Certification Practice Statement (CPS)

Version 4.1.0

November 21, 2023

OID: 2.16.356.100.1.9.2

DEEPAK KUMAR
Digitally signed by DEEPAK KUMAR
Date: 2023.12.27 12:39:47 +05'30'

Published by

Centre for Development of Advanced Computing (C-DAC)

Ministry of Electronics & Information Technology

Government of India

Approved by

Controller of Certifying Authorities

CERTIFICATION PRACTICE STATEMENT

Document Name	CPS of C-DAC CA
Release	Version 4.1.0
Status	Current
Issue Date	21-11-2023

DEFINITIONS

The following definitions are to be used while reading this CPS. Unless otherwise specified, the word "CA" used throughout this document refers to C-DAC CA, likewise CPS means CPS of C-DAC CA. Words and expressions used herein and not defined but defined in the Information Technology Act, 2000 and subsequent amendments, hereafter referred to as the ACT shall have the meaning respectively assigned to them in the Act.

The following terms bear the meanings assigned to them hereunder and such definitions are applicable to both the singular and plural forms of such terms:

- **"Act"** means Information Technology IT Act, 2000
- **"ITAct"** Information Technology IT Act,2000, its amendments, Rules thereunder, Regulations and Guidelines Issued by CCA
- **"ASP" or "Application Service Provider**" is an organization or an entity using Electronic Signature as part of their application to facilitate the user for requesting issuance and electronically sign the content through any empanelled ESP.
- **"Auditor**" means any accredited computer security professional or agency recognized and engaged by CCA for conducting audit of operation of CA;
- **"CA**" refers to C-DAC CA, a Certifying Authority, licensed by Controller of Certifying Authorities (CCA), Govt. of India under provisions of ITAct, and includes CA Infrastructure issuing Digital Signature Certificates & also for providing Trust services such as TS, OSCP & CRL
- **"CA Infrastructure"** The architecture, organization, techniques, practices, and procedures that collectively support the implementation and operation of the CA. It includes a set of policies, processes, server platforms, software and work stations, used for the purpose of administering Digital Signature Certificates and keys.
- "**CA Verification Officer**" means trusted person involved in identity and address verification of DSC applicant and according approval for issuance of DSC.
- "**Certification Practice Statement or CPS**" means a statement issued by a CA and approved by CCA to specify the practices that the CA employs in issuing Digital Signature Certificates;
- **"Certificate"**—A Digital Signature Certificate issued by CA.
- **"Certificate Issuance"**—The actions performed by a CA in creating a Digital Signature Certificate and notifying the Digital Signature Certificate applicant (anticipated to become a subscriber) listed in the Digital Signature Certificate of its contents.
- **"Certificate Policy"—**The India PKI Certificate Policy laid down by CCA and followed by CA addresses all aspects associated with the CA's generation, production, distribution, accounting, compromise recovery and administration of Digital Signature Certificates.
- **Certificate Revocation List (CRL)—**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.

- **"Controller" or "CCA"** means the Controller of Certifying Authorities appointed as per Section 17 subsection (1) of the Act.

- **Crypto Token/Smart Card—**A hardware cryptographic device used for generating and strong user's private key(s) and containing a public key certificate, and, optionally, a cache of other certificates, including all certificates in the user's certification chain.

- **"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 IT Act;

- **"Digital Signature Certificate Applicant" or "DSC Applicant" —**A person that requests the issuance of a Digital Signature Certificate by a Certifying Authority.

- **"Digital Signature Certificate Application" or "DSC Application" —**A request from a Digital Signature Certificate applicant to a CA for the issuance of a Digital Signature Certificate

- **Digital Signature Certificate -** Means a Digital Signature Certificate issued under sub-section (4) of section 35 of the Information Technology Act, 2000.

- **"ESP" or "eSign Service Provider"** is a Trusted Third Party as per definition in Second Schedule of Information Technology Act to provide eSign service. ESP is operated within CA Infrastructure & empanelled by CCA to provide Online Electronic Signature Service.

- **Organization -** An entity with which a user is affiliated. An organization may also be a user.

- **"Private Key**" means the key of a key pair used to create a digital signature;

- **"Public Key**" means the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate;

- **"Registration Authority" or "RA"** is an entity engaged by CA to collect DSC Application Forms (along with supporting documents) and to facilitate verification of applicant's credentials

- **"Relying Party**" is a recipient who acts in reliance on a certificate and digital signature.

- **"Relying Party Agreement"** Terms and conditions published by CA for the acceptance **of** certificate issued or facilitated the digital signature creation.

- **"Subscriber Identity Verification method**" means the method used for the verification of the information (submitted by subscriber) that is required to be included in the Digital Signature Certificate issued to the subscriber in accordance with CPS. CA follows the Identity Verification Guidelines laid down by Controller.

- **Subscriber** - A person in whose name the Digital Signature Certificate is issued by CA.

- **Time Stamping Service**: A service provided by CA to its subscribers to indicate the correct date and time of an action, and identity of the person or device that sent or received the time stamp.

- **Subscriber Agreement** - The agreement executed between a subscriber and CA for the provision of designated public certification services in accordance with this Certification Practice Statement

- **Time Stamp -** A notation that indicates (at least) the correct date and time of an action, and identity of the person or device that sent or received the time stamp.

- "**Trusted Person**" means any person who has:

    i. Direct responsibilities for the day-to-day operations, security and performance of those business activities that are regulated under the Act or Rules in respect of a CA, or

    ii. Duties directly involving the issuance, renewal, suspension, revocation of Digital Signature Certificates (including the identification of any person requesting a Digital Signature Certificate from a licensed Certifying Authority), creation of private keys or administration of CA's computing facilities.

Contents

1. Introduction

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

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.

The structure of this document is generally in conformity to the RFC 3647- 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.

The term "Certifying Authority" or CA as used in this CPS, refers to C-DAC CA. as the entity that holds the CA license from the Controller of Certifying Authorities (CCA), Govt. of India.
India PKI is a hierarchical PKI with the trust chain starting from the Root Certifying Authority of India (RCAI). RCAI is operated by the Office of Controller of Certifying Authorities, Government of India. Below RCAI there are Certifying Authorities (CAs) licensed by CCA to issue Digital Signature Certificates under the provisions of ITAct. These are also called Licensed CAs. C-DAC CA is a Licensed CA under RCAI.

1.1. Overview of CPS

India PKI CP defines certificate policies to facilitate interoperability among subscribers and relying parties for e-commerce and e-governance in India. The CP and Certifying Authorities (CAs) are governed by the Controller of Certifying Authorities (CCA). Certificates issued by CAs contain one or more registered Certificate Policy OID, which may be used by a Relying Party to decide whether a certificate can be trusted for a particular purpose.

The Certification Practice Statement (CPS) of C-DAC CA details the practices and operational procedures implemented to meet the assurance requirements. This CPS is consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practice Statement Framework. Controller of Certifying Authority issues licence to operate as Certifying Authority subject to successful compliance audit of CA per the CPS. The CPS is also

(i) intended to be applicable to and is a legally binding document between the CA, the Subscribers, the applicants, the Relying Parties, employees and contractors; and
(ii) intended to serve as notice to all parties within the context of the CA CPS

CPS refers to the various requirements specified under the following guidelines issued by CCA

(i) The identity Verification Guidelines [CCA-IVG]: For the identity verification for different types of certificates like personal, organizational person, SSL, encryption, code signing, system certificate etc.
(ii) Interoperability Guidelines for DSC [CCA-IOG]: For the certificate profile including content and format of the certificates, key usage, extended key usage etc.
(iii) X.509 Certificate Policy for India PKI [CCA-CP]: Assurance Class, Certificate policy id, validity of certificates, key size, algorithm, storage requirements, audit parameters etc.
(iv) e-Authentication guidelines [CCA-eAUTH]: The security procedures for key generation, key protection and audit logs, signature format, identity verification requirements etc.
(v) Security Requirements for Crypto Devices [CCA-CRYPTO]: The crypto device management & security requirements for holding subscribers' private key.
(vi) CA Site Specification [CCA-CASITESP]: Requirements for the construction of cryptographic site and security requirements.

