AUDIT CRITERIA FOR CERTIFYING AUTHORITIES

Version1.6

19 April 2024

Controller of Certifying Authorities

Ministry of Electronics and Information Technology

Table of Contents

1. Introduction

The Controller of Certifying Authorities has been appointed by the Government of India for enhancing the adoption of E-commerce and E-governance services through the wide use of digital signatures. As provided in the Information Technology Act 2000 (IT Act), the Controller of Certifying Authorities (CCA) superintends the task of licensing and regulating the working of Certifying Authorities. The Certifying Authorities (CAs) extend their role to issue digital signature certificates for electronic authentication of users.

The CCA has established the Root Certifying Authority of India (RCAI) under section 18(b) of the IT Act to digitally sign the public keys of Certifying Authorities (CA) in the country. The RCAI is operated as per the standards laid down under the Act.

The CCA License and certifies the public keys of CAs using its own private key that enables users in cyberspace to verify that a given certificate is issued by a licensed CA. The CCA also maintains the Repository of Digital Certificates, which contains all the certificates issued to the CAs in the country. A CA can issue Digital Signature Certificates (DSC) only after being duly licensed by the CCA as per provisions of the IT Act.

The CCA has issued multiple guidelines over a period of time to standardize the security and compliance requisites followed by CAs. Additionally, various guidelines have been published internationally intended to strengthen the security of the CA systemshavebeen included inthe guidelines for CA systems under RCAI. This documents describes integrated set of auditing requirements necessary (but not limited to) for the issuance and management of Publicly-Trusted Certificates.In the eKYC based identity verification and certificate issuance, a monthly audit of 5 percent of samples (subjected to a maximum) has been mandated

CCA mandates all CAs to get their operations audited annually by an empaneled auditor. Additionally, the CAs are required to conduct a half-yearly audit of their security policy, physical security and planning of their operation and a quarterly audit of their repositories. This document details the controls and the corresponding checks which need to be implemented for ensuring secure CA systems.

1.1. Objective

The audit criteria have been designed as a comprehensive reference for CAs and auditors to assess the adequacy and effectiveness of the controls implemented in CA systems. The detailed audit guidelines can be used as a reference for performing the audit to test the implementation of various controls.

1.2. Scope

The overall scope of the audit criteria will be as follows, however the applicability of the scope depends on latest guidelines issued by CCA and can be updated as and when new guidelines are issued:

- ✓ Applicable to all existing CAs in India
- ✓ Systems and information maintained by CA to provision Digital services to citizens
- ✓ Security requirements defined as part of regulations and guidelines released by CCA

1.3. Reference Documents

The audit criteria has been designed assimilating inputs from both Indian and international standards and guidelines. The controls are consistent with the requirement mentioned in the IT CA Rules 2000. Additionally requirements have been added from guidelines published by WebTrust and CA Browser Forum.

The list of documents referred for designing the criteria have been tabulated below:

References	Document
IT CA Rules SCHEDULE-II	Information Technology (Certifying Authorities) Rule, 2000
IT CA Rules SCHEDULE-III	Information Technology (Certifying Authorities) Rule, 2000
IT Regulations	Information Technology (Certifying Authority) Regulations, 2001
X.509 Policy	X.509 Certificate Policy for India PKI
WebTrust	Webtrust Principles and Criteria for Certification Authorities
CA Browser Forum	Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates
CA Browser Forum EV	Guidelines For The Issuance And Management Of Extended Validation Certificates
OCSP Guidelines	Online Certificate Status Protocol (OCSP) Service Guidelines for Certifying Authorities (CA)
Guidelines for SSL	Guidelines For Issuance of SSL Certificates
eSign Guidelines	e-authentication guidelines for eSign- Online Electronic Signature Service
Identity Verification Guidelines	Identity Verification Guidelines
eSign API Specifications	eSign API Specifications
ASP On-Boarding Guidelines	ASP On-Boarding Guidelines

1.4. Qualified Auditor

The CAs shall get the mandatory audit performed only by the CCA empaneled agency and auditors. The auditor shall be independent of the CA being audited and shall not be a software or hardware vendor which is, or has been providing services or supplying equipment to the said Certifying Authority. The auditor and the Certifying Authority shall not have any current or planned financial, legal or other relationship, other than that of an auditor and the audited party.

Additionally, the Audit organization is required to have personnel with the knowledge of digital signature technology, standards and practices; trusted computer information systems & trusted networking environments with relevant experience in information systems audit having ISO27001 Lead Auditor certification along with CISA, DISA, CISSP Certification or other relevant certification.

1.5. Auditors Report

The Certifying Authority shall get its operations audited annually by an auditor and such audit shall include, but not limited to:

- Security policy and planning;
- Physical security;
- Technology evaluation;
- Certifying Authority's services administration;
- Relevant Certification Practice Statement;
- Compliance to relevant Certification Practice Statement;
- Contracts/agreements;
- Regulations prescribed by the Controller;
- Policy requirements of Certifying Authorities Rules, 2000.
- WebTrust Requirements for Certification Authorities

The Auditor shall submit audit report to the CCA & CA within two weeks of the completion of such audit and where irregularities are found, the Certifying Authority shall take immediate appropriate action to remove such irregularities

1.6. Conventions

The key words “MUST”, “MUST NOT”, "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in these Requirements shall be interpreted in accordance with RFC 2119.

1.7. Terminology

S No.	Terminology	Definition
1	Act	The Information Technology Act, 2000 (21 of 2000)
2	Applicant	Certifying Authority applicant
3	Auditor	any internationally accredited computer security professional or agency appointed by the Certifying Authority and recognized by the Controller for conducting technical audit of operation of Certifying Authority
4	Controller	Controller of Certifying Authorities appointed under subsection (1) of Section 17 of the Act
5	Digital Signature Certificate	Digital Signature Certificate issued under sub-section (4) of section 35 of the Act
6	Information asset	all information resources utilized in the course of any Organization's business and includes all information, applications (software developed or purchased), and technology (hardware, system software and networks)
7	License	a license granted to Certifying Authorities for the issue of Digital Signature Certificates under these rules
8	licensed Certifying Authority	Certifying Authority who has been granted a licence to issue Digital Signature Certificates
9	trusted person	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 these Rules in respect of a Certifying Authority; 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 a Certifying Authority's computing facilities.
10	Hierarchical CA Model	A highest level (or “Root”) CA is deployed and subordinate CAs may be set up for various business units, domains or communities of interest. The Root CA validates the subordinate CAs, which in turn issue certificates to lower tier CAs or directly to subscribers. For Indian CAs, the root CA is CCA.

1.8. 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
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

2.1. Introduction

The Audit criteria for CAs has been designed referencing primarily the IT CA Rules along with the WebTrust and CA Browser Forum requirements, and is in harmony with the X.509 Certificate Policy for India PKI along with host of other industry standards and India specific regulations as detailed in Section 1.3.

Diagram below depicts the primary sections covered as part of the Audit Criteria

Each section contains a descriptive list of controls assimilated from various reference sources. Additionally, specific Audit Checks have been detailed for the auditor to clearly test the design and effectiveness of control implementation.

Following details have been covered as part of Section 3:

01 Controls to be implemented by CAs

02 Step by step Audit Checks for testing the controls

03 Source reference for each control

04 Control Classification - Mandatory of Recommended

Every care has been taken to avoid errors or omissions in creating the criteria. The Office of Controller of Certifying Authorities will not be held responsible for discrepancies, if any.

3. Detailed Audit Controls

3.1. Information Technology (IT) Security Guidelines

3.1.1. Implementation of Information Security

Control No.	Control	Audit Checks	Control Type	References	Compliance (Yes/No/NA)
Security Policy					
3.1.1.1	An information security policy document has been formulated that includes physical, personnel, procedural and technical controls and was submitted to the Controller before commencement of operation.	1. Obtain the softcopy/hardcopy of the information security policy 2. Check the following a. Controller received the policy approved by CA management before commencing operations b. Policy contains physical, personnel, procedural and technical controls c. information is classified depending upon its sensitivity for the CA as per IT Act-2000 d. both confidential and non-confidential information addressed in the policy e. CA has prepared detailed manuals for performing its	Mandatory	IT CA Rules 19.2	
3.1.1.2	CA shall ensure the security policy clearly addresses security of both confidential and non-confidential information. The Certifying Authority shall prepare detailed manuals for performing all its activities and shall scrupulously adhere to them.		Mandatory	WebTrust 3.9.5, IT Regulations 3	
3.1.1.3	The Certifying Authority shall as approved, in respect of security and risk management controls continuously ensure that security policies and safeguards are in place. Such controls include personnel security and incident handling measures to prevent fraud and security breaches. The security policy shall be approved by management,		Mandatory	IT Regulations 3, WebTrust 3.1.1	

	published and communicated to all employees.	activities f. CA ensures security and risk management controls are implemented g. policy has been approved by CA management. Verify by checking approval date. h. policy has been communicated to all employees via mail or training session 3. Obtain name of personnel responsible for ensuring that security procedures implementation and verify roles and responsibilities defined 4. Verify the all recent changes done to the policy since last audit 5. For sample recent changes done to the policy validate details were submitted to Controller within two weeks			
3.1.1.4	An authorized personnel shall be responsible for ensuring that security procedures within their area of responsibility are carried out correctly		Mandatory	WebTrust 3.9.8	
3.1.1.5	A review process shall be designed for maintaining the security policy. Review dates and responsibilities should be recorded.		Mandatory	WebTrust 3.1.3	
3.1.1.6	Any change made by the Certifying Authority in the security policy shall be submitted by it within two weeks to the Controller		Mandatory	IT CA Rules 19	
Risk Assessment					
3.1.1.7	The CA's security program shall include an annual Risk Assessment	1. Obtain copy of annual Risk Assessment plan 2. Check the following: a. Threats are identified and documented as part of risk assessment b. Standard operating procedures are present for combating threats. c. controls are in place to prevent misuse, alteration and destruction of sensitive information	Mandatory	IT CA Rules SCHEDULE-II 17.3 CA Browser Forum 5	
3.1.1.8	A list of foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any critical information shall be maintained.		Mandatory	CA Browser Forum 5	
3.1.1.9	The sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter cyber threats shall be verified.		Mandatory	CA Browser Forum 5	

		d. adequate cyber security tools are implemented by the CA such as DLP, Web Gateway, Email Gateway, Proxy Servers, and Firewalls, SSL/TLS, IDS/IPS, SAST, DAST, etc. e. a vulnerability assessment by the above mentioned tools are carried out at a pre decided interval. Report any scheduled VA left out. f. security plan has been developed g. updates and patches are applied in timely manner 3. Check the security plan covers the following safeguards: a. administrative, b. organizational, c. technical, and d. physical 4. Verify formal change management procedures have been developed			
3.1.1.10	A security plan shall be developed covering the following: • Security procedures to manage the risks • administrative, organizational, technical, and physical safeguards • cost of implementing the specific measures • security breach plan in case of any incidents		Mandatory	CA Browser Forum 5	
3.1.1.11	Hypervisors, operating system, database, and network device patches and updates shall be applied in a timely manner when deemed necessary based on a risk assessment and follow formal change management procedures		Mandatory	WebTrust 3.6.18	
Self-Assessment					
3.1.1.12	A documented security self-assessment plan shall be prepared by the CA	1. Obtain the self-assessment plan developed by the CA 2. Verify on a sample basis the for last two self-assessments conducted 3. Collect report of the self-assessment plan 4. Check the following: a. Findings of self-assessment were shared with the	Mandatory	IT CA Rules 2.e	
3.1.1.13	Self-Assessment shall be performed on a periodic basis and the findings shall be reported to management and discussed for closure		Mandatory	IT CA Rules 2.e	

		management b. Action was taken to address the finding			
Training					
3.1.1.14	The CA shall ensure all personnel performing duties with respect to operation of a CA,ESP, CSP shall receive comprehensive training covering the following: 1. CA/ESP/CSP/RA security principles and mechanisms 2. All PKI software versions in use on the CA system 3. All PKI duties they are expected to perform 4. Disaster recovery and business continuity procedures	1. Obtain the training plan and material for CA employees 2. Check the following: a. All relevant topics are covered in the training material b. Records of training are maintained by CA (e.g. Attendance sheet) c. Refresher training is conducted d. Training is given personnel in case of implementation of every new tool by the CA e. Personnel are trained with the update business continuity policy and procedures at regular intervals f. Training requirements are reviewed at least once a year 3. Obtain list of personnel entrusted with validation specialist duties 4. Check the following a. Validation specialist are trained to maintain required skill level b. All Validation Specialists have passed the examination provided by the CA 5. Obtain list of personnel responsible for trusted roles 6. Check if the changes made in CA, ESP,	Mandatory	X.509 Policy 5.3.3, IT CA Rules SCHEDULE-III.15	
3.1.1.15	Refresher training must be conducted as and when required, and the Certifying Authority must review these requirements at least once a year. Records of all trainings shall be maintained and reviewed periodically		Mandatory	IT CA Rules SCHEDULE III 16 CA Browser Forum 5.3.3	
3.1.1.16	CA shall ensure personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily		Mandatory	CA Browser Forum 5.3.3	
3.1.1.17	All Validation Specialists shall pass an examination provided by the CA on the information verification requirements		Mandatory	CA Browser Forum 5.3.3	
3.1.1.18	All individuals responsible for trusted roles shall be made aware of any significant changes in the CA, ESP CSP, or RA operations, as applicable.		Mandatory	X.509 Policy 5.3.4 CA Browser Forum 5.3.4	

		CSP operations were communicated with individuals responsible for trusted roles 7. Verify only trusted personals are performing verification at all levels			

3.1.2. Information Classification

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Information Classification					
3.1.2.1	Documented processes shall be created for classification, declassification, labeling, storage, access, destruction and reproduction of classified data.	1. Obtain copy of the process for handling classified data 2. Check the following a. procedure exists for classifying data based on its sensitivity for the CA b. procedures exist for destruction, access and reproduction of data c. Information is labeled in accordance with CA's information classification documented procedures.	Mandatory	IT CA Rules 19.1, WebTrust	
3.1.2.2	CA shall ensure information labeling and handling are performed in accordance with the CA's information classification documented procedures basis following categories: • Confidential • Restricted • Internal • Unclassified • Top Secret • Secret • Confidentiality • Restricted • Unclassified		Mandatory	WebTrust 3.2.4	

3.1.3. Information Management

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
System Administration					
3.1.3.1	The CA shall designate a trained "System Administrators" who will ensure that the protective security measures of the system are functional and who will maintain the security posture of CA's organization.	1. Obtain the name of system administrator appointed by the CA 2. Check the following: a. Roles and responsibilities of system administrator have been documented. b. a designated System Security Administrator has been appointed for System Administrator with roles and responsibilities documented c. proper training was provided to Security Administrator d. Security Administrator is solely responsible for changes done to information 3. Obtain the password management policy 4. Validate the process implemented in case of forgetting password or changeover to another person 5. Verify if the instance of usage of administrator's passwords is documented securely 6. Obtain the Active Directory of CA	Mandatory	IT CA Rules SCHEDULE-II 5.1	
3.1.3.2	The System Administrator may have a designated System Security Administrator who will assume security responsibilities and provide physical, logical and procedural safeguards for information		Recommended	IT CA Rules SCHEDULE-II 5.1	
3.1.3.3	CA shall ensure System Security Administrator is properly trained before assigning the system security responsibilities.		Mandatory	IT CA Rules SCHEDULE-II 5.1	
3.1.3.4	System Administrator shall solely be responsible for creating, classifying, and retrieving, modifying, deleting or archiving information.		Mandatory	IT CA Rules SCHEDULE-II 5.1	
3.1.3.5	The system administration's password and operation of trusted services must not be written down (in paper or electronic form) or shared with anyone.		Mandatory	IT CA Rules SCHEDULE-II 5.1	
3.1.3.6	A system for password management should be put in place to cover the eventualities such as forgotten password or changeover to another person in case of System Administrator		Mandatory	IT CA Rules SCHEDULE-II 5.1	

	(or System Security Administrator) leaving the organization. Every instance of usage of administrator's passwords must be documented.	employees 7. For sample user accounts verify the System Administrator promptly disabled access if the user is identified as having left the Data Centre, changed assignments, or is no longer requiring system access 8. Validate privileged access is given to users only on a need-to-know and need-to-do basis containing proper business justification and also only after the authorization is documented. 9. Obtain sample of security violations and verify the process followed for recording, investigating and management reviews done. 10. Conduct walkthrough to verify the PKI servers are monitored continuously 11. Obtain list of users who have access to the system 12. Verify only authorized personnel have access and no generic user is enabled or active			
3.1.3.7	The System Administrator shall promptly disable access to a user's account if the user is identified as having left the Data Centre, changed assignments, or is no longer requiring system access. Reactivation of the user's account must be authorized in writing by the System Administrator (Digitally signed E-mail may be acceptable).		Mandatory	IT CA Rules SCHEDULE-II 5.1	
3.1.3.8	The System Administrator must take steps to safeguards classified information as prescribed by its owner.		Mandatory	IT CA Rules SCHEDULE-II 5.1	
3.1.3.9	The System Administrator must authorize privileged access to users only on a need-to-know and need-to-do basis and also only after the authorization is documented.		Mandatory	IT CA Rules SCHEDULE-II 5.1	
3.1.3.10	All security violations must be recorded, investigated, and periodic status reports compiled for review by the management.		Mandatory	IT CA Rules SCHEDULE-II 5.1	
3.1.3.11	The System Administrator together with the system support staff, shall conduct a regular analysis of problems reported to and identify any weaknesses in protection of the information		Mandatory	IT CA Rules SCHEDULE-II 5.1	
3.1.3.12	The System Administrator shall ensure that the data, file and Public Key Infrastructure (PKI) servers are not left unmonitored while these systems are powered on.		Mandatory	IT CA Rules SCHEDULE-II 5.1	
3.1.3.13	The System Administrator should ensure that no generic user is enabled or active on the system.		Mandatory	IT CA Rules SCHEDULE-II 5.1	

Sensitive Information Control					
3.1.3.14	Electronic communication systems, such as router, switches, network device and computers, used for transmission of sensitive information should be equipped or installed with suitable security software and if necessary with an encryptor or encryption software. The appropriate procedure in this regard shall be documented.	1. Obtain documented procedure to ensure safety of communication systems 2. Obtain list of communication systems (i.e. router, switches & computers) used for transmission of sensitive information 3. Verify security implementation in devices is done as per the procedure	Mandatory	IT CA Rules SCHEDULE-II 5.2	
3.1.3.15	The Certifying Authority shall manage its functions in accordance with the levels of integrity and security approved by the Controller from time to time.	1. Verify the CA manages its functions in accordance with the levels of integrity and security approved by the Controller from time to time. 2. Validate the CA discloses information on the assurance levels of certificates that it issues and the limitations of its liabilities to each of its subscribers and relying parties	Mandatory	IT Regulations 3	
3.1.3.16	The Certifying Authority shall disclose information on the assurance levels of the certificates that it issues and the limitations of its liabilities to each of its subscribers and relying parties		Mandatory	IT Regulations 3	
Sensitive Information Security					
3.1.3.17	Highly sensitive information assets shall be stored on secure removable media and should be in an encrypted format to avoid compromise by unauthorized persons.	1. Refer the Process for handling classified data 2. Verify Highly sensitive information assets is stored on secure removable media and is in encrypted format 3. Verify highly sensitive information is classified in accordance as per Control No. 3.1.2.1 4. Validate access control mechanism exist for cases where multiple people have access to sensitive information and data 5. Conduct a walkthrough to verify removable electronic storage media is	Mandatory	IT CA Rules SCHEDULE-II 5.3	
3.1.3.18	Highly sensitive information shall be classified in accordance as per Control No. 3.1.2.1		Mandatory	IT CA Rules SCHEDULE-II 5.3	
3.1.3.19	Sensitive information and data, which are stored on the fixed disk of a computer shared by more than one person, must be protected by access control software (e.g., password). Security packages must be installed which partition or provide authorization to segregated directories/files.		Mandatory	IT CA Rules SCHEDULE-II 5.3	

3.1.3.20	Removable electronic storage media must be removed from the computer and properly secured at the end of the work session or workday.	removed from the computer and properly secured at the end of the work session or workday	Mandatory	IT CA Rules SCHEDULE-II 5.3	
Prevention of Computer Misuse					
3.1.3.21	The computer system shall be configured with minimum of the required accounts and network services.	1. For sample computer system verify configuration is done with minimum of the required accounts and network services. 2. Validate systems are not working on default settings 3. Obtain documented measures for safeguard the security of computers and computer information from misuse 4. Check the following: a. Implementation of measures for safeguarding computers and information from misuse b. Breach reporting process and remedial measures taken c. All incidents are reported to System Administrator d. Procedure to prevent future occurrence of an incident	Mandatory	X.509 Policy 6.5.1	
3.1.3.22	Prevention, detection, and deterrence measures shall be implemented to safeguard the security of computers and computer information from misuse. The measures taken shall be properly documented and reviewed regularly.		Mandatory	IT CA Rules SCHEDULE-II 5.5	
3.1.3.23	CA shall ensure adequate information is provided to all persons, including management, systems developers and programmers, end-users, and third party users warning them against misuse of computers.		Mandatory	IT CA Rules SCHEDULE-II 5.5	
3.1.3.24	Effective measures including reporting of suspected breach, investigation and remedial measures shall be established		Mandatory	IT CA Rules SCHEDULE-II 5.5	
3.1.3.25	All incidents related to breaches shall be reported to the System Administrator or System Security Administrator for appropriate action to prevent future occurrence. These will be responsible for investigation and follow up action			IT CA Rules SCHEDULE-II 5.5	
3.1.3.26	Procedure shall be set-up to establish the nature of any alleged abuse and determine the subsequent action required to be taken to prevent its future occurrence		Mandatory	IT CA Rules SCHEDULE-II 5.5	

3.1.4. Physical and Operational security

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Site Location & Design					
3.1.4.1	The location and construction of the facility housing CA and Certificate Status Provider (CSP) equipment shall be consistent with facilities used to house high value, sensitive information. The site shall not be in locations that are prone to natural or man-made disasters, like flood, fire, chemical contamination and explosions.	1. Verify the CA facility housing CA and CSP equipment is consistent with facilities used to house high value, sensitive information 2. Validate the site is located in secure area immune from natural or man-made disasters 3. Verify applicable building and safety regulations were complied to during construction 4. Conduct walkthrough to check the following: a. External walls are constructed of brick or reinforced concrete of sufficient thickness b. Ground level windows are fortified with sturdy mild steel grills c. All internal walls are tamper-evident d. Air-conditioning system, power supply system and uninterrupted power supply unit are installed e. Proper backup is present in case of power outage	Mandatory	X.509 Policy 5.1.1, IT CA Rules SCHEDULE-III 3.1	
3.1.4.2	Construction shall be done in compliance with all applicable building and safety regulations as laid down by the relevant Government agencies with use of fire resistant material and non-toxic chemicals.		Mandatory	IT CA Rules SCHEDULE-II 4.1.3	
3.1.4.3	CA Shall ensure all external walls shall be constructed of brick or reinforced concrete of sufficient thickness to resist forcible attack. Ground level windows shall be fortified with sturdy mild steel grills or impact-resistant laminated security glass. All internal walls must be from the floor to the ceiling and must be tamper-evident.		Mandatory	IT CA Rules SCHEDULE-II 4.1.5	
3.1.4.4	Air-conditioning system, power supply system and uninterrupted power supply unit with proper backup shall be installed depending upon the nature of operation. All ducting holes of the air-conditioning system must be designed so as to prevent intrusion of any kind.		Mandatory	IT CA Rules SCHEDULE-II 4.1.6	

3.1.4.5	Media library, electrical and mechanical control rooms shall be housed in separate isolated areas, with access granted only to specific, named individuals on a need basis.	f. Ducting holes are designed to prevent intrusion g. Media library, electrical and mechanical control rooms are housed in separate isolated areas h. Access to these areas is granted to specific, named individuals on a need basis i. Media library, electrical and mechanical control rooms is housed in separate isolated areas 5. For mission-critical and sensitive applications verify the facility is located and designed for reparability, relocation and reconfiguration 6. Verify containers are used for storing movable media and papers containing sensitive or plain text information 7. Verify measures CA has implemented to keep the location of DSC system hidden	Mandatory	IT CA Rules SCHEDULE-II 4.1.8	
3.1.4.6	Any facility that supports mission-critical and sensitive applications must be located and designed for reparability, relocation and reconfiguration. The ability to relocate, reconstitute and reconfigure these applications must be tested as part of the business continuity/disaster recovery plan.		Mandatory	IT CA Rules SCHEDULE-II 4.1.9	
3.1.4.7	All removable media and papers containing sensitive or plain text information shall be listed, documented and stored in a container properly identified in the CA Facility		Mandatory	IT CA Rules SCHEDULE-III 3.3	
3.1.4.8	CA shall ensure exact location of Digital Signature Certification System shall not be publicly identified.		Mandatory	IT CA Rules SCHEDULE-III 3.3	
Fire Protection					
3.1.4.9	No combustible materials shall be stored within hundred meters of the operational site	1. Conduct walkthrough to check the following: a. No combustible materials is stored within hundred meters of the operational site b. Automatic fire detection, fire suppression systems and audible alarms are installed at the operational site c. Fire extinguishers are installed at	Mandatory	IT CA Rules SCHEDULE-II 4.2	
3.1.4.10	Automatic fire detection, fire suppression systems and audible alarms as prescribed by the Fire Brigade or any other agency of the Central or State Government shall be installed at the operational site		Mandatory	IT CA Rules SCHEDULE-II 4.2	
3.1.4.11	Fire extinguishers shall be installed at the operational site and their locations clearly marked with appropriate signs.		Mandatory	IT CA Rules SCHEDULE-II 4.2	

3.1.4.12	Periodic testing, inspection and maintenance of the fire equipment and fire suppression systems should be carried out.	operational site d. Location of fire extinguishers is clearly marked with appropriate signs e. Periodic testing, inspection and maintenance of the fire equipment and fire suppression systems are carried out f. Eating, drinking and smoking are prohibited in the operational site g. Operational site is clean h. Procedures for the safe evacuation of personnel in an emergency are visibly pasted/displayed at prominent places i. Fire doors exist on security perimeters 2. Obtain schedule of safety trainings and fire drills and verify they are conducted on periodic basis	Mandatory	IT CA Rules SCHEDULE-II 4.3	
3.1.4.13	There shall be no eating, drinking or smoking in the operational site.		Mandatory	IT CA Rules SCHEDULE-II 4.2	
3.1.4.14	The work areas shall be kept clean at all times.		Mandatory	IT CA Rules SCHEDULE-II 4.2	
3.1.4.15	Procedures for the safe evacuation of personnel in an emergency shall be visibly pasted/displayed at prominent places at the operational site.		Mandatory	IT CA Rules SCHEDULE-II 4.2	
3.1.4.16	Periodic training and fire drills shall be conducted		Mandatory	IT CA Rules SCHEDULE-II 4.2	
3.1.4.17	Fire doors exist on security perimeters around CA operational facilities and are alarmed and conform to local fire regulations.		Mandatory	WebTrust 3.4.6	
Physical Access					
3.1.4.18	Responsibilities round the clock, seven days a week, three hundred sixty five days a year for physical security of the systems used for operation and also actual physical layout at the site of operation shall be defined and assigned to named individuals	1. Obtain copy of the responsibilities assigned for physical security and verify individuals have been assigned for the same 2. Conduct walkthrough to check the following a. All CA personnel have identity and authorization verified before they are included in the access list to CAs system	Mandatory	IT CA Rules SCHEDULE-II 4.4, CA Browser Forum 5.1.2	
3.1.4.19	All Certifying Authority personnel must have their identity and authorization verified before they are included in the access list for physical access to the Certifying Authority's system. All personnel are required to wear visible		Mandatory	WebTrust 3.4.9 IT CA Rules SCHEDULE-	

	identification. Employees are encouraged to challenge anyone not wearing visible identification.	b. All personnel wear visible identification c. Entrance to the main building and entrance to each security zone is video recorded round the clock. Verify on sample basis for last one year for any random date of each year d. Check the recording is carefully scrutinized and maintained for at least one year by verifying logs for a sample dates in the past year e. Biometric physical access security systems are installed and functioning in the operational site f. Unauthorized intrusion is manually or electronically monitored at all times at the CAs Site. Verify by checking the register/list maintained for same g. Physical access to CA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control. Verify by checking the access list / and checking the name of the personnel for dual custody. Physically see also, how the two personnel are involved in the operation h. A manned reception area is		III 13	
3.1.4.20	Dual control over the inventory and issue of access cards/keys during normal business hours to the Data Centre shall be in place.		Mandatory	IT CA Rules SCHEDULE-II 4.4	
3.1.4.21	Entrance to the main building where the Certifying Authority's facilities such as Data Centre, PKI Server and Network devices are housed and entrance to each security zone shall be video recorded round the clock. The recording must be carefully scrutinized and maintained for at least one year		Mandatory	IT CA Rules SCHEDULE-III 3.5	
3.1.4.22	Biometric physical access security systems shall be installed to control and audit access to the operational site		Mandatory	IT CA Rules SCHEDULE-II 4.4	
3.1.4.23	Unauthorized intrusion shall be manually or electronically monitored at all times at the CAs Site		Mandatory	IT CA Rules SCHEDULE-II 3.4.6	
3.1.4.24	Physical access to CA facilities and equipment should be limited to authorized individuals, protected through restricted security perimeters, and shall be operated under multiple person (at least dual custody) control. Personnel authorized for limited physical access shall not be allowed to gain unauthorized access to restricted area within operational site.		Mandatory	WebTrust 4.8.3, IT CA Rules SCHEDULE-II 4.4	
3.1.4.25	A manned reception area or other means to control physical access should be present at the CA operations site		Mandatory	WebTrust 3.4.3	
3.1.4.26	Unescorted access to Certifying Authority's server shall be limited to those personnel identified on an access list		Mandatory	IT CA Rules SCHEDULE-III 3.3	
3.1.4.27	Access security system shall be installed to control and audit details of personnel using the Digital Signature Certification System.		Mandatory	IT CA Rules SCHEDULE-III 3.6	

		present at operational site i. Unescorted access to server is limited to those personnel identified on an access list. Verify by checking list of personnel allowed j. Access security system is installed to control and audit details of personnel using the DSC System. k. Access security system works on the basis of digital signature certification system			
3.1.4.28	An inventory of access cards shall be maintained by the CA and periodically reviewed	1. Verify the CA maintains and inventory of access cards and reviews it periodically 2. Obtain the up-to-date list of personnel who possess cards/keys 3. Verify the list is updated regularly and archived for a period of three years 4. Validate the process followed in case of loss of access cards, check list of cases where cards were lost and verify if the process was followed. 5. Conduct a walkthrough to check the following: a. Any personnel not on access list is escorted at all times within the operational site b. All individuals, other than operations staff, sign in and sign out of the operational site and are accompanied by operations staff. Verify by checking register/log where entries have been made.	Mandatory	IT CA Rules SCHEDULE-III 3.7	
3.1.4.29	An up-to-date list of personnel who possess the cards/keys shall be regularly maintained and archived for a period of three years. Loss of access cards/keys shall be reported immediately to the Security Administrator; who shall take appropriate actions to prevent unauthorized access.		Mandatory	IT CA Rules SCHEDULE-III 3.8	
3.1.4.30	Any personnel not on the access list shall be properly escorted and supervised at all times within the operational site premises. All individuals, other than operations staff, shall sign in and sign out of the operational site and shall be accompanied by operations staff.		Mandatory	IT CA Rules IT CA Rules SCHEDULE-III 3.9, SCHEDULE II 4.4	
3.1.4.31	A site access log shall be maintained at the Certifying Authority's operational site and inspected periodically. All personnel entering and leaving CA operational facilities shall be logged (i.e., an audit trail of all access is securely maintained).		Mandatory	WebTrust 3.4.11, IT CA Rules SCHEDULE III 3.3	

3.1.4.32	A multi-tiered access mechanism must be installed at the Certifying Authority's operational site. The facility should have clearly laid out security zones within its facility with well-defined access rights to each security zone.	c. All personnel entering and leaving CA operational facilities are logged. Verify by checking the physical register or electronic media used for logging. d. CA operational facility has security zones laid out within the facility. Verify the documented proof for zoning performed. e. Access rights to all security zones are laid out. Verify by checking the access list for various security zones f. Security zones are separate from the other by floor to ceiling concrete reinforced walls. Conduct physical walkthrough of the zones to ascertain the same 6. Collect site access log and verify all entries are recorded and inspected periodically	Mandatory	IT CA Rules SCHEDULE III 3.4	
3.1.4.33	Each security zone must be separated from the other by floor to ceiling concrete reinforced walls.		Mandatory	IT CA Rules SCHEDULE III 3.4	
3.1.4.34	Alarm and intrusion detection system must be installed at every stage with adequate power backup capable of continuing operation even in the event of loss of main power.	1. Verify Alarm and intrusion detection system are installed at every stage with adequate power backup 2. Validate Electrical/Electronic circuits to external security alarm monitoring service are supervised 3. Validate access to PKI Server, root keys or any personal computer system or network device is prohibited	Mandatory	IT CA Rules SCHEDULE III 3.4	
3.1.4.35	Electrical/Electronic circuits to external security alarm monitoring service (if used) shall be supervised		Mandatory	IT CA Rules SCHEDULE III 3.4	
2 .1.4.36	Access to PKI Server, root keys or any personal computer system or network device shall be prohibited		Mandatory	IT CA Rules SCHEDULE III 3.4	

3.1.4.37	Access to infrastructure components essential to operation of Certifying Authority such as power control panels, communication infrastructure, Digital Signature Certification system, cabling, etc. shall be restricted to authorized personnel.	1. Verify list of personnel with access to essential components for CA is maintained 2. Validate no unauthorized personnel has access to these components by checking the controls implemented to prevent unauthorized access such as locked door, biometric etc.	Mandatory	IT CA Rules SCHEDULE III 3.8	
3.1.4.38	By-pass or deactivation of normal physical security arrangements shall be authorized and documented by security personnel.	1. Verify all By-pass or deactivation of normal physical security arrangements is authorized and documented by security personnel	Mandatory	IT CA Rules SCHEDULE III 3.9	
3.1.4.39	Intrusion detection systems shall be used to monitor and record physical access to the Digital Signature Certification system during and after office hours.	1. Conduct walkthrough to check the following: a. Intrusion detection systems are used to monitor and record physical access to the DSC system during and after office hours b. Computer System or PKI Server performing the DSC functions are dedicated to those functions and should not be used for any other purposes c. Emergency exits are tested periodically. Validate by checking proper functioning of emergency exits. d. Unauthorized access to areas storing hardware is prohibited. Verify by checking the access list for areas storing the hardware. e. Two person physical access control are present at both the	Mandatory	IT CA Rules SCHEDULE III 3.10	
3.1.4.40	Computer System or PKI Server performing the Digital Signature Certification functions shall be dedicated to those functions and should not be used for any other purposes.		Mandatory	IT CA Rules SCHEDULE III 3.11	
3.1.4.41	Emergency exits shall be tested periodically to ensure that the access security systems are operational		Mandatory	IT CA Rules CHEDULE II 4.4	
3.1.4.42	Unauthorized access to areas storing hardware shall be prohibited		Mandatory	X.509 Policy 5.1.2.1	
3.1.4.43	Two person physical access control shall be present at both the cryptographic module and computer system for CAs issuing Class 1, Class 2 and Class 3 certificates.		Mandatory	X.509 Policy 5.1.2.1	

		cryptographic module and computer system for CAs issuing Class 1, Class 2 and Class 3 certificates. Practical demonstration of the two person physical access should be done in the presence of the auditor.			
3.1.4.44	Removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules shall be placed in secure containers. Activation data shall either be memorized, or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.	1. Verify removable cryptographic modules are deactivated before storage 2. Validate activation information used to access or enable cryptographic modules is placed in secure containers. 3. Check the mechanism used to store activation data	Mandatory	X.509 Policy 5.1.2.1	
3.1.4.45	A security check shall be conducted if the facility housing the CA and CSP equipment is left unattended. At a minimum, the check shall verify the following the equipment should be in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”), for offline CAs all equipment other than PKI repository shall be shut down, security containers must be secured and physical security systems shall be functioning properly.	1. Verify the process of security check to be conducted if the facility housing the CA and CSP equipment is left unattended 2. Validate it covers the requirements mentioned in control description 3. Check the list of persons responsible for doing the security checks mentioned in control - 3.1.4.45 4. Verify if a group of people are assigned the security check responsibility a log identifying the person performing a check at each instance is maintained 5. Check if the facility is not continuously attended, the last person to depart initials a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated	Mandatory	X.509 Policy 5.1.2.1	
3.1.4.46	A person or group of persons shall be made explicitly responsible for making such checks mentioned in control - 3.1.4.45.When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.		Mandatory	X.509 Policy 5.1.2.1	

3.1.4.47	The Certifying Authority must ensure that no single individual may gain access to the Digital Signature Certificate server and the computer server maintaining all information associated with generation, issue and management of Digital Signature Certificate and private keys of the Certifying Authority. Minimum two individuals, preferably using a split-knowledge technique, such as twin passwords, must perform any operation associated with generation, issue and management of Digital Signature Certificate and application of private key of the Certifying Authority.	1. Verify the CA ensures no single individual can gain access to DSC server and the computer server maintaining all information associated with generation, issue and management of DSC and private keys of the CA 2. Validate minimum two individuals, preferably using a split-knowledge technique, such as twin passwords, perform any operation associated with generation, issue and management of DSC and application of private key of the CA. Practical demonstration of the same shall be performed during the audit.	Mandatory	IT CA Rules SCHEDULE III 12	
Inventory Management					
3.1.4.48	Inventory control processes and procedures shall be documented and implemented to manage the origination, arrival, condition, departure and destination of each device.	1. Obtain copy of Inventory control processes and procedures and check the following: a. Policy and procedure are implemented to manage the origination, arrival, condition, departure and destination of each device. b. Details of all media are inventoried c. An independent physical inventory check of all media is conducted at least every six months.Verify by checking latest report of physical inventory check d. An up-to-date inventory list of all documentation is maintained.	Mandatory	WebTrust 4.8.3	
3.1.4.49	Details of all media shall be inventoried. An independent physical inventory check of all media shall be conducted at least every six months.		Mandatory	IT CA Rules SCHEDULE II 8.3	
3.1.4.50	An up-to-date inventory list of all documentation shall be maintained to ensure control and accountability.		Mandatory	IT CA Rules SCHEDULE II 16	
3.1.4.51	All equipment related to CA Operations shall be inventoried		Mandatory	WebTrust 3.4.16	

		Verify by checking previous versions of inventory list to validate periodicity of update e. All equipment related to CA Operations are inventoried. Verify by conducting a random check on sample basis for the infrastructure and check its entry in to inventory			
Media Storage					
3.1.4.52	All sensitive information stored in any media shall bear or be assigned an appropriate security classification.	1. Obtain Media Management policy and verify the following: a. All sensitive information stored in any media is assigned an appropriate security classification b. Media library, electrical and mechanical control rooms are housed in separate isolated areas c. Access to these areas is given only to specific, named individuals on a need basis. Verify by checking the access list d. Such area is fire resistant and free of toxic chemicals. e. Storage media containing sensitive information is secured according to their classification f. Responsibilities for media library management and protection are clearly defined and assigned g. Access to the media library is	Mandatory	IT CA Rules SCHEDULE II 5.2	
3.1.4.53	Media library, electrical and mechanical control rooms shall be housed in separate isolated areas, with access granted only to specific, named individuals on a need basis. The area must be fire resistant and free of toxic chemicals.		Mandatory	IT CA Rules SCHEDULE II 4.1.8	
3.1.4.54	Storage media (i.e. floppy diskettes, magnetic tapes, portable hard disks, optical disks, etc.) containing sensitive information shall be secured according to their classification		Mandatory	IT CA Rules SCHEDULE II 5.2	
3.1.4.55	Responsibilities for media library management and protection shall be clearly defined and assigned.		Mandatory	IT CA Rules SCHEDULE II 8.3	
3.1.4.56	Access to the media library (both on-site and off-site) shall be restricted to the authorized persons only. A list of personnel authorized to enter the library shall be maintained.		Mandatory	IT CA Rules SCHEDULE II 8.3	
3.1.4.57	Media containing sensitive and back up data must be stored at three different physical locations in the country, which can be reached in few hours. Media that contains audit, archive, or backup information shall be duplicated and stored in a		Mandatory	X.509 Policy, IT CA Rules	

	location separate from the CA location.	restricted to the authorized persons only (verify by checking list of authorized personnel)			
3.1.4.58	A media management system shall be in place to account for all media stored on-site and off-site	h. Media containing sensitive and back up data is stored at three different physical locations in the country. Verify by identifying the three different physical locations where backup is stored	Mandatory	IT CA Rules SCHEDULE II 8.3	
3.1.4.59	All incoming/outgoing media transfers shall be authorized by management and users.		Mandatory	IT CA Rules SCHEDULE II 8.3	
3.1.4.60	All media shall have external volume identification. Internal labels shall be fixed, where available.	i. Media that containing audit, archive, or backup information is duplicated and stored in a location separate from the CA location.	Mandatory	IT CA Rules SCHEDULE II 8.3	
3.1.4.61	Procedures shall be in place to ensure that only authorized addition/removal of media from the library is allowed.	j. Media management system has been implemented by providing sample of the process followed.	Mandatory	IT CA Rules SCHEDULE II 8.3	
3.1.4.62	Media retention periods shall be established and approved by management in accordance with legal/regulatory and user requirements.	k. All incoming/outgoing media transfers are authorized by management and users. Verify by checking on sample basis.	Mandatory	IT CA Rules SCHEDULE II 8.3	
3.1.4.63	Proper records of all movements of computer tapes/disks between on-site and off-site media library must be maintained.	l. All media have external volume identification	Mandatory	IT CA Rules SCHEDULE II 8.4	
3.1.4.64	There shall be procedures to ensure the authorized and secure transfer to media to/from external parties and the off-site location including a means to authenticate the receipt shall be in place.	m. Procedures are in place to ensure that only authorized addition/removal of media from the library is allowed	Mandatory	IT CA Rules SCHEDULE II 8.4	
3.1.4.65	Computer media that are being transported to off-site data backup locations should be stored in locked carrying cases that provide magnetic field protection and protection from impact while loading and unloading and during transportation	n. Media retention procedure is established and approved by management o. Records of all movements of computer tapes/disks between on-site and off-site media library	Mandatory	IT CA Rules SCHEDULE II 8.4	

