plan

An Incident Management Plan has been developed and approved by the management of C-DAC CA. The plan includes the following areas:

a. Certifying Authority's certification n key compromise
b. Hacking of systems and network
c. Breach of physical security
d. Infrastructure non availability

An incident response action plan has also been established to ensure the readiness of C-DAC CA to respond to incidents. The plan includes the following areas:

a. Compromise control
b. Notification to user community
c. Revocation of affected Digital signature Certificates
d. Responsibilities of personnel handling incidents
e. Service restoration
f. Monitoring and audit trail analysis.
g. Investigation of the incident

## 4.9 Termination

C-DAC CA will make arrangements for its records and Certificates to be archived in a manner prescribed by the IT Act.

a. CDAC-CA can decide to cease its services or for the expiry of the license with a prior notice of ninety days to CCA with its intention to cease acting as a Certifying Authority.
b. Shall advertise sixty days before the expiry of license of ceasing to act as Certifying Authority in a manner approved by the CCA.
c. CDAC-CA shall make reasonable effort to ensure that discontinuing its certification services causes minimal disruption to its subscribers and relying parties requiring to verify the Digital Signatures by reference to the public keys contained in outstanding Digital Signature Certificates.
d. Any Certificates issued after the announcement of the termination date shall have the expiration date not exceeding the termination date.
e. CDAC-CA has made necessary arrangements for preserving the records for a period of seven years, as stipulated in the IT ACT 2000.
f. CDAC-CA shall destroy the certificate signing private key after the date expiry mentioned in the license or intimation and confirm the date and time of destruction of the private key to the CCA.

# 5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

This section describes physical, environmental and personnel security controls applied by the C-DAC CA in order to perform securely the functions of authentication , key generation, certificate issuance, certificate revocation, audit and archival.

Following sections contain extracts from the C-DAC CA's Security Policy document.

The technical and physical infrastructure of the C-DAC CA including the disaster recovery site facilities, established for the operation of the C-DAC CA, and its Repositories shall be fully secured in accordance with the requirements laid down under the IT Act.

## 5.1 Physical Security Controls

### 5.1.1 Site Location and Construction

C-DAC CA has established facility for C-DAC CA operations with physical security standards as per the physical and operational security guidelines mentioned in the Information Technology Act.

### 5.1.2 Physical access

C-DAC CA has implemented necessary physical security controls to restrict access to C-DAC CA physical premises, relevant network, Hardware and Software. C-DAC CA has implemented various manual /automated access control mechanisms to restrict access to trusted members only on a need to know and need to use basis. These measures are in conformity with the physical and operational security guidelines mentioned in the Information Technology Act.

### 5.1.3 Power Supply and Air Conditioning

5.1.3.1 Continuous power supply has been ensured by suitable deployment of UPS and DG set.

5.1.3.2 The air conditioning system installed in the C-DAC CA Facility is maintained with recommended temperature and humidity control.

### 5.1.4 Water exposures

C-DAC CA site is constructed so as to minimize the potential water related threats. Entire IT equipment has been placed on the raised false floor. Also, a water level sensor has been placed below the floor to detect any water leakage and raise the alarm.

### 5.1.5 Fire prevention and protection

C-DAC CA has taken reasonable precautions to detect, prevent and extinguish fires or other damaging exposure to flame or smoke. CDAC-CA's fire prevention and protection measures have been designed to comply with local fire safety regulations, which are compliant with the IT Act.

### 5.1.6 Media storage

C-DAC CA storage media are protected from environment threats such as temperature, humidity and magnetic and electrostatic interference and from any unauthorized access to it in conformance with the IT Act.

### 5.1.7 Waste disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information is rendered unreadable by using methods as per CDAC CAs waste disposal procedures. Cryptographic modules will be zeroized or physically destroyed to make it unreadable. Other waste is disposed off in accordance with the waste disposal procedures and disposal requirements.

### 5.1.8 Off-site backup

All critical data shall be incrementally backed up and stored according to security measures mentioned in the IT Act.

## 5.2 Procedural Controls

### 5.2.1 Trusted roles

Trusted Roles are those people who have an access to C-DAC CA facility and perform various functions of C-DAC CA. The personnel selected to carry out these roles must be responsible and skilled so as maintain the integrity of the C-DAC CA operations. Each of these trusted members is limited to the actions required to be performed to fulfil their tasks and responsibilities based on need-to-know and least privilege principle.

### 5.2.2 Number of persons required per task

At least two trusted members using two individual authentications are required to perform CA administrative operations.