1.2. Identification

The contact details are mentioned in section 1.5.2 of this CPS.

The following are the levels of assurance defined in the Certificate Policy. Each level of assurance has an OID that can be asserted in certificates issued by CA if the certificate issuance meets the requirements for that assurance level. The OIDs are registered under the CCA are as follows:

Assurance Level	**OID**
eKyc - Single Factor	2.16.356.100.2.4.1
eKyc – Multi Factor	2.16.356.100.2.4.2

The OIDs allocated to CA and CPS are as given below

Serial.	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 PKI Participants

1.3.1 PKI Authorities

1.3.1.1 Controller of Certifying Authorities (CCA)

In the context of the CPS, the CCA is responsible for:

1. Developing and administering India PKI CP.

2. Compliance analysis and approval of the licensed CAs CPS;
3. Laying down guidelines for Identity Verification , Interoperability of DSCs and Private Key storage
4. Ensuring continued conformance of Licensed CAs with the CPS by examining compliance audit results.

1.3.1.2 CA

The C-DAC CA is licensed by CCA as per Information Technology Act. The primary function of CA is to issue end entity certificates. The issuance of DSC is allowed only to users of eSign Service of C-DAC CA. The applicants are electronically authenticated to the eKYC services of C-DAC CA or other specified eKYC services by CCA.

C-DAC CA certificates are certified by Root Certifying Authority of India (RCAI). In India PKI hierarchy, Root certificate is the trust anchor for CA certificates. The following are the CA Certificates issued to CA.

Sl. No	CA Name	Certified by
1	C-DAC CA 2014	CCA India 2014
2	C-DAC CA 2022	CCA India 2022

CA created Sub-CAs to issue Digital Signature Certificates to end entities. Sub-CAs issue only short validity Digital Signature Certificates of 30 minutes to subscribers and CA do not suspends or revokes end-user Digital Signature Certificates. CA may suspend or revoke the Sub-CA Certificates. The CA maintains the Certificate Revocation List (CRL) CA for the revoked and suspended Digital Signature Certificates in its repository. CRL is signed by the issuing CA.

1.3.2 PKI Services

(i) **Certificate Services:** The Certificates issued by C-DAC CA are only for the purpose of eSign service. CA issues two classes of Certificates based on the verification and authentication requirements specified under CCA-IVG

(ii) **CRL Services:** CA makes available CRL on the URLs as listed below - freely downloadable by subscribers and relying parties, the details of the CRLs are mentioned below;

No	CA	CRL on the URLs
1	C-DAC CA 2014	https://esign.cdac.in/ca
2	C-DAC CA 2022	

(iii) **OCSP (Online Certificate Status Protocol) Validation Services:** CA provides OCSP validation services to Relying Parties for certificate status verification in real-time. The OCSP service of the CA is operated as per CCA-OCSP

(iv) **eSign online Digital Signature Services:** CA is empaneled as ESP to offer eSign online Digital Signature Service as per the CCA-EAUTH. e-KYC class of certificates will be issued as stated under CCA-CP.

eSign-Online Digital Signature Services is based on online Aadhaar eKYC or eKYC by CA. For CA eKYC-based eSign service or issuance of DSC, applicants are required to create an

eKYC account with CA. CA carries out the verification based on the following modes mentioned in CCA-IVG

1. Online Aadhaar eKYC,
2. Off-line Aadhaar eKYC

The DSCs are issued to applicants for document signing provided through the eSign Service of CA. The applicants are electronically authenticated to the eKYC services of CA or other specified eKYC services by CCA. CA provide a direct interface to the applicant for providing authentication information and also for accessing eKYC information retained in the CA eKYC database. CA issue short validity Digital Signature Certificates of 30 minutes to eSign users directly. After the generation of DSC and signature creation, ESP of CA ensures that the private keys are destroyed immediately. The subscriber's private key storage requirements are not applicable in this mode of DSC issuance.

CA does not suspend or revokes eKYC classes of Digital Signature Certificates. However, the CA maintains a null Certificate Revocation List (CRL) in its repository to satisfy the requirements of relying party applications. CRL is signed by issuing CA. Similarly, re-key and renewal do not apply to eKYC classes of Digital Signature Certificates.

The identity and address of the DSC applicant are obtained based on the authentication of the DSC applicant to the eKYC service. To retain the eKYC of the applicant by CA, the process of the applicant's identity verification is followed as specified under CCA-IVG. In the case of external eKYC service, the response received from the eKYC provider will be accepted provided with eKYC provider provides an eKYC response directly to CA up on the authentication by the applicant. The list of approved eKYC providers is specified by CCA and listed in CCA-eAUTH.

ESP of CA facilitates DSC application form generation; key generation of DSC applicant based on the authentication provided by the DSC applicant and ensures that the applicant's identity information and public key are properly bound. Additionally, the CA records the process that was followed for the issuance of each certificate. The process documentation and authentication requirements are as specified in the CCA-eAUTH and CCA-IVG.

Once the verification of the applicant is carried out and recorded in the CA eKYC database, the issuance of eKYC classes of DSC is implemented in an automated environment with the requirement of authentication of the applicant to the eKYC database. Issuance of eKYC classes and Class1-3 of DSCs are carried out from separate certificate issuance systems.

The users of the Application Service Provider (ASP) interface with ESP of CA for Signature and DSC issuance through the ASP gateway. ASPs are registered with the ESP of CA after a verification process. CA verifies the source of the request and authenticates users directly for each certificate request received from ASP before DSC issuance. Certificates are electronically verified to ensure that all the fields and extensions are properly populated. The certificates are of one-time use and the issued certificates are achieved. The private keys of applicants are destroyed immediately after certificate generation and signature function. The signatures along with the certificate are delivered to the end entity subscribers.

In the case of issuance of eKYC classes of DSC to the users of eSign Service, the requirements specified above will override the requirements specified for Class 1-3 in the respective sections of this CPS.

(v) **Time Stamping Service:** CA Provides Time Stamping Service as per CCA-TSP.

1.3.3 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate, who asserts that it uses its key and certificate in accordance with the certificate policy asserted in the certificate, and who does not itself issue certificates.

1.3.4 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The Relying Party can use the certificate to verify the integrity of a digitally signed message, or to identify the creator of a message. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

1.3.5 Applicability

C-DAC CA issues the following classes of certificates. The Assurance level and Applicability as defined under India PKI CP is given below

Assurance Level	Assurance	Applicability
eKYC - Single Factor	eKYC -Single Factor class of certificates shall be issued based on Single Factor authentication of subscriber to the applicable eKYC services. These certificates will confirm that the information in Digital Signature certificate provided by the subscriber is same as information retained in the eKYC databases pertaining to the subscriber	This level is relevant to environments where Single Factor authentication to eKYC service 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.
eKYC - Multi Factor	eKYC -Multi Factor class of certificates shall be issued based on Multi Factor authentication of subscriber to the applicable eKYC services. These certificates will confirm that the information in Digital Signature certificate provided by the subscriber same as information retained in the eKYC databases pertaining to the subscriber.	This level is relevant to environments where Multi Factor authentication to eKYC service 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

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Certificate usage is governed by the IT Act of 2000 and Interoperability Guidelines published by CCA.