3.1.4.66	All items of equipment containing storage media (fixed and removable disks) shall be checked to ensure that they do not contain sensitive data prior to their disposal.	are maintained. p. Procedure are present for secure transfer and disposal of media q. Computer media that are being transported to off-site data backup locations are stored in locked carrying cases that provide magnetic field protection r. All items of equipment containing storage media are checked to ensure that they do not contain sensitive data prior to their disposal.	Mandatory	WebTrust 3.4.21	
3.1.4.67	Procedures shall be in place to ensure the secure disposal of sensitive information assets on all corrupted/damaged or affected media both internal (e.g. hard disk/optical disk) and external (e.g. diskette, disk drive, tapes etc.) to the system		Mandatory	IT CA Rules SCHEDULE II 5.2	
Power and Air Conditioning					
3.1.4.68	Air-conditioning system and power supply system unit shall be installed by the CA	1. Conduct walkthrough of CA facility and check the following: a. existence of Air conditioning and power supply system b. backup power is present to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown	Mandatory	IT CA Rules SCHEDULE II 4.1	
3.1.4.69	CAs shall have backup power sufficient to automatically lockout input, finish any pending actions, and record the state of the equipment before lack of power or air conditioning causes a shutdown		Mandatory	X.509 Policy 5.1.3	
Waste Disposal					
3.1.4.70	Procedures shall be designed and implemented for disposing off sensitive waste material.	1. Verify procedure is present and implemented for disposing off the sensitive waste material 2. Validate all media used for storage of information pertaining to all functions	Mandatory	X.509 Policy 5.1.7, IT CA Rules SCHEDULE III 5	

3.1.4.71	All media used for storage of information pertaining to all functions associated with generation, production, issue and management of Digital Signature Certificate shall be scrutinized before being destroyed or released for disposal	associated of DSC is scrutinized before being destroyed or released for disposal. Verify by checking on sample basis, media was disposed off based on defined procedure	Mandatory	IT CA Rules SCHEDULE III 5	
Data Backup and Off-site Retention					
3.1.4.72	A Certifying Authority must ensure that facility used for off-site backup shall be within the country and shall have the same level of security as the primary Certifying Authority site.	1. Conduct walkthrough of the CA backup site and check the following: a. facility used for off-site backup is within the country and has the same level of security as the primary CA site b. backup procedures are documented and implemented c. Full system backups are made on periodic schedule d. Backups are performed and stored off-site not less than once every 7 days e. At least one full backup copy shall be stored at an offsite location f. One set of the original disks for all operating system and application software is maintained g. Backups of the system, application and data is performed on a regular basis h. Backups for application under development and data conversion	Mandatory	WebTrust, IT CA Rules SCHEDULE III 6	
3.1.4.73	Back-up procedures shall be documented, scheduled and monitored.		Mandatory	IT CA Rules SCHEDULE II 9	
3.1.4.74	Full system backups of the CAs, sufficient to recover from system failure, shall be made on a periodic schedule		Mandatory	X.509 Policy 5.1.8	
3.1.4.75	Backups shall be performed and stored off-site not less than once every 7 days. At least one full backup copy shall be stored at an offsite location (at a location separate from the CA equipment). Only the latest full backup need be retained.		Mandatory	X.509 Policy 5.1.8	
3.1.4.76	One set of the original disks for all operating system and application software must be maintained to ensure that a valid, virus-free backup exists and is available for use at any time.		Mandatory	IT CA Rules SCHEDULE II 9	
3.1.4.77	Backups of the system, application and data shall be performed on a regular basis. Backups should also be made for application under development and data conversion efforts.		Mandatory	IT CA Rules SCHEDULE II 9	

3.1.4.78	Data backup is required for all systems including personal computers, servers and distributed systems and databases.	efforts is also made i. Data backup is performed j. Critical system data and file server software have full backups taken weekly k. Documented proof of verifications of the integrity of backups every six months l. backups are kept in an area physically separate from the server m. information backups are rotated on a periodic basis to an off-site storage location n. Critical system data and file server software have incremental backups taken daily o. Systems that are completely static are backed up after changes or update in information p. Each LAN/system has a primary and backup operator to ensure continuity of business operations q. Security requirements of backup copies are consistent with control for information backed up	Mandatory	IT CA Rules SCHEDULE II 9	
3.1.4.79	Critical system data and file server software shall have full backups taken weekly.		Mandatory	IT CA Rules SCHEDULE II 9	
3.1.4.80	The Certifying Authority should verify the integrity of the backups at least once every six months		Mandatory	IT CA Rules SCHEDULE II 9	
3.1.4.81	The backups shall be kept in an area physically separate from the server. If critical system data on the LAN represents unique versions of the information assets, then the information backups should be rotated on a periodic basis to an off-site storage location.		Mandatory	IT CA Rules SCHEDULE II 9	
3.1.4.82	Critical system data and file server software must have incremental backups taken daily.		Mandatory	IT CA Rules SCHEDULE II 9	
3.1.4.83	Systems that are completely static may not require periodic backup, but shall be backed up after changes or updates in the information		Mandatory	IT CA Rules SCHEDULE II 9	
3.1.4.84	Each LAN/system should have a primary and backup operator to ensure continuity of business operations.		Mandatory	IT CA Rules SCHEDULE II 9	
3.1.4.85	The security requirements of backup copies shall be consistent with the controls for the information backed up.		Mandatory	WebTrust 4.2.4	
Environmental Protection					
3.1.4.86	Water detectors shall be installed under the raised floors throughout the operational site and shall be connected to audible alarms	1. Conduct walkthrough of the CA facility and check the following: a. Water detectors are installed under the raised floors throughout	Mandatory	IT CA Rules SCHEDULE II 4.3	

3.1.4.87	The temperature and humidity condition in the operational site shall be monitored and controlled periodically	the operational site and are connected to audible alarms b. temperature and humidity condition in the operational site is monitored and controlled periodically c. periodic inspection, testing and maintenance of equipment is scheduled. Verify by checking previous reports on a sample basis based on frequency d. personnel at operational site is trained to monitor and control various devices	Mandatory	IT CA Rules SCHEDULE II 4.3	
3.1.4.88	Periodic inspection, testing and maintenance of the equipment and systems shall be scheduled.		Mandatory	IT CA Rules SCHEDULE II 4.3	
3.1.4.89	Personnel at the operational site shall be trained to monitor and control the various equipment and devices installed at the operational site for the purpose of fire and environment protection.		Mandatory	IT CA Rules SCHEDULE II 4	
Third Party Access					
3.1.4.90	Access to the computer systems by other Organizations shall be subjected to a similar level of security protection and controls as in stated in Information Technology security guidelines under IT CA Rules	1. Verify access to computer systems by other organizations is subjected to a similar level of security protection and controls as stated in IT CA Rules 2. Validate in case Data Centre uses external service/facility provider for any of their operations, all related risks are evaluated before onboarding the outsourced vendor 3. Verify on sample basis the external service or facility provider has signed non-disclosure agreements with the management of the Data Centre/operational site 4. Check the external service/facility provider provides an equivalent level of security controls as required by Information Technology Security Guidelines	Mandatory	IT CA Rules SCHEDULE II 5.4	
3.1.4.91	In case the Data Centre uses the facilities of external service/facility provider (outsourcer) for any of their operations, the use of external service/facility providers (e.g. outsourcer) shall be evaluated in light of the possible security exposures and risks involved and all such agreements shall be approved by the information asset owner. The external service or facility provider shall also sign non-disclosure agreements with the management of the Data Centre/operational site.		Mandatory	IT CA Rules SCHEDULE II 5.4	
3.1.4.92	The external service/facility provider (e.g. outsourcer) shall provide an equivalent level of security controls as required by Information Technology Security Guidelines		Mandatory	IT CA Rules SCHEDULE II 5.4	

3.1.5. Personnel Security

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Personnel Security					
3.1.5.1	The Certifying Authority must ensure that all personnel performing duties with respect to its operation must: • be appointed in writing; • be bound by contract or statute to the terms and conditions of the position they are to fill; • have received comprehensive training with respect to the duties they are to perform; • be bound by statute or contract not to disclose sensitive Certifying Authority's security related information or subscriber information; • not be assigned duties that may cause a conflict of interest with their Certifying Authority's duties; • be aware and trained in the relevant aspects of the Information Technology Security Policy and Security Guidelines framed for carrying out Certifying Authority's operation	1. For sample CA personnel, perform the following checks: a. personnel received an offer letter with roles and responsibilities appointed in writing. Verify on sample basis for personnel b. personnel is bound by contract or statute to the terms and conditions of the position they are to fill. Verify by checking the contract c. personnel has received comprehensive training via sessions organized specifically for the job. Check training logs d. personnel is bound by statute or contract not to disclose sensitive CA's security related information or subscriber information and has signed NDA for same. e. personnel is not assigned duties that may cause a	Mandatory	IT CA Rules SCHEDULE III 14	

		conflict of interest with their CA's duties f. personnel is aware and trained in the relevant aspects of the Information Technology Security Policy and Security Guidelines			
3.1.5.2	A Certifying Authority must make available to his personnel the Digital Signature Certificate policies it supports, its Certification Practice Statement, Information Technology Security Policy and any specific statutes, policies or contracts relevant to their position	1. Validate CA has made available to his personnel the DSC policies, CPS, IT security guideline, Information Technology Security Policy and any specific statutes, policies or contracts relevant to their position 2. Verify the CA provides reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations and receive regular security/PKI based trainings.	Mandatory	IT CA Rules SCHEDULE III 17	
3.1.5.3	The CA shall provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.		Mandatory	WebTrust 3.3	
3.1.5.4	Prior to the engagement of any person whether as an employee, agent, or an independent contractor of the CA, the CA shall verify perform a background check. The scope of the background check shall include the following areas covering the past five years: • Employment; • Education (Regardless of the date of award, the highest educational degree shall be verified); • Place of residence (3 years); • Law Enforcement; and • References The background shall be refreshed every three years.	1. Check the documented procedure detailing the background check criteria for an employee or an independent contractor of the CA 2. Verify that the scope of background check contains the details covered in control description	Mandatory	WebTrust 3.3.7, X.509 Policy 5.3.2	

3.1.5.5	The CA and CSP shall make available to its personnel this certificate policy, the applicable CPS, and any relevant statutes, policies or contracts.	1. Verify the CA and CSP share all relevant statutes, policies or contracts with their personnel	Mandatory	X.509 Policy 5.3.7	
3.1.5.6	Personnel appointed to trusted roles (CA trusted roles) shall: • Have successfully completed an appropriate training program; • Have demonstrated the ability to perform their duties; • Be trustworthy; • Have no other duties that would interfere or conflict with their duties for the trusted role; • Have not been previously relieved of duties for reasons of negligence or nonperformance of duties; • Have not been denied a security clearance, or had a security clearance revoked for cause; • Have not been convicted of a felony offense; and • Be appointed in writing by an approving authority • Be bound by statute or contract not to disclose sensitive Certifying Authority's security related information or subscriber information;	1. Obtain the list of personnel having CA trusted roles 2. Verify for sample personnel, they adhere to the requirements mentioned in control description 3. Validate the personnel in Trusted Roles maintain skill levels consistent with the CA's training and performance programs.	Mandatory	X.509 Policy 5.3.1	
3.1.5.7	All personnel in Trusted Roles shall maintain skill levels consistent with the CA's training and performance programs.		Mandatory	CA Browser Forum 5.3.4	

3.1.6. System integrity and security measures

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Use of Security Systems or Facilities					
3.1.6.1	Security controls shall be installed and maintained on each computer system or computer node to prevent unauthorized users from gaining entry to the information system and to prevent unauthorized access to data.	1. For sample computers, check the minimum baseline security controls are installed and maintained on each computer system 2. Validate system software or resource of the computer system is accessible after being authenticated by access control system.	Mandatory	IT CA Rules SCHEDULE II 6.1	
3.1.6.2	Any system software or resource of the computer system should only be accessible after being authenticated by access control system.		Mandatory	IT CA Rules SCHEDULE II 6.1	
System Access Control					
3.1.6.3	Access control software and system software security features shall be implemented to protect resources. Management approval is required to authorize issuance of user identification (ID) and resource privileges. Approved access and integrity controls such as intrusion detection, virus scanning, prevention of denial-of service attacks and physical security measures shall be followed by the Certifying Authority for all its systems that store and process the subscribers' information and certificates.	1. For the system access controls implemented in CA facility check on sample basis the following: a. Management approval is required to authorize issuance of user identification (ID) and resource privileges b. Access control software and system software security features are implemented c. Approved access and integrity controls are implemented d. access control software or	Mandatory	IT CA Rules SCHEDULE II 6.2, IT Regulations 3	
3.1.6.4	The access control software or operating system of the computer system shall provide features to restrict access to the system and data resources. The use of common passwords such as "administrator" or "president" or "game" etc. to protect		Mandatory	IT CA Rules SCHEDULE II 6.2	

	access to the system and data resources represent a security exposure and shall be avoided. All passwords used must be resistant to dictionary attacks.	operating system of the computer system provides features to restrict access to the system and data resources			
3.1.6.5	An Access Control System manual documenting the access granted to different level of users shall be prepared to provide guidance to the System Administrator for grant of access.	e. All passwords used are resistant to dictionary attacks and contain letters, numerals and special characters.	Mandatory	IT CA Rules SCHEDULE II 6.2	
3.1.6.6	Each user shall be assigned a unique user ID. Adequate user education shall be provided to help users in password choice and password protection. Sharing of user IDs shall not be allowed.	f. A documented Access Control System manual is present g. Each user is assigned a unique user ID h. Sharing IDs is prohibited	Mandatory	IT CA Rules SCHEDULE II 6.2	
3.1.6.7	Stored passwords shall be encrypted using internationally proven encryption techniques to prevent unauthorized disclosure and modification.	i. Stored passwords are encrypted	Mandatory	IT CA Rules SCHEDULE II 6.2	
3.1.6.8	Stored passwords shall be protected by access controls from unauthorized disclosure and modification	j. Stored passwords are protected by access controls	Mandatory	IT CA Rules SCHEDULE II 6.2	
3.1.6.9	Automatic time-out for terminal inactivity should be implemented	k. Automatic time-out for terminal inactivity is implemented	Mandatory	IT CA Rules SCHEDULE II 6.2	
3.1.6.10	Where a second level access control is implemented through the application system, password controls similar to those implemented for the computer system shall be in place.	l. Activities of all remote users are logged and monitored closely m. facility to login as another user from one user's login is denied	Mandatory	IT CA Rules SCHEDULE II 6.2	
33.1.6.11	Activities of all remote users shall be logged and monitored closely	n. startup and shutdown procedure of the security software is Automated	Mandatory	IT CA Rules SCHEDULE II 6.2	
3.1.6.12	The facility to login as another user from one user's login shall be denied. However, the system should prohibit direct login as a trusted user (e.g. root in Unix, administrator in Windows NT or Windows 2000). This means that there must be a user account configured for the trusted administrator.	o. Sensitive Operating System files are protected against all known attacks using proven tools and techniques	Mandatory	IT CA Rules SCHEDULE II 6.2	

3.1.6.13	The startup and shutdown procedure of the security software must be Automated	p. Only System Administrator is allowed to modify systemoperated files	Mandatory	IT CA Rules SCHEDULE II 6.2	
3.1.6.14	Sensitive Operating System files, which are more prone to hackers must be protected against all known attacks using proven tools and techniques. That is to say no user will be able to modify them except with the permission of System Administrator.		Mandatory	IT CA Rules SCHEDULE II 6.2	
Password Management					
3.1.6.15	Quality standards for password shall be enforced. The quality level shall be increased progressively. The following control features shall be implemented for passwords: • Minimum of eight • characters without leading or trailing blanks; • Shall be different from the existing password and the two previous ones; • Shall be changed at least once every ninety days; for sensitive system password shall be changed at least once every thirty days; and • Shall not be shared, displayed or printed. Shall have at least on number, one capital letter, one small case letter and one special character	1. Verify on sample basis the passwords used across CA systems comply with the requirements mentioned in control 3.1.6.15 2. Verify on sample basis the password retries is limited to maximum three attempts (two for sensitive for sensitive systems) 3. Check the user ID is revoked after the user exhausts permissible limit of password retries on sample basis 4. Validate the initial or reset passwords is changed by the user upon first use 5. Check the passwords are encrypted in storage to prevent unauthorized disclosure and protect them from dictionary attacks and all known password cracking algorithms.	Mandatory	IT CA Rules SCHEDULE II 6.3	
3.1.6.16	Password retries shall be limited to a maximum of three attempted logons after which the user ID shall then be revoked; for sensitive systems, the number of password retries should be limited to a maximum of two.		Mandatory	IT CA Rules SCHEDULE II 6.3	
3.1.6.17	Initial or reset passwords must be changed by the user upon first use. Users shall follow defined policies and procedures in the selection and use of passwords.		Mandatory	WebTrust 3.6.6, IT CA Rules SCHEDULE II 6.3	

3.1.6.18	Passwords shall always be encrypted in storage to prevent unauthorized disclosure and protect them from dictionary attacks and all known password cracking algorithms.		Mandatory	IT CA Rules SCHEDULE II 6.3	
Privileged User's Management					
3.1.6.19	System privileges shall be granted to users only on a need-to-use basis. Login privileges for highly privileged accounts should be available only from Console and terminals situated within Console room.	1. For the privileged user management process, check the following on sample basis: a. System privileges are granted to users only on a need-to-use basis b. Login privileges for highly privileged accounts are available only from Console and terminals situated within Console room c. An audit trail of activities conducted by highly privileged users is maintained for two years and reviewed periodically at least every week by operator who is independent of System Administrator d. Privileged user is be allowed to log in to the computer system from remote terminal e. Separate user IDs are allowed to the user for performing privileged and normal (non-privileged) activities f. user IDs for emergency use are recorded and approved. g. Passwords are reset after	Mandatory	IT CA Rules SCHEDULE II 6.4	
3.1.6.20	An audit trail of activities conducted by highly privileged users shall be maintained for two years and reviewed periodically at least every week by operator who is independent of System Administrator		Mandatory	IT CA Rules SCHEDULE II 6.4	
3.1.6.21	Privileged user shall not be allowed to log in to the computer system from remote terminal. The usage of the computer system by the privilege user shall be allowed during a certain time period.		Mandatory	IT CA Rules SCHEDULE II 6.4	
3.1.6.22	Separate user IDs shall be allowed to the user for performing privileged and normal (non-privileged) activities.		Mandatory	IT CA Rules SCHEDULE II 6.4	
3.1.6.23	The use of user IDs for emergency use shall be recorded and approved. The passwords shall be reset after use.		Mandatory	IT CA Rules SCHEDULE II 6.4	

		emergency use			
User's Account Management					
3.1.6.24	Procedures for user account management shall be established to control access to application systems and data	1. For the User Account Management process, check the following on sample basis: a. Procedures have been designed and implemented for user account management b. Users are authorized by the computer system owner to access the computer services c. written statement of access rights is given to all users d. all users sign an undertaking to acknowledge that they understand the conditions of access e. Access is only provided after authorization is complete f. Formal record of all registered users of the computer services is maintained g. Access rights of users who have been transferred, or left the organization are removed immediately h. Periodic checks are carried out for redundant user accounts i. User accounts are suspended if any of the conditions mentioned in control 3.1.6.32	Mandatory	IT CA Rules SCHEDULE II 6.5	
3.1.6.25	Users shall be authorized by the computer system owner to access the computer services		Mandatory	IT CA Rules SCHEDULE II 6.5	
3.1.6.26	A written statement of access rights shall be given to all users.		Mandatory	IT CA Rules SCHEDULE II 6.5	
3.1.6.27	All users shall be required to sign an undertaking to acknowledge that they understand the conditions of access		Mandatory	IT CA Rules SCHEDULE II 6.5	
3.1.6.28	Where access to computer services is administered by service providers, access shall not be provided until authorization is completed. This shall include the acknowledgment of receipt of the accounts by the users		Mandatory	IT CA Rules SCHEDULE II 6.5	
3.1.6.29	A formal record of all registered users of the computer services shall be maintained.		Mandatory	IT CA Rules SCHEDULE II 6.5	
3.1.6.30	Access rights of users who have been transferred, or left the organization shall be removed immediately		Mandatory	IT CA Rules SCHEDULE II 6.5	
3.1.6.31	A periodic check shall be carried out for redundant user accounts and access rights that are no longer required. Redundant user accounts shall not be re-issued to another user		Mandatory	IT CA Rules SCHEDULE II 6.5	
3.1.6.32	User accounts shall be suspended under the following conditions:		Mandatory	IT CA Rules SCHEDULE II 6.5	

	• When an individual is on extended leave or inactive use of over thirty days. In case of protected computer system, the limit of thirty days may be reduced to fifteen days by the System Administrator. • Immediately upon the termination of the services of an individual. • Suspended or inactive accounts shall be deleted after a two months period. In case of protected computer systems, the limit of two months may be reduced to one month.	are met			
Data and Resource Protection					
3.1.6.33	All information assets shall be assigned an "owner" responsible for the integrity of that data/resource. Custodians shall be assigned and shall be jointly responsible for information assets by providing computer controls to assist owners.	1. Check the list of data assets and the corresponding owner/custodian for the same.	Mandatory	IT CA Rules SCHEDULE II 6.6	
3.1.6.34	The operating system or security system of the computer system shall: • Define user authority and enforce access control to data within the computer system; • Be capable of specifying, for each named individual, a list of named data objects (e.g. file, Programme) or groups of named objects, and the type of access allowed.	1. Verify the operating system or security system of the computer system define user authority and enforce access control to data within the computer system Check these are capable of specifying for each named individual, a list of named data objects (e.g. file, Programme) or groups of named objects, and the type of access allowed.	Mandatory	IT CA Rules SCHEDULE II 6.6	
3.1.6.35	For networked or shared computer systems, system users shall be limited to a profile of data objects required to perform their needed tasks	1. Verify for networked or shared computer systems, system users shall be limited to a profile of data objects required to perform their needed tasks	Mandatory	IT CA Rules SCHEDULE II 6.6	

3.1.6.36	Application Programmer shall not be allowed to access the production system	2. Validate that application programmer does not have access to the production system	Mandatory	IT CA Rules SCHEDULE II 6.6	
Sensitive Systems Protection					
3.1.6.37	Security tokens/smart cards/bio-metric technologies such as Iris recognition, finger print verification technologies etc. shall be used to complement the usage of passwords to access the computer system	1. For sensitive system protection, check the following have been implemented: a. Security tokens/smart cards/bio-metric technologies such as Iris recognition etc. are used to complement the usage of passwords to access the computer system b. For computer system processing sensitive data, identify the list of organizations which have access to sensitive data and check the access control measures implemented to establish its effectiveness c. Data in storage is encrypted	Mandatory	IT CA Rules SCHEDULE II 7	
3.1.6.38	For computer system processing sensitive data, access by other Organizations shall be prohibited or strictly controlled.		Mandatory	IT CA Rules SCHEDULE II 7	
3.1.6.39	For sensitive data, encryption of data in storage shall be considered to protect its confidentiality and integrity.		Mandatory	IT CA Rules SCHEDULE II 7	
Data Centre Operations Security					
3.1.6.40	Procedures shall be established to ensure that all changes to the job schedules are appropriately approved. The authority to approve changes to job schedules shall be clearly assigned.	1. For the jobs performed in the Data Centre check the following: a. procedures have been established to ensure that all changes to the job schedules are appropriately approved b. list of people who have been assigned authority to approve	Mandatory	IT CA Rules SCHEDULE II 8.1	
3.1.6.41	As far as possible, automated job scheduling should be used. Manual job scheduling should require prior approval from the competent authority.		Mandatory	IT CA Rules SCHEDULE II 8.1	

3.1.6.42	Procedures shall be established to ensure that only authorized and correct job stream and parameter changes are made.	changes to job schedule c. automated job scheduling is used d. Procedures are established to ensure that only authorized and correct job stream and parameter changes are made. e. Procedures are established to maintain logs of system activities f. Procedures are established to ensure that people other than well-trained computer operators are prohibited from operating the computer equipment g. Procedures are implemented to ensure the secure storage or distribution of all outputs/reports, in accordance with procedures defined by the owners for each system	Mandatory	IT CA Rules SCHEDULE II 8.2	
3.1.6.43	Procedures shall be established to maintain logs of system activities. Such logs shall be reviewed by a competent independent party for indications of dubious activities. Appropriate retention periods shall be set for such logs.		Mandatory	IT CA Rules SCHEDULE II 8.2	
3.1.6.44	Procedures shall be established to ensure that people other than well-trained computer operators are prohibited from operating the computer equipment		Mandatory	IT CA Rules SCHEDULE II 8.2	
3.1.6.45	Procedures shall be implemented to ensure the secure storage or distribution of all outputs/reports, in accordance with procedures defined by the owners for each system		Mandatory	IT CA Rules SCHEDULE II 8.2	

3.1.7. Disaster Recovery

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Incident and Compromise Handling Procedures					
3.1.7.1	An incident management plan shall be developed and approved by the management. The plan shall include the following areas: • Certifying Authority's certification key compromise; • Hacking of systems and network; • Breach of physical security; • Infrastructure availability; • Fraudulent registration and generation of Digital Signature Certificates; and • Digital Signature Certificate suspension and revocation information.	1. Obtain copy of the incident management plan 2. Verify the plan has been approved by the management 3. Validate the plan includes the areas mentioned in the control description	Mandatory	IT CA Rules SCHEDULE III 11.3	
3.1.7.2	An incident response action plan shall be established to ensure the readiness of the Certifying Authority to respond to incidents. The plan should include the following areas: • Compromise control; • Notification to user community; (if applicable) • Revocation of affected Digital Signature Certificates; (if applicable) • Responsibilities of personnel handling incidents; • Investigation of service disruption; • Service restoration procedure; • Monitoring and audit trail analysis; and	1. Verify an incident response action plan has been established by the CA 2. Validate the plan includes the areas mentioned in the control description	Mandatory	IT CA Rules SCHEDULE III 11.3	

	• Media and public relations.				
3.1.7.3	A formal security incident reporting procedure exists setting out the actions to be taken on receipt of an incident report. This includes a definition and documentation of assigned responsibilities and escalation procedures. Any incidents are reported to PA as a matter of urgency.	1. Verify the security incident reporting procedure and check the following: a. Procedure details actions to be taken on receipt of an incident report b. definition and documentation of assigned responsibilities and escalation procedures exist c. procedures have been established for reporting observed or suspected security weaknesses in, or threats to, systems or services as they are detected. d. Procedure exist and are implemented for reporting hardware and software malfunctions e. Procedures exist and are followed to assess that corrective action is taken for reported incidents f. formal problem management process and procedure exist g. help desk is set up to assist users in the resolution of problems. Check tickets raised on helpdesk and their resolution on sample basis	Mandatory	WebTrust 3.5.9	
3.1.7.4	Users of CA systems are required to note and report observed or suspected security weaknesses in, or threats to, systems or services as they are detected.		Mandatory	WebTrust 3.5.10	
3.1.7.5	Procedures exist and are followed for reporting hardware and software malfunctions.		Mandatory	WebTrust 3.5.11	
3.1.7.6	Procedures exist and are followed to assess that corrective action is taken for reported incidents.		Mandatory	WebTrust 3.5.12	
3.1.7.7	A formal problem management process exists that allows the types, volumes and impacts of incidents and malfunctions to be documented, quantified and monitored		Mandatory	WebTrust 3.5.13	
3.1.7.8	Procedures for identifying, reporting and resolving problems, such as nonfunctioning of Certifying Authority's system; breaches in Information Technology security; and hacking, shall be established and communicated to all personnel concerned. It shall include emergency procedures. Periodic reports shall be submitted for management review		Mandatory	IT CA Rules Section II 22	
3.1.7.9	A help desk shall be set up to assist users in the resolution of problems. A system for recording, tracking and reporting the status of reported problems shall be established to ensure that they are promptly managed and resolved with minimal impact on the user of the computing resources		Mandatory	IT CA Rules Section II 22	

Recovery Procedure					
3.1.7.10	Commitment shall be obtained in writing from computer equipment and supplies vendors to replace critical equipment and supplies within a specified period of time following a destruction of the computing facility.	1. Validate the recover procedure is documented and implemented 2. Verify written commitment in form of a contract has been taken from computer equipment and supplies vendors to replace critical equipment and supplies within a specified period of time following a destruction of the computing facility. 3. Check the business continuity plan includes procedures for emergency ordering of equipment and availability of services 4. Verify need for backup hardware is evaluated in accordance to business needs	Mandatory	IT CA Rules SCHEDULE II 24	
3.1.7.11	The business continuity plan shall be developed which inter alia include the procedures for emergency ordering of the equipment and availability of the services.		Mandatory	IT CA Rules SCHEDULE II 24	
3.1.7.12	The need for backup hardware and other peripherals should be evaluated in accordance to business needs		Mandatory	IT CA Rules SCHEDULE II 24	
Emergency Preparedness					
3.1.7.13	Emergency response procedures for all activities connected with computer operation shall be developed and documented. These procedures should be reviewed periodically	1. Verify emergency response procedure has been developed and documented 2. Validate emergency drills are held periodically	Mandatory	IT CA Rules SCHEDULE II 23	
3.1.7.14	Emergency drills should be held periodically to ensure that the documented emergency procedures are effective.		Mandatory	IT CA Rules SCHEDULE II 23	
Disaster Recovery/Management					
3.1.7.15	Disaster recovery plan shall be developed, properly documented, tested and maintained to ensure that in the event of a failure of the information system or destruction of the	1. Obtain copy of the documented disaster recovery plan and check the following: a. Plan has been tested and	Mandatory	IT CA Rules SCHEDULE II 26	

	facility, essential level of service will be provided. The disaster recovery framework should include: • emergency procedures, describing the immediate action to be taken in case of a major incident • fall back procedure, describing the actions to be taken to relocate essential activities or support services to a backup site • restoration procedures, describing the action to be taken to return to normal operation at the original site	maintained to ensure service will be provided in case of an emergency b. The DR framework includes requirements covered in control 3.1.7.15 c. The documentation covers definition of disaster, condition for activating plan, stage of crisis, decision making process and requirements covered in control 3.1.7.16 d. Specific disaster management plan is present for critical applications e. Responsibilities and reporting structure is clearly defined and will take effect immediately on the declaration of a disaster f. Each component/aspect of the plan has a person and a backup assigned to its execution g. Periodic training of personnel and users associated with computer system and network is conducted h. Test plan has been developed and documented i. Results of tests are documented for management review			
3.1.7.16	The documentation should include: • definition of a disaster; • condition for activating the plan; • stages of a crisis; • who will make decisions in the crisis • role of individuals for each component of the plan; • composition of the recovery team; and • decision making process for return to normal operation.		Mandatory	IT CA Rules SCHEDULE II 26	
3.1.7.17	Specific disaster management plan for critical applications shall be developed, documented, tested and maintained on a regular basis.		Mandatory	IT CA Rules SCHEDULE II 26	
3.1.7.18	Responsibilities and reporting structure shall be clearly defined which will take effect immediately on the declaration of a disaster		Mandatory	IT CA Rules SCHEDULE II 26	
3.1.7.19	Each component/aspect of the plan should have a person and a backup assigned to its execution		Mandatory	IT CA Rules SCHEDULE II 26	

3.1.7.20	Periodic training of personnel and users associated with computer system and network should be conducted defining their roles and responsibilities in the event of a disaster	j. DR plan is updated regularly	Mandatory	IT CA Rules SCHEDULE II 26	
3.1.7.21	Test plan shall be developed, documented and maintained. Periodic tests shall be carried out to test the effectiveness of the procedures in the plan. The results of the tests shall be documented for management review		Mandatory	IT CA Rules SCHEDULE II 26	
3.1.7.22	Disaster recovery plan should be updated regularly to ensure its continuing Effectiveness		Mandatory	IT CA Rules SCHEDULE II 26	
Compromise and Disaster Recovery					
3.1.7.23	The Certifying Authority must establish business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing and networking resources, nominated website, repository, software and/or data. Where a repository is not under the control of the Certifying Authority, the Certifying Authority must ensure that any agreement with the repository provides for business continuity procedures.	1. Verify the CA has established business continuity procedures 2. Validate the procedures cover the requirements mentioned in control description	Mandatory	IT CA Rules SCHEDULE III 11.1	
Secure facility after a natural or other type of disaster					
3.1.7.24	The Certifying Authority must establish a disaster recovery plan outlining the steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster. Where a repository is not under the control of the Certifying Authority the Certifying Authority must ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.	1. Validate the CAs DR plan covers steps to be taken to re-establish a secure facility in the event of a natural or other type of disaster 2. Verify in case the repository is not under CAs control, CA has signed an agreement with the repository provider that a disaster recovery plan be established and documented by the repository	Mandatory	IT CA Rules SCHEDULE III 11.2	

3.1.8. Audit Logging

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Audit Logging					
3.1.8.1	The CA and each Delegated Third Party shall record details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. The CA shall make these records available to its Qualified Auditor as proof of the CA's compliance with these Requirements.	1. Verify on sample basis the CA records details of the actions taken to process a certificate request and to issue a Certificate 2. Validate security audit logs for activities that are core to CAs operations are automatically collected 3. Check all security audit logs, both electronic and non-electronic, are retained and made available during compliance audits	Mandatory	CA Browser Forum 5.4.1	
3.1.8.2	Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used.		Mandatory	X.509 Policy 5.4	
3.1.8.3	The Certifying Authority must maintain secure and reliable records and logs for activities that are core to its operations and review them regularly to detect any anomaly in the system..All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits		Mandatory	X.509 Policy 5.4, IT Regulations 3	
Types of Events Recorded					
3.1.8.4	The Certifying Authority shall maintain record of all events relating to the security of his system. The records should be maintained in audit log file and shall include such events as: • System start-up and shutdown; • Certifying Authority's application start-up and	1. For sample audit log files, check the following details are recorded: a. System start-up and shutdown; b. CA's application start-up and shutdown;	Mandatory	IT CA Rules SCHEDULE III 9.1	

	shutdown; • Attempts to create, remove, set passwords or change the system • privileges of the PKI Master Officer, PKI Officer, or PKI Administrator; • Changes to keys of the Certifying Authority or any of his other details; • Changes to Digital Signature Certificate creation policies, e.g. validity period; • Login and logoff attempts; • Unauthorised attempts at network access to the Certifying Authority's system; • Unauthorised attempts to access system files; • Generation of own keys; • Creation and revocation of Digital Signature Certificates; • Attempts to initialize remove, enable, and disable subscribers, and update and recover their keys; • Failed read-and-write operations on the Digital Signature Certificate and Certificate Revocation List (CRL) directory.	c. Attempts to create, remove, set passwords or change the system d. privileges of the PKI Master Officer, PKI Officer, or PKI Administrator; e. Changes to keys of the CA or any of his other details; f. Changes to DSC creation policies g. Login and logoff attempts; h. Unauthorised attempts at network access i. Unauthorised attempts to access system files; j. Generation of own keys; k. Creation and revocation of DSC; l. Attempts to initialize remove, enable, and disable subscribers, and update and recover their keys; m. Failed read-and-write operations on the Digital Signature Certificate and Certificate Revocation List (CRL) directory.			
3.1.8.5	CA and Subscriber Certificate lifecycle management events, including the following shall be recorded: • Certificate requests, renewal, and re-key requests, and revocation; • All verification activities stipulated in these Requirements and the CA's Certification Practice Statement; • Date, time, phone number used, persons spoken to, and end results of verification telephone calls; • Acceptance and rejection of certificate requests;	1. On a sample basis validate the CA and Subscriber Certificate lifecycle management events, including the following are recorded: a. Certificate requests, renewal, and re-key requests, and revocation; b. All verification activities stipulated in these Requirements and the CA's Certification Practice Statement; c. Date, time, phone number used,	Mandatory	CA Browser Forum 5.4.1	

	• Issuance of Certificates; and • Generation of Certificate Revocation Lists and OCSP entries	persons spoken to, and end results of verification telephone calls; d. Acceptance and rejection of certificate requests; e. Issuance of Certificates; and f. Generation of Certificate Revocation Lists and OCSP entries			
3.1.8.6	All security auditing capabilities of the CA, CSP, and RA operating system and the CA, CSP, and RA applications required by this CP shall be enabled	1. Verify all security auditing capabilities of the CA, CSP, and RA operating system and the CA, CSP, and RA applications required by this CP are enabled	Mandatory	X.509 Policy 5.4.1	
3.1.8.7	A Certifying Authority should consider the use of automated security management and monitoring tools providing an integrated view of the security situation at any point in time. Records of the following application transactions shall be maintained: • Registration; • Certification; • Publication; • Suspension; and • Revocation.	1. Verify CA has implemented automated security management and monitoring tools providing an integrated view of the security situation at any point in time 2. Validate records of application transactions as mentioned in control 3.1.8.7 are maintained 3. Check the records and log files are reviewed regularly for the activities mentioned in control 3.1.8.8 4. Verify all logs contain date and time of the event and the identity of subscriber/ subordinate/ entity which caused the event	Mandatory	IT CA Rules SCHEDULE III 9.1	
3.1.8.8	Records and log files shall be reviewed regularly for the following activities: • Misuse; • Errors; • Security violations; • Execution of privileged functions; • Change in access control lists; • Change in system configuration		Mandatory	IT CA Rules SCHEDULE III 9.1	

3.1.8.9	All logs, whether maintained through electronic or manual means, should contain the date and time of the event, and the identity of the subscriber/subordinate/ entity which caused the event		Mandatory	IT CA Rules SCHEDULE III 9.1	
3.1.8.10	A Certifying Authority should also collect and consolidate, either electronically or manually, security information which may not be generated by his system, such as: • Physical access logs; • System configuration changes and maintenance; • Personnel changes; • Discrepancy and compromise reports; • Records of the destruction of media containing key material, activation data, or personal subscriber information	1. Verify the CA collects and consolidates electronically or manually, security information which may not be generated by his system such as covered in control 3.1.8.10 2. Verify all agreements and correspondence relating to services provided by CA are collected and consolidated, either electronically or manually, at a single location.	Mandatory	IT CA Rules SCHEDULE III 9.1	
3.1.8.11	To facilitate decision-making, all agreements and correspondence relating to services provided by Certifying Authority should be collected and consolidated, either electronically or manually, at a single location.		Mandatory	IT CA Rules SCHEDULE III 9.1	
3.1.8.12	Log entries shall include the following elements: • Date and time of entry; • Identity of the person making the journal entry; and • Description of the entry.	1. For sample log entries, check the following are recorded: a. Date and time of entry; b. Identity of the person making the journal entry; and c. Description of the entry.	Mandatory	CA Browser Forum 5.4.1	
3.1.8.13	The audit record shall include the following (either recorded automatically or manually for each auditable event): • The type of event, • The date and time the event occurred,	1. For sample audit records, check the following are included: a. The type of event, b. The date and time the event occurred, c. Success or failure where	Mandatory	X.509 Policy 5.4.1	

	• Success or failure where appropriate, and • The identity of the entity and/or operator that caused the even	appropriate, and d. The identity of the entity and/or operator that caused the even			
Frequency of Processing Audit Logs					
3.1.8.14	The Certifying Authority must ensure that its audit logs are reviewed by its personnel at least once every two weeks and all significant events are detailed in an audit log summary. Such reviews should involve verifying that the log has not been tampered with, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Action taken following these reviews must be documented	1. Verify the CA audit logs are reviewed by its personnel at least once every two weeks and all significant events are detailed in an audit log summary 2. Verify audit logs are reviewed at least every 30 days to examine significant sample of security audit data generated by the CA, CSP since the last review 3. Verify the Audit Administrator explains all significant events in an audit log summary	Mandatory	IT CA Rules SCHEDULE III 9.2	
3.1.8.15	Audit logs shall be reviewed at least once every 30 days. Statistically Significant sample of security audit data generated by the CA, CSP, or RA since the last review shall be examined (where the confidence intervals for each category of security audit data are determined by the security ramifications of the category and the availability of tools to perform such a review), as well as a reasonable search for any evidence of malicious activity.		Mandatory	X.509 Policy 5.4.2	
3.1.8.16	The Audit Administrator shall explain all significant events in an audit log summary. Actions taken as a result of reviews involving verifying that the log has not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries shall be documented.		Mandatory	X.509 Policy 5.4.2	