### 5.2.3 Identification and authentication for each role

5.2.3.1 An individual shall identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.2.3.2 C-DAC CA shall ensure that the personnel performing trusted roles —

a. Are restricted to actions authorised for their role through the use of their user account and/or digital certificate and C-DAC CA software and procedural controls.
b. Are using tokens /smart cards as access mechanisms to HSM / CA.

## 5.3 Personnel Controls

### 5.3.1 Background, qualifications, experience, and clearance requirements

A person is enrolled to the required role in CDAC post verifying the proof of background, qualification and experience needed to perform their prospective job responsibilities competently and satisfactorily verified as per C-DAC rules and regulations.

### 5.3.2 Background Check Procedures

C-DAC has followed appropriate government procedures for appropriate investigation of all personnel.

### 5.3.3 Training Requirements

C-DAC has provided comprehensive training to all the technical personnel for performing duties in the following areas:

a. Comprehensive training with respect to the duties to be performed
b. Awareness Relevant aspects of the IT Security Policy and Security Guidelines framed in IT (CA) Rules, 2000;
c. Training in the PKI software used to perform the operations
d. Training in the Disaster recovery and continuity procedures
e. Incident handling and reporting

### 5.3.4 Re-training frequency and requirements

Refresher training of technical personnel is conducted as and when required and once in a year. C-DAC reviews these requirements on a regular basis.

### 5.3.5 Job Rotation Frequency and Sequence

No Stipulation

### 5.3.6 Sanctions for unauthorized actions

If a trusted personnel is found guilty or an attempt for an unauthorized action, access to the facility and the operation system would be suspended immediately and an investigation would be invoked. Further disciplinary actions will be initiated as per C-DAC rules.

### 5.3.7 Contracting personnel requirements

Contractors are allowed access to the C-DAC CA facility, only under the supervision and presence of C-DAC CA trusted members.

### 5.3.8 Documentation supplied to personnel

Necessary provision is made to access required documents that would enable the respective personnel duties in consistent, competent and satisfactory manner. The document access to the role is subject to *need to use* and *need to know* basis.

# 6. TECHNICAL SECURITY CONTROLS

This section describes the necessary technical controls and procedures that are to be applied and followed in order to secure C-DAC CA in order to perform securely the functions of key generation, relying party authentication, certificate issuance, certificate revocation, audit and archival.

## 6.1 Key Pair Generation and Installation

### 6.1.1 Key Pair Generation

CDAC CA key pairs will be generated by at least five/four trusted personnel in pre-planned key generation ceremonies as per the key-generation procedures approved by CDAC CA. The events will be recorded, the procedure followed will be documented, internally audited and signed by all the trusted person involved in the key generation activity and will be stored for audit requirements for a period of time deemed appropriate

C-DAC CA's key pairs are generated using the trustworthy C-DAC CA Controlled key generation software and hardware. The cryptographic modules used for key generation meet the requirements of FIPS 140-2 level 3.

Subscribers, key pairs will be generated by eSign Service of ~~at~~ C-DAC CA in CDAC CA premises that shall be used for one time signing and shall be stored for a maximum of 30 minutes as per the e-authentication guidelines.

The key generation process shall generate statistically random key values that are resistant to known attacks.

### 6.1.2 Private Key Delivery to Entity

C-DAC CA private key is generated at system initialization stage. There is no requirement to deliver this key as this key remains in the C-DAC CA System.

Subscriber private key is generated at C-DAC CA end and since it is to be used only once for signing purpose and hence requires no delivery.

C-DAC CA Keys are generated in the highly secured storage device. C-DAC CA private key is stored on C-DAC CA's HSM conform to FIPS 140-2 level 3 .

### 6.1.3 Public Key Delivery to Certificate Issuer

C-DAC CA Public key shall be delivered to the Root CA as a PKCS 10 request. The media will be delivered to Root CA by trusted personal in a compact along with an authorisation letter from CA authorised representative.

For subscribers, C-DAC CA supports the requirements, where the public key is delivered to C-DAC CA using secure online channel.

### 6.1.4 C-DAC CA Public Key Delivery to Users

C-DAC CA supports the requirements where the CA public key certificate is available at C-DAC CA website and can be downloaded from the C-DAC CA Repository.

### 6.1.5 Key Sizes

The asymmetric key pair in C-DAC CA will be at least 2048 bits for Subscribers and C-DAC CA key pair will be of 2048 bits.

### 6.1.6 C-DAC CA Public Key Parameters Generation

C-DAC CA Application is configured to set parameters for CA public key & Subscriber Public key generation.