1.4.2 Prohibited Certificate Uses

Certificate usage is governed by the IT Act of 2000 and Interoperability Guidelines published by CCA.

1.5 Policy Administration

1.5.1 Organization administering the document

This CPS is administered by CA and is revised with the approval of CCA.

1.5.2 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

For more information or for feedback:
Visit C-DAC CA Portal at https://esign.cdac.in/ca.
Contact helpdesk at ess@cdac.in.

1.5.3 Person Determining Certification Practice Statement Suitability for the Policy

The determination of suitability of a CPS will be based on an independent auditor's results and recommendations.

1.5.4 CPS Approval Procedures

The CCA approve CPS of the CA and auditor's assessment will also be taken into account.

1.5.5 Waivers

There shall be no waivers to this CPS.

2 Publication & PKI Repository Responsibilities

2.1 PKI Repositories

CA maintains repository that contain the following information:

1. CA Certificates
2. Certificate Revocation List (CRL)
   a) Issued by the Licensed CA /Sub-CA
3. Digital Signature Certificates issued by CA/Sub-CA

2.1.1 Repository Obligations

CA maintains a repository and is available at https://esign.cdac.in/ca

2.2 Publication of Certificate Information

2.2.1 Publication of CA Information

See Section **Error! Reference source not found.**.

2.2.2 Interoperability

See Section **Error! Reference source not found.**.

2.3 Publication of Certificate Information

CA Certificates and CRLs are published as specified in this CPS in Section **Error! Reference source not found..**

2.4 Access Controls on PKI Repositories

The PKI Repository information which is not intended for public dissemination or modification is protected.

3 Identification & Authentication

The requirements for identification and authentication are specified under Information Technology Act, Rules and Guidelines issued there under. Before issuing a Certificate, the CA ensure that all Subject information in the Certificate conforms to the requirements that has been verified in accordance with the procedures prescribed in this CPS.

3.1 Naming

3.1.1 Types of Names

CAs issue certificates containing an X.500 Distinguished Name (DN) in the Issuer and Subject fields. Subject Alternative Name may also be used, and is marked as non-critical. Further requirements for name forms are specified in [CCA-IOG].

3.1.2 Need for Names to be Meaningful

The certificates issued pursuant to this CPS shall take care of the following

(i) Names used in the certificates identify the person in a meaningful way.
(ii) The DNs and associated directory information tree reflect organizational structures.
(iii) The common name represents the legal name of the subscriber.

3.1.3 Anonymity of Subscribers

CA does not issue subscriber certificates with anonymous identities.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms shall be in accordance with applicable Standards.

3.1.5 Uniqueness of Names

Name uniqueness for interoperability or trustworthiness is enforced in association with serial number.

3.1.6 Recognition, Authentication & Role of Trademarks

No stipulation.

3.1.7 Name Claim Dispute Resolution Procedure

The CA resolves any name collisions (in association with serial number) brought to its attention that may affect interoperability or trustworthiness.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

No stipulation

3.2.2 Authentication of Organization user Identity

No stipulation

3.2.3 Authentication of Individual Identity

The identity and address of the DSC applicant is obtained based on the authentication of DSC applicant to eKYC service. In order to retain eKYC of applicant by CA, the process of

applicant's identity verification is followed as specified under CCA-IVG. In the case of external eKYC service, the response received from eKYC provider will be accepted provided with eKYC provider provides eKYC response directly to CA up on authentication by applicant. The list of approved eKYC providers are specified by CCA and published in CCA-eAUTH.

CA facilitates key generation of DSC applicant and ensures that the applicant's identity information and public key are properly bound. Additionally, the CA records the process that was followed for issuance of each certificate. The process documentation and authentication requirements are as specified in the CCA-eAUTH and CCA-IVG

3.2.3.1 Authentication of Component Identities

No stipulation

3.2.4 Non-verified Subscriber Information

CA does not include non-verified Information of DSC applicant in certificates.

3.2.5 Validation of Authority

For the validation of eKYC response received from external eKYC provider, the digital signature of the external eKYC provider is verified.

3.2.6 Criteria for Interoperation

Certificates are issued in accordance with CCA-IOG in order to ensure interoperability.

3.3 Identification and Authentication for Re-Key Requests

No stipulation

3.4 Identification and Authentication for Revocation Request

No stipulation

4 Certificate Life-Cycle Operational Requirements

Communication among the CA, eKYC provider and subscriber are implemented with requisite security services (i.e., source authentication, integrity, non-repudiation, or confidentiality) applied to them commensurate with the assurance level of the certificate being managed.

No physical documents are involved in the DSC issuance process. All electronic logs sufficient to establish the eKYC enrolment (if applicable) and authentication are archived. CA implemented the mechanism, at least as strong as the certificates being managed, to secure web site using Secure Socket Layer (SSL) certificate and set up with appropriate algorithms and key

sizes satisfies the integrity and confidentiality requirements for certificate management. Based on the content of communication, all, or none of the security services are enforced.

4.1 Certificate requests

The ESP services provided by CA facilitate DSC application form generation, Key pair generation and submission of certificate request to CA based on the authentication provided by DSC applicant.

CA may trust on the response received from well recognized national data base or enroll DSC applicants directly to build their own eKYC database. The process for enrolling users to their own eKYC database is specified under section 5 of CCA-IVG.

4.1.1 Submission of Certificate Application

Ref 4.1

4.1.2 Enrollment Process and Responsibilities

Ref 4.1

4.2 Certificate Application Processing

CA provide interface to applicant to provide authentication for accessing eKYC information retained in the CA eKYC database. In the case of external eKYC service, the direct receipt of digitally signed response from eKYC provider is accepted.

4.2.1 Performing Identification and Authentication Functions

See Section 3.2.3

4.2.2 Approval or Rejection of Certificate Applications

ESP submit Certificate Applications to the CA for processing could result in either approval or denial.

4.3 Certificate Issuance

For the applicant, the ESP services provided by CA submit DSC application form and request to CA. Upon successful verification of source DSCs are issued by CA. The acceptance or rejection is depending on user authentication and consent.

4.3.1 CA Actions during Certificate Issuance

CA verifies the source of a certificate request before issuance. ESP of CA ensures that the private keys are generated on HSM. Certificates are electronically verified to ensure that all the fields and extensions are properly populated. After generation of DSC, ESP of CA ensures that

the private keys are destroyed. The certificates are of one time use and 30 minutes validity .The issued certificates are achieved

4.3.2 Notification to Subscriber of Certificate Issuance

The issuances of DSCs are tightly integrated with application. CA will notify the subject (End Entity Subscriber) of certificate issuance through application response.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The certificates are of one time use and the applicants can accept or reject DSCs after receipt.

4.4.2 Publication of the Certificate by the CA

The issued DSCs are archived by CA for seven years.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The key pair generation is facilitated by ESP of CA and destroyed after signature creation and certificate generation.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties are required to use public key certificates and associated public keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates.

4.6 Certificate Renewal

No stipulation

4.7 Certificate Re-Key

No stipulation

4.8 Certificate Modification

No stipulation

4.9 Certificate Revocation and Suspension

No stipulation

4.10 Certificate Status Services

CA supports the Online Certificate Status Protocol (OCSP) for obtaining the revocation status of Sub-CA certificates

5 Facility Management & Operational Controls

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

C-DAC CA 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 Controls

CA operation premises are actively monitored with redundant power and notification methods. Sensitive areas within the facility, such as power and network connection are also controlled within the protected facility.