Retention Period for Audit Logs and Archive					
3.1.8.17	The Certifying Authority must retain its audit logs onsite for at least twelve months	1. Verify on sample basis CA retains audit logs onsite for at least twelve months 2. Validate process has been established original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media is defined by the archive site.	Mandatory	IT CA Rules SCHEDULE III 9.3	
3.1.8.18	If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site.		Mandatory	X.509 Policy 5.5.2	
Protection of Audit Logs					
3.1.8.19	The electronic audit log system must include mechanisms to protect the log files from unauthorized viewing, modification, and deletion. Manual audit information must be protected from unauthorised viewing, modification and destruction	1. Verify the electronic audit log system include mechanisms to protect the log files from unauthorized viewing, modification, and deletion 2. Check the system has been configured to ensure only authorized people read and archive audit logs 3. Validate if it is acceptable for the system to over-write audit logs after they have been backed up and archived by asking the CA for practical demonstration	Mandatory	IT CA Rules SCHEDULE III 9.4	
3.1.8.20	System configuration and procedures shall be implemented together to ensure that: • Only authorized people have read access to the logs; • Only authorized people may archive audit logs; and, • Audit logs are not modified.		Mandatory	X.509 Policy 5.4.4	
3.1.8.21	It shall be acceptable for the system to over-write audit logs after they have been backed up and archived		Mandatory	X.509 Policy 5.4.4	
Records Archival					
3.1.8.22	Digital Signature Certificates stored and generated by the Certifying Authority must be retained for at least seven years after the date of its expiration. This requirement does not	1. Verify the following are stored for at least seven years a. DSC stored and generated by CA	Mandatory	IT CA Rules SCHEDULE III 10, IT	

	include the backup of private signature keys. Public Key Certificates and Certificate Revocation Lists must be archived for a minimum period of seven years to enable verification of past transactions	after the date of expiration b. Public Key certificates c. Certificate Revocation List d. Audit information e. subscriber agreements f. verification, identification and authentication information in respect of subscriber 2. Validate a second copy of all information retained or backed up is stored at three locations within the country including the CA site 3. Check the primary and secondary sites have security controls in place 4. Verify all information pertaining to CA's operation, Subscriber's application, verification, identification, authentication and Subscriber agreement is stored within the country and taken out of country only with CCA's permission 5. Verify information stored off-site is periodically verified for data integrity 6. On a sample basis verify archived records are sufficiently detailed to establish the proper operation of the component or the validity of any certificate (including those revoked or expired) issued by the CA		Regulations 3	
3.1.8.23	Audit information, subscriber agreements, verification, identification and authentication information in respect of subscriber shall be retained for at least seven years		Mandatory	IT CA Rules SCHEDULE III 10	
3.1.8.24	A second copy of all information retained or backed up must be stored at three locations within the country including the Certifying Authority site and must be protected either by physical security alone, or a combination of physical and cryptographic protection. These secondary sites must provide adequate protection from environmental threats such as temperature, humidity and magnetism. The secondary site should be reachable in few hours		Mandatory	IT CA Rules SCHEDULE III 10	
3.1.8.25	All information pertaining to Certifying Authority's operation, Subscriber's application, verification, identification, authentication and Subscriber agreement shall be stored within the country. This information shall be taken out of the country only with the permission of Controller and where a properlyconstitutional warrant or such other legally enforceable document is produced		Mandatory	IT CA Rules SCHEDULE III 10	
3.1.8.26	Information stored off-site must be periodically verified for data integrity		Mandatory	IT CA Rules SCHEDULE III 10	
3.1.8.27	CA, CSP, and RA archive records shall be sufficiently detailed to establish the proper operation of the component or the validity of any certificate (including those revoked or expired) issued by the CA		Mandatory	X.509 Policy 5.5.1	

Protection of Archive					
3.1.8.28	No unauthorized user shall be permitted to write to, modify, or delete the archive. For the CA and CSP, the authorized individuals are Audit Administrators. For the RA, authorized individuals are someone other than the RA (e.g., Information Assurance Officer or IAO).	1. Verify only authorized users are permitted to write to, modify, or delete the archive 2. Validate the contents of archives are not released 3. Check the archive media are stored in a safe, secure storage facility separate from the component (CA, CSP) with physical and procedural security controls equivalent or better than those for component. Verify the number of times such request to share individual record was made and the record of subscriber was released to his/ her satisfaction	Mandatory	X.509 Policy 5.5.3	
3.1.8.29	The contents of the archive shall not be released except as determined by the CCA, the Licensed CA, or as required by law. Records of individual may be released upon request of any subscribers involved in the transaction or their legally recognized agents.		Mandatory	X.509 Policy 5.5.3	
3.1.8.30	Archive media shall be stored in a safe, secure storage facility separate from the component (CA, CSP, or RA) with physical and procedural security controls equivalent or better than those for component		Mandatory	X.509 Policy 5.5.3	
Requirements for Time-Stamping of Records					
3.1.8.31	The Certifying Authority shall provide Time Stamping Service for its subscribers. Error of the Time Stamping clock shall not be more than 1 in 10^9. Archived records shall be time stamped such that order of events can be determined	1. Verify the VA provides time stamping service for its subscribers with error of the Time Stamping clock less than 1 in 10^9 . 2. Validate on a sample basis that logs in the archive are time stamped	Mandatory	X.509 Policy 5.5.5, IT Regulations 3	
Procedures to Obtain & Verify Archive Information					
3.1.8.32	Procedures detailing how to create, verify, package, and transmit archive information shall be published in the applicable CPS.	1. Verify for archived information, procedures have been established to perform following activities: a. Creation b. Verification c. Packaging d. Transmission	Mandatory	X.509 Policy 5.5.7	

Audit Trails and Verification					
3.1.8.33	Transactions that meet exception criteria shall be completely and accurately highlighted and reviewed by personnel independent of those that initiate the transaction.	1. Verify on sample basis the transactions that meet exception criteria are completely and accurately highlighted and reviewed by personnel independent of those that initiate the transaction 2. Check audit trails are captured and sensitive information is analyzed to check for indicate possible fraudulent use of the system 3. Verify automated or manual procedures are used to monitor and promptly report all significant security events 4. Validate real time clock of the computer system is set accurately to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases. 5. Check computer system access records are kept for a minimum of two years 6. Verify computer records of applications transactions and significant events are retained for a minimum period of two years or longer depending on specific record retention requirements.	Mandatory	IT CA Rules SCHEDULE II 10	
3.1.8.34	Adequate audit trails shall be captured and certain information needed to determine sensitive events and pattern analysis that would indicate possible fraudulent use of the system (e.g. repeated unsuccessful logons, access attempts over a series of days) shall be analyzed. This information includes such information as who, what, when, where, and any special information such as: • Success or failure of the event • Use of authentication keys, where applicable		Mandatory	IT CA Rules SCHEDULE II 10	
3.1.8.35	Automated or manual procedures shall be used to monitor and promptly report all significant security events, such as accesses, which are out-of pattern relative to time, volume, frequency, type of information asset, and redundancy. Other areas of analysis include: • Significant computer system events (e.g. configuration updates, system crashes) • Security profile changes • Actions taken by computer operations, system administrators, system programmers, and/or security administrators		Mandatory	IT CA Rules SCHEDULE II 10	
3.1.8.36	The real time clock of the computer system shall be set accurately to ensure the accuracy of audit logs, which may be required for investigations or as evidence in legal or disciplinary cases.		Mandatory	IT CA Rules SCHEDULE II 10	

3.1.8.37	The real time clock of the computer or communications device shall be set to Indian Standard Time (IST). Further there shall be a procedure that checks and corrects drift in the real time clock.		Mandatory	IT CA Rules SCHEDULE II 10	
3.1.8.38	Computer system access records shall be kept for a minimum of two years, in either hard copy or electronic form. Records, which are of legal nature and necessary for any legal or regulation requirement or investigation of criminal behavior, shall be retained as per laws of the land		Mandatory	IT CA Rules SCHEDULE II 10	
3.1.8.39	Computer records of applications transactions and significant events must be retained for a minimum period of two years or longer depending on specific record retention requirements.		Mandatory	IT CA Rules SCHEDULE II 10	
Audit Log Backup Procedures					
3.1.8.40	Audit logs and audit summaries must be backed up or copied if in manual form.	1. Validate audit logs and summaries are backed up and copied if in manual form	Mandatory	IT CA Rules SCHEDULE III 9.5	
Vulnerability Assessments					
3.1.8.41	Events in the audit process are logged, in part, to monitor system vulnerabilities. The Certifying Authority must ensure that a vulnerability assessment is performed, reviewed and revised, if necessary, following an examination of these monitored events.	1. Verify the events in the audit process are logged, in part, to monitor system vulnerabilities	Mandatory	IT CA Rules SCHEDULE III 9.6	

3.1.9. Compliance Audit and Other Assessments

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Frequency or circumstances of assessment					
3.1.9.1	The period during which the CA issues Certificates shall be divided into an unbroken sequence of audit periods. An audit period must NOT exceed one year in duration.	1. Verify the annual audits are conducted by the CA 2. Validate CA conducted a point-in-time readiness assessment before issuing Publicly-Trusted Certificates in case a valid audit report did not exist 3. Check the following: a. Point-in-time readiness assessment was completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates b. It was followed by a complete audit within ninety (90) days of issuing the first Publicly-Trusted Certificate.	Mandatory	CA Browser Forum 8.1	
3.1.9.2	If the CA does not have a currently valid Audit Report indicating compliance with the applicable audit schemes, then, before issuing Publicly-Trusted Certificates, the CA shall successfully complete a point-in-time readiness assessment performed in accordance with applicable standards.		Mandatory	CA Browser Forum 8.1	
3.1.9.3	The point-in-time readiness assessment shall be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and shall be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.		Mandatory	CA Browser Forum 8.1	
Identity/qualifications of assessor					
3.1.9.4	The CA's audit shall be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills: • Independence from the subject of the audit;	1. Validate that the audit was performed by only by the CCA empaneled agency and auditors. 2. Check the auditor is be independent of the CA being audited	Mandatory	CA Browser Forum 8.2	

	• The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme • Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function; • For audits conducted in accordance with any one of the ETSI standard, accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403; • For audits conducted in accordance with the WebTrust standard, licensed by WebTrust • Bound by law, government regulation, or professional code of ethics; and • Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors				
Assessor's relationship to assessed entity					
3.1.9.5	The auditor shall be a firm, which is independent from the entity being audited. The Controller shall determine whether an auditor meets this requirement	1. Verify the auditor is a firm, independent from CA 2. Validate the CCA verifies auditor meets above requirement	Mandatory	CA Browser Forum 8.3, X.509 Policy 8.3	
Topics covered by assessment					
3.1.9.6	CAs shall have a compliance audit mechanism in place to ensure that the requirements of this CP and applicable CPS are being implemented and enforced.	1. Obtain details of the compliance audit mechanism to verify requirements of this CP and applicable CPS are being implemented and enforced.	Mandatory	CA Browser Forum 8.4, X.509 Policy 8.4	

Actions taken as a result of deficiency					
3.1.9.7	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 shall take the following actions: • The auditor shall note the discrepancy; • The auditor shall notify the audited CA; and • The auditor shall notify the office of CCA.	1. For sample discrepancies raised by the auditor, verify the following actions were taken by the auditor: a. auditor noted discrepancy; b. The auditor notified the audited CA; and c. The auditor notified the office of CCA.	Mandatory	CA Browser Forum 8.5, X.509 Policy 8.5	
Communication of results					
3.1.9.8	An Audit Report, including identification of corrective measures taken or being taken by the CA, shall be provided to the Controller (in case of grant of license and its renewal) and the audited CA (in case of annual audit). The report shall identify the versions of the CP and CPS used in the assessment	1. Verify the audit reports are submitted to CCA and the audited CA 2. Validate the report identifies the versions of the CP and CPS used in the assessment	Mandatory	CA Browser Forum 8.6, X.509 Policy 8.6	

3.1.10. Licensing of Certifying Authorities

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Licensing of CA Authorities					
3.1.10.1	The following persons may apply for grant of a license to issue Digital Signature Certificates, namely:- • an individual, being a citizen of India and having a capital of five crores of rupees or more in his	1. Verify the following: a. applicant requirements or grant of license mentioned in description of control 3.1.10.1	Mandatory	IT CA Rules 8, IT Regulations 3	

	business or profession;
	• a company having–
	  ○ paid up capital of not less than five crores of rupees; and
	  ○ net worth of not less than fifty crores of rupees
	• a firm having –
	  ○ capital subscribed by all partners of not less than five crores of rupees; and
	  ○ net worth of not less than fifty crores of rupees
	• Central Government or a State Government or any of the Ministries or Departments, Agencies or Authorities of such Governments.
		are met
		b. For licence renewal audit and annual audit, verify the continued maintenance of net worth by CA in the last 5 years(if applicable).
		c. applicant submitted a performance bond or furnished a banker's guarantee from a scheduled bank in favour of the Controller in such form and in such manner as approved by the Controller for an amount of 50 lakhs/ 01crore rupees and the performance bond or banker's guarantee remains valid for a period of six years from the date of its submission
		d. validity of license is defined for five years from date of issue
		e. license is not transferable or heritable
		f. Controller has the authority to revoke or suspend the license in accordance with the provisions of the Act
		g. CA is bound to comply with all the parameters against which it was audited prior to issue of license and consistently and continuously complies with those parameters during the period for which the license remains valid.
		h. CA subjects itself to periodic audits			

3.1.10.2	The applicant being an individual, or a company, or a firm under sub-rule shall submit a performance bond or furnish a banker's guarantee from a scheduled bank in favour of the Controller in such form and in such manner as may be approved by the Controller for an amount of 50 lakhs/ 01 croreof rupees and the performance bond or banker's guarantee shall remain valid for a period of six years from the date of its submission		Mandatory	IT CA Rules 8	
3.1.10.3	The license shall be valid for a period of five years from the date of issue. The license shall not be transferable or heritable		Mandatory	IT Regulations 3	
3.1.10.4	The Controller can revoke or suspend the licence in accordance with the provisions of the Act		Mandatory	IT Regulations 3	
3.1.10.5	The Certifying Authority shall be bound to comply with all the parameters against which it was audited prior to issue of licence and shall consistently and continuously comply with		Mandatory	IT Regulations 3	

	those parameters during the period for which the licence shall remain valid.	i. CA ensures confidentiality of subscriber information j. CA complies with every order or direction issued by the Controller within the stipulated period.			
3.1.10.6	The Certifying Authority shall subject itself to periodic audits to ensure that all conditions of the licence are consistently complied with by it. As the cryptographic components of the Certifying Authority systems are highly sensitive and critical, the components must be subjected to periodic expert review to ensure their integrity and assurance.		Mandatory	IT Regulations 3	
3.1.10.7	The Certifying Authority shall always assure the confidentiality of subscriber information		Mandatory	IT Regulations 3	
3.1.10.8	The Certifying Authority shall comply with every order or direction issued by the Controller within the stipulated period.		Mandatory	IT Regulations 3	
3.1.10.9	To ensure the integrity of its digital certificates, the Certifying Authority shall ensure the use of approved security controls in the certificate management processes, i.e. certificate registration, generation, issuance, publication, renewal, suspension, revocation and archival	1. Verify the CA uses approved security controls in the certificate management processes, i.e. certificate registration, generation, issuance, publication, renewal, suspension, revocation and archival	Mandatory	IT Regulations 3	
3.1.10.10	The method of verification of the identity of the applicant of a Public Key Certificates shall be commensurate with the level of assurance accorded to the certificate.	2. Check the method of verification of the identity of the applicant of a Public Key Certificates commensurate with the level of assurance accorded to the certificate	Mandatory	IT Regulations 3	

3.2. Security Guidelines for Certifying Authorities

3.2.1. CA Business Practices Disclosure

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
CA Business Practices Disclosure					
3.2.1.1	The CA discloses its business practices including but not limited to the topics listed in RFC 3647 in its Certification Practice Statement (CPS)	1. Verify the CA has disclosed its business practices including but not limited to the topics listed in RFC 3647 7 in its CPS and CP	Mandatory	WebTrust 1.1	
3.2.1.2	The CA discloses its business practices including but not limited to the topics listed in RFC 3647 or RFC 2527 in its Certificate Policy (CP)		Mandatory	WebTrust 1.2	

3.2.2. Business Practices Management

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Certification Practice Statement (CPS) Management					
3.2.2.1	The Certification Practice Statement of the Certifying Authority shall comply with, and be governed by, the laws of the country	1. For the CA's CPS check the following: a. CPS complies with and is governed by laws of the country	Mandatory	IT CA Rules 18	

		b. PA has approved the CPS c. Responsibilities for maintaining the CPS have been formally assigned to individuals. d. CPS is modified and approved in as per the defined process e. CPS is available to appropriate parties f. Revisions to the CPS are made available to appropriate parties. g. CA updates CPS as and when required			
3.2.2.2	The Policy Authority (PA) has final authority and responsibility for approving the CA's Certification Practice Statement (CPS).		Mandatory	WebTrust 2.1.1	
3.2.2.3	Responsibilities for maintaining the CPS have been formally assigned.		Mandatory	WebTrust 2.1.2	
3.2.2.4	The CA's CPS is modified and approved in accordance with a defined review process.		Mandatory	WebTrust 2.1.3	
3.2.2.5	The CA makes available its Certification Practice Statement (CPS) to all appropriate parties		Mandatory	WebTrust 2.1.4	
3.2.2.6	Revisions to the CA's CPS are made available to appropriate parties.		Mandatory	WebTrust 2.1.5	
3.2.2.7	The CA updates its CPS to reflect changes in the environment as they occur		Mandatory	WebTrust 2.1.6	
Certificate Policy (CP) Management					
3.2.2.8	The Policy Authority (PA) has the responsibility of defining the business requirements and policies for using digital certificates and specifying them in a Certificate Policy (CP) and supporting agreements	1. No action required by the auditor for checking the controls as CP template is shared by CCA	Mandatory	WebTrust 2.2.1	
3.2.2.9	The PA has final authority and responsibility for specifying and approving Certificate Policy(s).		Mandatory	WebTrust 2.2.2	
3.2.2.10	Certificate Policy(s) are approved by the Policy Authority in accordance with a defined annual review process, including responsibilities for maintaining and tracking changes to the		Mandatory	WebTrust 2.2.3	

	Certificate Policy(s).				
3.2.2.11	A defined review process exists to assess that the Certificate Policy(s) are capable of support by the controls specified in the CPS.		Mandatory	WebTrust 2.2.4	
3.2.2.12	The PA makes available the Certificate Policies supported by the CA to Subscribers and Relying Parties		Mandatory	WebTrust 2.2.5	
CP and CPS Consistency					
3.2.2.13	The PA is responsible for ensuring that the CA's control processes, as stated in a Certification Practice Statement (CPS) or equivalent, fully comply with the requirements of the CP.	1. No action required by the auditor for checking the controls as CP template is shared by CCA	Mandatory	WebTrust 2.3.1	
3.2.2.14	The CA addresses the requirements of the CP when developing its CPS		Mandatory	WebTrust 2.3.2	
3.2.2.15	The CA assesses the impact of proposed CPS changes to ensure that they are consistent with the CP.		Mandatory	WebTrust 2.3.3	
3.2.2.16	A defined review process exists to ensure that Certificate Policy(s) are supported by the CA's CPS.		Mandatory	WebTrust 2.3.4	
3.2.2.17	All changes in Certificate Policy and certification practice statement shall be published on the web site of the Certifying Authority and brought to the notice of the Controller well in advance of such publication. However any change shall not contravene any provision of the Act, rule or regulation or made there under.		Mandatory	IT Regulations 3	

3.2.3. Change Management

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Change Management					
3.2.3.1	Software testing and change control procedures exist and are followed for the implementation of software on operational systems including scheduled software releases, modifications, patches, and emergency software fixes.	1. Obtain copy of CAs Change control procedures and check the following: a. Software testing and change control procedures are followed for the implementation of software on operational systems including scheduled software releases, modifications, patches, and emergency software fixes b. Change control procedures are followed for the hardware, network component, and system configuration changes c. Application systems are reviewed and tested when operating system changes occur d. On a sample basis check that the implementation of changes are strictly controlled by the use of formal change control procedures e. responsibilities for the change management process are defined and assigned f. risk and impact analysis, classification and prioritisation process are established as part of the procedure , check on sample basis g. only formally authorized changes are implemented in the production h. Authorisation procedures for change control is defined and documented	Mandatory	WebTrust 3.7.2	
3.2.3.2	Change control procedures exist and are followed for the hardware, network component, and system configuration changes.		Mandatory	WebTrust 3.7.3	
3.2.3.3	Application systems are reviewed and tested when operating system changes occur		Mandatory	WebTrust 3.7.6	
3.2.3.4	The implementation of changes is strictly controlled by the use of formal change control procedures to minimize the risk of corruption of information systems.		Mandatory	WebTrust 3.7.7	
3.2.3.5	Organizational responsibilities for the change management process shall be defined and assigned		Mandatory	IT CA Rules SCHEDULE II 21.1	
3.2.3.6	A risk and impact analysis, classification and prioritisation process shall be established		Mandatory	IT CA Rules SCHEDULE II 21.1	
3.2.3.7	No changes to a production system shall be implemented until such changes have been formally authorised. Authorisation procedures for change control shall be defined and documented.		Mandatory	IT CA Rules SCHEDULE II 21.1	

		i. Owners/Users are notified of all changes made to production system j. Fall-back procedures in the event of a failure in the implementation of the change process are established and documented k. Procedures to protect, control access and changes to production source code, data, execution statements and relevant system documentation are documented and implemented l. Version changes of all application software, system software and communication devices is documented			
3.2.3.8	Owners/Users shall be notified of all changes made to production system which may affect the processing of information on the said production system		Mandatory	IT CA Rules SCHEDULE II 21.1	
3.2.3.9	Fall-back procedures in the event of a failure in the implementation of the change process shall be established and documented.		Mandatory	IT CA Rules SCHEDULE II 21.1	
3.2.3.10	Procedures to protect, control access and changes to production source code, data, execution statements and relevant system documentation shall be documented and implemented		Mandatory	IT CA Rules SCHEDULE II 21.1	
3.2.3.11	Version changes of application software and all system software installed on the computer systems and all communication devices shall be documented. Different versions of application software and system software must be kept in safe custody		Mandatory	IT CA Rules SCHEDULE II 21.1	
Testing Of Changes To Production System					
3.2.3.12	All changes in computer resource proposed in the production system shall be tested and the test results shall be reviewed and accepted by all concerned parties prior to implementation.	1. On a sample basis verify all changes in computer resource proposed in the production system are tested and the test results are reviewed and accepted by all concerned parties prior to implementation. 2. Validate user acceptance tests are performed in a controlled environment which includes requirements mentioned in control 3.2.2.13	Mandatory	IT CA Rules SCHEDULE II 21.2	
3.2.3.13	All user acceptance tests in respect of changes in computer resource in production system shall be performed in a controlled environment which includes: (i) Test objectives, (ii) A documented test plan, and (iii) acceptance criteria.		Mandatory	IT CA Rules SCHEDULE II 21.2	

Review Of Changes					
3.2.3.14	Procedures shall be established for an independent review of programme changes before they are moved into a production environment to detect unauthorized or malicious codes	1. Verify the change management procedure mentions the following: a. an independent review of programme b. changes before they are moved into a production environment c. schedule and review the implementation of the changes in computer resource in the production system so as to ensure proper functioning 2. Validate on sample basis for latest changes/ fixes in computer resource in the production system are reviewed and approved 3. Verify periodic management reports on the status of the changes implemented in the computer resourced in the production system are submitted for management review 4. Check the software updates and patches are reviewed for security implications before being implemented 5. Verify the software updates and patches to rectify security vulnerability in critical systems used are promptly reviewed and implemented 6. Validate the information on the software updates and patches and their implementation on CA's system shall are clearly and properly documented	Mandatory	IT CA Rules SCHEDULE II 21.3	
3.2.3.15	Procedures shall be established to schedule and review the implementation of the changes in computer resource in the production system so as to ensure proper functioning		Mandatory	IT CA Rules SCHEDULE II 21.3	
3.2.3.16	All emergency changes/fixes in computer resource in the production system shall be reviewed and approved		Mandatory	IT CA Rules SCHEDULE II 21.3	
3.2.3.17	Periodic management reports on the status of the changes implemented in the computer resourced in the production system shall be submitted for management review		Mandatory	IT CA Rules SCHEDULE II 21.3	
3.2.3.18	Software updates and patches shall be reviewed for security implications before being implemented on Certifying Authority's system		Mandatory	IT CA Rules SCHEDULE III 7	
3.2.3.19	Software updates and patches to rectify security vulnerability in critical systems used for Certifying Authority's operation shall be promptly reviewed and implemented		Mandatory	IT CA Rules SCHEDULE III 7	
3.2.3.20	Information on the software updates and patches and their implementation on Certifying Authority's system shall be clearly and properly documented		Mandatory	IT CA Rules SCHEDULE III 7	

3.2.4. Operations Management

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Operations Management					
3.2.4.1	CA operating procedures are documented and maintained for each functional area.	1. Verify CA has documented operating procedures for functional areas and check the following: a. Formal management responsibilities and procedures exist to control all changes to CA equipment, software and operating procedures b. Duties and areas of responsibility are segregated c. Development and testing facilities are separated from operational facilities d. Prior to using external facilities management services, risks and related controls are identified, agreed upon with the contractor, and incorporated into the contract. e. Capacity demands are monitored and projections of future capacity requirements made f. On a sample basis check that the acceptance criteria for new information systems, upgrades and new versions are established and suitable tests of the system carried out prior to acceptance	Mandatory	WebTrust 3.5.1	
3.2.4.2	Formal management responsibilities and procedures exist to control all changes to CA equipment, software and operating procedures.		Mandatory	WebTrust 3.5.2	
3.2.4.3	Duties and areas of responsibility are segregated in order to reduce opportunities for unauthorized modification or misuse of information or services		Mandatory	WebTrust 3.5.3	
3.2.4.4	Development and testing facilities are separated from operational facilities		Mandatory	WebTrust 3.5.4	
3.2.4.5	Prior to using external facilities management services, risks and related controls are identified, agreed upon with the contractor, and incorporated into the contract.		Mandatory	WebTrust 3.5.5	
3.2.4.6	Capacity demands are monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.		Mandatory	WebTrust 3.5.6	
3.2.4.7	Acceptance criteria for new information systems, upgrades and new versions are established and suitable tests of the system carried out prior to acceptance		Mandatory	WebTrust 3.5.7	

3.2.5. Measures to handle computer virus

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Measure to handle computer virus					
3.2.5.1	Detection and prevention controls to protect against viruses and malicious software, including on offline or air gapped systems are implemented. Employee awareness programs are in place.	1. Verify detection and prevention controls to protect against viruses and malicious software, including on offline or air gapped systems are implemented 2. Check an employee awareness program is implemented 3. Validate names of personal responsible for ensuring all file servers and personal computers are equipped with up-to-date virus protection and detection software. 4. Check if virus detection software is being used to check storage drives internal and external to the system on a periodic basis 5. Verify all diskettes and software are screened and verified by virus detection software before being loaded onto the computer system 6. Check magnetic media like tape cartridge, floppies etc. brought from outside are used on thedata, file, PKI or computer server or personal computer on Intranet and Internet only after proper screening and verification by	Mandatory	WebTrust 3.5.8	
3.2.5.2	Responsibilities and duties shall be assigned to ensure that all file servers and personal computers are equipped with up-to-date virus protection and detection software.		Mandatory	IT CA Rules SCHEDULE II 11	
3.2.5.3	Virus detection software must be used to check storage drives both internal and external to the system on a periodic basis		Mandatory	IT CA Rules SCHEDULE II 11	
3.2.5.4	All diskettes and software shall be screened and verified by virus detection software before being loaded onto the computer system. No magnetic media like tape cartridge, floppies etc. brought from outside shall be used on the data, file, PKI or computer server or personal computer on Intranet and Internet without proper screening and verification by virus detection software		Mandatory	IT CA Rules SCHEDULE II 11	

		virus detection software			
3.2.5.5	A team shall be designated to deal with reported or suspected incidents of computer virus. The designated team shall ensure that latest version of antivirus software is loaded on all data, file, PKI servers and personal computers.	1. Verify a team is established for incidents management of computer virus 2. Validate the team ensures latest version of antivirus software is loaded on all data, file, PKI servers and personal computers.	Mandatory	IT CA Rules SCHEDULE II 11	
3.2.5.6	Procedures shall be established to limit the spread of viruses to other organization information assets. Such procedures inter alia shall include: • Communication to other business partners and users who may be at risk from an infected resource • Eradication and recovery procedures • Incident report must be documented and communicated per established procedures.	1. Verify by checking procedures are established to limit the spread of viruses to other organization information assets 2. Check awareness and training programs are in place to communicate virus protection practices, available controls, areas of high risk to virus infection and responsibilities	Mandatory	IT CA Rules SCHEDULE II 11	
3.2.5.7	An awareness and training programme shall be established to communicate virus protection practices, available controls, areas of high risk to virus infection and responsibilities		Mandatory	IT CA Rules SCHEDULE II 11	

3.2.6. Relocation of hardware and software

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Relocation of hardware and software					
3.2.6.1	Whenever computers or computer peripherals are relocated (e.g. for maintenance, installation at different sites or storage), the following guidelines shall apply: • All removable media will be removed from the computer system and kept at secure location. • Internal drives will be overwritten, reformatted or removed as the situation may be. • If applicable, ribbons will be removed from printers. • All paper will be removed from printers.	1. Perform walkthrough and verify Relocation of hardware and software is performed as per requirements mentioned in the control description	Mandatory	IT CA Rules SCHEDULE II 12	

3.2.7. Hardware and software maintenance

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Hardware and software maintenance					
3.2.7.1	Proper placement and installation of Information Technology equipment to reduce the effects of interference due to electromagnetic emanations.	1. For the hardware and software maintenance performed in the CA system check the following: a. secure placement and	Mandatory	IT CA Rules SCHEDULE II 13	

3.2.7.2	Maintenance of an inventory and configuration chart of hardware	installation of IT equipment has been done to prevent electromagnetic interference b. inventory and configuration chart of hardware are maintained c. security features within hardware are identified and implemented d. Authorization, documentation, and control of change made to the hardware is defined e. Provision of an uninterruptible power supply is present f. support facilities including power and air conditioning have been installed g. annual maintenance of hardware is in place h. maintenance agreements have been signed with the supplier of computer and communication hardware, software (both system and application) and firmware i. On a sample basis that maintenance personnel have signed non-disclosure agreements	Mandatory	IT CA Rules SCHEDULE II 13	
3.2.7.3	Identification and use of security features implemented within hardware.		Mandatory	IT CA Rules SCHEDULE II 13	
3.2.7.4	Authorization, documentation, and control of change made to the hardware		Mandatory	IT CA Rules SCHEDULE II 13	
3.2.7.5	Identification of support facilities including power and air conditioning		Mandatory	IT CA Rules SCHEDULE II 13	
3.2.7.6	Provision of an uninterruptible power supply.		Mandatory	IT CA Rules SCHEDULE II 13	
3.2.7.7	Organization must make proper arrangements for maintenance of computer hardware, software (both system and application) and firmware installed and used by them		Mandatory	IT CA Rules SCHEDULE II 13	
3.2.7.8	It shall be the responsibility of the officer in charge of the operational site to ensure that contract for annual maintenance of hardware is always in place.		Mandatory	IT CA Rules SCHEDULE II 13	
3.2.7.9	Organization must enter into maintenance agreements, if necessary, with the supplier of computer and communication hardware, software (both system and application) and firmware.		Mandatory	IT CA Rules SCHEDULE II 13	
3.2.7.10	Maintenance personnel will sign non-disclosure agreements		Mandatory	IT CA Rules SCHEDULE II 13	

3.2.8. Purchase and Licensing of Hardware and Software

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Purchase and Licensing of Hardware and Software					
3.2.8.1	Hardware and software products that contain or are to be used to enforce security, and intended for use or interface into any organization system or network, must be verified to comply with these Information Technology Security Guidelines prior to the signing of any contract, purchase or lease.	1. Validate the hardware and software products comply with the Information Technology Security Guidelines	Mandatory	IT CA Rules SCHEDULE II 14	
3.2.8.2	Software, which is capable of bypassing or modifying the security system or operating system, integrity features, must be verified to determine that they conform to these Information Technology Security Guidelines. Where such compliance is not possible, then procedures shall be in place to ensure that the implementation and operation of that software does not compromise the security of the system.	1. Verify procedures have been implemented to ensure that the implementation and operation of that software does not compromise the security of the system.	Mandatory	IT CA Rules SCHEDULE II 14	
3.2.8.3	There shall be procedures to identify, select, implement and control software (system and application software) acquisition and installation to ensure compliance with the Indian Copyright Act and Information Technology Security Guidelines.	1. Validate procedures have been implemented to identify, select, implement and control software (system and application software) acquisition and installation 2. Check that it is in compliance with the Indian Copyright Act and Information Technology Security Guidelines	Mandatory	IT CA Rules SCHEDULE II 14	
3.2.8.4	It is prohibited to knowingly install on any system whether test or production, any software which is not licensed for use on the specific systems or networks.	1. For software installed on the CA systems verify the following: a. only licensed software are	Mandatory	IT CA Rules SCHEDULE II 14	

		installed on systems used for CA operations b. licensing agreements exists for software installed and used on CA systems c. Illegally acquired or unauthorized software are not used on any computer, computer network or data communication equipment d. System Administrator or Network Administrator are responsible for removing any illegal software if detected			
3.2.8.5	No software will be installed and used on the system when appropriate licensing agreements do not exist, except during evaluation periods for which the user has documented permission to install and test the software under evaluation.		Mandatory	IT CA Rules SCHEDULE II 14	
3.2.8.6	Illegally acquired or unauthorized software must not be used on any computer, computer network or data communication equipment. In the event that any illegally acquired or unauthorized software is detected by the System Administrator or Network Administrator, the same must be removed		Mandatory	IT CA Rules SCHEDULE II 14	

3.2.9. System Software

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
System Software					
3.2.9.1	All system software options and parameters shall be reviewed and approved by the management.	1. For the CAs system software check the following: a. the system software operations and parameters are reviewed and approved by CA management b. System software are tested and its security functionality validated prior to implementation	Mandatory	IT CA Rules SCHEDULE II 15	
3.2.9.2	System software shall be comprehensively tested and its security functionality validated prior to implementation.		Mandatory	IT CA Rules SCHEDULE II 15	
3.2.9.3	All vendor supplied default user IDs shall be deleted or password changed before allowing users to access the computer system		Mandatory	IT CA Rules SCHEDULE II 15	

3.2.9.4	Versions of system software installed on the computer system and communication devices shall be regularly updated	c. Vendor supplied default IDs are deleted or password changes before users access the computer system d. On sample basis that the versions of system software installed on the computer system and communication devices are regularly updated e. Changes proposed in the system software are appropriately justified and approved by an authorized party (check for recent sample changes performed) f. log of all changes to system software are maintained, completely documented and tested to ensure the desired results g. no standing "Write" access is present for the system libraries h. All "Write" access are logged and reviewed by the System Administrator i. System Programmers are not allowed to have access to the application system's data and programme files in the production environment	Mandatory	IT CA Rules SCHEDULE II 15	
3.2.9.5	All changes proposed in the system software must be appropriately justified and approved by an authorized party		Mandatory	IT CA Rules SCHEDULE II 15	
3.2.9.6	A log of all changes to system software shall be maintained, completely documented and tested to ensure the desired results.		Mandatory	IT CA Rules SCHEDULE II 15	
3.2.9.7	There shall be no standing "Write" access to the system libraries. All "Write" access shall be logged and reviewed by the System Administrator for dubious activities.		Mandatory	IT CA Rules SCHEDULE II 15	
3.2.9.8	System Programmers shall not be allowed to have access to the application system's data and programme files in the production environment		Mandatory	IT CA Rules SCHEDULE II 15	
3.2.9.9	Procedures to control the use of sensitive system utilities and system programmes that could bypass intended security controls shall be in place and documented. All usage shall be logged and reviewed by the System Administrator and another	1. Verify documented procedure is present to control the use of sensitive system utilities and system programmes	Mandatory	IT CA Rules SCHEDULE II 15	

	person independent of System Administrator for dubious activities.	2. Validate all usage is logged and reviewed by the System Administrator and another person independent of System Administrator for dubious activities			

3.2.10. Documentation Security

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Documentation Security					
3.2.10.1	All documentation pertaining to application software and sensitive system software and changes made therein shall be updated to the current time, accurately and stored securely. An up-to-date inventory list of all documentation shall be maintained to ensure control and accountability.	1. Conduct a walkthrough of the documentation security process and verify the following: a. Documents pertaining to application software and sensitive system software are updated to the current time, accurately and stored securely. b. up-to-date inventory list of all documentation is maintained c. all documentation and subsequent changes are reviewed and approved by an independent authorized party prior to issue d. Access to application	Mandatory	IT CA Rules SCHEDULE II 16	
3.2.10.2	All documentation and subsequent changes shall be reviewed and approved by an independent authorized party prior to issue		Mandatory	IT CA Rules SCHEDULE II 16	
3.2.10.3	Access to application software documentation and sensitive system software documentation shall be restricted to authorized personnel on a "need-to-use" basis only		Mandatory	IT CA Rules SCHEDULE II 16	
3.2.10.4	Adequate backups of all documentation shall be maintained and a copy of all critical documentation and manuals shall be stored off-site.		Mandatory	IT CA Rules SCHEDULE II 16	

3.2.10.5	Documentation shall be classified according to the sensitivity of its contents/ implications	software documentation and sensitive system software documentation is restricted to authorized personnel on a "need-to-use" basis only e. Adequate backups of all documentation are maintained f. Copy of all critical documents and manuals is stored off site g. Documents are classified according to sensitivity h. Clear Desks policy has been implemented	Mandatory	IT CA Rules SCHEDULE II 16	
3.2.10.6	Organizations shall adopt a clean desk policy for papers, diskettes and other documentation in order to reduce the risks of unauthorized access, loss of and damage to information outside normal working hours.		Mandatory	IT CA Rules SCHEDULE II 16	

3.2.11. Firewalls

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Firewalls					
3.2.11.1	Intelligent devices generally known as "Firewalls" shall be used to isolate organization's data network with the external network. Firewall device should also be used to limit network connectivity for unauthorized use.	1. Verify firewalls have been installed to protect the data network and to prevent unauthorized use	Mandatory	IT CA Rules SCHEDULE II 18	
3.2.11.2	Networks that operate at varying security levels shall be isolated from each other by appropriate firewalls. The internal network of the organization shall be physically and logically isolated from the Internet and any other external connection by a firewall.	1. Obtain the network architecture of the CAs system and check the following: a. Networks that operate at varying security levels are isolated from each other by	Mandatory	IT CA Rules SCHEDULE II 18	

		appropriate firewalls b. internal network of the organization is physically and logically isolated from the Internet and any other external connection by a firewall c. Vulnerability assessment is performed on firewalls prior installation and half yearly thereafter d. All web servers for access by Internet users are isolated from other data and host servers.			
3.2.11.3	All firewalls shall be subjected to thorough test for vulnerability prior to being put to use and at least half-yearly thereafter.		Mandatory	IT CA Rules SCHEDULE II 18	
3.2.11.4	All web servers for access by Internet users shall be isolated from other data and host servers.		Mandatory	IT CA Rules SCHEDULE II 18	

3.2.12. Connectivity

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Connectivity					
3.2.12.1	Organization shall establish procedure for allowing connectivity of their computer network or computer system to non-organization computer system or networks. The permission to connect other networks and computer system shall be approved by the Network Administrator and documented	1. Conduct a walkthrough to check the implementation of the following: a. procedure is established for allowing connectivity of CA computer network or computer system to non-organization computer system or networks b. permission to connect other networks and computer system are approved by Network	Mandatory	IT CA Rules SCHEDULE II 19	
3.2.12.2	All unused connections and network segments should be disconnected from active networks. The computer system/personal computer or outside terminal accessing an		Mandatory	IT CA Rules SCHEDULE II 19	

	organization's host system must adhere to the general system security and access control guidelines	Administrator and documented c. All unused connections and network segments are disconnected from active networks d. suitability of new hardware/software particularly the protocol compatibility is assessed before connecting the same to the CA's network e. Internet access is not allowed to database server/ file server or server hosting sensitive data			
3.2.12.3	The suitability of new hardware/software particularly the protocol compatibility should be assessed before connecting the same to the organization's network.		Mandatory	IT CA Rules SCHEDULE II 19	
3.2.12.4	No Internet access should be allowed to database server/ file server or server hosting sensitive data.		Mandatory	IT CA Rules SCHEDULE II 19	

3.2.13. Technical Security Controls

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Activation Data					
3.2.13.1	The activation data used to unlock private keys, in conjunction with any other access control, shall have an appropriate level of strength for the keys or data to be protected and shall meet the applicable security policy requirements of the cryptographic module used to store the keys. Activation data may be user selected. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module	1. Validate the activation data used to unlock private keys have an appropriate level of strength for the keys or data to be protected and meet the applicable security policy requirements of the cryptographic module used to store the keys. 2. Verify data used to unlock private keys is protected from disclosure	Mandatory	X.509 Policy 6.4.1	

3.2.13.2	Data used to unlock private keys shall be protected from disclosure. After a predetermined number of failed login attempts, a facility to temporarily lock the account shall be provided	3. Check the data used to unlock private keys is protected from disclosure and account gets temporarily locker after a number of failed login attempts 4. Verify activation data is changed whenever the token is re-keyed or returned 5. Validate CA and CSP components are regularly synchronized with IST 6. Check the time derived is used for establishing time of components covered in control 3.2.13.4	Mandatory	X.509 Policy 6.4.2	
3.2.13.3	CAs, CSPs, shall change the activation data whenever the token is re-keyed or returned from maintenance		Mandatory	X.509 Policy 6.4.3	
3.2.13.4	All CA and CSP components shall regularly synchronize with a time service such as Indian Standard Time Service. Time derived from the time service shall be used for establishing the time of: • Initial validity time of a Subscriber's Certificate • Revocation of a Subscriber's Certificate • Posting of CRL updates • OCSP or other CSP responses.		Mandatory	X.509 Policy 6.8	

3.2.14. Network Communication Security

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Network Communication Security					
3.2.14.1	All sensitive information on the network shall be protected by using appropriate techniques. The critical network devices such as routers, switches and modems should be protected from physical damage.	1. Verify the CA network is protected by using appropriate techniques 2. Check physically critical network devices such as routers, switches and	Mandatory	IT CA Rules SCHEDULE II 17	