### 6.1.7 Hardware/Software Key Generation

C-DAC CA's key pairs is generated in a trustworthy hardware cryptographic module as described in Section 6.5

### 6.1.8 Key Usage Purposes (as per X.509 vv3 key usage field)

Key usage purposes are incorporated in C-DAC CA as detailed in chapter 7 Certificate and CRL profiles.

C-DAC CA ensures that CA signing key is the only key permitted to be used for signing Certificates and CRLs.

### 6.1.9 Time Stamp

All critical servers used in C-DAC CA setup is synchronized with national time source directly or indirectly. Accordingly, C-DAC CA will offer time stamping services. Time stamping server shall be synchronized to IST through NPL.

## 6.2 Private Key Protection

### 6.2.1 Standards for Cryptographic Module

The cryptographic module used by C-DAC CA system to generate CA keys is designed to comply with FIPS 140-2 level 3. Also Refer to Section 6.5

CADC CA has taken necessary measures to ensure that key pairs will be generated for eSign Service of CDAC CA is secured by HSM

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

C-DAC CA private key which is accessed through the hardware security module (HSM) requires the presence of two (2) out of three (3) persons to complete the generation successfully No single C-DAC CA trusted personnel is allowed to generate the CA private key. For accessing the HSM, minimum 2 out of 3 persons are required.

### 6.2.3 Private Key Backup

6.2.3.1 C-DAC CA has backed up its private keys. Backed up keys are stored in encrypted form and protected at a level no lower than those followed for storing the primary version of the key.

6.2.3.2 The CA's private key backups are stored in a secure storage facility away from where the original key is stored.

6.2.3.3 C-DAC CA shall not backup the private key of the subscriber.

6.2.3.4 Private Key Archival: C-DAC CA's private key shall be archived.

6.2.3.5 C-DAC CA private key is generated, within the cryptographic module, and cannot be not accessed by other entities. In all cases, private key is stored in an encrypted format in C-DAC CA and is decrypted only at the time of being used.

6.2.3.6 Method of Activating Private Key

All cryptographic functions are performed within the cryptographic module. The private key is never directly accessed by any other function. Activation functions are supported on the HSMs using hardware based tokens.

Method of Deactivating Private Key: The deactivation occurs when hardware token is removed.

6.2.3.7 Public Key Archival: C-DAC CA public key is archived as specified by the IT Act 2000.

6.2.3.8 Usage periods: Maximum usage period for the Public and Private keys of C-DAC CA – ten Years.

6.2.3.9 Usage period for the Public and Private keys of Subscriber – one time usage within in a maximum period of 30 minutes.

## 6.3 Computer/Systems Security Controls

### 6.3.1 Specific computer security technical requirements

CA PKI operation and data are carried on trustworthy computer system with the following requirements:

- CA software's are run on dedicated hardened computer system.
- The computer system has restricted access control with least privilege and on need-to-know basis.
- Multifactor authentication is applied for defense in depth with strong password policy.
- Physical access to the system and operation on CA system is allowed to only authorized CDAC-CA trusted personnel.

The computer security technical requirements are in accordance with IT Security Guidelines of IT CA Rules, 2000.

## 6.4 Network Security Controls

C-DAC CA has secured network in accordance with CDAC-CA security policies. The network is logically separated from other components. Network security controls are deployed. The communication between the network devices are encrypted. CDAC-CA uses UTM, firewalls to protect the CA network from internal and external intrusion and limit the nature and source of network activities that may access CA systems.

## 6.5 Cryptographic Module Engineering Controls

The cryptographic operations controls in C-DAC CA are validated to FIPS 140-2 Level 3 functionality and assurance.

# 7. CERTIFICATE AND CRL PROFILES

## 7.1 Certificate Profile

This section defines Certificate Profile and Certificate content requirements for Certificates issued under this CPS. The CDAC-CA Certificates issued under this CPS conform to the following:

- X-509 Version 3 digital Certificate

CA certificate Profile

The following tables show the basic fields for CA Certificates:

| | |
|---|---|
| Version | Version 3 |
| Serial number | Positive number of maximum Length 20 bytes and unique to each certificate issued by a issuer CA |
| Signature Algorithm | SHA256 with RSA Encryption (null parameters |
| Issuer DN | Subject DN of the issuing CA |
| Validity | Validity expressed in UTC Time for certificates valid through 2049 |
| Subject DN | The X.500 distinguished name of the entity associated with the public key certified in the subject public key field of the certificate (Common Name (CN),House Identifier, Street Address, State / Province, Postal Code, Organisational Unit (OU),Organisation (O),Country (C) ) |
| Subject Public Key | rsaEncryption {1 2 840 113549 1 1 1}, 2048 RSA Key modulus, public exponent |
| Signature | Issuer CA's signature |