The operation site has multiple tiers of security enforced through Photo ID badges, proximity cards and biometric access devices. All visitors are escorted by trusted persons and every visitor signs the visitor's log.

The facility is continually staffed (24x7), either by trusted persons or by an on-site guard service during non-business hours.

5.1.1 Site Location and Construction

C-DAC 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).

The system components and operation of CA are contained within a physically protected environment to deter, detect and prevent unauthorized use of, access to, or disclosure of sensitive information. The physical security standards are modeled as per the physical and operational security guidelines mentioned in the Information Technology Act.

CA's primary site consists of Five physical security tiers comprising of:

Tier 1: The common area in the vicinity of the CA operations set-up where in physical access check is performed. This is the area where common facilities are incorporated.

Tier 2: This is the first level where CA operations commence. This is manned by physical security personnel and also enforces physical proximity access control restricting entries only to CA authorized personnel.
Tier 3: Enables two factor authentications (biometrics and physical proximity). The receiving and dispatch are carried out in this area.
Tier 4: This is where the core CA operations are housed. Servers are installed in this area.
Tier 5: Certificate issuance and revocation is done in this area which houses the Certificate Manager server. The Key Ceremony is also done here. The HSM module is housed in this area.

5.1.2 Physical access

Necessary physical security controls to restrict access to physical premises, relevant network, hardware and Software of C-DAC 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 C-DAC CA data center facility are always escorted by authorized official after requisite approval and the same is recorded.

5.1.2.1 CA Physical Access

CA has implemented mechanism to protect equipment from unauthorized access.

The physical security requirements laid down for the CA equipment are:

1. No unauthorized access to the hardware is permitted
2. All removable media and paper containing sensitive plain-text information is stored in secure containers
3. All entry/exits are monitored either manually or electronically.
4. access logs are maintained and inspected periodically
5. Multiple layers of increasing security are provided in areas such as perimeter, building, and CA room

5.1.3 Power and Air Conditioning

C-DAC CA 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

C-DAC CA datacenter facility has been constructed to minimize the risk of the threats related to water. Datacenter facility of C-DAC 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 C-DAC CA/ eSign operations can be shifted to disaster recovery site.

5.1.5 Fire prevention and protection

C-DAC CA 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

C-DAC 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 C-DAC 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

C-DAC CA shall perform the secured transfer & disposal of media as per its Policy for Electronic waste (e-Waste) Management & Policy for Media Handling & Security, C-DAC CA 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

C-DAC 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 C-DAC CA who have an access to C-DAC CA facility or control the operations of C-DAC CA are considered as “Trusted Officials”. C-DAC CA 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

5.2.1.1 CA Administrator

The administrator is responsible for:

1. Installation, configuration, and maintenance of the CA;
2. Establishing and maintaining CA system accounts;
3. Configuring certificate profiles or templates and audit parameters, and;
4. Generating and backing up CA keys.
5. Administrators shall not issue certificates to subscribers.

5.2.1.2 CA Officer

The CA officer is responsible for issuing certificates, that is:

1. Registering new subscribers and requesting the issuance of certificates;
2. Verifying the identity of subscribers and accuracy of information included in certificates;
3. Approving and executing the issuance of certificates, and;

5.2.1.3 Audit Administrator

The Audit Administrator is responsible for:

1. Reviewing, maintaining, and archiving audit logs;
2. Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS;

5.2.1.4 System Administrator

The System Administrator is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.1.5 Organizational Registration Authority

No stipulation

5.2.1.6 PKI Sponsor

No stipulation

5.2.2 Number of persons required per task

C-DAC 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 C-DAC 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

C-DAC CA shall perform complete background check as per procedure prior to assigning the role of authorized trusted personal or trusted official. C-DAC 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

5.2.4 Roles Requiring Separation of Duties

Role separation is enforced either by the CA equipment, or procedurally, or by both means. Individuals may assume more than one role, except:

1. Individuals who assume an Officer role will not assume CA Administrator or Audit Administrator role;
2. Individuals who assume an Audit Administrator role will not assume any other role on the CA; and
3. Under no circumstances any of the four roles will perform its own compliance audit function.
4. No individual will be assigned more than one identity

5.3 Personnel Controls

5.3.1 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.

C-DAC 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

C-DAC CA 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

C-DAC 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 C-DAC 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

C-DAC 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 C-DAC 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 C-DAC CA policies and procedures will invite disciplinary actions. Such disciplinary actions may include without limitation termination of employment.

5.3.7 Documentation supplied to personnel

All the personnel involved in C-DAC CA services shall be required to read this CPS and other policy documents related to C-DAC 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.

5.4 Audit Logging Procedures

Audit log files are generated for all events relating to the security of the CAs. The security audit logs either automatically collected or if not possible, a logbook, paper form, or other physical mechanism are used. All security audits logs, both electronic and non-electronic, are retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with Section 0.

5.4.1 Types of Events Recorded

All security auditing capabilities of the CA operating system and the CA applications required by this CPS are enabled. Each audit record shall include the following (either recorded automatically or manually for each auditable event):

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

The following events shall be audited:

Auditable Event	CA
SECURITY AUDIT	
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	
Any attempt to delete or modify the Audit logs	
IDENTITY-PROOFING	
Successful and unsuccessful attempts to assume a role	
The value of *maximum number of authentication attempts* is changed	
The number of unsuccessful authentication attempts exceeds the maximum *authentication attempts* during user login	
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	
An Administrator changes the type of authenticator, e.g., from a password to a biometric	
LOCAL DATA ENTRY	
All security-relevant data that is entered in the system	
REMOTE DATA ENTRY	
All security-relevant messages that are received by the system	
DATA EXPORT AND OUTPUT	
All successful and unsuccessful requests for confidential and security-relevant information	
KEY GENERATION	
Whenever the Component generates a key (not mandatory for single session or one-time use symmetric keys)	
PRIVATE KEY LOAD AND STORAGE	
The loading of Component private keys	
All access to certificate subject Private Keys retained within the CA	
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE	
All changes to the trusted Component Public Keys, including additions and deletions	
PRIVATE AND SECRET KEY EXPORT	
The export of private and secret keys (keys used for a single session or message are excluded)	
CERTIFICATE REGISTRATION	
All certificate requests	
CERTIFICATE REVOCATION	
All certificate revocation requests	
CONFIGURATION	
Any security-relevant changes to the configuration of the Component	
ACCOUNT ADMINISTRATION	
Roles and users are added or deleted	

Auditable Event	CA
The access control privileges of a user account or a role are modified	
CERTIFICATE PROFILE MANAGEMENT	
All changes to the certificate profile	
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT	
All changes to the certificate revocation list profile	
MISCELLANEOUS	
Appointment of an individual to a Trusted Role	
Designation of personnel for multiparty control	
Installation of the Operating System	
Installation of the PKI Application	
Installation of hardware cryptographic modules	
Removal of hardware cryptographic modules	
Destruction of cryptographic modules	
System Startup	
Logon attempts to PKI Application	
Receipt of hardware / software	
Attempts to set passwords	
Attempts to modify passwords	
Back up of the internal CA database	
Restoration from back up of the internal CA database	
File manipulation (e.g., creation, renaming, moving)	
Posting of any material to a PKI Repository	
Access to the internal CA database	
All certificate compromise notification requests	
Loading tokens with certificates	
Shipment of Tokens	
Zeroing Tokens	
Re-key of the Component	
CONFIGURATION CHANGES	
Hardware	
Software	
Operating System	
Patches	
Security Profiles	
PHYSICAL ACCESS / SITE SECURITY	
Personnel Access to room housing Component	
Access to the Component	
Known or suspected violations of physical security	
ANOMALIES	
Software error conditions	
Software check integrity failures	
Receipt of improper messages	
Misrouted messages	
Network attacks (suspected or confirmed)	

Auditable Event	CA
Equipment failure	
Electrical power outages	
Uninterruptible Power Supply (UPS) failure	
Obvious and significant network service or access failures	
Violations of Certificate Policy	
Violations of Certification Practice Statement	
Resetting Operating System clock	

5.4.2 Frequency of Processing Audit Logs

Audit logs are examined for key security and operational events at least on a weekly basis. In addition, CA reviews its audit logs as required in the event of any suspicious or unusual activity based on irregularities and incidents within CA systems.