3.2.14.2	The network configuration and inventories shall be documented and maintained.	modems are protected from physical damage 3. Check the documented network configuration and inventories and verify these are updated regularly 4. For sample changes in the network check the following: a. Network Administrator's approval was taken b. Changes were documented c. Threats and risk assessment after changes in the network configuration is reviewed d. network operation are monitored for any security irregularity e. formal procedure is in place for identifying and resolving security problems 5. Verify the optical fibre in CAs operational sir is armored cable to ensure security against 6. electromagnetic transmission 7. Validate CA has provisions to use network diagnostic tools on need basis	Mandatory	IT CA Rules SCHEDULE II 17	
3.2.14.3	Prior authorization of the Network Administrator shall be obtained for making any changes to network configuration. The changes made in the network configuration shall be documented. The threat and risk assessment of the network after changes in the network configuration shall be reviewed. The network operation shall be monitored for any security irregularity. A formal procedure should be in place for identifying and resolving security problems.		Mandatory	IT CA Rules SCHEDULE II 17	
3.2.14.4	As far as possible, transmission medium within the Certifying Authority's operational site should be secured against electromagnetic transmission. In this regard, use of Optical Fibre Cable and armored cable may be preferred as transmission media as the case may be.		Mandatory	IT CA Rules SCHEDULE II 17	
3.2.14.5	Network diagnostic tools, e.g., spectrum analyzer, protocol analyzer should be used on a need basis		Mandatory	IT CA Rules SCHEDULE II 17	
Network Administrator					
3.2.14.6	Each organization shall designate a properly trained "Network Administrator" who will be responsible for operation, monitoring security and functioning of the network.	1. Obtain name of the Network administrator and verify the following: a. Network Administrator is properly trained b. Network Administrator regularly undertakes the	Mandatory	IT CA Rules SCHEDULE II 20	
3.2.14.7	Network Administrator shall regularly undertake the review of network and also take adequate measures to provide physical, logical and procedural safeguards for its security. Appropriate		Mandatory	IT CA Rules SCHEDULE II 20	

	follow up of any unusual activity or pattern of access on the computer network shall be investigated promptly by the Network Administrator	review of network and also takes adequate measures to provide physical, logical and procedural safeguards for its security c. Network Administrator promptly investigates unusual activity or pattern of access on the computer network d. Network Administrator is alerted in case of a possible breach			
3.2.14.8	System must include a mechanism for alerting the Network Administrator of possible breaches in security, e.g., unauthorized access, virus infection and hacking.		Mandatory	IT CA Rules SCHEDULE II 20	
3.2.14.9	Secure Network Management System should be implemented to monitor functioning of the computer network. Broadcast of network traffic should be minimized.	1. Verify secure network management system is implemented to monitor functioning of computer network 2. Validate only authorized and legal software are used on the network 3. Check the shared computer systems, network devices used for business applications comply with the requirement established in 3.1.6	Mandatory	IT CA Rules SCHEDULE II 20	
3.2.14.10	Only authorized and legal software shall be used on the network.		Mandatory	IT CA Rules SCHEDULE II 20	
3.2.14.11	Shared computer systems, network devices used for business applications shall comply with the requirement established in System Integrity and Security Measures (Section 3.1.6).		Mandatory	IT CA Rules SCHEDULE II 20	
3.2.14.12	Network connections from the Certifying Authority's system to external networks shall be restricted to only those connections which are essential to facilitate Certifying Authority's functional processes and services. Such network connections to the external network shall be properly secured and monitored regularly.	1. Understand the network connection process and check the following: a. Network connections for CA’s system to external networks are restricted to only essential connections b. Network connection are secured and monitored regularly c. Network connections are initiated by the systems	Mandatory	IT CA Rules SCHEDULE III 8	
3.2.14.13	Network connections should be initiated by the systems performing the functions of generation and management of Digital Signature Certificate to connect those systems performing the registration and repository functions but not vice versa. If this is not possible, compensating controls (e.g. use of proxy servers)		Mandatory	IT CA Rules SCHEDULE III 8	

	shall be implemented to protect the systems performing the function of generation and management of Digital Signature Certificate from potential attacks	performing the functions of generation and management of DSC to connect those systems performing the registration and repository functions but not vice versa			
3.2.14.14	Systems performing the Digital Signature Certification function should be isolated to minimise their exposure to attempts to compromise the confidentiality, integrity and availability of the certification function.	1. Verify Systems performing the DSC function are isolated to minimize their exposure to attempts to compromise the confidentiality, integrity and availability of the certification function 2. communications between the CA's systems connected on a network should be secured (encrypted and digitally signed) 3. Intrusion detection tools are deployed to monitor critical networks and perimeter networks and alert administrators of network intrusions and penetration attempts in a timely manner	Mandatory	IT CA Rules SCHEDULE III 8	
3.2.14.15	Communication between the Certifying Authority systems connected on a network shall be secure to ensure confidentiality and integrity of the information. For example, communications between the Certifying Authority's systems connected on a network should be encrypted and digitally signed		Mandatory	IT CA Rules SCHEDULE III 8	
3.2.14.16	Intrusion detection tools should be deployed to monitor critical networks and perimeter networks and alert administrators of network intrusions and penetration attempts in a timely manner		Mandatory	IT CA Rules SCHEDULE III 8	

3.3. Key Management Controls

3.3.1. Key Lifecycle Management Controls

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Key Generation					
3.3.1.1	The Certifying Authority shall use methods, which are approved by the Controller, to verify the identity of a subscriber before issuing or renewing any Public Key Certificate. The subscriber's key pair shall be generated by the subscriber or on a key generation system in the presence of the subscriber.	1. Conduct a walkthrough of the key generation process and check the following a. CA uses methods approved by Controller to verify identity of subscriber before issuing or renewing public key certificate b. Subscriber's key pair is generated by the subscriber or on a key generation system in the presence of the subscriber. c. key generation process generates statistically random key values that are resistant to known attacks d. Generation of CA keys occur within a cryptographic module meeting the applicable requirements of ISO 15782-1/FIPS 140-2 (or	Mandatory	IT CA Rules SCHEDULE III 18.1, IT Regulations 3	
3.3.1.2	The key generation process shall generate statistically random key values that are resistant to known attacks		Mandatory	IT CA Rules SCHEDULE III 18.1	
3.3.1.3	Generation of CA keys shall occur within a cryptographic module meeting the applicable requirements of ISO 15782-1/FIPS 140-2 (or equivalent)/ANSI X9.66 and the business requirements in accordance with the CPS. Such cryptographic devices perform key generation using a random number generator (RNG) or pseudo random number generator (PRNG).		Mandatory	WebTrust 4.1.1. CA Browser Forum 6.1	
3.3.1.4	The CA shall generate its own key pair in the same cryptographic device in which it will be used or the key pair shall be injected directly from the device where it was generated into the device where it will be used.		Mandatory	WebTrust 4.1.2	
3.3.1.5	CA key generation generates keys that: • use a key generation algorithm as disclosed within the		Mandatory	WebTrust 4.1.3	

	CA's CP and/or CPS; • have a key length that is appropriate for the algorithm and for the validity period of the CA certificate as disclosed in the CA's CP and/or CPS. The public key length to be certified by a CA is less than or equal to that of the CA's private signing key; and • take into account requirements on parent and subordinate CA key sizes and have a key size in accordance with the CA's CP and/or CPS.	equivalent)/ANSI X9.66 and the business requirements in accordance with the CPS e. CA generates its own key pair in the same cryptographic device in which it will be used f. CA generates keys in compliance with the requirements mentioned in 3.3.1.5 g. CA key generation ceremonies are independently witnessed by internal or external auditors. h. Private key of CA is adequately secured at each phase of its lifecycle 2. Verify the steps by referring a recent key generation activity			
3.3.1.6	CA key generation ceremonies are independently witnessed by internal or external auditors. The private key of the Certifying Authority shall be adequately secured at each phase of its life cycle, i.e. key generation, distribution, storage, usage, backup, archival and destruction.		Mandatory	WebTrust 4.1.4, IT Regulations 3	
3.3.1.7	The CA follows a CA key generation script for key generation ceremonies that includes the following: • definition and assignment of participant roles and responsibilities; • management approval for conduct of the key generation ceremony; • specific cryptographic hardware, software and other materials including identifying information, e.g., serial numbers; • specific steps performed during the key generation ceremony	1. Verify a CA key generation script exists and check the script for following requirements through a walkthrough: a. the script covers roles assigned, management approval, serial numbers, procedures for secure storage of cryptographic hardware etc **b.** steps for performing key generation are stated	Mandatory	WebTrust 4.1.5	

	• physical security requirements for the ceremony location (e.g., barriers, access controls and logging controls); • procedures for secure storage of cryptographic hardware and activation materials following the key generation ceremony (e.g., detailing the allocation of materials between storage locations); • sign-off on the script or in a log from participants and witnesses indicating whether key generation ceremony was performed in accordance with the detailed key generation ceremony script; and • notation of any deviations from the key generation ceremony script (e.g., documentation of steps taken to address any technical issues)	clearly in the script **c.** physical security requirements for the ceremony location are met d. sign-off is given for the key generation ceremony e. notation of any deviations from the key generation ceremony script are addressed			
3.3.1.8	The integrity of the hardware/software used for key generation and the interfaces to the hardware/software is tested before production usage.	1. Validate by asking CA to demonstrate the hardware/software used for key generation is tested before production usage	Mandatory	WebTrust 4.1.6	
Key Storage, Backup, and Recovery					
3.3.1.9	The CA's private (signing and confidentiality) keys are stored and used within a secure cryptographic device meeting the appropriate ISO 15408 protection profile or FIPS 140-1 level 3 recommendations for Cryptographic Modules Validation Listbased on a risk assessment and the business requirements of the CA and in accordance with the CA's CPS and applicable Certificate Policy(s).	1. For the Key Storage, Backup, and Recovery process, verify the following: a. CA's private (signing and confidentiality) keys are stored and used within a secure cryptographic device meeting the appropriate ISO 15408 protection profile or or FIPS 140-1 level 3 recommendations for	Mandatory	WebTrust 4.2.1, IT Regulations 3, CA Browser Forum 6.2.7, X.509 Policy 6.2.7	
3.3.1.10	If the CA's private keys are not exported from a secure cryptographic module, then the CA private key is generated, stored and used within the same cryptographic module.		Mandatory	WebTrust 4.2.2	

3.3.1.11	If the CA's private keys are exported from a secure cryptographic module to secure storage for purposes of offline processing or backup and recovery, then they are exported within a secure key management scheme that may include any of the following: • as cipher-text using a key which is appropriately secured; • as encrypted key fragments using multiple control and split knowledge/ownership; or • In another secure cryptographic module such as a key transportation device using multiple control.	Cryptographic Modules b. CA private key is generated, stored and used within the same cryptographic module if CA's private keys are not exported from a secure cryptographic module c. When CA's private keys are exported from a secure cryptographic module the requirements mentioned in control 3.3.1.11 d. Backup copies of the CA's private keys are maintained with the same or greater level of security controls as keys currently in use e. recovery of the CA's keys is carried out in as secure a manner as the backup process, using multi-person control.	Mandatory	WebTrust 4.2.3	
3.3.1.12	Backup copies of the CA's private keys are subject to the same or greater level of security controls as keys currently in use. The recovery of the CA's keys is carried out in as secure a manner as the backup process, using multi-person control.		Mandatory	WebTrust 4.2.4	
Key Distribution					
3.3.1.13	Keys shall be transferred from the key generation system to the storage device (if the keys are not stored on the key generation system) using a secure mechanism that ensures confidentiality and integrity	1. Verify the key is transferred from the key generation system to the storage device using a secure mechanism that ensures confidentiality and integrity	Mandatory	IT CA Rules SCHEDULE III 18.2	

3.3.1.14	The initial distribution mechanism for the CA's public key is controlled and initially distributed within a Certificate using one of the following methods: • machine readable media (e.g., smart card, flash drive, CD ROM) from an authenticated source; • embedding in an entity's cryptographic module; or • other secure means that ensure authenticity and integrity.	1. Validate the initial distribution mechanism for the CA's public key is controlled and initially distributed within a Certificate using one of the methods mentioned in control description	Mandatory	WebTrust 4.3.2	
3.3.1.15	The CA's public key is changed (rekeyed) periodically according to the requirements of the CPS with advance notice provided to avoid disruption of the CA services.	1. Verify by checking documentation of frequency of change of public key and validate CA's public key is changed (rekeyed) periodically according to the requirements	Mandatory	WebTrust 4.3.3	
3.3.1.16	The subsequent distribution mechanism for the CA's public key is controlled in accordance with the CA's disclosed business practices.	1. On a sample basis verify the distribution mechanism for the CA's public key is controlled in accordance with the CA's disclosed business practices	Mandatory	WebTrust 4.3.4	
3.3.1.17	If an entity already has an authenticated copy of the CA's public key, a new CA public key is distributed using one of the following methods: • direct electronic transmission from the CA; • placing into a remote cache or directory; • loading into a cryptographic module; or • any of the methods used for initial distribution	1. Validate on a sample basis if an entity has an authenticated copy of CAs public key, a new CA public key is distributed using one of the methods mentioned in control description	Mandatory	WebTrust 4.3.5	
3.3.1.18	The CA provides a mechanism for validating the authenticity and integrity of the CA's public keys.	1. Verify CA has a mechanism in place for validating the authenticity and integrity of the CA's public keys	Mandatory	WebTrust 4.3.6	

Key Usage					
3.3.1.19	A system and software integrity check shall be performed prior to Certifying Authority's key loading. Custody of and access to the Certifying Authority's keys shall be under split control. In particular, Certifying Authority's key loading shall be performed under split control	1. For the CAs key usage process, check the following: a. A system and software integrity check is performed prior to Certifying Authority's key loading b. Custody of and access to the CA's keys is under split control c. activation of the CA private signing key is performed using multi-party control (i.e., m of n) with a minimum value of m (e.g., m greater than 2 for Root CAs) d. activation of the CA private key is performed using multi-factor authentication e. CA signing key(s) used for generating certificates and/or issuing revocation status information, are not used for any other purpose f. CA follows established procedures in event of a compromise of private key of the CA for immediate revocation of the affected subscribers' certificates. g. CA ceases to use a key	Mandatory	IT CA Rules SCHEDULE III 18.4	
3.3.1.20	The activation of the CA private signing key shall be performed using multi-party control (i.e., m of n) with a minimum value of m (e.g., m greater than 2 for Root CAs).		Mandatory	WebTrust 4.4.1	
3.3.1.21	The activation of the CA private key shall be performed using multi-factor authentication (e.g., smart card and password, biometric and password, etc.).		Mandatory	WebTrust 4.4.2	
3.3.1.22	CA signing key(s) used for generating certificates and/or issuing revocation status information, shall not be used for any other purpose.		Mandatory	WebTrust 4.4.3	
3.3.1.23	In the event of a compromise of the private key the Certifying Authority shall follow the established procedures for immediate revocation of the affected subscribers' certificates. The CA ceases to use a key pair at the end of the key pair's defined operational lifetime or when the compromise of the private key is known or suspected		Mandatory	IT Regulations 3, WebTrust 4.4.4	
3.3.1.24	An annual review is required by the PA on key lengths to determine the appropriate key usage period with recommendations acted upon.		Mandatory	WebTrust 4.4.5	

		pair at the end of the key pair's defined operational lifetime			
3.3.1.25	Private Keys corresponding to Root Certificates MUST NOT be used to sign Certificates except in the following cases: • Self-signed Certificates to represent the Root CA itself; • Certificates for Subordinate CAs and Cross Certificates; • Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and • Certificates for OCSP Response verification	1. Verify the private keys corresponding to Root Certificate are not used to sign Certificates except in the cases mentioned in control description	Mandatory	CA Browser Forum 6.1.7, X.509 Policy 6.1.7	
Key Archival					
3.3.1.26	Archived CA keys are subject to the same or greater level of security controls as keys currently in use.	1. For the key archival process, check the following: a. Archived CA keys are subject to the same or greater level of security controls as keys currently in use b. For sample archived CA keys, verify, these were destroyed at the end of the archive period using dual control in a physically secure site. c. Subscriber private signature keys is not archived by the CA d. Archived keys are only accessed where historical	Mandatory	WebTrust 4.5.1 CA Browser Forum 6.3.1, X.509 Policy 6.3.1	
3.3.1.27	All archived CA keys are destroyed at the end of the archive period using dual control in a physically secure site. Subscriber private signature keys shall not be archived by the CA.		Mandatory	WebTrust 4.5.2, X.509 Policy 6.2.5	
3.3.1.28	Archived keys are only accessed where historical evidence requires validation. Control processes are required to ensure the integrity of the CA systems and the key sets.		Mandatory	WebTrust 4.5.3	
3.3.1.29	Archived keys are recovered for the shortest possible time period technically permissible to meet business requirements.		Mandatory	WebTrust 4.5.4	

3.3.1.30	Archived keys are periodically verified to ensure that they are properly destroyed at the end of the archive period.	evidence requires validation e. Archived keys are recovered for the shortest possible time period technically permissible to meet business requirements f. Archived keys are periodically verified to ensure that they are properly destroyed at the end of the archive period.	Mandatory	WebTrust 4.5.5	
Key Destruction					
3.3.1.31	Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space must be securely destroyed by over-writing. Private key destruction procedures must be described in the Certification Practice Statement or other publicly available document.	1. Conduct walkthrough of the key destruction process and check the following: a. Upon termination of use of a private key, all copies of the private key in computer memory and shared disk space are securely destroyed by over-writing b. Private key destruction procedures must be described in the CPS c. CA's private keys is destroyed only if the business purpose or application has ceased to have value or legal	Mandatory	IT CA Rules SCHEDULE III 20	
3.3.1.32	The CA's private keys shall be destroyed only if the business purpose or application has ceased to have value or legal obligations have expired as disclosed within the CA's CPS.		Mandatory	WebTrust 4.6.1	
3.3.1.33	Authorization to destroy a CA private key and how the CA's private key is destroyed (e.g., token surrender, token destruction, or key overwrite) are limited in accordance with the CA's CPS.		Mandatory	WebTrust 4.6.2	
3.3.1.34	All copies and fragments of the CA's private key are destroyed at the end of the key pair life cycle in a manner such that the private key cannot be retrieved.		Mandatory	WebTrust 4.6.3	

3.3.1.35	If a secure cryptographic device is accessible and known to be permanently removed from service, all CA private keys stored within the device that have ever been or potentially could be used for any cryptographic purpose are destroyed.	obligations have expired d. Authorization to destroy a CA private key and how the CA's private key is destroyed is done in accordance with CA's CPS 2. Validate if in case a secure cryptographic device is accessible and known to be permanently removed from service, all CA private keys stored within the device that have ever been or potentially could be used for any cryptographic purpose are destroyed. 3. Validate if a CA cryptographic device is being permanently removed from service, then any key contained within the device that has been used for any cryptographic purpose is erased from the device. 4. Verify if the CA cryptographic device case is intended to provide tamper-evident characteristics and the device is being permanently removed from service, then the case is destroyed 5. Validate backup or additional copies of CA keys that no longer serve a valid business purpose are destroyed in accordance with the CA's disclosed business practices 6. Verify the CA follows a CA key destruction script for key destruction ceremonies that includes the requirements covered	Mandatory	WebTrust 4.6.4	
3.3.1.36	If a CA cryptographic device is being permanently removed from service, then any key contained within the device that has been used for any cryptographic purpose is erased from the device.		Mandatory	WebTrust 4.6.5	
3.3.1.37	If a CA cryptographic device case is intended to provide tamper-evident characteristics and the device is being permanently removed from service, then the case is destroyed		Mandatory	WebTrust 4.6.6	
3.3.1.38	Backup or additional copies of CA keys that no longer serve a valid business purpose are destroyed in accordance with the CA's disclosed business practices.		Mandatory	WebTrust 4.6.7	
3.3.1.39	The CA follows a CA key destruction script for key destruction ceremonies that includes the following: • definition and assignment of participant roles and responsibilities; • management approval for conduct of the key destruction ceremony; • specific cryptographic hardware, software and other materials including identifying information, e.g., serial numbers, that contain the CA key copies to be destroyed; • specific steps performed during the key destruction ceremony, including; o HSM and/or cryptographic hardware zeroisation/initialisation o HSM and/or cryptographic hardware physical destruction o Deletion of any encrypted files containing the CA key or fragments thereof • physical security requirements for the ceremony location		Mandatory	WebTrust 4.6.8	

	(e.g., barriers, access controls and logging controls); • procedures for secure storage of cryptographic hardware and any associated activation materials following the key destruction ceremony pending their disposal or additional destruction • sign-off on the script or in a log from participants and witnesses indicating whether the key destruction ceremony was performed in accordance with the detailed key destruction ceremony script; and • notation of any deviations from the key destruction ceremony script (e.g., documentation of steps taken to address any technical issues).	in control 3.3.1.39 7. For a recent key destruction ceremony, verify name of the auditor who independently witnessed the process			
3.3.1.40	CA key destruction ceremonies are independently witnessed by internal or external auditors.		Mandatory	WebTrust 4.6.9	
Key Compromise					
3.3.1.41	A procedure shall be pre-established to handle cases where a compromise of the Certifying Authority's Digital Signature private key has occurred.	1. Conduct walkthrough of the key compromise process and check the following for sample incidents: a. Procedure has been pre-established to handle cases where a compromise of the CA's Digital Signature private key has occurred. b. CA immediately revokes all affected subscriber DSC c. CAs public keys are archived permanently to facilitate audit d. Archives of CA's public	Mandatory	IT CA Rules SCHEDULE III 21.3, IT Regulations 3, X.509 Policy 5.7.3	
3.3.1.42	The Certifying Authority should immediately revoke the affected keys and Digital Signature Certificates in the case of Subscriber private key compromise.		Mandatory	IT CA Rules SCHEDULE III 21.3, IT Regulations 3	
3.3.1.43	The Certifying Authority's public keys shall be archived permanently to facilitate audit or investigation requirements		Mandatory	IT CA Rules SCHEDULE III 21.3	

3.3.1.44	Archives of Certifying Authority's public keys shall be protected from unauthorized modification	keys are protected from unauthorized modification	Mandatory	IT CA Rules SCHEDULE III 21.3	
3.3.1.45	The CA's business continuity plans address the compromise or suspected compromise of a CA's private keys as a disaster.	1. Verify the CA's business continuity plans address the compromise or suspected compromise of a CA's private keys as a disaster 2. Validate disaster recovery procedures include the revocation and reissuance of all certificates that were signed with that CA's private key, in the event of the compromise or suspected compromise 3. Check the recovery procedures used if the CA's private key covers the requirements mentioned in control 3.3.1.47	Mandatory	WebTrust 4.7.1	
3.3.1.46	Disaster recovery procedures include the revocation and reissuance of all certificates that were signed with that CA's private key, in the event of the compromise or suspected compromise of a CA's private signing key.		Mandatory	WebTrust 4.7.2	
3.3.1.47	The recovery procedures used if the CA's private key is compromised include the following actions: • how secure key usage in the environment is re-established; • how the CA's old public key is revoked; • how affected parties are notified (e.g., impacted CAs, Repositories, Subscribers and CVSPs); • how the CA's new public key is provided to the end entities and Relying Parties together with the mechanism for their authentication; and • how the subscriber's public keys are re-certified.		Mandatory	WebTrust 4.7.3	
3.3.1.48	In the event that the CA has to replace its Root CA private key, procedures are in place for the secure and authenticated revocation of the following: • the old CA root public key; • the set of all certificates (including any self-signed) issued by a Root CA or any CA based on the compromised private key; and • any subordinate CA public keys and corresponding certificates that require recertification	1. Validate CA has a procedure in place in the event that the CA has to replace its private key	Mandatory	WebTrust 4.7.4	

3.3.1.49	The CA's business continuity plan for key compromise addresses who is notified and what actions are taken with system software and hardware, symmetric and asymmetric keys, previously generated signatures and encrypted data.	1. Verify CA's business continuity plan addresses list of people to be notified and what actions are taken with system software and hardware, symmetric and asymmetric keys, previously generated signatures and encrypted data	Mandatory	WebTrust 4.7.5	
Cryptographic Hardware Life Cycle Management					
3.3.1.50	CA cryptographic hardware which does not contain CA keys is sent from the manufacturer or alternate CA site via registered mail (or equivalent) using tamper evident packaging. Upon the receipt of CA cryptographic hardware from the manufacturer or alternate site, authorized CA personnel inspects the tamper evident packaging to determine whether the seal is intact.	1. Conduct a walkthrough of process of transfer of cryptographic hardware 2. Verify for sample cryptographic hardware which does not contain CA keys is sent from the manufacturer or alternate CA site via registered mail (or equivalent) using tamper evident packaging 3. Validate the cryptographic hardware from the manufacturer, acceptance testing and verification of firmware settings is performed upon the receipt of CA 4. Validate CA takes measure to prevent tampering of cryptographic hardware covering the characteristics mentioned in control (3.3.1.52) description	Mandatory	WebTrust 4.8.1	
3.3.1.51	Upon the receipt of CA cryptographic hardware from the manufacturer, acceptance testing and verification of firmware settings is performed. Upon the receipt of CA cryptographic hardware that has been serviced or repaired, acceptance testing and verification of firmware settings is performed.		Mandatory	WebTrust 4.8.2	
3.3.1.52	To prevent tampering, CA cryptographic hardware is stored and used in a secure site, with access limited to authorized personnel, having the following characteristics: • inventory control processes and procedures to manage the origination, arrival, condition, departure and destination of each device; • access control processes and procedures to limit physical access to authorized personnel; • recording of all successful or failed access attempts to the CA facility and device storage mechanism (e.g., a safe) in audit logs;		Mandatory	WebTrust 4.8.3	

	• incident handling processes and procedures to handle abnormal events, security breaches, and investigation and reports; and • monitoring processes and procedures to verify the ongoing effectiveness of the controls.				
3.3.1.53	When not attached to the CA system, the CA cryptographic hardware is stored in a tamper resistant container that is stored securely under multiple controls (i.e., a safe).	1. Validate use of tamper resistant containers to store the CA cryptographic hardware	Mandatory	WebTrust 4.8.4	
3.3.1.54	The handling of CA cryptographic hardware, including the following tasks, is performed in the presence of no less than two trusted employees: • installation of CA cryptographic hardware; • removal of CA cryptographic hardware from production; • servicing or repair of CA cryptographic hardware (including installation of new hardware, firmware, or software); and • disassembly and permanent removal from use	1. Obtain names of employees responsible for handling of CA cryptographic hardware 2. Validate by discussing with them if they were present during installation, removal servicing, repair, disassembly and permanent removal of CA cryptographic hardware	Mandatory	WebTrust 4.8.5	
3.3.1.55	Devices used for private key storage and recovery and the interfaces to these devices are tested before usage for integrity.	1. Verify by checking reports of the testing performed on devices used for private key storage	Mandatory	WebTrust 4.8.6	
3.3.1.56	Correct processing of CA cryptographic hardware is verified on a periodic basis.	1. Validate the processing of cryptographic hardware is verified on a periodic basis.	Mandatory	WebTrust 4.8.7	
3.3.1.57	Diagnostic support is provided during troubleshooting of CA cryptographic hardware in the presence of no less than two trusted employees	1. Validate diagnostic support is provided and check the names of trusted employees responsible for overlooking support	Mandatory	WebTrust 4.8.8	

Key Escrow					
3.3.1.58	If a third party provides CA private key escrow services, a contract exists that outlines the liabilities and remedies between the parties.	1. Verify if third party provides CA private key escrow services, a contract exists that outlines the liabilities and remedies between the parties 2. Validate if CA private keys are held in escrow, escrowed copies of CA private signing keys have the same or greater level of security controls as keys currently in use	Mandatory	WebTrust 4.9.1	
3.3.1.59	If CA private signing keys are held in escrow, escrowed copies of the CA private signing keys have the same or greater level of security controls as keys currently in use.		Mandatory	WebTrust 4.9.2	
Key Transportation					
3.3.1.60	CA keys are prepared for transport in a physically secure environment by personnel in Trusted Roles and under multi-person control	1. Conduct walkthrough of the key transportation process and check the following: a. CA keys are prepared for transport in a physically secure environment by personnel in Trusted Roles and under multi-person control b. CA has individuals assigned for Trusted Roles and they have received training to perform their responsibilities. c. CA keys remain in a physically secure environment until ready to be transported by CA personnel or common	Mandatory	WebTrust 4.10.1	

3.3.1.61	CA keys remain in a physically secure environment until ready to be transported by CA personnel or common carrier.	carrier d. CA keys are only transported on hardware devices and in tamper-evident packaging e. For hardware device containing entire CA key, two CA employees will be required to physical transport the key f. For CA key divided into fragments on multiple hardware devices, measures mentioned in control 3.3.1.64 are followed g. Activation materials are transported separately from the CA key in tamper evident packaging h. Packaging for CA keys and activation materials are reviewed for evidence of tampering upon receipt i. CA keys and activation materials are stored in a physically secure environment by personnel in Trusted Roles and under multi-person control upon receipt j. All CA key transportation activities are logged k. For a recent key transportation ceremony,	Mandatory	WebTrust 4.10.2	
3.3.1.62	CA keys are only transported on hardware devices and in tamper-evident packaging as disclosed in the CA's business practices.		Mandatory	WebTrust 4.10.3	
3.3.1.63	If the hardware device contains the entire CA key, it is physically transported by at least two CA employees and remains under multi-person control from origin to destination.		Mandatory	WebTrust 4.10.4	
3.3.1.64	If the CA key is divided into fragments on multiple hardware devices: • If transported by CA employees, each fragment is transported separately using different transportation routes, methods, and/or times; or • If transported by common carrier, each fragment is sent using a different common carrier at different times. Shipments require signature service, tracking, are insured.		Mandatory	WebTrust 4.10.5	
3.3.1.65	Activation materials are transported separately from the CA key (i.e. by a different method and/or at a different time) in tamper-evident packaging		Mandatory	WebTrust 4.10.6	
3.3.1.66	Upon receipt at the destination, packaging for CA keys and activation materials are reviewed for evidence of tampering. If evidence of tampering is discovered, the Policy Authority is notified of a possible breach event		Mandatory	WebTrust 4.10.7	
3.3.1.67	Upon receipt at the destination, CA keys and activation materials are stored in a physically secure environment by personnel in Trusted Roles and under multi-person control.		Mandatory	WebTrust 4.10.8	

3.3.1.68	Personnel involved in a CA key transportation event are in Trusted Roles and have received training in their role and responsibilities.	verify name of the auditor who independently witnessed the process	Mandatory	WebTrust 4.10.9	
3.3.1.69	A log is maintained of all actions taken as part of the CA key transportation event and is retained in accordance with the CA's disclosed business practices.		Mandatory	WebTrust 4.10.10	
3.3.1.70	Internal or external auditors accompany CA personnel during CA key transportation events.		Mandatory	WebTrust 4.10.11	
Key Changeover					
3.3.1.71	Certifying Authority and Subscriber keys shall be changed periodically. Key change shall be processed as per Key Generation guidelines.	1. Conduct walkthrough of the key changeover process and check the following: a. The frequency of changing CA and subscriber keys b. Key change is processed as per Key Generation guidelines c. CA provides reasonable notice to subscriber's relying parties of any change to new key pair used by CA d. All keys have validity period less than 5 years e. Validity period of keys is defined as per requirements mentioned in control 3.3.1.75 f. Key is often changed to minimize risk from	Mandatory	IT CA Rules SCHEDULE III 21.1, X.509 Policy 5.6, CA Browser Forum 5.6	
3.3.1.72	The Certifying Authority shall provide reasonable notice to the Subscriber's relying parties of any change to a new key pair used by the Certifying Authority to sign Digital Signature Certificates.		Mandatory	IT CA Rules SCHEDULE III 21.1	
3.3.1.73	The Certifying Authority shall define its key change process that ensures reliability of the process by showing how the generation of key interlocks – such as signing a hash of the new key with the old key.		Mandatory	IT CA Rules SCHEDULE III 21.1	
3.3.1.74	All CA keys must have validity periods of no more than ten years.		Mandatory	IT CA Rules SCHEDULE III 21.1	

3.3.1.75	To minimize risk from compromise of a CA's private signing key, that key may be changed often; from that time on, only the new key shall be used for certificate signing purposes. The older, but still valid, certificate will be available to verify old signatures until all of the certificates signed using the associated private key have also expired. If the old private key is used to sign CRLs, then the old key shall be retained and protected.	compromise	Recommended	X.509 Policy	
Key Migration					
3.3.1.76	CA key migration events occur in a physically secure environment by those in Trusted Roles under multi-person control	1. Validate CA migration is done in a physically secure environment 2. Check vendor-supplied hardware and software tools are tested by the CA prior the key migration event 3. Verify In house developed software tools are developed and tested by the CA prior to the key migration event	Mandatory	WebTrust 4.11.1	
3.3.1.77	Vendor-supplied hardware and software tools are tested by the CA prior the key migration event, and are operated in accordance with vendor-supplied documentation and instructions.		Mandatory	WebTrust 4.11.2	
3.3.1.78	In-house developed software tools are developed and tested by the CA prior to the key migration event in accordance with its standard software development process		Mandatory	WebTrust 4.11.3	
3.3.1.79	The CA follows a CA key migration script for key migration events that includes the following: • definition and assignment of participant roles and responsibilities; • management approval for conduct of the key migration event • specific cryptographic hardware, software and other materials including identifying information, e.g., serial numbers, that contain the CA key copies to be migrated and new hardware where the keys are being migrated to; • specific steps performed during the key migration ceremony, including; • Hardware preparation	1. Obtain a copy of the CA key migration script and check the following: **a.** Script covers roles assigned, management approval,serial numbers, procedures for secure storage of cryptographic hardware etc. **b.** Steps for performing key migration are stated clearly in the script **c.** physical security	Mandatory	WebTrust 4.11.4	

	○ Software tool installation and setup ○ Cryptographic hardware setup and initialization ○ CA key migration ○ CA key verification • physical security requirements for the event location (e.g., barriers, access controls and logging controls); • procedures for secure storage of cryptographic hardware and any associated activation materials following the migration event • sign-off on the script or in a log from participants and witnesses indicating whether the key migration was performed in accordance with the detailed key migration script; and • notation of any deviations from the key migration script (e.g., documentation of steps taken to address any technical issues).	requirements for the ceremony location are met d. sign-off is given for the key migration ceremony e. notation of any deviations from the key generation ceremony script are addressed			
3.3.1.80	A log is maintained of all actions taken as part of the CA key migration event and is retained in accordance with the CA's disclosed business practices.	1. Validate logs are maintained for CA key migration event 2. For a recent key migration ceremony, verify name of the auditor who independently witnessed the process 3. Verify upon successful completion of a CA key migration event, remaining copies of the CA keys, and older cryptographic hardware that no longer serve a business purpose shall be securely destroyed	Mandatory	WebTrust 4.11.5	
3.3.1.81	CA key migration events shall be witnessed by internal or external auditors		Mandatory	WebTrust 4.11.6	
3.3.1.82	Upon successful completion of a CA key migration event, remaining copies of the CA keys, and older cryptographic hardware that no longer serve a business purpose shall be securely destroyed in accordance with the CA's disclosed business practices		Mandatory	WebTrust 4.11.7	

Private Key Protection and Cryptographic Module Engineering Controls					
3.3.1.83	The Certifying Authority must protect its private keys from disclosure. The Certifying Authority must back-up its private keys. Backed-up keys must be stored in encrypted form and protected at a level no lower than those followed for storing the primary version of the key.	1. Conduct walkthrough of Private Key Protection and Cryptographic Module Engineering Controls and check the following: a. CA protects private keys from disclosure b. CA backs up its private keys and stores them in encrypted format c. private key backups are stored in a secure storage facility, away from where the original key is stored d. Backup measures are taken to ensure continued availability of private key e. Use of a CA private signing key requires action by at least two persons f. Signature keys are not escrowed by a third party	Mandatory	IT CA Rules SCHEDULE III 19	
3.3.1.84	The Certifying Authority's private key backups should be stored in a secure storage facility, away from where the original key is stored. Continued availability of the private key be ensured through approved backup measures in the event of loss or corruption of its private key.		Mandatory	IT CA Rules SCHEDULE III 19, IT Regulations 3	
3.3.1.85	Use of a CA private signing key shall require action by at least two persons		Mandatory	X.509 Policy 6.2.2	
3.3.1.86	The cryptographic module may store Private Keys in any form as long as the keys are not accessible without authentication mechanism that is in compliance with FIPS 140-2 rating of the cryptographic module.		Recommended	X.509 Policy 6.2.7	

3.3.2. Subscriber Key Lifecycle Controls

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
CA-Provided Subscriber Key Generation Services					
3.3.2.1	Subscriber key generation is performed within a secure cryptographic device meeting the applicable ISO 15782-1/FIPS 140-2/ANSI x9.66 requirements based on a risk assessment and the business requirements of the CA and in accordance with the applicable CP.	1. No action is required from the auditor to check the controls as Subscriber key generations services are not provided by CAs	Not Applicable	WebTrust 5.1.1, CA Browser Forum 6.1.1.3	
3.3.2.2	Subscriber key generation performed by the CA (or RA or card bureau) uses a key generation algorithm as specified in the CP.		Not Applicable	WebTrust 5.1.2	
3.3.2.3	Subscriber key generation performed by the CA (or RA) uses a prime number generator as specified in an ANSI X9 or ISO standard		Not Applicable	WebTrust 5.1.3	
3.3.2.4	Subscriber key generation performed by the CA (or RA or card bureau) results in key sizes in accordance with the CP.		Not Applicable	WebTrust 5.1.4	
3.3.2.5	Subscriber key generation performed by the CA (or RA) is performed by authorized personnel in accordance with the CA's CPS.		Not Applicable	WebTrust 5.1.5	
3.3.2.6	When subscriber key generation is performed by the CA (or RA or card bureau), the CA (or RA or card bureau) securely (confidentially) delivers the subscriber key pair(s) generated by the CA (or RA or card bureau) to the subscriber in accordance with the CP.		Not Applicable	WebTrust 5.1.6	

3.3.2.7	The Certifying Authority's public verification key must be delivered to the prospective Digital Signature Certificate holder in an on-line transaction in accordance with PKIX-3 Certificate Management Protocol, or via an equally secure manner. The Certifying Authority shall ensure that the subscriber can verify the Certifying Authority's Public Key Certificate, if he chooses to do so, by having access to the Public Key Certificate of the Controller	1. Conduct walkthrough and check the following: a. CAs public verification key is delivered to the prospective Digital Signature Certificate holder in an on-line transaction in accordance with PKIX-3 Certificate Management Protocol, or via an equally secure manner. b. Certifying Authority ensures that the subscriber can verify the Certifying Authority's Public Key Certificate, if he chooses to do so, by having access to the Public Key Certificate of the Controller			
CA-Provided Subscriber Key Storage and Recovery Services					
3.3.2.8	Certifying Authority's keys shall be stored in tamper-resistant devices and can only be activated under split-control by parties who are not involved in the set-up and maintenance of the systems and operations of the Certifying Authority. The key of the Certifying Authority may be stored in a tamper-resistant cryptographic module or split into sub-keys stored in tamper-resistant devices under the custody of the key custodians	1. Conduct walkthrough of the CA-Provided Subscriber Key Storage and Recovery Services and check the following: a. CAs key is stored in tamper resistant device b. CAs key custodians ensure that the CA's key component or the activation code is always under his sole custody c. Change of key custodian is	Mandatory	IT CA Rules SCHEDULE III 18.3	
3.3.2.9	The Certifying Authority's key custodians shall ensure that the Certifying Authority's key component or the activation code is always under his sole custody. Change of key custodians shall be approved by the Certifying Authority's management and		Mandatory	IT CA Rules SCHEDULE III 18.3	

	documented	approved by CAs management and documented			
3.3.2.10	Subscriber private keys stored by the CA (or RA) are stored in encrypted form using a cryptographic algorithm and key length based on a risk assessment and requirements of the CP.	d. Subscriber private keys stored by the CA are stored in encrypted form using a cryptographic algorithm and key length	Mandatory	WebTrust 5.2.1	
3.3.2.11	If the CA generates key pair(s) on behalf of a Subscriber, the CA (or RA) ensures that the subscriber's private keys are not disclosed to any entity other than the owner (i.e., the subscriber) of the keys.	e. CA ensures that the subscriber's private keys are not disclosed to any entity other than the owner (i.e., the subscriber) of the keys if Ca generates key pair(s) on behalf of subscriber	Mandatory	WebTrust 5.2.2	
3.3.2.12	If the CA (or RA) generates public/private signing key pair(s), it does not maintain a copy of any private signing key, once the subscriber confirms receipt of that key.	f. CA does not maintain a copy of any private signing key	Mandatory	WebTrust 5.2.3	
3.3.2.13	If the CA (or RA) provides subscriber (confidentiality) key storage, backup and recovery, subscriber private (confidentiality) key backup and recovery services are only performed by authorized personnel.	g. key backup and recovery services are only performed by authorized personnel if the CA provides subscriber (confidentiality) key storage, backup and recovery, subscriber private	Mandatory	WebTrust 5.2.4	
3.3.2.14	If the CA (or RA) provides subscriber key storage, backup and recovery, controls exist to ensure that the integrity of the subscriber's private (confidentiality) key is maintained throughout its life cycle.	h. Backup and recovery, controls exist for encryptions to ensure that the integrity of the subscriber's private (confidentiality) key is maintained throughout its life cycle.	Mandatory	WebTrust 5.2.5	

Requirements for Subscriber Key Management					
3.3.2.15	The CP specifies the appropriate ISO 15782-1/FIPS 140-2 level requirement for cryptographic modules used for subscriber key generation	1. Conduct walkthrough of the CA-Provided Subscriber Key Management process and check the following: a. CP specifies the appropriate ISO 15782-1/FIPS 140-2 level requirement for cryptographic modules used for subscriber key generation b. CP specifies the key generation algorithm(s) that is used for subscriber key generation c. CP specifies the acceptable key sizes for subscriber key generation d. CP specifies the private key protection requirements for stored subscriber private keys e. CP states the circumstances and authority of when the subscriber's private key will be restored and the control processes f. CP specifies the private key protection requirements for backup copies of subscriber private keys stored by the	Mandatory	WebTrust 5.4.1	
3.3.2.16	The CP specifies the key generation algorithm(s) that is used for subscriber key generation.		Mandatory	WebTrust 5.4.2	
3.3.2.17	The CP specifies the acceptable key sizes for subscriber key generation.		Mandatory	WebTrust 5.4.3	
3.3.2.18	The CA or RA provides or makes available the mechanisms to allow the Subscriber to access (i.e., private key owner verification method), manage and control the usage of their private keys.		Not Applicable	WebTrust 5.4.4	
3.3.2.19	The CP specifies the private key protection requirements for stored subscriber private keys.		Mandatory	WebTrust 5.4.5	
3.3.2.20	The CP states the circumstances and authority of when the subscriber's private key will be restored and the control processes		Mandatory	WebTrust 5.4.6	
3.3.2.21	The CP specifies the private key protection requirements for backup copies of subscriber private keys stored by the subscriber.		Mandatory	WebTrust 5.4.7	
3.3.2.22	Subscriber Agreements describe the required processes to be followed by the Subscriber of any use of the cryptographic mechanism (e.g., HSM or ICC and software application).		Mandatory	WebTrust 5.4.8	
3.3.2.23	The CP specifies the acceptable uses for subscriber key pairs.		Mandatory	WebTrust 5.4.9	
3.3.2.24	The CP specifies the requirements for subscriber key usage.		Mandatory	WebTrust 5.4.10	