**User certificate**

The following tables show the basic fields for user Certificates:

| | |
|---|---|
| Version | Version 3 |
| Serial number | Positive number of maximum Length 20 bytes and unique to each certificate issued by a issuer CA |
| Signature Algorithm | SHA256 with RSA Encryption (null parameters |

| | |
|---|---|
| Issuer DN | Subject DN of the issuing CA |
| Validity | Validity expressed in UTC Time for certificates valid through 2049 |
| Subject DN | The X.500 distinguished name of the entity associated with the public key certified in the subject public key field of the certificate ( Common Name, Serial Number, Unique Identifier, State or Province Name, Postal Code, Telephone number, Pseudonym, Organisation, Country) |
| Subject Public Key | rsaEncryption {1 2 840 113549 1 1 1}, 2048 RSA Key modulus, public exponent |
| Signature | Issuer CA's signature |

### 7.1.1 Version Number(s)

C-DAC CA Certificate is x.509 version 3 in accordance with ITU-T Rec. X.509 (2000)

### 7.1.2 Certificate Extensions Populated

The following tables shows the minimum extensions for CA Certificates:

| | |
|---|---|
| authorityKeyIdentifier | Identifies the CA certificate that must be used to verify the CA certificate. It contains subjectKeyIdentifier of the issuing CA certificate |
| subjectKeyIdentifier | unique value associated with the Public key |
| basicConstraints | CA Boolean = True, pathLenConstraints 0 |
| keyUsage | keyCertSign and cRLSign |
| certificatePolicies | The value must contain the OID representing the India PKI certificate policy the certificate is valid for . (Policy Identifier=2.16.356.100.2) |
| cRLDistributionPoints | location of CRL information |
| authorityInfoAccess | location of OCSP Responder (only required if OCSP is needed to check revocation status of CA Certificate) |

**User certificate**

The following tables shows the minimum extensions for user Certificates

| | |
|---|---|
| authorityKeyIdentifier | Identifies the CA certificate that must be used to verify the subscriber's certificate. Issuing CA SubjectkeyIndetifier |
| subjectKeyIdentifier | Octet String of unique value associated with the Public key |
| basicConstraints | CA=False |
| keyUsage | DigitalSignature, nonRepudiation(optional) |
| certificatePolicies | The value must contain the OID representing the India PKI certificate policy the certificate is valid for .( (Policy Identifier=2.16.356.100.2.4.1) |
| cRLDistributionPoints | location of CRL information |

### 7.1.3 Algorithm Object Identifiers

C-DAC CA supports the following algorithms –

a. RSA 2048 digital signature in accordance with PKCS#1

b. RSA 2048 key transfer in accordance with Internet RFC 1421 and 1423 and PKCS#1
c. SHA-2 in accordance with US FIPS PUB 180-1 and ANSI X9.30 (Part2)
d. Triple-DES in accordance with ANSI X9.52
e. Message Authentication Code (MAC) in accordance with US FIPS PUB 113, ANSI X9.9 and X9.19
f. DSA, ECDSA, AES, DES, IDEA, CAST-128

#### 7.1.4 Name Forms

C-DAC CA supports unique person name for the following categories of Subscriber –

a. Individual

## 7.2 CRL Profile

Certificate Revocation List issued by C-DAC CA under this CPS shall contain the list of revoked certificates.

#### 7.2.1 Version Number

X-509 Version 2 CRL (RFC 2459 "Internet X.509 Public Key Infrastructure Certificate and CRL Profile)

The support for CRL extensions including, Issuing Distribution Point, CRL Number and Authority Key Identifier

# 8. SPECIFICATION ADMINISTRATION

This section brings out the change control, publication related policies and CPS approval procedures.

## 8.1 Specification Change Procedure

Prior to making any of these changes in C-DAC CA CPS, C-DAC CA shall obtain comments from the relevant agency and shall be submitted to the CCA for approval. Comments received shall be reviewed by C-DAC CA management. The decision to implement the proposed changes is at the sole discretion of C-DAC CA management, subject to approval from CCA. C-DAC CA will adhere to its change management control procedures. Changes to the CPS will be notified to the CCA as and when they are made. Current version of the CPS will be available at C-DAC CA website.

## 8.2 Publication and Notification Policies

8.2.1 All items in C-DAC CA CPS are subject to the publication and notification requirement.

8.2.2 All publication will be done via C-DAC CA website at https://esign.cdac.in/ca

## 8.3 Approval Procedure

Once a revised CPS is ready, C-DAC CA shall submit the propsed changes to the CCA for approval. The changes shall be adopted only after due approval from the CCA for its publication on C-DAC CA web site.