The processing of audit logs includes a review of the audit logs and recording of significant events in an audit log summary. It includes a verification that the log has not been tampered with, a brief inspection of all log entries, and a detailed investigation of any irregularities in the logs. Actions taken based on audit log reviews are recorded.

5.4.3 Retention Period for Audit Logs

See Section 2.

5.4.4 Protection of Audit Logs

System configuration and procedures are implemented together to ensure that:

1. Only authorized people have read access to the logs;
2. Only authorized people may archive audit logs; and,
3. Audit logs are not modified.
4. After back-up and archived, the audit logs are allowed by the system to be over-written.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries shall be archived as per Section 0.

5.4.6 Audit Collection System (internal vs. external)

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by CA personnel.

Audit processes are invoked at system startup, and cease only at system shutdown. In the case of failure of audit collection system, CA operations are suspended until the problem is remedied.

5.4.7 Notification to Event-Causing Subject

This CPS imposes no requirement to provide notice (that an event was audited) to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

Events in the audit log are recorded, in part, to monitor system vulnerabilities. A vulnerability assessment is performed, reviewed, and revised following an examination of these monitored events.

5.5 Records Archival

5.5.1 Types of Records Archived

CA retains an archive of information and actions that are material to each certificate application and to the creation, Issuance and revocation of each certificate issued by the CA. These records include all relevant evidence regarding:

Data To Be Archived
Certification Practice Statement
Contractual obligations
System and equipment configuration
Modifications and updates to system or configuration
Certificate requests
Subscriber identity authentication data as per Section 3.2.3
Documentation of delivery of certificates
All certificates issued or published
All CRLs and CRLs issued and/or published
All Audit Logs
All Audit Log Summaries
Other data or applications to verify archive contents
Compliance audit reports

5.5.2 Retention Period for Archive

Records associated with certificates are archived for a period of 7 years from the date of expiry of the certificate.

5.5.3 Protection of Archive

CA protects its archived records so that only authorized persons can access the archived data. CA protects the archive against unauthorized viewing, modification, deletion, or other tampering, by storage within a trustworthy system. The media holding the archive data and the systems required to process the archive data are maintained to ensure that the archive data can be accessed for the time period

5.5.4 Archive Backup Procedures

CA creates back-up copies of archives compiled as and when the archives are created. Backup copies of the archive and copies of paper-based records are maintained in an off-site disaster recovery/ warehouse facility. CA has implemented a process to scan and digitize the physical documents to ensure tracking and easy retrieval.

5.5.5 Requirements for Time-Stamping of Records

Archived records are time stamped such that order of events can be determined. Certificates, CRLs, other revocation databases and usage entries contain time and date information provided by System time, which is synchronized with IST (NPLI).

5.5.6 Archive Collection System (internal or external)

The archive collection system is internal to the CA.

5.5.7 Procedures to Obtain & Verify Archive Information

Only CA trusted personnel are permitted to access the archived data. Additionally, the archive information may be made available to the CCA upon request.

5.6 Key Changeover

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

The following table provides the maximum lifetimes for certificates and associated private keys.

Key	2048 Bit Keys/ECC 256	
	Private Key	Certificate
Intermediate CA	10 years	10 years
Sub-CA	10 years	10 years
Time Stamping	3 years	3 years
OCSP Responder	1 year	1 year
Human Subscriber Signature certificate	3 years	3 years

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If a CA detects a potential hacking attempt or other form of compromise, it will perform an investigation in order to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in Section 0 shall be followed. Otherwise,

the scope of potential damage shall be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

CA will inform CCA if any of the following cases occur:

1. Suspected or detected compromise of the CA system;
2. Physical or electronic attempts to penetrate the CA system;
3. Denial of service attacks on the CA system; or
4. Any incident preventing CA from issuing a CRL within 24 hours of the time specified in the next update field of its currently valid CRL. A CA will make all efforts to restore capability to issue CRL as quickly as possible.

5.7.2 Computing Resources, Software, and/or Data are corrupted

CA have a Disaster Recovery center as per the guidelines of IT Act. The disaster recovery site will be made operational using the latest available backup data.

If CA equipment is damaged or rendered inoperative, but the signature keys are not destroyed, CA makes all efforts to establish the operation as quickly as possible, giving priority to the ability to generate CRL or make use of Disaster Recovery facility for CRL generation.

If both primary and Disaster recovery sites cannot be used to establish revocation capability in a reasonable time-frame, the CA may request for revocation of its certificate(s) to CCA.

5.7.3 Private Key Compromise Procedures

If CA signature keys are compromised, lost, or suspected to be compromised:

CCA shall be notified at the earliest feasible time so that RCAI can revoke the CA certificate;

1. A CA key pair shall be generated by CA in accordance with procedures set forth in this applicable CPS;
2. New CA certificates shall be requested in accordance with the initial registration process set elsewhere in this CP;
3. If the CA can obtain accurate information on the certificates it has issued and that are still valid (i.e., not expired or revoked), the CA may re-issue (i.e., renew) those certificates with the not After date in the certificate as in original certificates; and
4. The CA shall also investigate what caused the compromise or loss, and what measures must be taken to preclude recurrence.

5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster whereby CA installation is physically damaged and all copies of the CA Signing Key are destroyed as a result, the CA shall request that its certificates be revoked. The CA shall follow steps 1 through 4 in Section 0 above.

5.8 CA Termination

C-DAC CA shall reserve right to terminate the CA operations and in such scenario, C-DAC 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. C-DAC 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 C-DAC CA 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 C-DAC 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.

6 Technical security controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

C-DAC CA shall ensure following for key generation process; The following table provides the requirements for key pair generation for the various entities.

Entity	FIPS 140-1/2 Level	Hardware or Software	Generated in Entity Module
CA	3	Hardware	Yes
Sub-CA	3	Hardware	Yes
Time Stamp Authority	3	Hardware	Yes
OCSP Responder	3	Hardware	Yes
Human Subscriber Signature	2 for eKYC Class	Hardware	Yes

For CA key pair generation, multiparty controls are used as specified in Section 5.2 . CA creates a verifiable audit trail for key pair generation as per the security requirements Procedures which are followed and the same will be documented. The process is validated by an Auditor.

6.1.2 Private Key Delivery to Subscriber

Subscriber private key is generated by ESP of CA and destroyed after one time usage. The certificate is of maximum validity 30 minutes. The signature along with certificate is delivered to the end entity subscribers.

In the case CA as eKYC provider, the user id and associated PIN created by the user during the enrollment process to CA eKYC database and the OTP sent to the mobile of applicant is verified for applicant authentication.