3.3.2.25	The CP specifies the private key protection requirements for archived subscriber private keys.	subscriber. g. Subscriber Agreements describe the required processes to be followed by the Subscriber h. CP specifies acceptable uses for subscriber key pairs i. CP specifies the requirements for subscriber key usage. j. CP specifies the private key protection requirements for archived subscriber private keys k. CP specifies the requirements for destruction of archived subscriber keys at the end of the archive period l. CP specifies the means through which subscriber key destruction is performed m. CP or CPS specifies the requirements for destruction of all copies and fragments of the subscriber's private key at the end of the key pair life cycle n. CP specifies the requirements for use and handling of cryptographic hardware and subscriber authentication processes	Mandatory	WebTrust 5.4.11	
3.3.2.26	The CP specifies the requirements for destruction of archived subscriber keys at the end of the archive period.		Mandatory	WebTrust 5.4.12	
3.3.2.27	The CP specifies the means through which subscriber key destruction is performed.		Mandatory	WebTrust 5.4.13	
3.3.2.28	The CP or CPS specifies the requirements for destruction of all copies and fragments of the subscriber's private key at the end of the key pair life cycle.		Mandatory	WebTrust 5.4.14	
3.3.2.29	CP specifies the requirements for use and handling of cryptographic hardware and subscriber authentication processes (and subsequent actions) where the cryptographic hardware is in other physical locations (i.e., an HSM attached to a mainframe or remote server).		Mandatory	WebTrust 5.4.15	
3.3.2.30	The CP specifies the requirements for notification of the CA or RA in the event of subscriber key compromise.		Mandatory	WebTrust 5.4.16	

		o. CP specifies the requirements for notification of the CA in the event of subscriber key compromise.			
Certificate Operational Periods and Key Pair Usage Periods					
3.3.2.31	Subscriber SSL Certificates issued after 1 March 2018 must have a Validity Period no greater than 825 days. Subscriber Certificates issued after 1 July 2016 but prior to 1 March 2018 must have a Validity Period no greater than 39 months.	1. For sample SSL certificates issued after 1 March 2018, verify the validity period is not greater than 825 days 2. For sample certificates issued after 1 July 2016 but prior to 1 March 2018, verify the validity period is not greater than 39 months	Applicable for SSL Certificates	CA Browser Forum 6.3.2	
Confidentiality of Subscriber's Information					
3.3.2.32	Procedures and security controls to protect the privacy and confidentiality of the subscribers' data under the Certifying Authority's custody shall be implemented. Confidential information provided by the subscriber must not be disclosed to a third party without the subscribers' consent, unless the information is required to be disclosed under the law or a court order.	1. Verify CA has implemented procedures and security controls to protect privacy and confidentiality of subscribers' data 2. Validate confidential information provided by the subscriber is not disclosed to a third party without the subscribers' consent, unless the information is required to be disclosed under the law or a court order 3. Check the data on usage of DSC and transactional data is protected to ensure the subscribers' privacy 4. Verify a secure communication	Mandatory	IT CA Rules SCHEDULE III 22	
3.3.2.33	Data on the usage of the Digital Signature Certificates by the subscribers and other transactional data relating to the subscribers' activities generated by the Certifying Authority in the course of its operation shall be protected to ensure the subscribers' privacy		Mandatory	IT CA Rules SCHEDULE III 22	
3.3.2.34	A secure communication channel between the Certifying Authority and its subscribers shall be established to ensure the authenticity,		Mandatory	IT CA Rules SCHEDULE III	

	integrity and confidentiality of the exchanges (e.g. transmission of Digital Signature Certificate, password, private key) during the Digital Signature Certificate issuance process.	channel between the CA and its subscribers is established to ensure the authenticity, integrity and confidentiality of the exchange		22	

3.4. Certificate Management Controls

3.4.1. Certificate Lifecycle Management

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Subscriber Registration					
3.4.1.1	For authenticated certificates, the CA verifies or requires that the RA verify the credentials presented by a subscriber as evidence of identity or authority to perform a specific role in accordance with the requirements of the CP.	1. Conduct a walkthrough of the Subscriber registration process and check the following for a sample of subscriber registrations: a. CA verifies or requires that the RA verify the credentials presented by a subscriber as evidence of identity or authority to perform a specific role in accordance with the requirements	Mandatory	WebTrust 6.1.1	
3.4.1.2	For domain and/or IP address validated certificates, the CA validates or requires that the RA validate (as determined by the CP) the organization's ownership, control, or right to use the domain name and/or IP address		Mandatory	WebTrust 6.1.2	

3.4.1.3	The CA or RA verifies the accuracy of the information included in the requesting entity's certificate request in accordance with the CP.	of the CP for authenticated certificates b. the CA validates or requires that the RA validate (as determined by the CP) the organization's ownership, control, or right to use the domain name and/or IP address for domain and/or IP address validated certificates c. CA verifies the accuracy of the information included in the requesting entity's certificate request in accordance with the CP d. CA checks the Certificate Request for errors or omissions in accordance with the CP e. CA uses the RA's public key contained in the requesting entity's Certificate Request to verify signature on the Certificate Request submission for end entity certificates f. CA verifies the uniqueness of the subscriber's distinguished name within the boundaries or community defined by the CP	Mandatory	WebTrust 6.1.3	
3.4.1.4	The CA or RA checks the Certificate Request for errors or omissions in accordance with the CP.		Mandatory	WebTrust 6.1.4	
3.4.1.5	For end entity certificates, the CA uses the RA's public key contained in the requesting entity's Certificate Request to verify signature on the Certificate Request submission.		Mandatory	WebTrust 6.1.5	
3.4.1.6	The CA verifies the uniqueness of the subscriber's distinguished name within the boundaries or community defined by the CP.		Mandatory	WebTrust 6.1.6	
3.4.1.7	Encryption and access controls are used to protect the confidentiality and integrity of registration data in transit and in storage.	1. Verify encryption and access controls are used to protect the confidentiality and integrity of registration data in transit and in storage.	Mandatory	WebTrust 6.1.7	
3.4.1.8	At the point of registration (before certificate issuance) the RA or CA informs the Subscriber of the terms and conditions regarding use of the certificate.	1. Conduct walkthrough and check the following: a. Before certificate issuance the CA informs the Subscriber of the	Mandatory	WebTrust 6.1.8	

3.4.1.9	The CA requires that an entity requesting a certificate must prepare and submit the appropriate certificate request data (Registration Request) to an RA (or the CA) as specified in the CP.	terms and conditions regarding use of the certificate. b. The entity requesting a certificate prepares and submits the appropriate certificate request data (Registration Request) to an RA (or the CA) as specified in the CP.	Mandatory	WebTrust 6.1.10	
3.4.1.10	The CA requires that the requesting entity submit its public key in a self-signed message to the CA for certification. The CA requires that the requesting entity digitally sign the Registration Request using the private key that relates to the public key contained in the Registration Request in order to: • allow the detection of errors in the certificate application process; and • Prove possession of the companion private key for the public key being registered.	1. Verify requesting entity submits its public key in a self-signed message to the CA for certification 2. Validate the requesting entity digitally signs the Registration Request using the private key that relates to the public key contained in the Registration Request 3. Validate certificate request is treated as acceptance of the terms of conditions by the requesting entity 4. Check the identity of RA authorized to issue registration requests is validated by the CA	Mandatory	WebTrust 6.1.11	
3.4.1.11	The certificate request is treated as acceptance of the terms of conditions by the requesting entity to use that certificate as described in the Subscriber Agreement		Mandatory	WebTrust 6.1.12	
3.4.1.12	The CA validates the identity of the RA authorized to issue registration requests under a specific CP.		Mandatory	WebTrust 6.1.13	
3.4.1.13	The CA requires that RAs submit the requesting entity's certificate request data to the CA in a message (Certificate Request) signed by the RA. The CA verifies the RA's signature on the Certificate Request.	1. Verify the RAs submit the requesting entity's certificate request data to the CA in a message (Certificate Request) signed by the RA	Mandatory	WebTrust 6.1.14	
3.4.1.14	The CA requires that the RA secure that part of the certificate application process for which it (the RA) assumes responsibility in accordance with the CA's CPS.	1. Verify that the RA secures that part of the certificate application process for which it assumes responsibility in accordance with the CA's CPS	Mandatory	WebTrust 6.1.15	

3.4.1.15	The CA requires that RAs record their actions in an audit log.	1. Verify all RA activities are recorded in an audit log	Mandatory	WebTrust 6.1.16	
3.4.1.16	The CA verifies the authenticity of the submission by the RA in accordance with the CA's CPS.	1. Check that the authenticity of the submission by the RA is verified by the CA	Mandatory	WebTrust 6.1.17	
Certificate Issuance					
3.4.1.17	The CA generates certificates using Certificate Request Data and manufactures the certificate as defined by the appropriate Certificate Profile in accordance with ISO 9594/X.509 and ISO 15782-1 formatting rules as disclosed within the CP.CA shall verify the source of a certificate request before issuance.	1. Conduct walkthrough of the Certificate Issuance process to check the following: a. CA generates certificates using Certificate Request Data and manufactures the certificate as defined by the appropriate Certificate Profile b. CA verifies source of certificate request before issuance c. Validity periods are set by CA in compliance with the CP d. Extension fields are formatted in accordance with with the CP e. CA signs the end entity's public key and other relevant information with the CA's private signing key f. CA publishes the certificate after the certificate has been accepted by the requesting entity as disclosed in the CA's business practices g. CA notifies the RA when a certificate is issued to a subscriber for whom the RA submitted a certificate request h. Authorized individual issues direct command for Root CA to	Mandatory	WebTrust 6.4.1,CA Browser Forum 4.3, X.509 Policy 4.3	
3.4.1.18	Validity periods are set in the CP and are formatted in accordance with ISO 9594/X.509 and ISO 15782-1 as disclosed within the CP.		Mandatory	WebTrust 6.4.2	
3.4.1.19	Extension fields are formatted in accordance with ISO 9594/X.509 and ISO 15782-1 as disclosed within the CP.		Mandatory	WebTrust 6.4.3	
3.4.1.20	The CA signs the end entity's public key and other relevant information with the CA's private signing key.		Mandatory	WebTrust 6.4.4	
3.4.1.21	The CA publishes the certificate after the certificate has been accepted by the requesting entity as disclosed in the CA's business practices.		Mandatory	WebTrust 6.4.5, CA Browser Forum 4.3	
3.4.1.22	When an RA is used, the CA notifies the RA when a certificate is issued to a subscriber for whom the RA submitted a certificate request. Certificate issuance by the Root CA SHALL require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in		Mandatory	WebTrust 6.4.6	

	order for the Root CA to perform a certificate signing operation.	perform a certificate signing operation i. Certificates are issued based on approved subscriber registration, certificate renewal or certificate rekey requests in accordance with the CP j. CA issues a signed notification to the RA when a certificate is issued to a subscriber for whom the RA submitted a certificate request k. CA issues an out-of-band notification to the Subscriber when a certificate is issued l. copies of certificates are retained for the appropriate period of time specified in the CP			
3.4.1.23	Certificates are issued based on approved subscriber registration, certificate renewal or certificate rekey requests in accordance with the CP.		Mandatory	WebTrust 6.4.7	
3.4.1.24	The CA issues a signed notification to the RA when a certificate is issued to a subscriber for whom the RA submitted a certificate request.		Mandatory	WebTrust 6.4.8, X.509 Policy 4.3	
3.4.1.25	The CA issues an out-of-band notification to the Subscriber when a certificate is issued. Where this notification includes initial activation data, then control processes ensure safe delivery to the Subscriber.		Mandatory	WebTrust 6.4.9	
3.4.1.26	Whether certificates expire, are revoked or are suspended, copies of certificates are retained for the appropriate period of time specified in the CP.		Mandatory	WebTrust 6.4.10	
Certificate Distribution					
3.4.1.27	Only authorized CA personnel administer the CA's repository or alternative distribution mechanism.	1. Conduct walkthrough of certificate distribution process to check the following: a. Only authorized CA personnel administer the CA's repository or alternative distribution mechanism b. performance of the CA's repository or alternative distribution mechanism is monitored and managed c. integrity of the repository or alternative distribution mechanism is maintained and administered	Mandatory	WebTrust 6.5.2	
3.4.1.28	The performance of the CA's repository or alternative distribution mechanism is monitored and managed.		Mandatory	WebTrust 6.5.3	
3.4.1.29	The integrity of the repository or alternative distribution mechanism is maintained and administered.		Mandatory	WebTrust 6.5.4	

Certificate Acceptance					
3.4.1.30	Procedures shall be developed for certificate acceptance and publication of the certificate by the CA.The subject must confirm acceptance of the certificate upon notification of issuance bythe CA.	1. Verify procedures have been developed for certificate acceptance and publication and subject confirms acceptance of certificate 2. Verify CA notifies of certificate issuance to other entities	Mandatory	X.509 Policy 4.4, CA Browser Forum 4.4	
3.4.1.31	Notification of certificate issuance by the CA to other entities		Mandatory	X.509 Policy 4.4, CA Browser Forum 4.4	
Key Pair and Certificate Usage					
3.4.1.32	Subscribers and CAs shall protect their private keys from access by any other party. Subscribers and CAs shall use their private keys for the purposes as constrained by the extensions (such as key usage, extended key usage, certificate policies, etc.) in the certificates issued to them	1. Check that the CAs protect their private keys from access by any other party. 2. Verify CAs use their private keys for the purposes as constrained by the extensions in the certificates issued to them	Mandatory	X.509 Policy 4.5.1, CA Browser Forum 4.5	
Certificate Renewal					
3.4.1.33	A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been revoked or compromised, and the Subscriber name and attributes are unchanged.	1. Certificate renewal is not performed as part of current CA systems Hence all the controls are not applicable and no action is required from the auditor's side.	Not Applicable	X.509 Policy 4.6	
3.4.1.34	In addition, the validity period of the certificate must not exceed the remaining lifetime of the private key		Not Applicable	X.509 Policy 4.6	

3.4.1.35	The Certificate Renewal Request includes at least the subscriber's Distinguished Name, the Serial Number of the certificate (or other information th0 at identifies the certificate), and the requested validity period. (The CA will only renew certificates that were issued by itself.)		Not Applicable	WebTrust 6.2.1	
3.4.1.36	The CA requires that the requesting entity digitally sign the Certificate Renewal Request using the private key that relates to the public key contained in the requesting entity's existing public key certificate		Not Applicable	WebTrust 6.2.2	
3.4.1.37	The CA issues a new certificate using the subscriber's previously certified public key, only if its cryptographic security is still sufficient for the new certificate's intended lifetime and no indications exist that the subscriber's private key has been compromised		Not Applicable	WebTrust 6.2.3	
3.4.1.38	For renewal of authenticated certificates, the CA or the RA process the certificate renewal data to verify the identity of the requesting entity and to identify the certificate to be renewed.		Not Applicable	WebTrust 6.2.4	
3.4.1.39	For domain validated certificates, the CA or the RA process the certificate renewal data to re-validate the domain in accordance with the requirements of the CP.		Not Applicable	WebTrust 6.2.5	
3.4.1.40	The CA or the RA validate the signature on the Certificate Renewal Request		Not Applicable	WebTrust 6.2.6	
3.4.1.41	The CA verifies the existence and validity of the certificate to be renewed. The CA does not renew certificates that have been revoked, expired or suspended		Not Applicable	WebTrust 6.2.7	
3.4.1.42	The CA or the RA verifies that the request, including the extension of the validity period, meets the requirements defined in the CP.		Not Applicable	WebTrust 6.2.8	

3.4.1.43	The CA requires that RAs submit the Certificate Renewal Data to the CA in a message (Certificate Renewal Request) signed by the RA.		Not Applicable	WebTrust 6.2.9	
3.4.1.44	The CA requires that the RA secures that part of the certificate renewal process for which it (the RA) assumes responsibility in accordance with the CP.		Not Applicable	WebTrust 6.2.10	
3.4.1.45	The CA requires that RAs record their actions in an audit log.		Not Applicable	WebTrust 6.2.11	
3.4.1.46	The CA verifies the authenticity of the submission by the RA.		Not Applicable	WebTrust 6.2.12	
3.4.1.47	The CA verifies the RA's signature on the Certificate Renewal Request		Not Applicable	WebTrust 6.2.13	
3.4.1.48	The CA checks the Certificate Renewal Request for errors or omissions. This function may be delegated explicitly to the RA		Not Applicable	WebTrust 6.2.14	
3.4.1.49	The CA or RA notifies Subscribers prior to the expiration of their certificate of the need for renewal in accordance with the CP		Not Applicable	WebTrust 6.2.15	
3.4.1.50	The CA issues a signed notification indicating the certificate renewal has been successful.		Not Applicable	WebTrust 6.2.16	
3.4.1.51	The CA makes the new certificate available to the end entity in accordance with the CP.		Not Applicable	WebTrust 6.2.17	
3.4.1.52	A certificate renewal shall be achieved using one of the following processes: • Initial registration process • Identification & Authentication for Re-key, except the old key can also be used as the new key		Not Applicable	X.509 Policy 4.6.3	

Certificate Re-Key					
3.4.1.53	A certificate re-key shall be achieved using one of the following processes: • Initial registration process • Identification & Authentication for Re-key	1. Verify Certificate re-key is achieved using one of the following processes: a. Initial registration process	Mandatory	X.509 Policy 4.7.3, CA Browser Forum 4.7, X.509 Policy 4.7	
Certificate Validation					
3.4.1.54	The CA makes certificate status information available to relevant entities (Relying Parties or their agents) using an established mechanism in accordance with the CP. This is achieved using: • Request Response Method – A request signed by the Relying Party to the Certificate Status Provider's responder. In turn, the Certificate Status Provider's responder responds with the certificate status duly signed. (OCSP is an example protocol using this method.) • Delivery Method – A CRL signed by the CA and published within the policy's time frame.	1. Check that the certificate status information is made available to relevant entities by the CA using an established mechanism in accordance with the CP 2. Verify Request Response Method and Delivery Method are used for Validation	Mandatory	WebTrust 6.8.1	
Certificate Revocation List (CRL) Controls					
3.4.1.55	The CA digitally signs each CRL that it issues so that entities can validate the integrity of the CRL and the date and time of issuance.	1. Verify that the CRL issued by the CA is digitally signed by the CA 2. Validate that the CRLs are issued at fixed intervals even if no changes have been	Mandatory	WebTrust 6.8.2	

3.4.1.56	The CA issues CRLs at regular intervals, as specified in the CP, even if no changes have occurred since the last issuance.	made 3. Validate on sample basis a CRL entry identifying a revoked certificate remains on the CRL until the end of the certificate's validity period. 4. CRLs are archived in accordance with the requirements of the CP including the method of retrieval 5. CAs include a monotonically increasing sequence number for each CRL issued by that CA 6. CRL contains entries for all revoked unexpired certificates issued by the CA 7. Old CRLs are retained for the appropriate period of time specified in the CA's CP.	Mandatory	WebTrust 6.8.3	
3.4.1.57	At a minimum, a CRL entry identifying a revoked certificate remains on the CRL until the end of the certificate's validity period.		Mandatory	WebTrust 6.8.4	
3.4.1.58	If certificate suspension is supported, a certificate suspension (hold) entry, with its original action date and expiration date remain on the CRL until the normal expiration of the certificate or until the suspension is lifted.		Mandatory	WebTrust 6.8.5	
3.4.1.59	CRLs are archived in accordance with the requirements of the CP including the method of retrieval.		Mandatory	WebTrust 6.8.6	
3.4.1.60	CAs include a monotonically increasing sequence number for each CRL issued by that CA		Mandatory	WebTrust 6.8.7	
3.4.1.61	The CRL contains entries for all revoked unexpired certificates issued by the CA.		Mandatory	WebTrust 6.8.8	
3.4.1.62	Old CRLs are retained for the appropriate period of time specified in the CA's CP.		Mandatory	WebTrust 6.8.9	
Certificate Revocation and Suspension					
3.4.1.63	A certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. The CA SHALL provide a process for Subscribers to request revocation of their own Certificates. The process MUST be described in the CA's Certificate Policy or Certification Practice Statement. The CA SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and related inquiries	1. For sample cases, validate certificate is revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid 2. Verify the CA provides a process for Subscribers to request revocation of their own Certificates and the process is described in the CA's Certificate Policy or	Mandatory	X.509 Policy 4.9.1, CA Browser Forum 4.9	

		Certification Practice Statement. 3. Check the CA maintains a continuous 24x7 ability to accept and respond to revocation requests and related inquiries			
3.4.1.64	The CA provides a means of rapid communication to facilitate the secure and authenticated revocation or renovation of the following: • one or more certificates of one or more subscribers; • the set of all certificates issued by a CA based on a single public/private key pair used by a CA to generate certificates; and • all certificates issued by a CA, regardless of the public/private key pair used. The CA SHALL provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. The CA SHALL publicly disclose the instructions through a readily accessible online means.	1. Check that the CA provides a means of rapid communication to facilitate the secure and authenticated revocation or renovation of the elements mentioned in the control 2. Verify the CA provides Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. 3. Validate the CA has publicly disclosed the instructions through a readily accessible online means.	Mandatory	WebTrust 6.6.1, X.509 Policy 4.9.3, CA Browser Forum 4.9.3	
3.4.1.65	The CA verifies or requires that the RA verify the identity and authority of the entity requesting revocation or suspension and reactivation of a certificate in accordance with the CP. The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate	1. Validate that CA verifies the identity and authority of the entity requesting revocation or suspension and reactivation of a certificate in accordance with the CP 2. Verify the Subscriber or Issuing CA can initiate revocation.	Mandatory	WebTrust 6.6.2, X.509 Policy 4.9.2, CA Browser Forum 4.9.2	

3.4.1.66	If an external RA accepts and forwards revocation requests to the CA, the CA provides a signed acknowledgement of the revocation request and confirmation of actions to the requesting RA.	1. Verify for past instances where the CA provides a signed acknowledgement of the revocation request and confirmation of action	Mandatory	WebTrust 6.6.4	
3.4.1.67	The CA updates the Certificate Revocation List (CRL) and other certificate status mechanisms in the timeframes specified within the CP and in accordance with the format defined in ISO 9594/X.509 and ISO 15782-1.	1. Verify that the CA maintains and updates the Certificate Revocation List (CRL)	Mandatory	WebTrust 6.6.5	
3.4.1.68	The Certifying Authority shall publish a notice of suspension or revocation of any certificate in the Certificate Revocation List in its repository immediately after receiving an authorised request of such suspension or revocation. The CA records all certificate revocation requests and their outcome in an audit log.	1. Verify CA publishes a notice of suspension or revocation of any certificate in the Certificate Revocation List in its repository immediately after receiving an authorised request of such suspension or revocation. 2. Check all certification revocation requests and their outcome are logged	Mandatory	IT Regulation 3, WebTrust 6.6.6	
3.4.1.69	The Subscriber of a revoked or suspended certificate is informed of the change of status of its certificate.	1. Check the following on a sample basis: a. Subscriber of a revoked or suspended certificate is informed of the change of status of its certificate. b. Certificate suspension requests are processed and validated in accordance with the requirements of the CP c. CA notifies the Subscriber in the event of a certificate suspension d. CA updates the Certificate Revocation List (CRL) and other certificate status mechanisms upon certificate suspension e. Suspension is handled in one of the three ways mentioned in the control description (3.4.1.56)	Mandatory	WebTrust 6.6.9	
3.4.1.70	Certificate suspension requests are processed and validated in accordance with the requirements of the CP.		Mandatory	WebTrust 6.7.5	
3.4.1.71	The CA or RA notifies the Subscriber in the event of a certificate suspension.		Mandatory	WebTrust 6.7.4	
3.4.1.72	The CA updates the Certificate Revocation List (CRL) and other certificate status mechanisms upon certificate suspension. Changes in certificate status are completed in a time frame determined by the CP.		Mandatory	WebTrust 6.7.6	
3.4.1.73	Once a certificate suspension (hold) has been issued, the suspension is handled in one of the following three ways: • an entry for the suspended certificate remains on the		Mandatory	WebTrust 6.7.8	

	CRL with no further action; • the CRL entry for the suspended certificate is replaced by a revocation entry for the same certificate; or • the suspended certificate is explicitly released and the entry removed from the CRL.	f. certificate suspension (hold) entry remains on the CRL until the expiration of the underlying certificate or the expiration of the suspension, whichever is first g. CA verifies or requires that the external RA verify the identity and authority of the entity requesting that the suspension of a certificate be lifted h. Certificate suspensions and the lifting of certificate suspensions are recorded in an audit log			
3.4.1.74	A certificate suspension (hold) entry remains on the CRL until the expiration of the underlying certificate or the expiration of the suspension, whichever is first.		Mandatory	WebTrust 6.7.9	
3.4.1.75	The CA verifies or requires that the external RA verify the identity and authority of the entity requesting that the suspension of a certificate be lifted.		Mandatory	WebTrust 6.7.11	
3.4.1.76	Certificate suspensions and the lifting of certificate suspensions are recorded in an audit log.		Mandatory	WebTrust 6.7.12	
Certificate Status Services					
3.4.1.77	Revocation entries on a CRL or OCSP Response must NOT be removed until after the Expiry Date of the revoked Certificate	1. Check the certificate status services for the following: a. Revocation entries on a CRL or OCSP Response are not removed until after the Expiry Date of the revoked Certificate b. CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions. c. CA maintains an online 24x7	Mandatory	CA Browser Forum 4.10.1	
3.4.1.78	The CA shall operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.		Mandatory	CA Browser Forum 4.10.2	
3.4.1.79	The CA shall maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.		Mandatory	CA Browser Forum 4.10.2	

3.4.1.80	The CA shall maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint	Repository that application software can use to automatically check the current status of all unexpired Certificates d. CA maintains a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report	Mandatory	CA Browser Forum 4.10.2	

3.4.2. Subordinate CA Certificate and Cross Certificate Lifecycle Management

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Subordinate CA Certificate and Cross Certificate Lifecycle Management					
3.4.2.1	The Parent CP specifies the requirements for submission of Sub-CA and cross certification requests.	1. No action required from auditor to check the controls as there is no provision for subordinate CA in the current system. Hence all the controls are not applicable	Not Applicable	WebTrust 7.1.1	
3.4.2.2	The Parent CA authenticates the Sub-CA or cross certificate request in accordance with the Parent's CP.		Not Applicable	WebTrust 7.1.2	
3.4.2.3	The Parent CA performs an assessment of the Sub-CA or cross certificate applicant's compliance with the requirements of the Parent CA's CP before approving a Sub-CA or cross certificate request, or alternatively the Sub-CA or cross certificate applicant presents its CPS for assessment.		Not Applicable	WebTrust 7.1.3	
3.4.2.4	Where Sub-CA and cross certificate renewal is permitted, the Parent CA's CP specifies the requirements for		Not Applicable	WebTrust 7.1.4	

	submission of Sub-CA or cross certificate renewal requests				
3.4.2.5	Where Sub-CA certificate and cross certificate renewal is permitted, the Parent CA authenticates the Sub-CA or cross certificate renewal request in accordance with the CA's CP.		Not Applicable	WebTrust 7.1.5	
3.4.2.6	The Parent CA's CP specifies the requirements for submission of Sub-CA rekey requests		Not Applicable	WebTrust 7.1.6	
3.4.2.7	The Parent CA authenticates the Sub-CA certificate rekey request in accordance with the CP.		Not Applicable	WebTrust 7.1.7	
3.4.2.8	The Parent CA generates certificates: • using the appropriate certificate profile in accordance with the CP and ISO 9594/X.509 and ISO 15782-1 formatting rules; • with the validity periods formatted in accordance with ISO 9594/X.509, ISO 15782-1 and the CP; and • where extensions are used, with extension fields formatted in accordance with ISO 9594/X.509, ISO 15782-1 and the CP		Not Applicable	WebTrust 7.1.8	
3.4.2.9	The Parent CA signs the Sub-CA or cross certificate with the Parent CA's private signing key		Not Applicable	WebTrust 7.1.9	
3.4.2.10	The Parent CA makes Sub-CA and cross certificates available to relevant entities (e.g., Relying Parties) using an established mechanism (e.g., a repository such as a directory) in accordance with the Parent CA's CP.		Not Applicable	WebTrust 7.1.10	

3.4.2.11	The Parent CA verifies the identity and authority of the entity requesting revocation of a Sub-CA or cross certificate in accordance with the Parent CA's CP.		Not Applicable	WebTrust 7.1.11	
3.4.2.12	The Parent CA updates the Certificate Revocation List (CRL) and other Sub-CA or cross certificate status mechanisms upon certificate revocation in accordance with the Parent CA's CP.		Not Applicable	WebTrust 7.1.12	

3.4.3. Publication and repository responsibilities

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Repositories					
3.4.3.1	The CA shall develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements	1. Verify the CA develops, implements, enforces, and annually updates a Certificate Policy and/or Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements 2. Check the CA makes revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with this Policy 3. Validate CA ensures continued accessibility and availability of its Public Key Certificates and Certificate Revocation Lists in its repository to its subscribers and relying parties	Mandatory	CA Browser Forum 2	
3.4.3.2	The CA shall make revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with this Policy. The Certifying Authority shall ensure the continued accessibility and availability of its Public Key Certificates and Certificate Revocation Lists in its repository to its subscribers and relying parties.		Mandatory	CA Browser Forum 2.1, IT Regulations 3	

Publication of information					
3.4.3.3	The CA shall publicly disclose its Certificate Policy and/or Certification Practice Statement through an appropriate and readily accessible online means that is available on a 24x7 basis.	1. Verify the CA has publicly disclosed its CP and CPS and these are readily accessible online on a 24x7 basis 2. Validate the CP and CPS are structured in accordance with RFC 3647 3. Validate the CA publicly gives effect to the Requirements mentioned in control description (3.4.3.5) and represents that it will adhere to the latest published version 4. Check that the CA hosts test web pages to allow ASPs to test their software with Subscriber 5. Verify the CA hosts separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired	Mandatory	CA Browser Forum 2.2	
3.4.3.4	Effective as of 31 May 2018, the Certificate Policy and/or Certification Practice Statement must be structured in accordance with RFC 3647. Prior to 31 May 2018, the Certificate Policy and/or Certification Practice Statement must be structured in accordance with either RFC 2527 or RFC 3647. The Certificate Policy and/or Certification Practice Statement must include all material required by RFC 3647 or, if structured as such, RFC 2527.		Mandatory	CA Browser Forum 2.2	
3.4.3.5	The CA shall publicly give effect to these Requirements and represent that it will adhere to the latest published version. The CA may fulfill this requirement by incorporating these Requirements directly into its Certificate Policy and/or Certification Practice Statements or by incorporating them by reference using a clause such as the following (which must include a link to the official version of these Requirements): [Name of CA] conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.		Mandatory	CA Browser Forum 2.2	
3.4.3.6	The CA shall host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root		Mandatory	CA Browser Forum 2.2	

	Certificate. At a minimum, the CA shall host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired				
Access controls on repositories					
3.4.3.7	The CA shall make its Repository publicly available in a read-only manner	1. Check that the CA's repository is publically available in read only format		CA Browser Forum 2.3	

3.4.4. Certificate, crl and oscp profiles

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Certificate profile					
3.4.4.1	Effective September 30, 2016, CAs shall generate non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.	1. Verify CAs generates non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG. 2. For sample Certificates, check the following: a. Certificates is of type X.509 v3 b. basicConstraints extension appears as a critical extension c. basicConstraints extension is set true	Mandatory	CA Browser Forum 7.1	
3.4.4.2	Certificates must be of type X.509 v3.		Mandatory	CA Browser Forum 7.1.1	
3.4.4.3	basicConstraints - This extension must appear as a critical extension. The CA field must be set true. The pathLenConstraint field should NOT be present.		Mandatory	CA Browser Forum 7.1.2.1	

3.4.4.4	keyUsage - This extension must be present and must be marked critical. Bit positions for keyCertSign and cRLSign must be set. If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit must be set.	d. pathLenConstraint field is not present e. keyUsage extension is present and marked critical f. Bit positions for keyCertSign and cRLSign are set g. digitalSignature bit is set, If the Root CA Private Key is used for signing OCSP responses h. certificatePolicies and extendedKeyUsage are not present	Mandatory	CA Browser Forum 7.1.2.1	
3.4.4.5	certificatePolicies - This extension should NOT be present		Mandatory	CA Browser Forum 7.1.2.2	
3.4.4.6	extendedKeyUsage - This extension must NOT be present		Mandatory	CA Browser Forum 7.1.2.1	
CRL Profile					
3.4.4.7	CA shall make a full and complete CRL available to the OCSP Responders	1. Check that the CA has made the full and complete CRL available to the OCSP responder	Mandatory	X.504 Policy 7.2.1	
OCSP Profiles					
3.4.4.8	OCSP requests and responses shall be in accordance with RFC 2560	1. Verify the OCSP requests and responses are in accordance with RFC 2560	Mandatory	X.504 Policy 7.3	

3.5. Identity Verification Controls

3.5.1. Naming

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Naming					
3.5.1.1	The CAs shall generate and sign certificates containing an X.500 Distinguished Name (DN) in the Issuer and in Subject fields. Subject Alternative Name may also be used, if marked non-critical.	1. Verify the CA generates and signs certificates containing an X.500 Distinguished Name (DN) in the Issuer and in Subject fields 2. Conduct walkthrough to check the following on sample basis: a. Names used in the certificates identify the person or object to which they are assigned in a meaningful way. b. All DNs and associated directory information tree accurately reflect organizational structures. c. CA and subscriber certificates do not contain anonymous or pseudonymous identities d. Rules for interpreting name forms are in accordance with applicable Standards e. Name uniqueness of Root CA, licensed CA and SubCA is	Mandatory	X.509 Policy 3.1.1, CA Browser Forum 3.1.1	
3.5.1.2	The certificates issued pursuant to CP are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the person or object to which they are assigned in a meaningful way.		Mandatory	X.509 Policy 3.1.2, CA Browser Forum 3.1.2	
3.5.1.3	All DNs and associated directory information tree shall accurately reflect organizational structures.		Mandatory	X.509 Policy 3.1.2, CA Browser Forum 3.1.2	
3.5.1.4	CA and subscriber certificates shall not contain anonymous or pseudonymous identities.		Mandatory	X.509 Policy 3.1.3, CA Browser Forum 3.1.3	
3.5.1.5	Rules for interpreting name forms shall be in accordance with applicable Standards		Mandatory	X.509 Policy 3.1.4, CA Browser	

		enforced f. CCA resolves name collisions, check by identifying cases of name collisions that were encountered and the process followed to resolve the same		Forum 3.1.4	
3.5.1.6	Name uniqueness of Root CA, licensed CA and SubCA shall be enforced		Mandatory	X.509 Policy 3.1.5, CA Browser Forum 3.1.5	
3.5.1.7	The CCA shall resolve any name collisions (other than subscribers) brought to its attention that may affect interoperability or trustworthiness		Mandatory	X.509 Policy 3.1.7, CA Browser Forum 3.1.7	

3.5.2. Initial identity validation

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Initial identity validation					
3.5.2.1	In all cases where the party named in a certificate generates its own keys that party shall be required to prove possession of the private key, which corresponds to the public key in the certificate request. For signature keys, this may be done by the entity using its private key to sign a value and providing that value to the issuing CA. The CA shall then validate the signature using the party's public key.	1. Verify using samples, cases where the party named in a certificate generates its own keys that party is required to prove possession of the private key, which corresponds to the public key in the certificate request 2. Validate using samples, cases where the requests for certificates in the name of an organizational user include the user name, organization name, address, and documentation of the existence of the organization 3. Check the CA ensures the applicant's identity information is verified 4. Verify the process documentation and	Mandatory	X.509 Policy 3.2.1, CA Browser Forum 3.2.1	
3.5.2.2	Requests for certificates in the name of an organizational user shall include the user name, organization name, address, and documentation of the existence of the organization. The CA shall verify the information relating to the authenticity of the requesting representative.		Mandatory	X.509 Policy 3.2.2, CA Browser Forum 3.2.2	

3.5.2.3	A CA shall ensure that the applicant's identity information is verified. The CA shall ensure that the applicant's identity information and public key are properly bound. Additionally, the CA shall record the process that was followed for issuance of each certificate. Process information shall depend upon the certificate level of assurance and shall be addressed in the applicable CPS	authentication is done as per description given in control 3.5.2.4	Mandatory	X.509 Policy 3.2.3, CA Browser Forum 3.2.3	
3.5.2.4	The process documentation and authentication requirements shall include the following: • The identity of the person performing the identity verification; • A signed declaration by that person that he or she verified the identity of the applicant; • The applicant shall present one photo ID. The applicant shall also present a document as a proof of residential address. • Unique identifying numbers from the Identifier (ID) of the verifier and from an ID of the applicant; • The date and time of the verification; and • A declaration of identity signed by the applicant using a handwritten signature or equivalent per Indian Laws.		Mandatory	X.509 Policy 3.2.3, CA Browser Forum 3.2.3	
3.5.2.5	For Class 2 and Class 3 certificates, identity shall be established by in-person proofing before the CA, to confirm identities; information provided shall be verified to ensure legitimacy	1. Verify for Class 2 and Class 3 certificates, identity is established by in-person proofing before the CA, to confirm identities 2. Validate CA does not include any non-verified information in the certificates	Mandatory	X.509 Policy 3.2.3, CA Browser Forum 3.2.3	
3.5.2.6	Information that is not verified shall not be included in certificates.		Mandatory	X.509 Policy 3.2.4, CA Browser Forum 3.2.4	

3.5.3. Identification and authentication for revocation request

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Identification and authentication for revocation request					
3.5.3.1	Revocation requests shall be authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated public key, regardless of whether or not the private key has been compromised	1. For sample revocation requests, verify the revocation requests are authenticated 2. Validate CA has a process implemented to suspend/revoke the certificate on verifying the subscriber's identity in case of loss of key	Mandatory	X.509 Policy 3.4, , CA Browser Forum 3.4	
3.5.3.2	In the case of loss of key, CA can suspend/revoke the certificate on verifying the subscriber's identity. In the case where subscriber is not in a position to communicate (death, unconscious state, mental disorder), on receiving such information CA can suspend the certificate and after verification the certificate can be revoked.		Mandatory	X.509 Policy 3.4, CA Browser Forum 3.4	

3.5.4. Identification and authentication for re key requests

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Identification and authentication for re-key requests					
3.5.4.1	The CAs and subscribers shall identify themselves through use of their current Signing Key or by using the initial identity-proofing process	1. Verify CAs and subscribers identify themselves through use of their current Signing Key or by using the initial	Mandatory	X.509 Policy 3.3.1, CA Browser	

		identity-proofing process 2. Validate identity is established through the initial identity-proofing process for each assurance level as per the CP 3. Check on sample basis when current Signing Key is used for identification and authentication purposes, the life of the new certificate does not exceed beyond the initial identity-proofing times specified in the CP		Forum 3.3.1	
3.5.4.2	Identity shall be established through the initial identity-proofing process for each assurance level per the CP		Mandatory	X.509 Policy 3.3.1, CA Browser Forum 3.3.1	
3.5.4.3	When current Signing Key is used for identification and authentication purposes, the life of the new certificate shall not exceed beyond the initial identity-proofing times specified in the table above.		Mandatory	X.509 Policy 3.3.1, CA Browser Forum 3.3.1	

3.5.5. General Guidelines to CAs

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
General					
3.5.5.1	CA shall make sure the following text shall be displayed to the user before submission / signing of DSC application form. *Section 71 of IT Act stipulates that if anyone makes a misrepresentation or suppresses any material fact from the CCA or CA for obtaining any DSC such person shall be punishable with imprisonment up to 2 years or with fine up to one lakh rupees or with both.*	1. Validate the text mentioned in control 3.5.5.1 is displayed to the user before submission/ signing of DSC application form 2. Check eKYC information collected from applicant is not shared by CA and comply to all the provisions of IT Act for protecting the information specifically Rule 33 and 34 of IT CA Rules 3. Check that subscriber's registered information with CA such as video, photo, ID cards, phone number, PAN/Aadhaar, other information	Mandatory	Identity Verification Guidelines (IVG) Section 1.1	
3.5.5.2	The eKYC information collected from applicant shall not be shared by CA and comply with all the provisions of IT Act for protecting the information specifically Rule 33 and 34 of IT CA Rules		Mandatory	IVG Sect. 1.1	
3.5.5.3	The subscriber's registered information with CA such as video, photo, ID cards, phone number, PAN/Aadhaar,		Mandatory	IVG Sect. 1.1	

	other information submitted and not a part of certificate in readable form are confidential and its access shall be limited to only authorized CA personnel. Access, sharing, photographic images/video and/or retention of such information by anybody other than CA, as applicable under the provisions of IT Act, shall be liable for penalty for breach of confidentiality and privacy under section 72 of IT Act.	submitted and not a part of certificate in readable form are confidential and its access has been limited to only authorized CA personnel.			
eKYC Account					
3.5.5.4	eKYC account of DSC applicant is mandatory for applying for a DSC or availing eSign service. The verified information held by CA shall be used for issuance of DSC or eSign. For eSign service based on online Aadhaar authentication, eKYC account is not required	Conduct a walkthrough of the e KYC facility and check the following: 1. Take details of issued certificatesand validate on sample basis CA maintains eKYC account of DSC applicant for applying for a DSC or availing eSign services and verified information held by CA is only used for issuance of DSC or providing eSign service. 2. Verifyinformation which is required in DSC application form and not present in the eKYC of applicant has been submitted by the eKYC applicant and verified by CA before activating the eKYC account. 3. Verify • the mobile authentication of applicant is implemented by CA before accessing the web interface for submitting the details for the eKYC account creation. • Inspect the coverage of sessions till completion. • Check whether the CA software accepts	Mandatory	IVG Sect. 1.2	
3.5.5.5	The eKYC account of the DSC applicant shall be created by CA based on eKYC of applicant (Bank, Organisational, PAN and Offline Aadhaar) or a direct verification (Foreign Nationals) . The information which are required in DSC application form and not present in the eKYC of applicant shall be submitted by the eKYC applicant and verified by CA before activating the eKYC account.		Mandatory	IVG Sect. 1.2	
3.5.5.6	Prior to submitting information for the eKYC account creation of an applicant, the CA shall authenticate the applicant using the applicant's mobile number and the same mobile number shall be used in the subsequent authentication also. Upon successful authentication of the applicant, start a new session for all the associated with the eKYC account creation process and continue the session till its completion. Also, the same mobile number should be a part of the eKYC account of the applicant.		Mandatory	IVG Sect. 1.2	

3.5.5.7	For eKYC account creation, CA shall provide the interface only to the applicant. Also, CA shall not provide any provision to submit the applicant's details other than the applicant.	mobile number other than that used for authentication. 4. Examine how CA prevent the access to the web interface for submission of applicant details other than the designated single and dedicated web interface. 5. Validate how CA prevent link based access for the submission of DSC applicant details. 6. Verify CA maintains a logical one account in case the eKYC account holder requires more than one accounts (for e.g personal and organizational), and CA carried out all verification procedures for each eKYC option included and provides an option to the user for selecting the account mode (personal/organizational). 7. The maximum validity of eKYC account is 2 years. The account (with same username, PAN, Mobile) can be extended only through carrying a fresh verification of the applicant. 8. Validate CA rejects the requests for which CA is not able to ascertain the genuineness of the eKYC data submitted by the applicant 9. Verify that CA notifies applicant about subscriber agreement for the use of KYC information for DSC issuance and provides option to accept or reject the same. 10. Verify option provided to applicant to access notifications, history of eSign	Mandatory	IVG Sect. 1.2	
3.5.5.8	The DSC applicant's access to the website of CA for submission of details for eKYC account creation, video verification and Online Aadhaar authentication shall be only through a single & dedicated interface provided by CA and link-based access shall not be permitted for these interfaces.		Mandatory	IVG Sect. 1.2	
3.5.5.9	In case eKYC account holder requires more than one account (fore.g personal and organizational), eKYC account holder must undergo all the verification procedures mentioned for the additional eKYC option. CA should treat both eKYC accounts logically under one eKYC account of the eKYC applicant. The mobile number and PAN can be the same. For user authentication, CA shall provide an option for selecting the account mode (personal/organizational)		Mandatory	IVG Sect. 1.2	
3.5.5.10	The validity of eKYC account shall not be more than 2 years. The account (with same username, PAN, Mobile) can be extended only through carrying a fresh verification of the applicant under these guidelines.		Mandatory	IVG Sect. 1.2	
3.5.5.11	In case CA is not able to ascertain the genuineness of the e-KYC data submitted by applicant, CA shall reject the request		Mandatory	IVG Sect. 1.2	
3.5.5.12	CA shall notify applicant the subscriber agreement for the use of KYC information for DSC issuance by CA on successful authentication by the applicant. The applicant shall have option to accept or reject the same		Mandatory	IVG Sect. 1.2	
3.5.5.13	Applicant shall be able to access notifications, history of eSign transactions, account modification etc., activation & deactivation info and also manage any queries/disputes through eKYC account maintained by CA.		Mandatory	IVG Sect. 1.2	

3.5.5.14	Applicant shall have an option to activate, deactivate and close account at any point.	transactions, account modification etc., activation & deactivation info and also manage any queries/disputes through eKYC account. 11. Verify an option to activate, deactivate and close account is available for the applicant 12. Appropriate fraud detection and preventive security mechanisms have been implemented. Specifically check page capturing PIN is free from the threat like phishing attacks, malicious plug-in, hijack clicks/key strokes etc 13. Check CA has approval of CCA for maintaining eKYC for applicants for particular mode of eKYC (Aadhaar offline, Aadhaar online, Organizational KYC, Banking, PAN eKYC and eKYC for foreign applicants) 14. Verify the format of the eKYC account ID be of the format: id@id-type.esp-id. The allowed eKYC account id type are username, Mobile and PAN. The PIN shall be created along with eKYC account ID. eKYC account user ID change is not allowed after creation. 15. Verify that PIN reset shall be with mobile OTP and email verification. In the absence of email, it shall be mobile OTP and video verification. In the case of banking where email is not captured earlier, the PIN reset shall be allowed only after successful matching of fresh eKYC with the registered eKYC details.	Mandatory	IVG Sect. 1.2	
3.5.5.15	Appropriate fraud detection and preventive security mechanisms shall be implemented against enrollment frauds. Specifically CA should make sure that the page capturing PIN shall be free from the threat like phishing attacks, malicious plug-in, hijack clicks/key strokes etc		Mandatory	IVG Sect. 1.2	
3.5.5.16	CA shall have approval of CCA for maintaining eKYC account for applicants.		Mandatory	IVG Sect. 1.2	
3.5.5.17	The format of the eKYC account ID shall be of the format: id@id-type.esp-id. The allowed eKYC account id type are username, Mobile and PAN. The PIN shall be created along with eKYC account ID. eKYC account user ID change is not allowed after creation.		Mandatory	IVG Sect. 1.2	
3.5.5.18	The PIN reset shall be with mobile OTP and email verification. In the absence of email, it shall be mobile OTP and video verification. In the case of banking where email is not captured earlier, the PIN reset shall be allowed only after successful matching of fresh eKYC with the registered eKYC details.		Mandatory	IVG Sect. 1.2	

DSC Application Form					
3.5.5.19	DSC application form shall be generated by CA based on the verified information held in eKYC account maintained by CA after obtaining the two-factor authentication of the applicant.	1. Validate DSC application form can be generated by CA based on the verified information held in eKYC account maintained by CA after obtaining the two-factor authentication of the applicant. 2. Validate the electronic signature of the applicant in the DSC application form has been affixed using the eSign service of the CA. 3. Validate power of attorney is not allowed for the purpose of DSC application to CA and issuance of DSC.	Mandatory	IVG Sect. 1.3	
3.5.5.20	The electronic signature of the applicant in the DSC application form shall be affixed using the eSign service of the CA.		Mandatory	IVG Sect. 1.3	
3.5.5.21	Power of attorney is not allowed for the purpose of DSC application to CA and Issuance of DSC		Mandatory	IVG Sect. 1.3	
Mandatory Information in the DSC application Form					
3.5.5.22	Name, address (residence/organisation), email, Mobile Number, PAN/Aadhaar no (Last four digit), Photo, Date, type certificate (personal/organisational), signature of applicant and Class are mandatory in the eKYC account and DSC application form for issuance of DSC. Email is optional for eKYC account to be created only for the purpose of eSign.	1. Verify for mandatory information i.e., Name, address (residence/organisation), email, Mobile Number, PAN/Aadhaar no (Last four digit), Photo, Date, type certificate (personal/organisational), signature of applicant and Class in the eKYC account and DSC application form for issuance of DSC. 2. Verify either PAN or Aadhaar Number taken for all categories of DSC applicants.	Mandatory	IVG Sect. 1.4	
3.5.5.23	For all categories of DSC applicants, it is mandatory to provide either PAN or Aadhaar Number.		Mandatory	IVG Sect. 1.4	
Name					
3.5.5.24	The name of the DSC applicant shall be same as the name in respective eKYC	1. Validate name of the DSC applicant is same as the name in respective eKYC	Mandatory	IVG Sect. 1.5	

3.5.5.25	For proof of Identity, copy of at least one photo Identity proof bearing name of the applicant , as mentioned in the Annexure IV , shall be submitted	2. Verify proof of Identity, copy of at least one photo Identity proof bearing name of the applicant as per IVG has been collected.	Mandatory	IVG Sect. 1.5	
Address					
3.5.5.26	The address of the DSC applicant shall be residential or organisational.	1. Validate residential or organizational address be provided 2. Verify address proof of DSC applicant as per IVG collected.	Mandatory	IVG Sect. 1.6	
3.5.5.27	For address proof, the applicable list of documents are given in Annexure IV		Mandatory	IVG Sect. 1.6	
Mobile Number					
3.5.5.28	Mobile Number of applicant is a pre-requisite for creation of eKYC account by CA for applicant.	1. Mobile number is mentioned as mandatory pre-requisite for creation of eKYC account by CA 2. Validate CA send a SMS OTP for the proof of possession of mobile number and the same is verified by capturing through the interface provided by CA. Such verification OTP is random, communicated only to the mobile number under verification, and is not based on any predetermined parameters to avoid the compromise.	Mandatory	IVG Sect. 1.7	
3.5.5.29	For the proof possession of mobile number, CA shall send a SMS OTP and the same shall be verified by capturing through the interface provided by CA. Such verification OTP shall be random, communicated only to the mobile number under verification, and shall not be based on any predetermined parameters to avoid the compromise.		Mandatory	IVG Sect. 1.7	
Email Address					
3.5.5.30	Email id of the applicant is mandatory for issuance of DSC based on the eKYC account activated by CA. Email id is optional for the eKYC accounts activated only for the purpose of eSign	1. Validate email id of the applicant is mandatory for issuance of DSC based on the eKYC account activated by CA. 2. Validate unique email id for each	Mandatory	IVG Sect. 1.8	

3.5.5.31	CAs shall put in measures to ensure that email addresses that are included in Digital Signature Certificates (DSC) are unique to the DSC applicant.	applicant are included in DSC 3. Validate CA send an email OTP or challenge response or verification URL to the email of DSC applicant and verify response through the interface provided by CA. Such verification factors is random, communicated only to the email ID under verification, and not based on any predetermined parameters to avoid the compromise. 4. Verify CA preserve the proof of verification with their digital signature 5. Validate that no disposable email is accepted by CA.	Mandatory	IVG Sect. 1.8	
3.5.5.32	Provisions can be made for issuance of multiple DSC with a single email Id where it is established that these multiple DSCs are being issued to same DSC applicant.		Mandatory	IVG Sect. 1.8	
3.5.5.33	For email verification, CA shall send an email OTP or challenge response or verification URL to the email of DSC applicant and verify response through the interface provided by CA. Such verification factors shall be random, communicated only to the email ID under verification, and shall not be based on any predetermined parameters to avoid the compromise. CA should preserve the proof of verification with their digital signature		Mandatory	IVG Sect. 1.8	
3.5.5.34	No disposable email (fast temporary email without registration) shall be accepted by CA.		Mandatory	IVG Sect. 1.8	
PAN					
3.5.5.35	CA shall electronically verify the PAN number through the eKYC service provided by Income tax and accept only if the verification is successful, the name of the PAN holder and Date of Birth match and also the Aadhaar seeding status is operative. CA shall preserve the proof of verification with their digital signature.	1. Validate CA electronically verifes the PAN number with Income tax database through eKYC service and accept only if the verification is successful, the name of the PAN holder and Date of Birth match and also the Aadhaar seeding status is operative. 2. Verify CA preserve the proof of verification with their digital signature	Mandatory	IVG Sect. 1.9	
Verification					
3.5.5.36	Verification is the electronic verification of the identity and information submitted by eKYC applicant for the purpose of creating an eKYC account with CA for eSign or DSC issuance.	1. Validate verification for the purpose of creating an eKYC account with CA for eSign or DSC issuance is the electronic verification of the identity and	Mandatory	IVG Sect.1.10	

3.5.5.37	CA shall allow only the automatic population of digitally signed information received from source of eKYC like Aadhaar or Bank in the electronic application form. The information received from the other source (like PAN and GSTN) shall be used only for cross verifying the information submitted by the applicant in the interface provided by CA.	information submitted by eKYC applicant. 2. Validate CA allow only the automatic population of digitally signed information received from source of eKYC . 3. The information received from the other source (like PAN and GSTN) is only used for cross verifying the information submitted by the applicant in the interface provided by CA.	Mandatory	IVG Sect.1.10	
Physical verification/Video verification					
3.5.5.38	The physical verification of DSC applicant shall be carried out using online interactive video verification directly by CA as per Annexure VI or by online Aadhaar eKYC Biometric Authentication	1. Validate physical verification of DSC applicant is carried out using online interactive video verification directly by CA as per Annexure VI of IVG or by online Aadhaar eKYC Biometric Authentication 2. Verify CA checks any indication of alteration or falsification in video recording	Mandatory	IVG Sect.1.11	
3.5.5.39	CA shall check any indication of alteration or falsification in video recording		Mandatory	IVG Sect.1.11	
Documents verification					
3.5.5.40	In lieu of the attestation of documents exists in the paper-based DSC application; CA shall verify the uploaded supporting documents using direct online interactive video verification of the original documents held by the DSC applicant or online verification from source of issuance of the documents	1. Validate CA verifies the uploaded supporting documents using direct online interactive video verification of the original documents held by the DSC applicant or online verification from source of issuance of the documents 2. Verify on sample basis originals of the identity and address proof has been verified during the video verification, if	Mandatory	IVG Sect.1.12	
3.5.5.41	If applicable, the originals of the identity and address proof shall be verified during the video verification.		Mandatory	IVG Sect.1.12	

3.5.5.42	The video verification of the original documents shall be carried out as per Annexure VI	applicable as per IVG 3. Validate video verification of the original documents is carried out by CA as per Annexure VI of IVG	Mandatory	IVG Sect.1.12	
3.5.5.43	Using online verification, CA shall verify the authenticity of the document submitted and the digitally signed proof of the online verification shall be maintained.	Verify whether CA is verifying the authenticity of the documents through online process and proof retained	Mandatory	IVG Sect.1.12	
3.5.5.44	For the digitally signed documents received from the issuing authority or the same fetched through Digi locker by CA, further verification of supporting documents through video is not required.	Verify whether the documents fetched through Digilocker bearing the electronic signature of the issuer	Mandatory	IVG Sect.1.12	
Key pair generation/Storage					
3.5.5.45	CA shall issue class 3 level individual signing certificate (both Personal & organizational) to the private key generated on a FIPS 140-2 level 2/3 validated Hardware cryptographic module (crypto tokens) with both Class 2 and Class 3 OID in the policy field. CA shall not issue class 2 level individual Signing certificates alone instead CA shall issue Class 3 individual signing certificates with a combination of both class 2 & class 3 certificates by including Class 2 OID in the Class 3 certificates. Class 3 individual signing certificates shall be qualified as both class 2 & class 3 individual signing certificates.	1. Verify CA not issues any class 2 level individual Signing certificates (both Personal & organizational) alone instead CA issues Class 3 individual signing certificates with a combination of both class 2 & class 3 certificates by including Class 2 OID in the Class 3 certificates. 2. Verify CA has procedure in place to ensure that no class 3 level individual signing certificate are issued in cases where the key pair has not been generated on a FIPS 140-2 level 2/3 validated Hardware cryptographic module (crypto tokens). 3. Validate CA follows options mentioned under control **3.5.5.41for** protection of crypto token against "PIN reset compromise 4. Verify a list of approved cryptographic device manufacturers / suppliers and information relating to their FIPS 140-2 Level 2/3 validated tokens is published on	Mandatory	IVG Sect.1.13	
3.5.5.46	CA shall put procedure in place to ensure that no Class 3 individual Signing DSCs are issued in cases where the key pair has not been generated on a FIPS 140-2 level 2/3 validated Hardware cryptographic module (crypto tokens).		Mandatory	IVG Sect.1.13	
3.5.5.47	For protection of crypto token against "PIN reset compromise , a) CA shall not support PIN reset procedure for subscriber's crypto token, unless the crypto token is re-initialized / formatted. For the convenience of DSC applicant on such scenarios, CA shall re-issue the		Mandatory	IVG Sect.1.13	

	certificate for the remaining period of validity of the certificate. Such re-issuance shall be provided free of cost, at least once per certificate. CA may provide additional re-issuance which may be charged extra by CA to the user. CA shall carryout such re-issuance only after authentication of the subscriber. b) From 01.04.2023 onwards, CA shall not allow the download of DSC to crypto token having default password.	the website of the CA. 5. Check in case of Class 1 certificate, if the subscriber prefers to use software Cryptographic module, the corresponding risk is made known to the DSC applicant and an undertaking is taken to the effect that the DSC applicant is aware of the risk associated with storing private keys on a device other than a FIPS 140-2 Level 2/3 validated cryptographic module. 6. Verify the software is provided by CA for key generation and CA certify the public key only if the key pair generation is carried out using the same software provided by them. 7. CA shall verify the software provided for the key-pair generation is audited as per the Security guidelines 8. Verify the CA software not allow the download of DSC to crypto token having default password. 9. Check CA follows Terms and conditions for use of HSM for class 3 Organisational Person DSCs on FIPS 140-2 level 2/3 certified HSMs as per annexure II of IVG in case of DSC (Class 3) being applied for by Organisation person and key-pairs are proposed to be generated on HSM. Verify whether CA has verified the key attestation by HSM and the already issued cerificates to the key pair generated on the HSM			
3.5.5.48	A list of approved cryptographic device manufacturers / suppliers and information relating to their FIPS 140-2 Level 2/3 validated tokens must be published on the website of the CA.		Mandatory	IVG Sect.1.13	
3.5.5.49	In respect of Class 1 certificate, if the subscriber prefers to use software Cryptographic module, the corresponding risk shall be made known to the DSC applicant and an undertaking shall be taken to the effect that the DSC applicant is aware of the risk associated with storing private keys on a device other than a FIPS 140-2 Level 2/3 validated cryptographic module.		Mandatory	IVG Sect.1.13	
3.5.5.50	For personal signing certificates, subscribers' key generation shall be strictly using the software provided by CA and shall not be generated outside of the crypto device.				
3.5.5.51	Terms and conditions for use of HSM for class 3 Organisational Person DSCs on FIPS 140-2 level 2/3 certified HSMs shall be as per annexure II. For individual signing certificates, the CA should verify the validity of the Key attestation by HSM and also verify no certificates with different DN have been issued earlier.		Mandatory	IVG Sect.1.13	
Invoice/Acknowledgement					

3.5.5.52	To ensure there is no tax evasion in the DSC issuance service a) For Personal Digital Signature Certificate issuance (Class 3), CA shall generate, issue and send the GST tax invoice to the DSC applicant through email. b) For Organizational Person Digital Signature Certificate issuance (Class 2 and Class 3), CA shall generate, issue and send the GST tax invoice to the DSC applicant or applicant's organization through email. c) Except in the case of organisation person certificate through the organization, GeM, tender, person authorized by the organization, etc, CA shall not accept the payment towards DSC issuance in advance, directly or indirectly, causing financial liability in any manner, before the mobile authentication of the DSC applicant. CA shall carry out periodic reconciliation of invoices with corresponding DSC issued to subscribers. The copy of the TAX invoice shall be preserved by CA. The applicant's interface software should be integrated with the payment gateway for accepting fees from DSC applicants for the issuance of certificates.	1. Check Tax invoices are issued by CA as per the requiremenrs 2. Check CA has provided option for the online payment 3. Check the reconciliation report generated by CA. 4. Verify the TAX invoices have been preserved by CAs 5. Verify the proof of sending TAX invoice via email to the DSC applicant.	Mandatory	IVG Sect.1.14	
Subscriber Agreement					
3.5.5.53	CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with the eKYC applicant.	1. Validate CA allows the usage of eKYC service only after having a digitally signed subscriber agreement with the	Mandatory	IVG Sect.1.15	

		eKYC applicant.			
3.5.5.54	For eKYC account creation based on the KYC information source such as Offline Aadhaar KYC, Banking and organisational , the eSign of the subscriber shall be based on the information received from the KYC information source.	2. Validate, for eKYC account creation based on the KYC information source such as Offline Aadhaar KYC, Banking and organisational , the eSign of the subscriber is based on the information received from the KYC information source.	Mandatory	IVG Sect.1.15	
DSC Issuance					
3.5.5.55	DSC shall be issued only up on satisfying the verification requirements specified in the respective eKYC sections in this document. The maximum time limit for the download of DSC shall be 30 days from the date of completion of verification/approval. If the download of DSC is not carried out by the applicant within 30 days, applicable verification requirements specified in the respective eKYC sections in this document shall be carried out by CA before DSC issuance	1. Validate maximum time limit for the download of DSC is 30 days from the date of completion of verification/ approval. 2. Verify on sample basis, if the download of DSC is not carried out by the applicant within 30 days, applicable verification specified in the respective eKYC sections of IVG is carried out by CA before DSC issuance	Mandatory	IVG Sect.1.16	
Archival					
3.5.5.56	CAs shall preserve the digitally signed documents, proof of verification information, logs etc. as per the requirements mentioned in the Information Technology Act.	1. Check digitally signed documents, proof of verification information, logs etc. are preserved and archived by CA as per Act. 2. Check on sample basis archival information of the Digital Signature Certificate is available for 7 years from the date of its expiry.	Mandatory	IVG Sect.1.17	
3.5.5.57	Archival of information shall be 7 years from the date of expiry of the Digital Signature Certificate		Mandatory	IVG Sect.1.17	
Role of Trusted person					
3.5.5.58	CA shall make sure that the CA Verification Officer's roles and responsibilities are not be delegated or controlled by anyone else.	1. Obtain the list of personnel having CA trusted roles 2. Verify the CA Verification Officer's roles	Mandatory	IVG Sect.1.18	

3.5.5.59	All the CA Verification Officers shall be exclusive employees of the CA and shall not have any current or planned financial, legal or other relationship with any external entity facilitating DSC issuance.	and responsibilities are not being delegated or controlled by anyone else. 3. Check all the CA Verification Officers are exclusive employees of the CA and do not have any current or planned financial, legal or other relationship with any external entity facilitating DSC issuance. 4. Check only CA trusted persons/ Verification Officers approves and certify each account information including name timestamp etc. using their own digital signature 5. Check CA has sufficient Verification Officers by gauging the max. approval done in a day corresponding to the number of Verification Officer involved. 6. Submit the List of trusted personnel of CA to CCA.	Mandatory	IVG Sect.1.18	
3.5.5.60	CA trusted person/Verification Officer shall approve and certify each account information including name timestamp etc. using their own digital signature		Mandatory	IVG Sect.1.18	
Special purpose certificates					
3.5.5.61	Apart from the details required for creation of eKYC account, the additional details shall be verified by CA in accordance with the type of special purpose certificate.	1. Validate, apart from the details required for creation of eKYC account, the additional details is verified by CA in accordance with the type of special purpose certificate. 2. Validate that only organisational persons are allowed to apply for special purpose certificate.	Mandatory	IVG Sect.1.19	
3.5.5.62	Only organisational persons are allowed to apply for special purpose certificate.		Mandatory	IVG Sect.1.19	
Encryption Certificate					
3.5.5.63	For encryption certificates, CA shall provide key escrow facility, where key pair is securely stored and managed by CA. The key shall be retrievable again by the DSC applicant at any point of time, even after expiry of the certificate. This shall be retained by CA for minimum of	1. Check for encryption certificates, CA provides key escrow facility, where key pair is securely stored and managed . 2. Check the key is retrievable again by the DSC applicant at any point of time, even	Mandatory	IVG Sect.1.20	

	7 years from the expiry of the certificate. CA shall allow the download of the escrowed key only after a successful video verification of the applicant.	after expiry of the certificate. 3. Check escrowed key is retained by CA for minimum of 7 years from the expiry of the certificate from Jan 01, 2021 onwards. 4. Check CA allows the download of the escrowed key only after a successful video verification of the applicant. 5. Validate CA allows subscriber to download encryption keys and certificates for preservation, also.			
3.5.5.64	The encryption keys and certificates shall be preserved by subscriber also.		Mandatory	IVG Sect.1.20	
First factor Authentication					
3.5.5.65	The first factor authentication to eKYC account shall be PIN	1. Validate first factor authentication to eKYC account is PIN			
Second factor Authentication					
3.5.5.66	The second factor authentication can be SMS-OTP or the other authentication mode specified in the eSign API	1. Validate second factor authentication is SMS-OTP or the other authentication mode specified in the eSign API 2. Validate eKYC account is activated using PIN and OTP only.	Mandatory	IVG Sect.1.21	
3.5.5.67	The eKYC account shall be activated using PIN and OTP. Subsequently other authentication can be used in place of OTP however OTP shall be retained as a fallback option.		Mandatory	IVG Sect.1.21	
SMS-OTP					
3.5.5.68	CA shall always send OTP to eKYC account holder with PURPOSE relevant to the authentication seeking for. OTP should be a newly generated random number for each transaction.	1. Validate CA always send OTP to eKYC account holder with PURPOSE relevant to the authentication seeking for 2. Verify whether the OTP is a newly generated random number for each transaction. 3. Validate OTP is sent only to the verified	Mandatory	IVG Sect.1.23	
3.5.5.69	OTP shall be sent only to the verified mobile number registered in the eKYC account.		Mandatory	IVG Sect.1.23	

		mobile number registered in the eKYC account.			
Registration Authorities(RAs)					
3.5.5.70	The role of RA is strictly restricted as a business partner. For business-related accounting purposes, the reference code of RA may be included in the DSC applicant's interface.	1. Verify whether CA software has any interface to RA.	Mandatory	IVG Sect.1.24	
Additional Physical verification					
3.5.5.71	The additional physical verification of DSC applicant is optional, however if opted the OID 2.16.356.100.10.2 shall be mentioned in the policy id field of certificate.	1. Verify whether CA has provided option for DSC applicant to opt for additional physical verification? 2. Check the list of authorised person employed by the CA and the mode of employment. 3. Inspect the proof of physical verification carried out by the authorised person.	Mandatory	IVG Sect.1.25	
3.5.5.72	For highest level of assurance, in addition to all the requirements mentioned in this document, an authorised person employed by the CA shall verify the physical presence of DSC applicant and also verify the genuineness of all the documents submitted.		Mandatory	IVG Sect.1.25	
3.5.5.73	The authorised person employed by the CA shall also verify the possession and proof of registration of the mobile number, address proof, identity, ink signature verification, neighborhood enquiry etc. or any additional requirements to eliminate the possibility of impersonation.				

3.5.6. Guidelines for maintaining eKYC account by CA

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Authentication for eKYC Account					
3.5.6.1	CA to verify the applicant one time and issue DSC subsequently based on 2-factor authentication by applicant. The two factor authentication includes the PIN set by the applicant and a second factor, as permitted by the guidelines issued by CCA. (Eg: OTP sent to the verified mobile)	Conduct a walkthrough of the eKYC facility and check the following: 1. CA verifies the applicant and issued DSC based on 2-factor authentication by applicant 2. The two factor authentication includes the PIN set by the applicant and a second factor, as permitted by the guidelines issued by CCA. (Eg: OTP sent to the verified mobile) 3. Subscriber sets the PIN and UserID as mentioned in control 3.5.6.2	Mandatory	Identity Verification Guidelines (IVG) Section 2.1	
3.5.6.2	As a part of KYC, before activation, subscriber shall set PIN and "user ID" a) The eSign Address is in the form "@.". b) The ESP-ids are eMudhra, nCode, CDAC, Capricorn, NSDLeGov etc. id-types are mobile number, PAN and username. c) To ensure ease of use by subscribers, it is recommended that CA shall keep user name limited to few characters. d) CA shall ensure username is unique within their system. For Personal eKYC accounts, the mobile number and PAN shall be unique.		Mandatory	IVG Sect. 2.1	
Aadhaar e KYC					

3.5.6.3	These guidelines are intended to be used to create eKYC account who have Aadhaar Number registered in UIDAI Database.	Check the following: 1. CA obtained approval of CCA for Online Aadhaar eKYC 2. Specify any major non-compliance in the audit period w.r.t UIDAI requirements	Mandatory	IVG Sect. 2.2	
3.5.6.4	CAs are required to follow the requirements specified by UIDAI strictly for eKYC authentication of DSC applicant		Mandatory	IVG Sect. 2.2	
3.5.6.5	As part of the e-KYC process prescribed by UIDAI under Aadhaar Act, the applicant for DSC authorizes CA (through Aadhaar eKYC) to obtain their demographic data along with his/her photograph (digitally signed and encrypted) to CAs for verification.		Mandatory	IVG Sect. 2.2	
Aadhaar online eKYC					
3.5.6.6	This section is allowed as per the OM(File No. 13(6)/2018-EG-II(Pt)), dated 18 Jan 2022 , to use Aadhaar e-KYC authentication by Certifying Authorities under the CCA for issue of Digital Signature Certificate (DSC) under Section 3A of the IT Act along with the e-signature also in compliance with Section 4(4)(b)(i) of the Aadhaar Act, 2016 as amended.	Check the following: 1. CA maintained a copy of OM and it is available to employees for reference. 2. Verify the proof of e-KYC User Agency (KUA) 3. Check all the interface(s) provided by CA for key-in Aadhaar number /VID/OTP etc and verify it is direct or not. 4. Verify & confirm that CA has not provided any option to subscriber for changing the information received through Aadhaar eKYC 5. Check only the already authenticated person can perform aadhaar authentication. 6. Verify the implementation in respect of **Session and re-direction of page** for accessing CA interface page to capture the authentication information. 7. Verify the validation of the CA interface page to capture the authentication information includes parent page	Mandatory	IVG Sect. 2.2.1	
3.5.6.7	CA shall be an authorized e-KYC User Agency (KUA) of Unique Identification Authority of India (UIDAI).		Mandatory	IVG Sect. 2.2.1	
3.5.6.8	In the case of online Aadhaar Biometric/OTP-based eKYC account enrollment, in addition to the UIDAI requirements a) CA shall ensure that the applicant is already authenticated and started a session as per 1.3(3). b) CA shall start a new session and redirect the user to the dedicated CA interface page for capturing authentication information. (Aadhaar no, Biometric or OTP, consent, etc) . c) For each eKYC request to UIDAI, CA should implement validations at the server side which shall include parent page validation, CA OTP, captcha and session validation prior to submitting the request to		Mandatory	IVG Sect. 2.2.1	

	UIDAI. d) Only one Aadhaar authentication shall be processed per one session and session time shall be limited to 10 minutes. e) The Aadhaar Number shall not be displayed on the user interface. Only the Name, Last four digits of the Aadhaar and photo shall be displayed to the DSC applicants. f) CA shall look for any external sites linking to them in an unauthorized manner and consuming the purpose by spoofing or scraping the CA website/application. CA shall ensure that they use captcha implementation or similar security to avoid automated attacks and ensure only a human is doing the process on CA enrolment application steps. The request for Aadhaar authentication shall only be accepted directly from the CA-controlled application.	validation, CA OTP, captcha and session validation prior to submitting the request to UIDAI. 8. Check CA software allow more than one authentication in a single session. 9. Verify the display interface to user and check that only the Name, Last four digits of the Aadhaar and photo is displayed 10. Verify the webpage security parameters 11. Validate the verified information received through online Aadhaar e-KYC is used for creation eKYC account of user. 12. Validate the DSC application form is generated by populating the information received from UIDAI. 13. Verify that a separate authentication is obtained for eSign on the DSC application form(two authentication is mandatory. One for obtaining eKYC data from UIDAI and other for affixing signature of applicant on the application form) 14. Validate CA store the unique UID Token of Aadhaar holder against such eKYC Account. 15. Verify & confirm that email is captured and verified and included in the eKYC account. 16. Validate that CA l allow the usage of eKYC service only after having a digitally signed subscriber agreement with eKYC applicant			
3.5.6.9	Up on receipt of Aadhaar eKYC XML from UIDAI, CA decrypts, validates UIDAI signature, reads and extracts demographic data, and photo.		Mandatory	IVG Sect. 2.2.1	
3.5.6.10	The verified information received through online Aadhaar e-KYC shall be used for creation eKYC account of user.		Mandatory	IVG Sect. 2.2.1	
3.5.6.11	The DSC application form should be generated by populating the information received from UIDAI.		Mandatory	IVG Sect. 2.2.1	
3.5.6.12	The application should be signed by DSC applicant. The verified information received through e-KYC services can be used for obtaining eSign of DSC applicant by CA through a separate user eKYC authentication.		Mandatory	IVG Sect. 2.2.1	
3.5.6.13	If PAN of the applicant is to be included in eKYC account for embedding it in the certificate, CA shall verify the same prior to inclusion in the eKYC account.		Mandatory	IVG Sect. 2.2.1	

3.5.6.14	On successful Aadhaar eKYC Authentication for the eKYC Account, CA shall store the unique UID Token for that Aadhaar holder against such eKYC Account. This shall be used for referring to same user during any re-verification requirements.		Mandatory	IVG Sect. 2.2.1	
3.5.6.15	For DSC issuance, email shall be included in the eKYC account after verification by CA.		Mandatory	IVG Sect. 2.2.1	
3.5.6.16	CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with eKYC applicant.		Mandatory	IVG Sect. 2.2.1	
Aadhaar online eKYC – OTP					
3.5.6.17	Subscriber submits Aadhaar Number and performs provides OTP authentication through the interface provided by CA to UIDAI.	Conduct walkthrough to check the following steps are performed for Aadhaar online eKYC -OTP 1. Subscriber submits Aadhaar Number OTP only through the interface provided by CA 2. CA receive Aadhaar e-KYC XML and create e-KYC account for the applicant op on successful authentication by subscriber,." 3. CA performs interactive video verification (Annexure VI) and also perform a photo match of Aadhaar eKYC photo with the video.. 4. For each DSC issuance, CA check the video verification/Biometric carried out is not older than 2 days.	Mandatory	IVG Sect. 2.2.1.1	
3.5.6.18	Up on Successful authentication, CA receive Aadhaar e-KYC XML and create e-KYC account for the applicant.		Mandatory	IVG Sect. 2.2.1.1	
3.5.6.19	The mobile number is mandatory. CA shall capture the mobile number of the user and carryout verification of Mobile Number.		Mandatory	IVG Sect. 2.2.1.1	
3.5.6.20	CA does interactive video verification (Annexure VI) and also does a photo match of Aadhaar eKYC photo with the video.		Mandatory	IVG Sect. 2.2.1.1	
3.5.6.21	For each DSC issuance, video verification shall have been carried out within last 2 days. The in-person verification can also be substituted by Aadhaar Biometric Authentication.		Mandatory	IVG Sect. 2.2.1.1	
Aadhaar online eKYC – Biometric					
3.5.6.22	Subscriber submits Aadhaar Number and performs biometric authentication through the interface provided by CA to UIDAI.	Conduct walkthrough to check the following steps are performed for Aadhaar online eKYC	Mandatory	IVG Sect. 2.2.1.2	

3.5.6.23	Up on successful authentication, CA receives Aadhaar e-KYC XML and creates e-KYC account for applicant.	-Biometric 1. Subscriber submits Aadhaar Number and perform Biometric only through the interface provided by CA 2. CA receive Aadhaar e-KYC XML and create e-KYC account for the applicant op on successful authentication by subscriber. 3. CA captures the mobile number of the applicant and carryout verification of Mobile Number. 4. For each DSC issuance, CA check the Biometric authentication carried out is not older than 2 days. 5. CA verifies the matching face in CA eKYC record/ photo submitted by applicant with face in Aadhaar Photo of the same applicant...	Mandatory	IVG Sect. 2.2.1.2	
3.5.6.24	The mobile number is mandatory. CA shall capture the mobile number of the applicant and carryout verification of Mobile Number.		Mandatory	IVG Sect. 2.2.1.2	
3.5.6.25	For each DSC issuance, Aadhaar eKYC Biometric authentication of applicant shall have carried out within last 2 days and CA should accept only if the face in Aadhaar Photo matches against that in CA eKYC record of same applicant. The in-person verification can also be substituted by interactive video verification (Annexure VI) provided that CA should successfully verifies the matching face in video with the photograph of eKYC record of the same applicant.		Mandatory	IVG Sect. 2.2.1.2	
Aadhaar offline eKYC					
3.5.6.26	Subscriber uploads eKYC XML within CA app/website and provides the "share code/phrase" which is used to encrypt the offline KYC XML.	Conduct walkthrough to check the following steps are performed for Aadhaar offline eKYC 1. Subscriber uploads eKYC XML within CA app/website and provides the "share code/phrase" 2. CA decrypts XML, validates UIDAI signature, reads the Aadhaar eKYC XML, and extracts demographic data, mobile number (when available), and photo. 3. CA uses the mobile number within offline KYC 4. CA captures email for communications, alerts, and PIN reset options. If CA	Mandatory	IVG Sect. 2.2.2	
3.5.6.27	CA decrypts XML, validates UIDAI signature, reads the Aadhaar eKYC XML, and extracts demographic data, mobile number (when available), and photo.		Mandatory	IVG Sect. 2.2.2	
3.5.6.28	CA shall accept the mobile number within offline KYC only, no changes are allowed.		Mandatory	IVG Sect. 2.2.2	
3.5.6.29	For issuance of DSC, CA captures email for communications, alerts, and PIN reset options and it must be verified.		Mandatory	IVG Sect. 2.2.2	
3.5.6.30	If PAN of the applicant is to be included in eKYC account for embedding it into the certificate, CA shall verify the same prior to inclusion in the eKYC account.		Mandatory	IVG Sect. 2.2.2	

3.5.6.31	Subscriber sets up initial PIN and user ID.	captures email, it must be verified by sending an OTP to email. 5. If PAN of the applicant is to be included in eKYC account for embedding it into the certificate, check CA verifies the same prior to inclusion in the eKYC account. 6. Subscriber sets up initial PIN and user ID. 7. CA does interactive video verification as per IVG and also does a photo match of Aadhaar eKYC photo with the video 8. Verify video verification has been carried out by CA within last 2 days of DSC issuance 9. CA allows the usage of eKYC service only after having a digitally signed subscriber agreement with eKYC applicant.	Mandatory	IVG Sect. 2.2.2	
3.5.6.32	CA does interactive video verification (Annexure VI) and also does a photo match of Aadhaar eKYC photo with the video.		Mandatory	IVG Sect. 2.2.2	
3.5.6.33	For each DSC issuance, video verification shall have carried out within last 2 days		Mandatory	IVG Sect. 2.2.2	
3.5.6.34	CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with eKYC applicant.		Mandatory	IVG Sect. 2.2.2	
Organisational KYC for Organisational Person Certificates					
3.5.6.35	For organisational person certificate, the Organization Name (O Value) in the certificate shall match the organization name and also in compliance with naming convention specified CCAIOG	1. Validate for organisation person certificate, Organization Name (O Value) in the certificate matches the organization name and also in compliance with naming convention specified CCAIOG 2. Validate minimum requirements for issuance of DSC by CA to organization person is as per control 3.5.6.13 3. Verify on sample basis CA carries out verification of the existence of organization & authorized signatory of the organization as per IVG.	Mandatory	IVG Sect. 2.3	
3.5.6.36	The minimum requirements for Issuance of DSC to organisation person include: a) eKYC account of Applicant b) Applicant ID Proof or Proof of individuals association with organisation c) Letter of Authorization by Organization to Authorized Signatory for self authorisation and also to other DSC applicants. d) eKYC account of Authorized Signatory and		Mandatory	IVG Sect. 2.3	

	authorization to DSC applicant e) Proof of existence of organization	4. Validate all the information submitted by eKYC applicant for eKYC account has to be digitally signed by authorized signatory. 5. Check CA follows criteria for the eligibility of government organisation and its authorised signatory as per IVG 6. KYC of organisational eKYCapplicant has been submitted to CA and CA has carried out the verification. 7. Check eKYC account request include Name, Office address, photo, PAN, mobile no, Organisational ID, email etc. 8. Validate mobile number and PAN of the applicants are mandatory. 9. Validate copy of the organisational ID card and PAN to be provided to CA. 10. Check CA carry out interactive video verification as per Annexure VI of IVG and verifies the photo match of eKYC photo with the video. 11. Check the face in Aadhaar Photo against that in KYC record is verified by CA in the case of online Aadhaar eKYC Biometric Authentication 12. Check CA does original document verification as part of video verification. 13. Check CA activates eKYC account after mobile, email and PAN verification 14. Check CA allows the usage of eKYC service only after having a digitally signed subscriber agreement with eKYC applicant. 15. Check CA provides Organizational eKYC applicant to set up PIN and user			
3.5.6.37	CA shall carry out the verification of the existence of organization & authorised signatory of the organization as per IVG. All the information submitted by eKYC applicant for eKYC account shall be digitally signed by authorised signatory.		Mandatory	IVG Sect. 2.3	
3.5.6.38	The criteria for the eligibility of government organisation and its authorised signatory are given in the annexure V of IVG				
3.5.6.39	KYC of organisational eKYC applicant shall be submitted to CA and CA carryout the verification.		Mandatory	IVG Sect. 2.3	
3.5.6.40	The eKYC account request shall include Name, Office address, photo, PAN, mobile no, Organisational ID, email etc. The mobile number and PAN of the applicants are mandatory. The copy of the organisational ID card and PAN shall also be submitted to CA.		Mandatory	IVG Sect. 2.3	
3.5.6.41	CA shall carry out interactive video verification as per Annexure VI and shall verify the photo match of eKYC photo with the video. The original document verification is also a part of video verification. The in-person verification can also be substituted by Aadhaar eKYC Biometric Authentication provided that CA successfully verifies the face in Aadhaar Photo against that in KYC record.		Mandatory	IVG Sect. 2.3	
3.5.6.42	CA activates eKYC account after mobile, email and PAN verification. CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with eKYC applicant.		Mandatory	IVG Sect. 2.3	
3.5.6.43	CA shall provide Organizational eKYC applicant to set up PIN and user ID upon the authentication by CA.		Mandatory	IVG Sect. 2.3	
3.5.6.44	In case of any change in account holder's status or information, the request for change shall be submitted with the authorization of authorised signatory.		Mandatory	IVG Sect. 2.3	