6.1.3 Public Key Delivery to Certificate Issuer

C-DAC 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 C-DAC 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 Relying Parties

C-DAC CA shall publish its own CA public key for relying parties at its repository on C-DAC CA portal (at https://esign.cdac.in/ca).

6.1.5 Key Sizes

The key length size of the C-DAC CA shall be 2048-bit RSA key pair and Subscribers shall have keys which are 2048 bits long RSA key or Elliptical Curve Cryptography (ECC) 256 bits long key.

6.1.6 Public Key Parameters Generation & Quality Checking

C-DAC CA shall ensure that its CA application is configured to set parameters for CA and Subscriber public key generation. RSA and ECC keys are generated in accordance with FIPS 186-2.

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

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

6.2.2 Private Key Multi-Person Control

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

6.2.3 Private Key Escrow

Not applicable

6.2.4 Private Key Backup

6.2.4.1 Backup of CA Private Signature Key

CA private signature keys are backed up under the same multi-person control as the original signature key. Numbers of backup copies are limited to three and securely stored under the same multi-person control as the operational key.

6.2.4.2 Backup of Subscriber Private Signature Key

The ESP of CA generate key pair and destroy after certificate generation.

6.2.5 Private Key Archival

At the end of the validity period, CA private key will be destroyed and will not be archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA key pairs are generated and secured by hardware cryptographic modules. CA ensures that The CA private keys are backed up in secure manner and transferred in an encrypted form.

6.2.7 Private Key Storage on Cryptographic Module

CA stores Private Keys in hardware cryptographic module and keys are not accessible without authentication mechanism that is in compliance with FIPS 140-2 rating of the cryptographic module.

6.2.8 Method of Activating Private Key

The user must be authenticated to the cryptographic module before the activation of any private key(s). Acceptable means of authentication include but are not limited to pass-phrases, Personal Identification Numbers (PINs) or biometrics. Entry of activation data is protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.9 Methods of Deactivating Private Key

Cryptographic module that has been activated is never left unattended or otherwise available to unauthorized access. After use, cryptographic modules are deactivated. After deactivation, the

use of the cryptographic modules based CA key pair requires the presence of the trusted roles with the activation data in order to reactivate said CA key pair.

6.2.10 Method of Destroying Private Key

Private signature keys will be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. Destroying private key inside cryptographic modules requires destroying the key(s) inside the HSM using the 'zeroization' function of the cryptographic modules in a manner that any information cannot be used to recover any part of the private key. All the private key back-ups are destroyed in a manner that any information cannot be used to recover any part of the private key. If the functions of cryptographic modules are not accessible in order to destroy the key contained inside, then the cryptographic modules will be physically destroyed. The destruction operation is realized in a physically secure environment

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Management

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Certificate Operational Periods/Key Usage Periods

See Section 5.6

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data used to unlock private keys is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data holders are responsible for their accountability and protection.

When they are not used, activation data are always stored in a safe for which access is controlled by holders in limited roles.

6.4.2 Activation Data Protection

The activation data used to unlock private keys is protected from disclosure.

After a predetermined number of failed login attempts, a facility to lock the account temporarily has been provided. The activation data written on paper is stored securely in a safe.

6.4.3 Other Aspects of Activation Data

CA changes the activation data whenever the HSM is re-keyed or returned from maintenance. Before sending a cryptographic module for maintenance, all sensitive information contained in the cryptographic module is destroyed.

Subscribers are responsible to ensure the protection of their activation data

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The following computer security functions are provided by the operating system, or through a combination of operating system, software, and physical safeguards.

1. Require authenticated logins for trusted roles
2. Provide Discretionary Access Control
3. Provide a security audit capability
4. Require a trusted path for identification and authentication
5. Provide domain isolation for process
6. Provide self-protection for the operating system

CA computer systems are configured with minimum required accounts and network services.

CA has implemented a combination of physical and logical security controls to ensure that the CA administration is net carried out with less than two person control.

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life-Cycle Technical Controls

6.6.1 System Development Controls

The system development controls for the CA are as follows:

1. Hardware and software are purchased in such a way so as to reduce the likelihood that any particular component was tampered with.

2. All hardware must be shipped or delivered via controlled methods that provide a continuous chain of accountability, from the purchase location to the operations location

3. The hardware and software are dedicated to performing the PKI activities. There are no other applications; hardware devices, network connections, or component software installed which is not part of the PKI operation.

4. Proper care is taken to prevent malicious software from being loaded onto the equipment. Only applications required performing the PKI operations is obtained from sources authorized by local policy.

5. CA hardware and software are scanned for malicious code on first use and periodically thereafter.

6.6.2 Security Management Controls

The configuration of the CA system as well as any modification and upgrade is documented and controlled. There is a mechanism for detecting unauthorized modification to the CA software or configuration. A formal configuration management methodology is used for installation and ongoing maintenance of the CA system. The CA software, when first loaded, is verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Controls

Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.

6.7 Network Security Controls

CA employs appropriate security measures to ensure that they are guarded against denial of service and intrusion attacks. Such measures include the use of hardware firewalls, hardware filtering routers, and intrusion detection systems. Unused network ports and services are turned off. Protocols that provide network security attack vector(s) is not permitted through the boundary control devices.

Any boundary control devices used to protect the network on which PKI equipment is hosted will deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 Time Stamping

All CA components are regularly synchronized with a time service such as Indian Standard Time Service. Time derived from the time service is used for establishing the time of:

- Initial validity time of a Subscriber's Certificate
- Posting of CRL updates

Asserted times is accurate to within three minutes. Electronic or manual procedures are used to maintain system time. Clock adjustments are auditable events as listed in Section 0.

7 Certificate and CRL profiles

7.1 Certificate Profile

Certificate profiles are listed under CCA-IOG, Annexure III - Reference Certificate Profiles. The CA Certificates issued under this CPS conform to X-509 Version 3 digital Certificate.

The End User Certificate Profile (issued for personal use) and CA certificate profiles are given below

CA Certificate Profile

CA CERTIFICATE -BASIC FIELDS	
Version	Version 3
Serial number	Positive number of maximum Length 20 bytes and unique to each certificate issued by 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
EXTENSIONS	
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 profile

END ENTITY CERTIFICATE -BASIC FIELDS	
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) or ECDSA with SHA256 {1 2 840 10045 4 3 2}
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,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 OR ecPublicKey { 1.2.840.10045.2.1}, namedCurve, { 1.2.840.10045.3.1.7} (NIST curve P-256)
Signature	Issuer CA's signature
EXTENSIONS	
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)
Extended Key Usage	Document Signing: {1.3.6.1.4.1.311.10.3.12}
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 or 2.16.356.100.2.4.2)
cRLDistributionPoints	location of CRL information

7.2 CRL Profile

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

7.2.1 Full and Complete CRL

A CA makes a full and complete CRL available and published on the repository.

Field	**Value**
Version	V2 (1)
Issuer Signature Algorithm	sha256WithRSAEncryption {1 2 840 113549 1 1 11}
Issuer Distinguished Name	Per the requirements in [CCA-IOG]
thisUpdate	expressed in UTCTime until 2049
nextUpdate	expressed in UTCTime until 2049 (>= thisUpdate + CRL issuance frequency)
Revoked certificates list	0 or more 2-tuple of certificate serial number and revocation date (in Generalized Time)
Issuer's Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
CRL Extension	**Value**
CRL Number	c=no; monotonically increasing integer (never repeated)
Authority Key Identifier	c=no; Octet String (same as in Authority Key Identifier field in certificates issued by the CA)
CRL Entry Extension	**Value**
Reason Code	c=no; optional

7.2.2 Distribution Point Based Partitioned CRL

CA issues only full and complete CRL signed by CA

7.3 OCSP Profile

OCSP requests and responses are as per RFC 2560 as listed below.

7.3.1 OCSP Request Format

Requests sent to Issuer CA OCSP Responders are not required to be signed. The following table lists the fields that are expected by the OCSP Responder.

Field	**Value**
Version	V1 (0)
Requester Name	DN of the requestor (required)
Request List	List of certificates as specified in RFC 2560
Request Extension	**Value**
None	None
Request Entry Extension	**Value**
None	None

7.3.2 OCSP Response Format

See RFC2560 for detailed syntax. The following table lists which fields are populated by the OCSP Responder.

Field	**Value**
Response Status	As specified in RFC 2560
Response Type	id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1}
Version	V1 (0)
Responder ID	Octet String (same as subject key identifier in Responder certificate)
Produced At	Generalized Time
List of Responses	Each response will contain the certificate id; certificate status[1], thisUpdate, nextUpdate[2],
Responder Signature	sha256 WithRSAEncryption {1 2 840 113549 1 1 11}
Certificates	Applicable certificates issued to the OCSP Responder
Response Extension	**Value**
Nonce	c=no; Value in the nonce field of request (required, if present in request)
Response Entry Extension	**Value**
None	None

[1] If the certificate is revoked, the OCSP Responder provide revocation time and revocation reason from CRL entry and CRL entry extension.

[2] The OCSP Responder use thisUpdate and nextUpdate from CA CRL.

8 Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessments

Annual compliance audit by CCA empanelled Auditor is carried out of CAs infrastructure apart from half yearly internal audit

8.2 Identity and Qualifications of Assessor

CCA empanel auditors based on the competence in the field of compliance audits, qualifications and thorough familiarity with requirements of the IT Act, CP and CPS. The auditors perform such compliance audits as per the terms of empanelment and also under the guidance of CCA

8.3 Assessor's Relationship to Assessed Entity

The auditor is independent from the entity being audited. The office of CCA determines whether an auditor meets this requirement.

8.4 Topics Covered by Assessment

CA has a compliance audit mechanism in place to ensure that the requirements of this CPS are enforced.

8.5 Actions Taken as a Result of Deficiency

Office of CCA may determine that a CA is not complying with its obligations set forth in this CPS or the applicable CP. When such a determination is made, the office of CCA may suspend operation of CA, or may revoke the CA certificate, or may direct that other corrective actions be taken which allow operation to continue.

When the auditor finds a discrepancy between how the CA is designed or is being operated or maintained, and the requirements of this CP, or the applicable CPS, the auditor take the following actions:

1. The auditor note the discrepancy;
2. The auditor notify the audited CA; and
3. The auditor notifies the office of CCA.

8.6 Communication of Results

On completion of audit by an empanelled auditor, Auditor submit an Audit Report, including identification of corrective measures taken or being taken by CA, to the office of CCA and a copy to CA. The report identifies the version of the CPS used for the assessment

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance and Renewal Fees

The fees for various types of certificates are made available on CA website at URL and will be updated from time to time.

9.1.2 Certificate Access Fees

CA is not charging any fees to relying parties or other public for accessing the certificate information from the repository. The certificate search facility is provided free of cost at its website (URL).

9.1.3 Revocation Status Information Access Fees

CA does not charge a fee for access to any revocation status information through CRL.

9.1.4 Fees for Other Services

No stipulation

9.1.5 Refund Policy

If applicable, the refund policy and other payments terms are governed as per the terms in the subscriber agreement.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

CA maintain reasonable levels of insurance coverage to address all foreseeable liability obligations to PKI Participants described in Section 1.3 of this CPS

9.2.2 Other Assets

CA also maintains reasonable and sufficient financial resources to maintain operations, fulfill duties, and address commercially reasonable liability obligations to PKI Participants described in Section 1.3 of this CPS.

9.2.3 Insurance or Warranty Coverage for End-Entities

CA offers no protection to end entities that extends beyond the protections provided in this CPS

9.3 Confidentiality of Business Information

CA maintain the confidentiality of confidential business information that is clearly marked or labeled as confidential, or by its nature reasonably is understood to be confidential, and treat such information with the same degree of care and security as the CA treats its own most confidential information.

9.4 Privacy of Personal Information

CA stores, process, and disclose personally identifiable information in accordance with the provisions of IT Act.

9.5 Intellectual Property Rights

CA will not knowingly violate any intellectual property rights held by others.

9.5.1 Property Rights in Certificates and Revocation Information

CAs claims all Intellectual Property Rights in and to the Certificates and revocation information that they issue. However, permission to reproduce and distribute Certificates and revocation information on a nonexclusive royalty-free basis, may be granted provided that the recipient agrees to distribute them at no cost.

9.5.2 Property Rights in the CPS

This CPS is based on the pro forma CPS published by Office of CCA for Licensed CAs. All Intellectual Property Rights in this CPS pertaining to CA are owned by the CA.

9.5.3 Property Rights in Names

The Certificate Applicant may claim all rights, if any, in any trademark, service mark, or trade name of the Certificate Applicant contained in any Application.

9.5.4 Property Rights in Keys

CA claim property rights to the keys used (e.g., CA key pair, time stamp authority key pair, etc.) Subject to any agreements between CA and its customers, ownership of and property rights in key pairs corresponding to Certificates of Subscribers is specified in this CPS.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

CA represents and warrants that:

1. signing private key is protected and that no unauthorized person has ever had access to that private key;

2. All representations made by CA in any applicable agreements are true and accurate, to the best knowledge of CA; and

3. Each Subscriber has been required to represent and warrant that all information supplied by the Subscriber in connection with, and/or contained in the Certificate is true.

4. Only verified information appears in the certificate

9.6.2 Subscriber

A Subscriber is required to sign a document (e.g., a subscriber agreement in the case of CA as eKYC provider) containing the requirements the Subscriber shall meet respecting use of the certificate before being issued the certificate.

In signing the document described above, each Subscriber should agree to the following:

1. Subscriber shall accurately represent itself in all communications with the CA conducted.
2. Subscriber shall authorize ESP of CA to generate key pair , generate certificate and destroy private key up on successful authentication.
3. The Subscriber lawfully holds the private key corresponding to public key identified in the Subscriber's certificate.
4. The Subscriber will abide by all the terms, conditions, and restrictions levied on the use of their eKYC information and certificates.
5. Subscriber shall promptly notify the appropriate CA upon change of eKYC information already submitted. Such notification shall be made directly or indirectly through mechanisms consistent with this CPS.
6. The subscriber shall follow all the applicable duties as mentioned in the IT Act.

9.6.3 Relying Party

Parties who rely upon the certificates issued under a policy defined in this document shall:

1. Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
2. Check each certificate for validity, using procedures described in RFC 5280, prior to reliance;
3. Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with application upgrades will often invalidate digital signatures and should be avoided.

9.6.4 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

To the extent permitted by applicable law and any other related agreements, CA disclaims all warranties other than any express warranties contained in such agreements or set forth in this CPS.

9.8 Limitations of Liabilities

CA limit liabilities as long as CA meet the liability requirements stated in ITAct CA is responsible for verification of any Subscriber to whom it has issued a certificate and to all relying parties who reasonably rely on such certificate in accordance with this CPS, for damages suffered by such persons that are caused by the failure of the CA to comply with the terms of its CPS or its Subscriber Agreement, and sustained by such persons as a result of the use of or reliance on the certificate.