3.5.6.45	CA shall accept the mobile number within Organisational KYC only, no changes are allowed.	ID upon the authentication by CA. 16. Validate the request for change in account holder's status or information accepted by CA is with the authorization of authorised signatory. 17. Validate CA accepts the mobile number within Organisational KYC only, no changes are allowed. 18. Verify video verification has been carried out by CA within last 2 days of DSC issuance	Mandatory	IVG Sect. 2.3	
3.5.6.46	For DSC issuance, the video verification shall have carried out within last 2 days		Mandatory	IVG Sect. 2.3	
Verification of Authorised Signatory					
3.5.6.47	The scanned copy of the documents for existence of organization & authorization to authorized signatories as per Annexure I of IVG shall be submitted to CA and the originals shall be verified during video verification.	For verification of authorised signatory check the following: 1. CA accepts the scanned copy of the documents for existence of organization & authorization to authorized signatories as per IVG and verifies the originals during video verification. 2. The verification of authorised signatory is followed as per steps 4-7 of 2.3.1 of IVG 3. The proof of verification for the following are maintained by CA - Secondary verification like face-to-face interaction/web site reference/ call to organizational telephone numbers to confirm the organizational identity of authorised person. 4. Validate CA creates eKYC account after successful confirmation of organization identity of authorized person and DSC/eKYCaccount of authorized	Mandatory	IVG Sect. 2.3.1	
3.5.6.48	The steps 4-7 of 2.3 shall be followed for the verification prior to the eKYC account creation.				
3.5.6.49	CA shall also carryout secondary verification like face-to-face interaction/web site reference/call to organizational telephone numbers to confirm the organizational identity of authorised person and the proof of the verification shall be maintained.		Mandatory	IVG Sect. 2.3.1	
3.5.6.50	Upon successful confirmation of organizational identity of authorised person, CA shall create an eKYC account and may issue DSC to authorised signatory. The DSC/eKYC Account of the authorized signatory shall be registered with CA and shall be mapped with the name of the verified organisation. Subsequently all the information submitted by eKYC applicant for eKYC account shall be digitally signed by authorised signatory. The DSC of the authorised signatory shall be asserted with OID 2.16.356.100.10.3 in the policy id field along with policy id for class of certificate		Mandatory	IVG Sect. 2.3.1	

3.5.6.51	In case the company is a single director company with no other authorized signatories, or a proprietorship organization, it can be considered for self-authorization, provided that Information is verified in MCA website. In case of proprietorship organization where applicant himself/herself is the proprietorship, self-authorization / no authorization is required.	signatory has been mapped with the name of the verified organisation. 5. The certificate to authorised signatory is asserted with OID 2.16.356.100.10.3. 6. Validate CA verifies information on MCA website in case the company is a single director company with no other authorized signatories, or a proprietorship organization.	Mandatory	IVG Sect. 2.3.1	
Banking eKYC for Banking Customers					
3.5.6.52	This section is applicable only for persons having Banking account and Banks submit the KYC of the Banking Customer to CA directly after obtaining consent and authentication from the customer. The video verification is not mandatory.	1. For banking eKYC for banking customers check the following: 2. CA verifies the source of request and signature of bank prior to accepting KYC information 3. CA has an agreement/undertaking with Bank 4. CA carries out verification of existence of Bank , authorized signatory's identity as mentioned the Identity Verification guidelines 5. DSC used for signature by bank is registered with CA and mapped with the bank ID/Name 6. KYC details should include Name, address, photo, PAN, mobile no, Bank account No, Bank IFSC code. 7. mobile number and PAN of the applicants are mandatory 8. CA allows eKYC applicant to set up PIN and user ID up on the authentication by CA	Mandatory	IVG Sect. 2.4	
3.5.6.53	CA shall verify the source of the request and signature of bank prior to accept KYC information		Mandatory	IVG Sect. 2.4	
3.5.6.54	CA shall have an agreement/undertaking with Bank.		Mandatory	IVG Sect. 2.4	
3.5.6.55	CA shall carry out verification of existence of Bank, authorised signatory's identity as mentioned in Annexure I of the Identity Verification guidelines		Mandatory	IVG Sect. 2.4	
3.5.6.56	The DSC to be used for signature by bank shall be registered with CA and shall be mapped with the bank ID/Name		Mandatory	IVG Sect. 2.4	
3.5.6.57	The KYC details shall include Name, address, photo, PAN/Aadhaar Number, mobile no, Bank account No, Bank IFSC code (if applicable).		Mandatory	IVG Sect. 2.4	
3.5.6.58	The mobile number and PAN/Aadhaar Number(last four digit) of the applicants are mandatory		Mandatory	IVG Sect. 2.4	

3.5.6.59	CA shall allow eKYC applicant to set up PIN and user ID up on the authentication by CA	9. CA activates eKYC account after mobile verification. 10. CA allows usage of eKYC service only after having a digitally signed subscriber agreement with eKYC applicant. 11. If email is not present in the KYC provided by Bank, the same is captured by CA and accepted only after verification 12. CA accepts the mobile number within bank KYC only, no changes are allowed 13. Verify CA received KYC of the account holder from the Bank within last 24 hours for DSC issuance.	Mandatory	IVG Sect. 2.4	
3.5.6.60	CA activates eKYC account after mobile verification. CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with eKYC applicant.		Mandatory	IVG Sect. 2.4	
3.5.6.61	If email is not present in the KYC provided by Bank, the same can be captured by CA and shall accept only after verification.		Mandatory	IVG Sect. 2.4	
3.5.6.62	CA shall accept the mobile number within bank KYC only, no changes are allowed		Mandatory	IVG Sect. 2.4	
3.5.6.63	For each DSC issuance, CA shall have received KYC of the account holder from the Bank within last 24 hours.		Mandatory	IVG Sect. 2.4	
PAN eKYC for Personal Certificates					
3.5.6.64	This section is applicable only for persons who submit the PAN & other KYC information to CA directly. The mobile number, PAN of the applicant and Government ID having address (Annexure IV) are mandatory. The scanned copy of the PAN card and Government ID having address shall be submitted to CA	For PAN eKYC for customer, check the following: 1. The subscriber has submitted the mobile number, PAN and One Government ID with address. 2. CA carries out the verification of Mobile Number and PAN (eKYC) 3. Verify that the mobile number is registered in the name of applicant using sevices provided by the telecom companies. 4. Verify the name of applicant in the banking records using penny drop process 5. CA carries out video verification of applicant as per Annexure VI of IVG. The original PAN and Government ID having address displayed during video verification in a clear readable form.	Mandatory	IVG Sect. 2.5	
3.5.6.65	CA shall carryout verification of Mobile Number and PAN(eKYC).		Mandatory	IVG Sect. 2.5	
	The mobile number should be registered in the name of the eKYC applicant and the same shall be verified by CA through the services provided by Telecom companies. Or CA should use the banking penny drop process to cross verify (exact or reasonable match) the name of the DSC applicant with the name registered in the bank account. The proof of the verification shall be preserved.				
3.5.6.66	The video verification of the applicant shall be carried out by CA as per Annexure VI of IVG. During the video verification, the applicant shall display original PAN card and Government ID having address for cross verification by CA. Both the PAN		Mandatory	IVG Sect. 2.5	

	details and address in the Id captured in the video shall be in a clear and readable form.	6. CA verifies the PAN Number of the applicant through the electronic service provided by Income Tax. CA also verifies the name submitted by applicant is matching with the name in the response received from Income Tax. Also the proof of verification is archived. 7. CA verifies the Government ID having address submitted to CA against the original displayed during the video verification. 8. CA accept only name as in PAN and residential address as in address proof 9. CA activates eKYC account after video, mobile, email and PAN verification. 10. CA allows usage of eKYC service only after having a digitally signed subscriber agreement obtained from eKYC applicant. 11. CA carries out fresh enrollment process to accept any change in account holder's information after activation of account. 12. CA allows eKYC applicant to set up PIN and user ID up on the authentication by CA. 10. Verify video verification has been carried out by CA within last 2 days of DSC issuance.			
3.5.6.67	CA shall electronically verify the PAN number with Income tax database through eKYC service and accept only if the name is matching correctly. The digitally signed proof of the verified response shall be preserved by CA.		Mandatory	IVG Sect. 2.5	
3.5.6.68	CA shall verify the Government ID having address submitted to CA against the original displayed during the video verification.		Mandatory	IVG Sect. 2.5	
3.5.6.69	The eKYC account request shall include Name (as in PAN), residential address (as in address id), photo, PAN, mobile no, email etc.		Mandatory	IVG Sect. 2.5	
3.5.6.70	CA activates eKYC account after mobile, email, PAN and video verification. CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with the eKYC applicant.		Mandatory	IVG Sect. 2.5	
3.5.6.71	In case of any change in account holder's information after activation of account, CA shall carry out fresh enrollment.		Mandatory	IVG Sect. 2.5	
3.5.6.72	CA shall allow eKYC applicant to set up PIN and user ID up on the authentication by CA.		Mandatory	IVG Sect. 2.5	
3.5.6.73	For DSC issuance, video verification shall have carried out within last 2 days		Mandatory	IVG Sect. 2.5	
eKYC for foreign applicants					
3.5.6.74	This section is applicable only for foreign applicants who submit the KYC information to CA directly. An applicant is deemed as foreign applicant if the address (residential or organizational) provided in the DSC application form does not belong to India or identity document submitted is not issued by	For eKYC for foreign applicants, check the following 1) The eKYC applicant has submitted email id, mobile number, photo, scanned copy of proof of identity and scanned copy of	Mandatory	IVG Sect. 2.6	

	authorities under Government of India.	proof of address. 2) For organisational person certificate, a) Scanned copy of organisational id, organisational email id, organisational phone number, organisational address and letter of authorization from organisation are submitted. b) For the proof of organisational existence, publically verifiable and listed/recognized by local government reference of organisation in database/registry have been submitted by the applicant. c) the ekYC account created based on the receipt of letter of request issued from Indian government organisation satisfy the following - The organisation is already registered/empanelled in government organizations of India, - The organizations submit the details of DSC applicant and address proof/existence of organisation. 3) For Personal certificate a) For identity proof, the scanned copy of Passport/Local Govt issued identity/PAN/OCI passport is received from DSC applicant. b) For the address proof the scanned copy of passport/OCI passport/local government issued id having address/bank details having address/any utility bills in the name of applicant issued within three months/ document issued from embassy with residential address is provided by the applicant.			
3.5.6.75	For all categories of applicants, email id, mobile number, photo, scanned copy of proof of identity and scanned copy of proof of address are required to be submitted to CA.		Mandatory	IVG Sect. 2.6	
3.5.6.76	For organisational person certificate, a) Scanned copy of Organisational id, Organisational email id, mobile number, Organisational address and letter of authorization from organisation are required. b) For the proof of organisational existence, publically verifiable and listed/recognized by local government reference of organisation in database/registry shall be provided. c) If the organisation is already registered/empanelled in government organizations of India, then the scanned copy of the letter of request issued from Indian government organisation with the details of DSC applicant can be accepted as address proof/existence of organisation for DSC issuance.		Mandatory	IVG Sect. 2.6	
3.5.6.77	For Personal certificate, a) For identity proof, the scanned copy of Passport/Local Govt issued identity/PAN/OCI passport can be submitted. b) For the address proof the scanned copy of passport/OCI passport/local government issued id having address/bank details having address/any utility bills in the name of applicant issued within three months/ document issued from embassy with residential address can be provided		Mandatory	IVG Sect. 2.6	
3.5.6.78	The video verification shall be carried out by CA as per Annexure VI of IVG. All the originals shall be verified during the video verification. The telephonic verification shall be carried out by direct call to the applicant or SMS OTP verification and the proof of verification shall be recorded.		Mandatory	IVG Sect. 2.6	

	Email shall also be verified by CA.	4) CA carries out the video verification, document verification, telephonic verification and email verification.			
3.5.6.79	For telephonic verification, CA can also verify over telephonic call, where CA originates to or receives the call from the mobile number under verification, and validates the number holder with at least 2 questions establishing relation to DSC application	5) CA activates eKYC account after mobile, email, PAN (if submitted) and video verification. CA obtains a digitally signed subscriber agreement from eKYC applicant.	Mandatory	IVG Sect. 2.6	
3.5.6.80	CA activates eKYC account after mobile, email, PAN (if submitted) and video verification. CA shall allow the usage of eKYC service only after having a digitally signed subscriber agreement with the eKYC applicant.	6) The change in account holder's information after activation of account is not carried out by CA instead CA carry out a fresh enrollment.	Mandatory	IVG Sect. 2.6	
3.5.6.81	In case of any change in account holder's information after activation of account, CA shall carry out a fresh enrollment.	7) A fresh video verification is carries out before each DSC issuance during the validity period of eKYC account. Such video verification for DSC issuance is valid for 2 days.	Mandatory	IVG Sect. 2.6	
3.5.6.82	CA shall allow eKYC applicant to set up PIN and user ID up on the authentication by CA. Except in the case of mobile number verification, OTP can be sent to the email of the eKYC user.		Mandatory	IVG Sect. 2.6	
3.5.6.83	During the validity period of eKYC account, a fresh video verification shall have carried out for each DSC issuance within last 2 days		Mandatory	IVG Sect. 2.6	

3.5.7. Guidelines for issuance of special purpose DSC

SSL Certificate					
Control	Control	Audit Checks	Control Type	References	Compliance

No.					((Yes/No/NA)
3.5.7.1	The issuances of SSL certificates by Licensed CAs are limited only to .IN domain.	For the issuances of SSL certificates by Licensed CAs, check the following :- The issuance of SSL certificates are only to .IN domain The applicants of SSL certificates are from organisation only The Applicant submit the following a. DSC Application Form b. Applicant ID Proof c. Authorization Letter by Organization Authorized Signatory d. Authorized Signatory Proof e. Proof of Organizational Existence	Mandatory	IVG Sect.3.1	
3.5.7.2	Only organisational persons are eligible to apply for SSL certificates on behalf of their organizations.		Mandatory	IVG Sect. 3.1	
3.5.7.3	The applicant (requestor) shall make an application to the CA in a digitally signed application form. This shall contain the domain name(s) to be certified, the Certificate Signing Request (CSR) and the information of the requestor and the organization. This shall be accompanied with necessary supporting documents. The minimum set of documents to be submitted includes: a. DSC Application Form b. Applicant ID Proof c. Authorization Letter by Organization Authorized Signatory d. Authorized Signatory Proof e. Proof of Organizational Existence		Mandatory	IVG Sect. 3.1	
Domain Name Verification					
3.5.7.4	Each value provisioned for subject alternative names (dnsNames) shall undergo domain name verification to prove the ownership / control of the domain by the requestor of the certificate. This shall be accomplished by a) Validating the request by communication to: webmaster@domainname.com, administrator@domainname.com, admin@domainname.com,hostmaster@domainname.com, postmaster@domainname.com, or any email ID listed in the technical, registrant, or administrative contact field of the domain's Registrar record; OR b) Requiring a practical demonstration of domain control (Eg:	For domain verification check the following:- The emails with unique id send to email contain in technical, registrant, or administrative contact field of the domain's Registrar record and the receipt of confirmation Practical demonstration of domain control as mentioned in IVG	Mandatory	IVG Sect. 3.1	
			Mandatory	IVG Sect. 3.1	

	making changes to DNS zone file or adding a unique file / filename on the domain under verification); This is achieved by CA sharing a unique Request Token or a Random Value, valid for a short duration, with the applicant and validating this data against the content of the file name provided or the DNS value (CNAME, TXT or CAA record) of the domain.				
3.5.7.5	In case of wildcard domains, these shall undergo additional checks, to not to wrongly issue, for a domain listed in public suffix list (PSL). If the domain is listed in PSL, the application shall be refused, unless applicant proves ownership of entire domain namespace.	Verify the additional verification in the case of wild card certificate as mentioned in IVG	Mandatory	IVG Sect. 3.1	
3.5.7.6	In case of IP Address, in place of domain name, it shall be verified to have the applicant's control over the IP, by means of (i) change in agreed information in an URL containing the IP address, OR (ii) IP assignment document of IANA or Regional Internet Registry, OR (iii) performing r-DNS lookup resulting in a domain name verified by above procedure.	Verify the procedure followed for applicant's control over the IP as mentioned in IVG	Mandatory	IVG Sect. 3.1	
Organization Person verification					
3.5.7.7	The verification of the identity & address of the applicant shall be made using, any one or more the following a) Identity of the applicant shall be verified by obtaining a legible copy of employment ID and PAN card which noticeably shows the Applicant's face. The copy of the document shall be inspected for any indication of alteration or falsification. A video verification as per the procedure mentioned in Identity Verification Guidelines should be carried out by CA to ascertain the photo match of applicant with the photo presented in the identity proof & DSC application form. The PAN number should be electronically verified with income tax database for matching of name as	1. Check the verification procedure for identity & address of the applicant are followed as per IVG. 2. Examine audit trails of already issued certificates	Mandatory	IVG Sect. 3.1	

	submitted in the DSC application form.				
3.5.7.8	The applicant should submit an authorization letter from the authorized signatory of the organization stating the authorization to apply for SSL certificate. The letter should contain name, photo, designation and address of the applicant. CA may ask additional documents for the confirmation of applicant's affiliation to organization.	Check the procedure followed and audit trails of already issued certificates	Mandatory	IVG Sect. 3.1	
3.5.7.9	CA should confirm that the applicant is able to receive communication to organisational telephone and email.	Check the procedure followed and audit trails of already issued certificates	Mandatory	IVG Sect. 3.1	
Organization Verification					
3.5.7.10	The organization verification includes authorization proof to applicant and existence of organization.	Verify the authorization proof to applicant and existence of organization in compliance with IVG	Mandatory	IVG Sect. 3.1	
3.5.7.11	Sufficient document evidence should be provided by the applicant for proof of authorized signatory	Check the procedure followed by CA meets the requirements	Mandatory	IVG Sect. 3.1	
3.5.7.12	Apart from the organizational person verification, the additional process documentation and authentication requirements for SSL certificate shall include the following: a) The organization owns the domain name, or the organization is given the exclusive right and authority to use the domain name b) Proof that the applicant has the authorization to apply for SSL certificate on behalf of the organization in the asserted capacity.(e.g. Authorization letter from organization to applicant)	Verify the documents to check the compliance	Mandatory	IVG Sect. 3.1	

3.5.7.13	c) The documents/procedure required for proof of existence of organization are as per IVG	Check the documents/procedure required for proof of existence of organization are as per IVG	Mandatory	IVG Sect. 3.1	
Document Signer Certificate					
3.5.7.14	The applicant of Document Signer certificate should be an Organizational person of that Organization. The verification requirements for Document Signer Certificate shall be as per section 2.3 of IVG	1. Verify Document Signer Certificate is issued to an organizational person of the organization only and verification requirements as per section 2.3 of IVG has been followed for issuance of for Document Signer Certificate s. 2. Verify declaration mentioned in control 3.5.7.15 are obtained from subscribers.	Mandatory	IVG Sect. 3.2	
3.5.7.15	The following declarations should be obtained from subscriber in the Document Signer Certificate application form • I hereby declare and understand that Organizational Document Signer Certificate issued to us will be used only for automated signing of documents/information and will not be used in any other context including individual signature. • I hereby declare that necessary controls have been built in software applications to ensure that there is no misuse • I hereby declare and understand that the documents/ messages authenticated using Organizational Document Signer Certificate issued to us is having organizational accountability.		Mandatory	IVG Sect. 3.2	

3.6. Extended Valid Certificate Controls

Not Applicable

3.7. Online Certificate Status Protocol (OCSP) Controls

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Online Certificate Status Protocol (OCSP) Controls					
3.7.1	The CA shall support an OCSP capability using the GET or the POST method for DSC issued under PKI India Hierarchy.	1. Conduct a walkthrough to check the following: a. CA supports an OCSP capability using the GET or the POST method b. CA operates OCSP capability to provide a response time of ten seconds or less c. OCSP responses is signed by an OCSP Responder whose Certificate is signed by the CA	Mandatory	OCSP Guidelines 1	
3.7.2	The CA shall operate OCSP capability to provide a response time of ten seconds or less under normal operating conditions.		Mandatory	OCSP Guidelines 2	
3.7.3	OCSP responses must be signed by an OCSP Responder whose Certificate is signed by the CA or its subCA that issued the Certificate whose revocation status is being checked.		Mandatory	OCSP Guidelines 3	
3.7.4	In the case of certificates issued under special purpose trust chain for SSL and Code Signing, If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder MUST NOT respond with a "good" status. The CA SHOULD monitor the responder for such requests as part of its security response procedures.	1. Validate for sample cases where certificates are issued under special purpose trust chain for SSL and Code Signing, if OCSP responder receives a request for status of a certificate that has not been issued, then the responder does not respond with a "good" status. 2. Check the CA monitors the responder for such requests as part of its security response procedures.	Mandatory	OCSP Guidelines 4	
3.7.5	As part of Interoperability initiative, certificates issued by CAs should have *id-ad-ocspaccesslocation*pointing to the CA's OCSP responder	1. Verify that the certificates issued by the CA have id-ad-ocspaccesslocation pointing to the CA's OCSP responder	Mandatory	OCSP Guidelines 5	
3.7.6	The end to end process must be automated for providing OCSP response to a Relying Party. There must not be any manual intervention unless an error condition arises	1. Verify the process for providing OCSP response is automated 2. Check the following: a. OCSP accepts both signed and	Mandatory	OCSP Guidelines 6	

3.7.7	The OCSP must accept both signed and unsigned OCSP requests	unsigned OCSP requests b. OCSP doesn't use precomputed or Cached responses for certificate Status c. OCSP Responder is able to support nonce extension in request and responses d. CA has modified its CPS to reflect the above requirements e. Scope of the CA audit includes OCSP service operations f. The OCSP responder certificate and subscriber certificates comply with latest version of interoperability Guidelines for Digital Signature Certificates issued under Information Technology Act	Mandatory	OCSP Guidelines 7	
3.7.8	The OCSP must not use precomputed or Cached responses for certificate Status		Mandatory	OCSP Guidelines 8	
3.7.9	The OCSP Responder should be able to support nonce extension in request and responses		Mandatory	OCSP Guidelines 9	
3.7.10	All CAs should modify their CPS to reflect the above requirements and the scope of the CA audit should include OCSP service operations		Mandatory	OCSP Guidelines 10	
3.7.11	The OCSP responder certificate and subscriber certificates shall comply with latest version of interoperability Guidelines for Digital Signature Certificates issued under Information Technology Act		Mandatory	OCSP Guidelines 11	

3.8. SSL Certificate Controls

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
SSL Certificate Controls					
3.8.1	The maximum validity of subscriber certificates shall be limited to 825 days.	Verify the certificate validity is limited to 825 days	Mandatory	Guidelines for SSL 1	
3.8.2	CAs must restrict server authentication certificates to .in domains	Check CA issue certificate to .in domain	Mandatory	Guidelines for SSL 2	
3.8.3	Only authorized organizational persons are entitled to apply for SSL certificates on behalf of an organization	Verify only authorized organizational persons are entitled to apply for SSL certificates on behalf of an organization	Mandatory	Guidelines for SSL 3	

3.8.4	CA shall not issue SSL certificates to any organisational entity unless it owns/controls that domain name.	Verify the organisation owns/controls that domain name.	Mandatory	Guidelines for SSL 4	
3.8.5	Verification of Subject Identity Information shall be as per 4.1 of Identity Verification Guidelines issued by Controller and published at www.cca.gov.in	Verify the verification of Subject Identity Information is performed as per 4.1 of Identity Verification Guidelines issued by Controller and published at www.cca.gov.in	Mandatory	Guidelines for SSL 5	
3.8.6	The CA shall NOT issue a certificate with subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name.	Validate that the CA does not issue a certificate with subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name	Mandatory	Guidelines for SSL 6	
3.8.7	CA shall issue SSL and code signing certificates from the trust chain created specifically for that purpose.	Verify CA issues SSL and code signing certificates from the trust chain created specifically for that purpose	Mandatory	Guidelines for SSL 7	
3.8.8	The special purpose trust chain shall be operated in offline mode at Root CA and CA level	Check the special purpose trust chain is operated in offline mode	Mandatory	Guidelines for SSL 8	
3.8.9	Controller will issue necessary guidelines to conform the latest Baseline requirements of CA Browser forum time to time. The CA shall update the CPS and implement the guidelines immediately	Verify that the CA has updated its CPS based on updates issued by Controller	Mandatory	Guidelines for SSL 9	
3.8.10	The subscriber agreement contains provisions imposing obligations and warranties on the Application relating to the accuracy of information, protection of Private Key, acceptance of certificate, use of certificate, reporting and revocation, termination of use of certificate, responsiveness and acknowledgement & acceptance	For sample subscriber agreements, verify the agreement contains provisions imposing obligations and warranties on the Application	Mandatory	Guidelines for SSL 10	
3.8.11	The CA maintains controls and procedures to provide reasonable assurance that • it screens proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located, when the	Verify that the CA provides reasonable assurance for the elements mentioned in the control description	Mandatory	Guidelines for SSL 11	

	subjectcountryName field is present. • the CA uses an internal database of all previously revoked Certificates and previously rejected certificate requests to identify subsequent suspicious certificate requests.				
3.8.12	The CA maintains controls to provide reasonable assurance that OCSP responses do not respond with a "good" status for Certificates that have not been issued	Verify the procedure of the CA to generate OCSP response to check the procedure has controls to prevent the CA from sending "good" response when the certificates have not been issued	Mandatory	Guidelines for SSL 12	
3.8.13	The CA maintains controls to provide reasonable assurance that it performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) and subjected to maximum of 5000 of the Certificates issued during the period commencing immediately after the previous self-assessment samples was taken.	Verify that the CA provide reasonable assurance that it performs ongoing self-assessments on at least a quarterly basis against a randomly selected sample of at least three percent (3%) and subjected to maximum of 5000 of the Certificates issued during the period commencing immediately after the previous self-assessment samples was taken Obtain report of self-assessment performed recently	Mandatory	Guidelines for SSL 13	
3.8.14	CA shall implement risk detection techniques for every certificate request including subscriber information and CSR with globally acceptable sources like google safe browsing checks, Debian weak keys, other weak key detection techniques, etc.	Verify that the CA has implemented risk detection techniques for every certificate request including subscriber information and CSR with globally acceptable sources like google safe browsing checks, Debian weak keys, other weak key detection techniques, etc	Mandatory	Guidelines for SSL 14	
3.8.15	The CA maintains controls to provide reasonable assurance that the CA operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions	Verify that the CA maintains controls to provide reasonable assurance that the CA operates and maintains its CRL and OCSP capability	Mandatory	Guidelines for SSL 15	

3.8.16	The CA shall maintain audit logs are retained for at least seven years.	Validate CA maintains audit logs for at least seven years	Mandatory	Guidelines for SSL 16	
3.8.17	CA shall not issue certificate to where the domain name is a TLD / ccTLD itself (eg: .in) or second level domains (eg: co.in, firm.in, net.in, org.in, gen.in, etc), or a Public Suffix List (eg: gov.in, nic.in, etc)	Verify that CA not issue certificate to domains where the domain name is a TLD / ccTLD itself (eg: .in) or second level domains (eg: co.in, firm.in, net.in, org.in, gen.in, etc), or a Public Suffix List (eg: gov.in, nic.in, etc)	Mandatory	Guidelines for SSL 17	
3.8.18	Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, the CA must establish and follow a documented procedure that determines if the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix”. If a wildcard would fall within the label immediately to the left of a registry-controlled or public suffix, CAs must refuse issuance unless the applicant proves its rightful control of the entire Domain Namespace.	Verify that CA follows the documented procedure that determines if the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix as per SSL guidelines	Mandatory	Guidelines for SSL 18	
3.8.19	SignedCertificateTimestampList field must be populated with Signed Certificate Timestamp (SCT) returned by Log operators when a valid certificate is submitted to a log.	Verify that SignedCertificateTimestampList field must be populated with Signed Certificate Timestamp (SCT) .	Mandatory	Guidelines for SSL 19	
3.8.20	CA shall perform the CAA record validation (in DNS Zone) and ensure that, it does not limit the issuance to some other CA. In case the domain’s CAA record indicate the issuance authorization to any other CA, the CA shall ensure that the applicant/requestor modifies the CAA record to authorize them or remove the current record / authorization, before processing such requests.	Verify that CA perform the CAA record validation (in DNS Zone) as per SSL guidelines and ensure that, it does not limit the issuance to some other CA.	Mandatory	Guidelines for SSL 20	

3.9. E-Authentication Controls

3.9.1. Requirements for e-authentication using e-KYC Services

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Requirements for e-authentication using e-KYC Services					
3.9.1.1	eSign user should have unique id	1. Validate on a sample basis that each eSign user has an unique Id 2. Verify that the application service provider has gone through the approval process of ESP and has an agreement/undertaking 3. Validate the eSign service provider adheres to e-KYC compliance requirements independently 4. Check the eSign user Account with CA is as per CA eKYC Implementation Requirements	Mandatory	eSign Guidelines 2.1	
3.9.1.2	Application Service Provider should have gone through an approval process of ESP and should have agreement/ undertaking with them.		Mandatory	eSign Guidelines 2.1	
3.9.1.3	eSign Service Provider should adhere to e-KYC compliance requirements independently		Mandatory	eSign Guidelines 2.1	
3.9.1.4	eSign user Account with CA should be as per CA eKYC Implementation Requirements		Mandatory	eSign Guidelines 2.1	

3.9.2. Authentication and DSC Application Form

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)

Authentication and DSC Application Form					
3.9.2.1	The mode of e-authentication should be biometric or OTP or PIN or combination of PIN and OTP in accordance with e-KYC Services	1. Verify the mode of e-authentication is biometric or OTP or PIN or combination of PIN and OTP in accordance with e-KYC Servicesby conducting a walkthrough 2. Obtain samples of digitally signed information received from e-KYC service provider 3. Verify the digitally signed information contains name, address, email id, mobile phone number, photo etc of eSign user and response code. 4. Validate response code is recorded on application form and included in DSC as well 5. Verify the application form is programmatically filled	Mandatory	eSign Guidelines 2.2	
3.9.2.2	DSC application form is based on the digitally signed information received from e-KYC service provider. The digitally signed information from e-KYC services include name, address, email id, mobile phone number, photo etc of eSign user and response code		Mandatory	eSign Guidelines 2.2	
3.9.2.3	The response code, should be recorded on the application form and included in the DSC as well.		Mandatory	eSign Guidelines 2.2	
3.9.2.4	The application form should programmatically be filled with the digitally signed information received from e-KYC services.		Mandatory	eSign Guidelines 2.2	
3.9.2.5	The filled-in application form should be preserved. The following events should be recorded • Authentication of user • Response received from e-KYC ServicesCommunication with CAs for Certificate issuance	1. Obtain samples of filled in application forms 2. Verify the authentication of user, response received from e-KYC services and communication with CAs are recorded 3. Verify the consent of the eSign user for DSC is obtained electronically	Mandatory	eSign Guidelines 2.2	
3.9.2.6	The consent of the eSign user for getting a Digital Signature Certificate should be obtained electronically.		Mandatory	eSign Guidelines 2.2	

3.9.3. Security Procedure for Key Pair Generation and Certificate Issuance

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Key Pair Generation					
3.9.3.1	ESP should facilitate generation of key pairs on their Hardware Security Module. The key pairs shall be unique to the eSign user. The private key will be destroyed after one time use	1. Validate the ESP facilitates generation of key pairs of their HSM 2. Obtain samples and verify key pair is unique to each eSign user 3. Verify the private key is destroyed after one time use 4. Validate the private key is secured by HSM in in accordance with FIPS 140-2 level 3 recommendations for Cryptographic Modules Validation List 5. Validate ESP's HSM is different from CAs HSM	Mandatory	eSign Guidelines 2.3	
3.9.3.2	The private key of the eSign user shall be secured by Hardware security module (HSM) in accordance with FIPS 140-2 level 3 recommendations for Cryptographic Modules Validation List.		Mandatory	eSign Guidelines 2.3	
3.9.3.3	HSM of ESP should be separate from that of CAs for DSC issuance		Mandatory	eSign Guidelines 2.3	
Certificate Issuance					
3.9.3.4	The validity of the certificate shall be not more than 30 minutes for one time use only so revocation and suspension services will not be applicable vis-à-vis such certificates	1. Verify validity of certificate is limited to 30 minutes for one time use 2. Verify the Certificate Signing Request is sent to CA by ESP for issuing the DSC. 3. Obtain sample from the repository maintained by CA, and verify DSC is published in the repository	Mandatory	eSign Guidelines 2.4	
3.9.3.5	On successful key generation, the Certificate Signing Request is sent to CA by ESP for issuing the DSC.		Mandatory	eSign Guidelines 2.4	
3.9.3.6	The DSC should be published in the Repository maintained by CA		Mandatory	eSign Guidelines 2.4	

3.9.4. Authentication of Electronic Record by Applying Digital Signature

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Authentication and DSC Application Form					
3.9.4.1	The consent of the eSign user for digital signing of electronic record would have already been obtained electronically.	1. Check that CA stores the consent of eSign user for getting their consent 2. Validate that these consents are obtained electronically	Mandatory	eSign Guidelines 2.5	
3.9.4.2	eSign user should be given an option to reject the Digital Signature Certificate	1. Validate that the CA gives an option of rejecting DSC to eSign user	Mandatory	eSign Guidelines 2.5	

3.9.5. Evidence Requirements and Essential Security Requirements

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Evidence Requirements					
3.9.5.1	Digital Signature Certificate issuance: Record all relevant information concerning the e-authentication of eSign user for generation of key pair and subsequent certification functions for	1. Obtain records of all relevant information for e-authentication of eSign user for generation of key pair	Mandatory	eSign Guidelines 2.6	

	a minimum period of 7 years (ref The Information Technology (Certifying Authorities) Rules, 2000, Rule 27), in particular for the purpose of providing evidence for certification purposes. Such electronic record should be preserved accordingly in secure environment	2. Validate that this data is stored for a minimum period of 7 years 3. Verify the records are preserved in a secure environment			
3.9.5.2	Digital Signature creation: Record all relevant information concerning the e-authentication of eSign user for accessing the key pair for a minimum period of 7 years, in particular for the purpose of providing evidence of Digital signature creation. Such electronic record should be preserved accordingly in secure environment		Mandatory	eSign Guidelines 2.6	
Essential Security Requirements					
3.9.5.3	eSign xml request and response should be as per the eSign API specification. The communication between ASP and ESP should be secured (e.g. SSL, VPN, etc).	1. Conduct a walkthrough to check on sample basis the following: a. eSign xml request and response is as per the eSign API specification. b. communication between ASP and ESP is secured (e.g. SSL, VPN, etc). c. eSign xml request is digitally signed prior to sending it to ESP d. ESP verifies ASP's digital signature on each eSign xml request received e. e-KYC request is as per e-KYC provider's specifications f. e-KYC response is as per e-KYC provider's specifications	Mandatory	eSign Guidelines 2.7	
3.9.5.4	The eSign xml request should be digitally signed prior to sending it to ESP. ESP should verify ASP's digital signature on each eSign xml request received.		Mandatory	eSign Guidelines 2.7	
3.9.5.5	The e-KYC request should be as per e-KYC provider's specifications		Mandatory	eSign Guidelines 2.7	
3.9.5.6	The e-KYC response shall be as per e-KYC provider's specifications		Mandatory	eSign Guidelines 2.7	
3.9.5.7	ESP should form a digitally signed Certificate Generation Request with ESP's key prior to sending it to CA system. The CA system should accept only digitally signed Certificate Signing Request (CSR) from designated ESP systems over a secure link		Mandatory	eSign Guidelines 2.7	

3.9.5.8	CA system shall be configured to issue only e-KYC class end entity individual digital signature certificate(s).	g. ESP forms a digitally signed Certificate Generation Request with ESP's key prior to sending it to CA system. h. CA system accepts only digitally signed Certificate Signing Request (CSR) from designated ESP systems over a secure link i. CA system is configured to issue only e-KYC class end entity individual digital signature certificate(s). j. eSign xml response formed by ESP is digitally signed prior to sending it to ASP k. OTP request conforms to e-KYC provider's OTP request API specifications l. ESP systems used for e-KYC service request and response is different from ESP systems used to communicate with CA servers. m. eSign user key generation and management systems of ESP should is separate from CA systems in use for issuing end user certificate. n. CA system used for issuing e-KYC class based DSCs are be independent of CA systems used for other classes of DSCs	Mandatory	eSign Guidelines 2.7	
3.9.5.9	The eSign xml response formed by ESP should be digitally signed prior to sending it to ASP		Mandatory	eSign Guidelines 2.7	
3.9.5.10	OTP request should conform to e-KYC provider's OTP request API specifications		Mandatory	eSign Guidelines 2.7	
3.9.5.11	The ESP systems used for e-KYC service request and response should be different from ESP systems used to communicate with CA servers.		Mandatory	eSign Guidelines 2.7	
3.9.5.12	The eSign user key generation and management systems of ESP should be separate from CA systems in use for issuing end user certificate.		Mandatory	eSign Guidelines 2.7	
3.9.5.13	The CA system used for issuing e-KYC class based DSCs should be independent of CA systems used for other classes of DSCs		Mandatory	eSign Guidelines 2.7	
3.9.5.14	Key Generation for eSign user should happen on HSM and also should be secured by HSM The private key of the user should be secured by Hardware security module (HSM) in accordance with FIPS 140-2 level 3 recommendations for Cryptographic Modules Validation List		Mandatory	eSign Guidelines 2.7	
3.9.5.15	ESP should deploy trustworthy systems and employ trusted personal for eSign online electronic signature service.		Mandatory	eSign Guidelines 2.7	

		o. Key Generation for eSign user happens on HSM and is secured by HSM p. Private key of the user is secured by Hardware security module (HSM) in accordance with FIPS 140-2 level 3 recommendations for Cryptographic Modules Validation List q. ESP deploys trustworthy systems and employs trusted personal for eSign online electronic signature service.			