The verification requirements for certificate issuance by CA are as specified under IT Act and reasonable effort by CA. CA cannot guarantee the activities or conduct of the subscribers.

CA shall not be liable for any indirect, exemplary, special, punitive, incidental, and consequential losses, damages, claims, liabilities, charges, costs, expenses or injuries (including without limitation loss of use, data, revenue, profits, business and for any claims of Subscribers or Users or other third parties including Relying parties).

CA shall not be liable for any delay, default, failure, breach of its obligations under the Subscribers Agreement and Relying Party Terms & Conditions.

All liability is limited to actual and legally provable damages. CA's liability is as per the IT Act, other governing Indian laws and Agreement. If the liability is not dealt under the provisions of ITACT 2000, the following caps limit CA's damages concerning specific certificates.

Class	Liability Caps
eKYC - Single Factor	Indian Rupees -one thousand
eKYC - Multi Factor	Indian Rupees -one thousand

9.9 Indemnities

Indemnification by Subscribers

To the extent permitted by applicable law, subscriber agreement requires Subscribers to indemnify CA for:

- False and misrepresentation of fact by the subscriber on the enrollment to eKYC service of CA
- Suppression of a material fact on the eKYC information if the omission was made negligently or with intent to deceive any party, or
- The subscriber's failure to protect the subscriber's authentication secret or device , to use a trustworthy system, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the subscriber's authentication secret.

Indemnification by relying parties

To the extent permitted by applicable law, relying party agreement requires, relying parties to indemnify CA for:

- The relying party's failure to perform the representations and warranties as outlined in the applicable section of this CPS.
- The relying party's reliance on a certificate that is not reasonable under the circumstances, or
- The relying party's failure to check the status of such certificate to determine if the certificate is expired.

9.10 Term and Termination

9.10.1 Term

The CPS becomes effective upon approval by the Office of CCA. Amendments to this CPS become effective upon ratification by approval by CCA and publication by CA at URL. There is no specified term for this CPS.

9.10.2 Termination

While this CPS may be amended from time to time, it shall remain in force until replaced by a newer version or explicitly terminated by CCA.

9.10.3 Effect of Termination and Survival

Upon termination of this CPS, CA is nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates. The sections 5.5 and 9.0 of this CPS shall survive the termination or expiration of this CPS.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, CA uses commercially reasonable methods to communicate, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for Amendment

CA will review this CPS at least once every year. Additional reviews may be enacted at any time at the discretion of the CCA.

If the Office of CCA wishes to recommend amendments or corrections to this CPS, such modifications will be submitted to CCA for approval.

CA will use reasonable efforts to notify subscribers and relying parties of changes.

9.12.2 Notification Mechanism and Period

Errors and anticipated changes to this CPS resulting from reviews are published online at URL.

This CPS and any subsequent changes is made publicly available within seven days of approval.

9.12.3 Circumstances under Which OID Must be changed

CCA determines the requirement for changing the Certificate Policy OIDs.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among Licensed CAs and Customers

Unless the provision for dispute resolution under the ITAct is invoked, any dispute based on the contents of this CPS, between CA and one of its customers who has availed specific services will be resolved according to provisions in the applicable agreement between the parties.

9.13.2 Alternate Dispute Resolution Provisions

No stipulations.

9.14 Governing Law

The laws of India and more particularly the Information Technology Act, 2000, The Information Technology (Certifying Authorities) Rules, 2000 and Information Technology (Certifying Authority) Regulations, 2001, and the guidelines issued and clarifications made from time to time by the Controller of Certifying Authorities, Ministry of Electronics and Information Technology shall govern the construction, validity, enforceability and performance of actions per this CPS.

9.15 Compliance with Applicable Law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

Except where specified by other contracts, no party may assign or delegate this CPS or any of its rights or duties under this CPS, without the prior written consent of the other party (such consent not to be unreasonably withheld) Further, that Office of CCA may assign and delegate this CPS to any party of its choice.

9.16.3 Severability

If any provision of this CPS is held to be invalid by a court of competent jurisdiction, then the remaining provisions will nevertheless remain in full force and effect.

9.16.4 Waiver of Rights

No waiver of any breach or default or any failure to exercise any right hereunder is construed as a waiver of any subsequent breach or default or relinquishment of any future right to exercise such right. The headings in this CPS are for convenience only and cannot be used in interpreting this CPS.

9.16.5 Force Majeure

CA is not liable for any failure or delay in its performance under this CPS due to causes that are beyond their reasonable control, including, but not limited to, an act of God, act of civil or military authority, fire, epidemic, flood, earthquake, riot, war, and failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action.

9.17 Other Provisions

No stipulation.

10 Bibliography

The following documents were used in part to develop this CPS:

FIPS 140-2	Security Requirements for Cryptographic Modules, 1994-01 http://csrc.nist.gov/cryptval/
FIPS 186-2	Digital Signature Standard, 2000-01-27 http://csrs.nist.gov/fips/fips186.pdf
ITACT 2000	The Information Technoligy Act, 2000, Government of India, June 9, 2000.
RFC 3647	Certificate Policy and Certificate Practices Framework, Chokhani, Ford, Sabett, Merrill, and Wu. November 2003.
CCA-IOG	Interoperability Guidelines for DSC ,http://www.cca.gov.in/cca/?q=guidelines.html
CCA-CP	X.509 Certificate Policy for India PKI ,http://www.cca.gov.in/cca/?q=guidelines.html
CCA-IVG	Identity Verification Guidelines, http://www.cca.gov.in/cca/?q=guidelines.html
CCA-TSG	Time Stamping Services Guidelines for CAs, http://www.cca.gov.in/cca/?q=guidelines.html
CCA-OCSP	OCSP Service Guidelines for CAs ,http://www.cca.gov.in/cca/?q=guidelines.html
CCA-SSL	Guidelines For Issuance Of SSL Certificates,

	http://www.cca.gov.in/cca/?q=guidelines.html
CCA-OID	OID Hierarchy for India PKI(OID) ,http://www.cca.gov.in/cca/?q=guidelines.html
CA-eAUTH	e-authentication guidelines ,http://www.cca.gov.in/cca/?q=guidelines.html
CCA-eAPI	eSign API Specifications, http://www.cca.gov.in/cca/?q=guidelines.html
CCA-CASITESP	CA SITE SPECIFICATION ,http://www.cca.gov.in/cca/?q=guidelines.html
CCA-CRYPTO	Security Requirements for Crypto Devices ,http://www.cca.gov.in/cca/?q=guidelines.html
CCA-CALIC	CA Licensing Guidelines ,http://www.cca.gov.in/cca/?q=guidelines.html

11 Acronyms and Abbreviations

AES	Advanced Encryption Standard
CA	Certifying Authority
CCA	Controller of Certifying Authorities
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSP	Certificate Status Provider
DN	Distinguished Name
DNS	Domain Name Service
FIPS	(US) Federal Information Processing Standard
FIPS PUB	(US) Federal Information Processing Standard Publication
HR	Human Resources
HTTP	Hypertext Transfer Protocol
IAO	Information Assurance Officer
ID	Identifier
IETF	Internet Engineering Task Force
IT	Information Technology
OID	Object Identifier
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
RA	Registration Authority
RFC	Request For Comments
RSA	Rivest-Shamir-Adleman (encryption algorithm)
RCAI	Root Certifying Authority Of India
SHA-2	Secure Hash Algorithm, Version 1
SSL	Secure Sockets Layer
TLS	Transport Layer Security
UPS	Uninterrupted Power Supply