3.9.6. ESign - Digital Signature Certificate and Profiles

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
eSign - Digital Signature Certificate and Profile					
3.9.6.1	The end-user Digital Signature Certificates issued by CA should contain the following fields specific to eSign-Online Electronic Signature service along with other specified fields in IOG • Common Name - "Name of the person as in e-KYC response • Unique Identifier - This attribute shall be used for SHA	1. Validate that the end-user DSC issued by the CA contain the elements mentioned in the control description	Mandatory	eSign Guidelines 4.1	

	256 hash of e-KYC ID for individuals • Pseudonym - Response code/e-KYC unique Number in the case of e-KYC Service (Mandatory) (2.5.4.65 - id-at-pseudonym)				

3.9.7. ESign API

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
eSign API					
3.9.7.1	The API specifications remain common for all eSign Service provider. However, the parameter values that will vary for each ESP are 'eSign Service URL' and 'ASP ID' (Unique User ID provided by the ESP).	1. Validate same API specification are present for all ESPs with difference in the eSign service URL and ASP ID	Mandatory	eSign API Specifications	
3.9.7.2	ASP provides eSign facility to public should integrate with all other ESPs within one month after onboarding with first ESP.	1. Verify ASP providing eSign facility to public integrated with all other ESPs within one month after onboarding with first ESP	Mandatory	eSign API Specifications	
3.9.7.3	To support strong end to end security and avoid request tampering and man-in-the-middle attacks, it is essential that the requests and responses are digitally signed. The usage of HTTPS shall ensure transport layer encryption, while digital signing of XML shall ensure integrity & authenticity of data.	1. Validate requests and responses are digitally signed 2. Verify HTTPs is used for transport layer encryption	Mandatory	eSign API Specifications	
3.9.7.4	Once ASP submits the Request XML, ESP provides a 'pending for completion' (status=2) response which will contain the response code (as an acknowledgement). At this stage, ASP is expected to guide the user with proper information as under:	1. Conduct walkthrough of the process of ASP submitting the Request XML 2. Validaye ESP provides a 'pending	Mandatory	eSign API Specifications	

	1. Redirect the user to the authentication page of the ESP. 2. Provide information to the user to authenticate over ESP's mobile app. (ESP may also support push notification for mobile app users, and allowing to authenticate on mobile through eKYC provider)	for completion' (status=2) response which contains the response code (as an acknowledgement)			
3.9.7.5	CA shall implement a comprehensive eKYC service to fulfil the KYC requirements of eSign user. • eKYC system shall be a protected and shall not be exposed to any external services directly. • The access of eKYC information shall be on need basis for the services prescribed. • The access to such information by other services shall be bound by authentication of eSign user by two factors, namely the PIN and an OTP • The information of PIN shall not be stored in plain text format. The authentication of PIN shall be always verified after compare against the stored value. • The PIN information in plain text shall not be part of any logs or data monitoring systems.	1. Validate the eKYC service for eSign user cover the requirements mentioned in the control description	Mandatory	eSign API Specifications	
3.9.7.6	eKYC Service shall operate with the minimum required functions. The functions shall include: • Creation of eSign user account • Fetch eSign user information by ESP / CA systems (with user authentication) • Trigger OTP to the user • Mobile application based Access tokens • eSign user functionalities	1. Validate the minimum required functions mentioned in the control description are performed as part of the eKYC service	Mandatory	eSign API Specifications	
3.9.7.7	eKYC system shall provide provision for online enrolment to eSign users and the same should be able access through ESP page	1. Conduct walkthrough and check if the eKYC system provisioned for	Mandatory	eSign API Specifications	

	or ASP applications. Such enrolment is bound by procedures and requirements defined under Identity Verification Guidelines. On successful enrolment of an eKYC User, following data eSign user information is recorded in eKYC user account. These fields are subject to verification against the prescribed 'Verified Source'. (Aadhaar Offline XML, Bank eKYC, Organizational KYC)	online enrolment to eSign users can be accessed through ESP page or ASP applications 2. Validate on successful enrolment of eKYC user, all required information mentioned in control description is covered			
3.9.7.8	Aadhaar Offline XML shall be verified on its receipt for a valid digital signature by UIDAI	3. Check Aadhaar Offline XML is verified on its receipt for a valid digital signature by UIDAI	Mandatory	eSign API Specifications	
3.9.7.9	Bank sends eKYC to CA directly up on authentication by user as a banking customer Bank eKYC shall be verified on its receipt by CA for a valid digital signature by respective bank.	4. Verify the bank sends eKYC to CA directly up on authentication by user as a banking customer Bank and eKYC is verified on its receipt by CA for a valid digital signature by respective bank	Mandatory	eSign API Specifications	
3.9.7.10	The existence of Organization and verification of authorised signatory as per IVG is a prerequisite. Organization should send KYC List to CA in electronic form or physical paper form signed by authorised signatory CA should verify the source and signature of the signatory of Organization	1. Verify the oranisation sends KYC List to CA in electronic form or physical paper form signed by authorised signatory. Check CA also verifies the source and signature of the signatory of Organization	Mandatory	eSign API Specifications	
3.9.7.11	The eKYC user information shall be allowed to access for eSign process and DSC issuance. For access of such data for eSign process, ESP shall implement necessary rest API based eKYC request, as per the formats provided under section 4.3 of eSign API Specifications guidelines.	2. Verify the eKYC user is allowed to access eSign process and DSC issuance and for accessing such data ESP implements necessary API based eKYC request as per format provided in the guidelines	Mandatory	eSign API Specifications	
3.9.7.12	The audit logs (both success & Failure) of eKYC user authentications shall be maintained by eKYC Provider with timestamp and user id. The maximum retries with failed authentication by a user (for specific transaction) shall be limited to 5 attempts	3. Validate the audit logs of eKYC user are maintained by eKYC provider with timestamps and user id. 4. Check maximum retries with failed authentication by a user is limited	Mandatory	eSign API Specifications	

		to 5 attempts			
3.9.7.13	ESP should implement an internal secure API communication, in order to send OTP to the user. Alternatively, ESP may also implement Time Based OTP (TOTP) functionality using compliant TOTP authenticators and/or ESPs own authenticator app through eKYC provider. ESP can also implement ESP mobile app based authentication, as an alternate to OTP.	1. Validate if ESP has implemented any one of the following a. internal secure API communication to send OTP b. Time based OTP using compliant TOTP authenticators c. ESP mobile app based authentication	Mandatory	eSign API Specifications	
3.9.7.14	ESP shall offer a subscriber portal to meet the following requirements through eKYC provider. • PIN change functionality • Signing History • Other modifications to user data This portal shall implement single factor authentication including either PIN, or OTP, or Mobile app to login to the system. The portal shall be secured and permit minimum of the requirements stated in this section. Any request for modifications to KYC data shall undergo necessary verification procedures laid down by CCA.	1. Check the portal created by ESP to meet the requirements of eKYC provider 2. Verify the portal offers PIN change functionality, signing history and other modifications 3. Validate single factor authentication is implemented to include either PIN, or OTP, or Mobile app to login to the system	Mandatory	eSign API Specifications	
3.9.7.15	ESP may offer mobile based authentication. The requirements for the same need to be fulfilled as under, in order to qualify for Mobile based authentication. Such qualified mobile app-based authentication shall be equivalent to OTP authentication. Thereby, any such signing process shall have PIN + Mobile app authentication to fulfil KYC data access. Requirements to be fulfilled by such mobile applications:	1. Verify if ESP offers mobile based authentication, the requirements covered in control description are met 2. Check the mobile app-based authentication is equivalent to OTP authentication and any signing process shall have PIN +	Mandatory	eSign API Specifications	

	• Mobile app shall be owned and operated by ESP with complete control on its code, architecture, security and publishing requirements. • Mobile app shall support largely used Mobile operating systems. However, it shall not support any operating systems or its versions, which are known to have security issue or deprecation. • Mobile app shall have a secure architecture and undergo vulnerability assessments to avoid any exploitation. • User shall login to the mobile app using a secure procedure involvement PIN + OTP authentication. This first time usage shall have a secure layer to create and make a handshake with KYC server with generation of a unique Access Token. • Such access token shall be generated in the mobile device in a secure area / element supported by the platform, and shared with eKYC server for enrolment of the device against that eKYC user. • Access Token shall be marked for expiry in 3 months from its last successful usage. In case of expired access token, mobile app shall clear the local Access Token and force the user for fresh login. • System shall support multiple access Tokens against one eKYC user, towards supporting multiple mobile devices. • Subscriber portal shall provide necessary option for accessToken history and revocation of accessTokens. • Any signing transaction 'waiting for user authentication' shall be queued and shown separately on the mobile app. It is also recommended to show new signing transactions as a push notification. • User shall be able to open the mobile app (with or without a local sign in functionality) and confirm the signature with PIN authentication. • Mobile app may also support additional eSign user functions using same level of security required for eSign user portal.	Mobile app authentication to fulfil KYC data access.			

	• Mobile app should be secure enough to avoid any kind of access breach, or any kind of hacks to gain direct access to the token and the eKYC server endpoint consumed by such mobile app.				
3.9.7.16	Request/Response format of eSign API 2.X	The following should be verified 1. Obtain all the request/ response format specified under eSign API 2.X and cross verify with request/ response of a sample transaction	Mandatory	eSign API 2.X Specifications	
3.9.7.17	Request/Response format of eSign API 3.X	The following should be verified 1. Obtain all the request/ response format specified under eSign API 3.X and cross verify with request/ response of a sample transaction	Mandatory	eSign API 3.X Specifications	
3.9.7.18	Request/Response format of eSign API 1.X	The following should be verified 1. Obtain all the request/ response format specified under eSign API 1.X and cross verify with request/ response of a sample transaction	Mandatory	eSign API 1.X Specifications	

3.9.8. On boarding Process and Agreement

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
ASP Eligibility Criteria					
3.9.8.1	The agency which desires to integrate eSign service should either be: • A Central/ State Government Ministry / Department or an undertaking owned and managed by Central • / State Government, or	1. Obtain list of agencies integrated eSign Services 2. For sample agencies verify if they come under either of the categories mentioned in the control description	Mandatory	ASP On-Boarding Guidelines 1.7	

	• An Authority constituted under the Central / State Act, or
	• A Not-for-profit company / Special Purpose organization of national importance, or
	• A bank / financial institution / telecom company, or
	• A legal entity registered in India:
	  ○ Should be an organization incorporated under Companies Act, 1956, Registrar of Firms, LLPRegistered; OR An association of persons or a body of individuals, in India, whether incorporated or not
	  ○ Should not have been blacklisted by any State Government, Central Government, Statutory,Autonomous, or Regulatory body.				

On Boarding Process					
3.9.8.2	Organization intending to avail eSign service shall make a formal request to one or more ESP.	1. Conduct a walkthrough of the on boarding process and check the following: a. Formal request is made to ESP to avail eSign service b. Application form is made specific to particular ESP c. Application form is submitted in original, and bear the signature/ attestation of Authorized signatory of the organization d. For paperless mode, application should be digitally signed	Mandatory	ASP On-Boarding Guidelines 1.9	
3.9.8.3	Application form should be made specific to particular ESP. For this purpose, each ESP may share a format of application form		Mandatory	ASP On-Boarding Guidelines 1.9	
3.9.8.4	Application form should be submitted in original, and bear the signature / attestation of Authorized signatory of the organization.		Mandatory	ASP On-Boarding Guidelines 1.9	
3.9.8.5	In case of application form being submitted through paperless mode (email, etc), it shall be digitally / electronically signed by authorized signatory of the organization.		Mandatory	ASP On-Boarding Guidelines 1.9	
3.9.8.6	ESP shall grant the access to eSign only after receiving completed application form from ASP.		Mandatory	ASP On-Boarding Guidelines 1.9	

3.9.8.7	ASP shall submit supporting documents towards KYC verification and other requirements of on-boarding. These documents should be duly attested & forwarded by the authorized signatory of the organization. The list of documents to be submitted shall be as given at Annexure 2.11.2	e. ESP grants the access to eSign only after receiving completed application form f. All supporting documents, duly attested are submitted g. ASP agrees to the terms of service with the ESP to enable eSign in their application/ software	Mandatory	ASP On-Boarding Guidelines 1.10	
3.9.8.8	The ASP should enter / agree to the terms of service with the eSign Service Provider (ESPs) to enable eSign in their application / software.		Mandatory	ASP On-Boarding Guidelines 1.11	
3.9.8.9	ASP has to submit the Digital Signature Certificate to ESP, so that ESP can configure it in their system and validate/verify each transaction received from the ASP. Such Digital Signature Certificate should fulfill the criteria given below: • Should be a valid certificate issued by a CA licensed under Information technology (IT) Act. • Should be either an Organizational Person Digital Signature Certificate or an Organizational Document Signer Certificate. • The O value in the certificate should be the legal entity name of the ASP organization. • Should be either Class 2 or Class 3 certificate. • Should be valid for at least six months from date of submission	1. For sample DSC verify the following criteria is fulfilled: a. Should be a valid certificate issued by a CA licensed under Information technology (IT) Act. b. Should be either an Organizational Person Digital Signature Certificate or an Organizational Document c. Signer Certificate. The O value in the certificate should be the legal entity name of the ASP organization. d. Should be either Class 2 or Class 3 certificate. e. Should be valid for at least six months from date of submission	Mandatory	ASP On-Boarding Guidelines 1.12	

3.9.8.10	ASP shall build the required infrastructure for adopting eSign service. ESP provides access to pre-production environment and enables the ASP to establish end- to -end connectivity to carry out eSign services testing and integration	1. Verify ASP has built the required infrastructure for adopting eSign service. 2. Check the ESP provides access to pre-production environment and enables the ASP to establish end-to -end connectivity to carry out eSign services testing and integration	Mandatory	ASP On-Boarding Guidelines 1.13	
3.9.8.11	ASP shall submit the audit report in original to the ESP. Such audit report should not be older than 3 months. In case, ASP is taking service from multiple ESPs, common audit report can be submitted. ASP Audit report should be carried out by Auditor empaneled by Cert-in /IS Auditor	1. Validate audit report not older than 3 months was submitted to the ESP 2. Check the audit was carried out by Auditor empaneled by Cert-in /IS Auditor 3. Validate ASP carried out the audit prior to completion of one year from the date of completion of last audit. 4. For e-KYC compliance, validate ESP carried out necessary auditing of ASP as applicable	Mandatory	ASP On-Boarding Guidelines 1.14	
3.9.8.12	ASP should carry out the audit prior to the completion of one year from the date of completion of last audit. Audit report shall also be examined on a yearly basis by ESP by requesting a fresh audit report. ASP should submit annual compliance report with the same audit requirements and procedures provided here, upon request by ESP, within 30 days, In respect of e-KYC compliance requirements, ESP shall carryout necessary auditing of ASP as applicable separately.		Mandatory	ASP On-Boarding Guidelines 1.14	
3.9.8.13	ASP shall notify ESP about its readiness for migration to production environment. Subsequently ASP completes the go live checklist and submits the request for Go Live checklist. ESP should take an undertaking from ASP or an agreement should be executed between ESP and ASP.	1. Obtain sample Go Live checklist for some of the ASPs 2. Validate the checklist was completed by ASP 3. Verify ESP obtained an undertaking from ASP or an agreement is executed between ESP and ASP.	Mandatory	ASP On-Boarding Guidelines 1.15	

3.9.8.14	ESP shall ensure successful scrutiny of the following before granting production access: • Application form • Supporting documents • Acceptance of terms of service • Digital Signature Certificate submission • Integration / testing completion in preproduction / testing environment • Audit report • Go Live checklist • Internal approvals and clearance within ESP organization ESP shall ensure that such information is securely shared with the relevant person in ASP organization.	1. ESP to demonstrate that it scrutinized the following before granting production access: a. Application form b. Supporting documents c. Acceptance of terms of service d. Digital Signature Certificate submission e. Integration / testing completion in preproduction / testing environment f. Audit report g. Go Live checklist h. Internal approvals and clearance within ESP organization	Mandatory	ASP On-Boarding Guidelines 1.16	

3.9.9. CA Requirements

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
CA Requirements					
3.9.9.1	The CA system used for issuing e-KYC class based DSCs should be independent of CA systems used for other classes of DSCs.	1. Verify the CA system used for issuing e-KYC class based DSCs is independent of CA systems used for other classes of DSC 2. Check the CA system accepts only digitally signed CSR from designated ESP over a secure link 3. Verify the CA system is configured to	Mandatory	eSign Guidelines 7	
3.9.9.2	The CA system should accept only digitally signed Certificate Signing Request (CSR) from designated ESP systems over a secure link.		Mandatory	eSign Guidelines 7	

3.9.9.3	CA system shall be configured to issue only e-KYC class end entity individual digital signature certificates. ESP shall be allowed access to CA systems only for submitting CSR for issuance of e-KYC classes of DSCs to be used for eSign.	issue only e-KYC class end entity individual digital signature certificates 4. Validate ESP is allowed access to CA systems only for submitting CSR for issuance of e-KYC classes of DSCs to be used for eSign.	Mandatory	eSign Guidelines 7	
3.9.9.4	All Digital Signature Certificates issued by the Certifying Authorities shall conform to ITU X.509 version 3 standard as per rule 6 and shall inter alia contain the following data, namely:- • Serial Number • Signature Algorithm ldentifier • Issuer • Validity period of the Digital Signature Certificate; • Name of the subscriber • Public Key information of the subscriber	1. Obtain sample DSCs and verify the certificates contains the following: a. Serial Number b. Signature Algorithm ldentifier c. Issuer d. Validity period of the Digital Signature Certificate; e. Name of the subscriber f. Public Key information of the subscriber	Mandatory	IT CA Rules 7	

3.9.10. Audit Logging Procedures

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
Audit Logging					
3.9.10.1	Audit log files shall be generated for all events relating to the security of the eSign-Online Electronic Signature Service. Where possible, the security audit logs shall be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism shall be used.	1. Conduct a walkthrough of the audit logging process followed by CA and on sample basis check the following: a. Audit log files are generated for all events relating to the security of the eSign-Online Electronic Signature	Mandatory	e-authentication guidelines for eSign	

3.9.10.2	All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section 3.9.10 shall be maintained in accordance with controls covered below	Service. b. Security audit logs are automatically collected or a logbook, paper form, or other physical mechanism is used. c. All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits d. Security audit logs for each auditable event defined in this section 3.9.10 are maintained e. All security auditing capabilities of the operating system and the applications required are enabled	Mandatory	e-authentication guidelines for eSign	
3.9.10.3	All security auditing capabilities of the operating system and the applications required shall be enabled		Mandatory	e-authentication guidelines for eSign	
3.9.10.4	At a minimum, each audit record shall include the following (either recorded automatically or manually for each auditable event): • The type of event, • The date and time the event occurred, • Success or failure where appropriate, and • The identity of the entity and/or operator that caused the event.	1. For sample audit records check the following are recorded: a. The type of event, b. The date and time the event occurred, c. Success or failure where appropriate, and d. The identity of the entity and/or operator that caused the event	Mandatory	e-authentication guidelines for eSign	
3.9.10.5	The following events shallbe covered under security: • Any changes to the Audit parameters, e.g., audit frequency, type of event audited • Any attempt to delete or modify the Audit logs	1. For sample audit records check the following are covered under security: a. Any changes to the Audit parameters, e.g., audit frequency, type of event audited b. Any attempt to delete or modify the Audit logs	Mandatory	e-authentication guidelines for eSign	
3.9.10.6	The following events shall be covered under logical access: • Successful and unsuccessful attempts to assume a role	1. For sample audit records check the following are covered under logical access:	Mandatory	e-authentication guidelines for eSign	

	• 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	a. Successful and unsuccessful attempts to assume a role b. The value of maximum number of authentication attempts is changed c. The number of unsuccessful authentication attempts exceeds the maximum authentication attempts during user login d. An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts e. An Administrator changes the type of authenticator, e.g., from a password to a biometric			
3.9.10.7	The following events shall be covered under key generation: • Generation of Signing Key Pair for eSign users • Deletion of key pair after signature	1. For sample audit records check the following are covered under key generation: a. Generation of Signing Key Pair for eSign users b. Deletion of key pair after signature	Mandatory	e-authentication guidelines for eSign	
3.9.10.8	The following events shall be covered under securing key: • Securing eSign user Signing private key • Retrieval of eSign user Signing private key for usage	1. For sample audit records check the following are covered under key securing: a. Securing eSign user Signing private key b. Retrieval of eSign user Signing private key for usage	Mandatory	e-authentication guidelines for eSign	
3.9.10.9	The following events shall covered under eSign online electronic signature services: • All eSign Online Electronic Signature Signing requests received from ASP • All e-KYC response received from e-KYC Provider • All electronic DSC Application Form Generated • Proof of eSign user's consent for	1. For sample audit records check the following are covered under eSign online electronic signature services: a. All eSign Online Electronic Signature Signing requests received from ASP b. All e-KYC response received from e-KYC Provider	Mandatory	e-authentication guidelines for eSign	

	- key pair generation, - DSC application form submission to CA, - Generate CSR based on the digitally signed information received from e-KYC services - signature generation on the hash submitted • Mechanism Implemented for acceptance of DSC by eSign user • Communication to CA in respect of Certification. • Response sent to ASP	c. All electronic DSC Application Form Generated d. Proof of eSign user's consent for i. key pair generation, ii. DSC application form submission to CA, iii. Generate CSR based on the digitally signed information received from e-KYC services iv. signature generation on the hash submitted e. Mechanism Implemented for acceptance of DSC by eSign user f. Communication to CA in respect of Certification. g. Response sent to ASP			
3.9.10.10	The following events shall be covered under essential security requirements: • Identification and Authentication • Domain Separation • Cryptographic Requirements	1. For sample audit records check the following are covered under essential security requirements: a. Identification and Authentication b. Domain Separation c. Cryptographic Requirements	Mandatory	e-authentication guidelines for eSign	
3.9.10.11	The following events shall be covered under account administration: • Roles and users are added or deleted • The access control privileges of a user account or a role are modified • eSign Online Electronic Signature Service API • All changes to the eSign Online Electronic Signature Service API	1. For sample audit records check the following are covered under account administration: a. Roles and users are added or deleted b. The access control privileges of a user account or a role are modified c. eSign Online Electronic Signature Service API d. All changes to the eSign Online Electronic Signature Service API	Mandatory	e-authentication guidelines for eSign	

3.9.10.12	The following events shall be covered under miscellaneous: • Appointment of an individual to a Trusted Role • Designation of personnel for multiparty control • Installation of the Operating System • Installation of the eSign Online Electronic Signature Service Application • Installation of hardware cryptographic modules • Removal of hardware cryptographic modules • Destruction of cryptographic modules • Zeroization of cryptographic modules • System Startup • Logon attempts to eSign Online Electronic Signature Service Application • Receipt of hardware / software • Attempts to set passwords • Attempts to modify passwords • Back up of the internal eSign Services database • Restoration from back up of the internal eSign Services database • File manipulation (e.g., creation, renaming, moving) • Access to the internal eSign Online Electronic Signature Service database • Re-key of the eSign Online Electronic Signature Service signing certificate	1. For sample audit records check the following are covered under miscellaneous: a. Designation of personnel for multiparty control b. Installation of the Operating System c. Installation of the eSign Online Electronic Signature Service Application d. Installation of hardware cryptographic modules e. Removal of hardware cryptographic modules f. Destruction of cryptographic modules g. Zeroization of cryptographic modules h. System Startup i. Logon attempts to eSign Online Electronic Signature Service Application j. Receipt of hardware / software k. Attempts to set passwords l. Attempts to modify passwords m. Back up of the internal eSign Services database n. Restoration from back up of the internal eSign Services database o. File manipulation (e.g., creation,	Mandatory	e-authentication guidelines for eSign	

		renaming, moving) p. Access to the internal eSign Online Electronic Signature Service database q. Re-key of the eSign Online Electronic Signature Service signing certificate			
3.9.10.13	The following events shall be covered under configuration changes: • Hardware • Software • Operating System • Patches • Security Profiles	1. For sample audit records check the following are covered under configuration changes: a. Hardware b. Software c. Operating System d. Patches e. Security Profiles	Mandatory	e-authentication guidelines for eSign	
3.9.10.14	The following events shall be covered under physical access/site security: • Personnel Access to room housing eSign- Online Electronic Signature Service • Access to the eSign- Online Electronic Signature Service • Known or suspected violations of physical security	1. For sample audit records check the following are covered under physical access/site security:: a. Personnel Access to room housing eSign- Online Electronic Signature Service b. Access to the eSign- Online Electronic Signature Service c. Known or suspected violations of physical security	Mandatory	e-authentication guidelines for eSign	
3.9.10.15	The following events shall be covered under anomalies: • Software error conditions • Software check integrity failures • Receipt of improper messages • Misrouted messages • Network attacks (suspected or confirmed) • Equipment failure	1. For sample audit records check the following are covered under anomalies: a. Software error conditions b. Software check integrity failures c. Receipt of improper messages d. Misrouted messages e. Network attacks (suspected or confirmed)	Mandatory	e-authentication guidelines for eSign	

	• Electrical power outages • Uninterruptible Power Supply (UPS) failure • Obvious and significant network service or access failures • Violations of eSign- Online Electronic Signature Service	f. Equipment failure g. Electrical power outages h. Uninterruptible Power Supply (UPS) failure i. Obvious and significant network service or access failures j. Violations of eSign- Online Electronic Signature Service			
3.9.10.16	The following events shall be covered under Auditable Event/ Audit Criteria(ESP) for reports: • Agreement between ESP e-KYC Provider and its Compliance audit report • Report of Vulnerability Assessment and Penetration Test • Agreement between ESP-ASP • Compliance audit report of ASP • Any other applicable agreements and its compliance reports	1. For sample audit records check the following are covered under Auditable Event/ Audit Criteria(ESP) for reports: a. Agreement between ESP e-KYC Provider and its Compliance audit report b. Report of Vulnerability Assessment and Penetration Test c. Agreement between ESP-ASP d. Compliance audit report of ASP e. Any other applicable agreements and its compliance reports	Mandatory	e-authentication guidelines for eSign	
3.9.10.17	The following events shall be audited in respect of eSign service: • The isolation of CA system used for issuing e-KYC class from the CA system used for issuing other classes of DSCs • Digitally signed Certificate Signing Request (CSR) from ESP systems • Ensuring no DSCs other than e-KYC class of certificates are issued from ESP • Secure communication between ESP and CA system	1. For sample audit records check the following events are audited as part of eSign service: a. The isolation of CA system used for issuing e-KYC class from the CA system used for issuing other classes of DSCs b. Digitally signed Certificate Signing Request (CSR) from ESP systems c. Ensuring no DSCs other than e-KYC class of certificates are issued from ESP d. Secure communication between ESP and CA system	Mandatory	e-authentication guidelines for eSign	

Frequency of Processing Audit Logs					
3.9.10.18	Frequency of ESP audit log processing shall be in accordance with the requirements set for the CAs in Section 5.4.2 of the [CCACP].	1. Validate the frequency of ESP audit log processing are in accordance with the requirements set for the CAs in Section 5.4.2 of the [CCACP].	Mandatory	e-authentication guidelines for eSign	
Retention Period for Audit Logs and Archive					
3.9.10.19	The minimum retention periods for archive data are listed below for the various assurance levels. • e-KYC OTP Single Factor - 7 Years • e-KYC Multi Factor - 7 Years	1. For samples of archived data, verify the minimum retention period is as listed in control 3.9.10.19 2. Check in cases where original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media is defined. 3. Verify applications required to process the archive data are maintained for the minimum retention period specified in control 3.9.10.19	Mandatory	e-authentication guidelines for eSign	
3.9.10.20	If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined. Applications required to process the archive data shall also be maintained for the minimum retention period specified above		Mandatory	e-authentication guidelines for eSign	
Protection of Audit Logs					
3.9.10.21	Protection of ESP audit log shall be in accordance with the requirements set for the CAs in Section 5.4.4 of the [CCA-CP].	1. Validate ESP audit logs are protected in accordance with the requirements set for the CAs in Section 5.4.4 of the [CCA-CP]	Mandatory	e-authentication guidelines for eSign	

Audit Log Backup Procedures					
3.9.10.22	Audit logs and audit summaries shall be archived per requirements mentioned in control 3.9.10.19	1. For sample records check the audit logs and audit summaries are archived as per control 3.9.10.19	Mandatory	e-authentication guidelines for eSign	
Audit Collection System (internal vs. external)					
3.9.10.23	ESP audit collection requirements shall be in accordance with the requirements set for the CAs in Section 5.4.6 of the [CCA-CP]	1. Validate the ESP audit collection requirements is in accordance with the requirements set for the CAs in Section 5.4.6 of the [CCA-CP]	Mandatory	e-authentication guidelines for eSign	
Records Archival					
3.9.10.24	Types of Records Archived - ESP's archival of records shall be sufficiently detailed to establish the proper operation of the ESP Service or the validity of any signature generated by ESP.	1. Validate the following on sample basis for the record archival process a. ESP's archival of records is sufficiently detailed to establish the proper operation of the ESP Service or the validity of any signature generated by ESP b. All data covered in control 3.9.10.25 is archived by CA or ESP c. archive retention period for ESP Service is same as those listed for CA in Section 5.5.2 of the [CCACP]. d. Protection of ESP Service archives is same as those listed	Mandatory	e-authentication guidelines for eSign	
3.9.10.25	Data To Be Archived (CA Or ESP) • Contractual obligations • System and equipment configuration • Modifications and updates to system or configuration • eSign- Digital Signature signing requests • eSign user's Digital Signature and Certificate • Response received from e-KYC Services and DSC application form • Record of eSign- Digital Signature signing Re-key • All Audit Logs • All Audit Log Summaries		Mandatory	e-authentication guidelines for eSign	

	• Other data or applications to verify archive contents • Compliance audit reports •	for CA in Section 5.5.3 of the [CCACP]. e. Archived records are time stamped such that order of events can be determined f. eSign- Online Electronic Signature Service can be reestablish as soon as possible in case of a Disaster. Check the disaster recovery plan g. Form C is archived in machine readable or human readable format (XML or PDF) with a digital signature of ESP. h. Forms is versioned and stored to provide a complete history of compliance. i. CA has established a managed process for creating, maintaining, and verifying archive			
3.9.10.26	Retention Period for Archive - The archive retention period for ESP Service shall be the same as those listed for CA in Section 5.5.2 of the [CCACP].		Mandatory	e-authentication guidelines for eSign	
3.9.10.27	Protection of Archive - Protection of ESP Service archives shall be the same as those listed for CA in Section 5.5.3 of the [CCACP].		Mandatory	e-authentication guidelines for eSign	
3.9.10.28	Requirements for eSign- Online Electronic Signature Service records - Archived records shall be time stamped such that order of events can be determined.		Mandatory	e-authentication guidelines for eSign	
3.9.10.29	Business Continuity Capabilities after a Disaster - In the case of a disaster whereby a ESP Service installation is physically damaged and all copies of the eSign-Online Electronic Signature Service Signing Key are destroyed as a result, the eSign- Online Electronic Signature Service shall reestablish services as soon as practical		Mandatory	e-authentication guidelines for eSign	
3.9.10.30	Archival Format. - The Form C should be archived in machine readable or human readable format (XML or PDF) with a digital signature of ESP. The forms should be versioned and stored to provide a complete history of compliance.CA must have managed process for creating, maintaining, and verifying archive.		Mandatory	e-authentication guidelines for eSign	

3.9.11. eKYC Service Modes

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
eKYC Service Modes					
3.9.11.1	The eSign service will have two modes of verification of eSign user. Online Aadhaar eKYC authentication (API 2.x version) of eSign user is facilitated by CA	1. For eKYC Service Modes, verify the following: a. eSign service has only two modes of verification of eSign user. b. Online Aadhaar eKYC authentication (API 2.x version) of eSign user is facilitated by CA c. Offline Aadhaar eKYC authentication(API 3.x version) is carried out by eSign user and authentication response is submitted to CA. d. CA further confirms the submission and accepts the same. e. Offline Aadhaar eKYC authentication of eSign user requires one time registration. f. procedure for registration given in the IVG section 5 is followed. g. eKYC accounts of registered and verified users are used for eSign	Mandatory	e-authentication guidelines for eSign	
3.9.11.2	Offline Aadhaar eKYC authentication(API 3.x version) will be carried out by eSign user and authentication response will be submitted to CA. CA further confirm the submission and accept the same. Offline Aadhaar eKYC authentication of eSign user requires one time registration.		Mandatory	e-authentication guidelines for eSign	
3.9.11.3	The procedure to be followed for registration is given in the IVG section 5. The API specification for interface with ESP is specified under eSign API version 3.x. The eKYC accounts of registered and verified users are used for eSign		Mandatory	e-authentication guidelines for eSign	

3.9.12. CA eKYC Implementation Requirements

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
eKYC Service Modes					
3.9.12.1	This section is applicable to CA that maintains eKYC accounts of registered users. ESP use registered & verified information of eSign user retained on eKYC system for eSign service. CA may also use the same verified user information for DSC issuance. In both cases, two factor authentications is required for CA or ESP to use the eKYC account holder's information retained in the eKYC account held by CA.	1. Verify the ESP uses registered & verified information of eSign user retained on eKYC system for eSign service 2. Validate two factor authentication is implemented to use the eKYC account holder's information retained in the eKYC account held by CA.	Mandatory	e-authentication guidelines for eSign	
Data Protection and Privacy					
3.9.12.2	eKYC Data Protection - eKYC data protection should be part of the design and implementation of eKYC systems, services, products and practices	1. Verify eKYC data protection is part of the design and implementation of eKYC systems, services, products and practices 2. Validate the eKYC user's account information is used only for DSC issuance and authentication purpose only 3. Check by reviewing reports, the risk assessment of eKYC system is carried out and security measures are in place	Mandatory	e-authentication guidelines for eSign	
3.9.12.3	Privacy of eKYC Data - Ensure to process the data that is necessary to achieve specific eKYC user's account management & authentication. The eKYC user's account information should be used only for DSC issuance and authentication purpose only.		Mandatory	e-authentication guidelines for eSign	
3.9.12.4	Risk Assessment - Risk assessment of eKYC system should have carried out and security measures should be in place		Mandatory	e-authentication guidelines for eSign	

3.9.12.5	Operational Requirements - The eKYC system should have made operational only after Risk assessment, VA/PT and Audit.	4. Verify eKYC system is made operational only after Risk assessment, VA/PT and Audit	Mandatory	e-authentication guidelines for eSign	
Identification					
3.9.12.6	Transaction ID - Generated by ASP calling the API, this is logged and returned in the output for correlation. Should be unique for the given ASP-ESP combination	1. Verify the transaction ID is unique for the ASP-ESP combination 2. Validate the response code is a part of DSC and is of length 32 3. Check the CA permits eSign signer to have one or more eKYC user account	Mandatory	e-authentication guidelines for eSign	
3.9.12.7	Response Code - Generated by ESP on eKYC user authentication request and should be a part of DSC . The Response Code should be of length 32.		Mandatory	e-authentication guidelines for eSign	
3.9.12.8	eKYC user ID - eSign signer can have one or more eKYC user account		Mandatory	e-authentication guidelines for eSign	
eKYC System security					
3.9.12.9	Network Security - The e-KYC services systems (database) must be configured as secure systems as per the definitions of IT Act and should not have direct interface with system other than eKYC Server. The communication between eKYC server and e-KYC service systems (database) should be in request response mode	1. For sample eKYC services systems (database), check the systems are configured as secure systems as per the definitions of IT Act and do not have direct interface with system other than eKYC Server. 2. Verify the communication between eKYC server and e-KYC service systems (database) is in request response mode 3. Check the CA e-KYC service systems are dedicated only for e-KYC service purpose	Mandatory	e-authentication guidelines for eSign	
3.9.12.10	Dedicated for the Purpose - The CA e-KYC service systems should be dedicated only for e-KYC service purpose		Mandatory	e-authentication guidelines for eSign	

eKYC Account Management					
3.9.12.11	eKYC User authentication - The authentication should be carried out using OTP sent to registered mobile eSign user and PIN. Access Token registered for the mobile Application based on OTP and PIN	1. Validate the eKYC user authentication is carried out using OTP sent to registered mobile eSign user and PIN and access Token is registered for the mobile Application based on OTP and PIN 2. Validate the e-KYC request is as per the format specified in eSign API specifications and ESP sends digitally signed eKYC Request with ESP's key. 3. Verify the e-KYC response is as per the format specified in eSign API specifications and the response is digitally signed using a CA eKYC System key 4. Check on sample basis OTP or Mobile Token Response is sent with purpose and Request and Response are preserved 5. Verify clear text transmission, storage or capture of passwords, maintain audit trails, and lock the account after repeated unsuccessful attempts are not allowed for PIN Management 6. Check CA has implemented mechanism for eKYC user to set eKYC user id and PIN and the PIN is of 6 characters in length 7. Validate the OTP and Mobile	Mandatory	e-authentication guidelines for eSign	
3.9.12.12	ESP e-KYC Request to CA e-KYC System - The e-KYC request should be as per the format specified in eSign API specifications ESP should send digitally signed eKYC Request with ESP's key.		Mandatory	e-authentication guidelines for eSign	
3.9.12.13	e-KYC response to ESP - The e-KYC response should be as per the format specified in eSign API specifications. The response should be digitally signed using a CA eKYC System key		Mandatory	e-authentication guidelines for eSign	
3.9.12.14	OTP or Mobile Token Authentication - Each OTP or Mobile Token Response should be sent with purpose and Request and Response should be preserved		Mandatory	e-authentication guidelines for eSign	
3.9.12.15	PIN Management - For PIN management, do not allow clear text transmission, storage or capture of passwords, maintain audit trails, and lock the account after repeated unsuccessful attempts. CA should implement mechanism for eKYC user to set eKYC user id and PIN. PIN shall be 6 characters in length		Mandatory	e-authentication guidelines for eSign	
3.9.12.16	Consent - The OTP and Mobile Access token verified along with PURPOSE text is deemed as consent		Mandatory	e-authentication guidelines for eSign	

		Access token verified along with PURPOSE text is deemed as consent			
Audit Requirements					
3.9.12.17	Audit Trail of Account Creation and Maintenance - The audit trail of eKYC account creation, modification, suspension, deletion etc should be maintained by CA with the details of authorised individual who carried out the operation. The date/time stamp, requested source details etc. also should be accessible for audit	1. Verify the CA maintains audit trail of eKYC account creation, modification, suspension, deletion etc. with the details of authorised individual who carried out the operation. 2. Validate the date/time stamp, requested source details etc. also are accessible for audit 3. On sample basis, check a monthly audit of ten percent (subjected to maximum of 5000) of the eKYC account creation & modification has been carried out by an IS Auditor in the following month and the report is made available during Annual CA compliance Audit	Mandatory	e-authentication guidelines for eSign	
3.9.12.18	A monthly audit of ten percent (subjected to maximum of 5000) of the eKYC account creation & modification should be carried out by an IS Auditor in the following month and the report should be made available during Annual CA compliance Audit		Mandatory	e-authentication guidelines for eSign	
Account Monitoring facility to eKYC user					
3.9.12.19	The history of eKYC account changes should be made available to eKYC users	1. Verify history of eKYC account changes is made available to eKYC users 2. Validate ESP provides access to the signed transaction details to	Mandatory	e-authentication guidelines for eSign	
3.9.12.20	ESP should provide access to the signed transaction details to eSign users		Mandatory	e-authentication guidelines for eSign	

3.9.12.21	ASP should provide mechanism for viewing the signed documents to eSign users.	eSign users 3. Check the ASP provides mechanism to eSign users for viewing the signed documents.	Mandatory	e-authentication guidelines for eSign	

3.9.13. e-Authentication & Electronic Signature Guidelines for Remote Key-Storage

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
General Requirements					
3.9.13.1	In order to provide the assurance of sole control over the private key of subscriber in a remote secure device, the authentication for activating the private key for signature function shall be secure and reliable. The authentication data shall be communicated to the HSM managing the private key in a secure manner. The authentication software/firmware shall be executed in the area protected by HSM securing the subscriber private key.	Verify the following 1. Authentication data is communicated to the HSM managing the private key in a secure manner. 2. the authentication software/firmware is executed in the area protected by HSM securing the subscriber private key.	Mandatory	e-authentication guidelines for eSign	
3.9.13.2	The requirements for creation, management and authentication to eKYC account of subscribers and signature creation based on the one time key pair generation and short validity certificates are specified in the earlier sections. The objective of this section is to specify the requirements for ESPs to act as a trusted third party for keeping the subscriber private keys and associated public key certificate. The deviation and additional requirements of subscriber private key life cycle management are described in this section. All other aspects relating to empanelment, signature generation,	Verify the following 1. authentication to eKYC account of subscribers and signature creation based on the one time key pair generation and short validity certificates are in accordance with e-authentication guidelines 2. the aspects relating to empanelment, signature generation, certificate & signature standards are the same as	Mandatory	e-authentication guidelines for eSign	

	certificate & signature standards are the same as eSign service for short validity certificate based electronic signature.	eSign service for short validity certificate based electronic signature.			
3.9.13.3	The overall functionality of the remote key-storage based solution is similar to EU standards (eIDAS, QSCD), however the actual implementation is specific to India PKI based on the architecture & protocol level implementation detailed in the eSign Remote API 1.0.	Check the CA implementation is based on the architecture & protocol level implementation detailed in the eSign Remote API 1.0.	Mandatory	e-authentication guidelines for eSign	
3.9.13.4	As in the case of crypto token, HSM based remote key-storage also shall use PIN as primary authentication. The additional modes of authentication shall be used at eKYC account level by CAs. The ESP/TTP shall use additional modes of authentication at application level before redirecting user to HSM secure key access environment.	Verify that at least two modes of authentication is used , the PIN as primary authentication for HSM key access and one at eKYC account level.	Mandatory	e-authentication guidelines for eSign	
Security Procedure For Protection of Subscriber's Key					
3.9.13.5	For securing private keys of subscriber whether CA implemented any additional functionalities apart from the requirements as mentioned in this document.	Check the additional functionalities apart from the requirements as mentioned in this document, if so provide details	Optional	e-authentication guidelines for eSign	
HSM functionality					
3.9.13.6	A Hardware Security Module (HSM) to ensure the security and subscriber control of private key. The HSM used for securing private keys of subscribers shall be at least FIPS 140-2 Level 3 validated/certified. In addition to generation, authentication, and usage of subscriber private keys, the HSM shall support SAM for secure execution of code.	Check the following 1. HSMs used for securing private keys of subscribers are at least FIPS 140-2 Level 3 validated/certified 2. HSM support SAM for secure execution of code in addition to generation, authentication, and usage of subscriber private keys	Mandatory	e-authentication guidelines for eSign	
3.9.13.7	HSM shall be capable of implementing a secure channel establishment protocol stack for secure subscriber authentication data using secure communication protocol stacks like: TLS 1.2, TLS 1.3 or others offering similar or higher security.	Verify HSM is capable of implementing a secure channel establishment protocol stack for secure subscriber authentication data using secure communication protocol stacks	Mandatory	e-authentication guidelines for eSign	

		like: TLS 1.2, TLS 1.3 or others offering similar or higher security.			
3.9.13.8	The HSM shall not permit export or output of subscriber private keys in any form except for the backup of the entire HSM.	Validate HSM not permit export or output of subscriber private keys in any form except for the backup of the entire HSM.	Mandatory	e-authentication guidelines for eSign	
3.9.13.9	For synchronization of keys in HSM between Main and DR site, FIPS certified synchronization features of HSM shall be used.	Validate the synchronization of keys in HSM between Main and DR site, use FIPS certified synchronization features of HSM only	Mandatory	e-authentication guidelines for eSign	
Subscriber Authentication Module (SAM)					
3.9.13.10	Subscriber Authentication Module (SAM) is software which shall reside in the tamper proof environment protected by HSM. SAM shall utilize the secure channel interface through KMS to securely communicate with the subscribers, including the subscriber authentication.	The requirements mentioned in this section may be examined and verified by the means of one of more of the following : logs generated, code examination, product specification, input/output examination, architecture design , software audit report by cert-in empanelled auditor and testing Verify the following are implemented by CA and examine the proof if applicable:- 1. Subscriber Authentication Module (SAM) reside in the tamper proof environment protected by HSM 2. SAM is utilizing the secure channel interface through KMS to securely communicate with the subscribers, including the subscriber authentication. 3. the software functions such as creation, destruction, signing, authentication is implemented as independent modules under an integrated module in the SAM, 4. the authentication code is not executed	Mandatory	e-authentication guidelines for eSign	
3.9.13.11	In the SAM, the software functions such as creation, destruction, signing, authentication shall be implemented as independent modules under an integrated module.		Mandatory	e-authentication guidelines for eSign	
3.9.13.12	The verification of authentication code must not be executed by any application other than that reside in SAM		Mandatory	e-authentication guidelines for eSign	
3.9.13.13	CA shall provide access to subscriber for key generation & setting Authpin only after the satisfactory completion of identity verification as per IVG		Mandatory	e-authentication guidelines for eSign	
3.9.13.14	SAM shall verify the authentication of subscriber before facilitating any subscriber bound functions		Mandatory	e-authentication guidelines for eSign	
3.9.13.15	Subscriber actions such as communicating with the HSM for PKCS-10 request generation, obtaining the PKCS-10 from the HSM, and setting the Authpin shall be implemented in a single secure session thus providing binding among the subscriber, subscriber's key pair, and Authpin.		Mandatory	e-authentication guidelines for eSign	
3.9.13.16	HSM shall receive the authentication code submitted by subscribers in an encrypted form by the public key corresponding to the private key generated in the HSM.		Mandatory	e-authentication guidelines for eSign	

3.9.13.17	CA/ESP shall not deploy any software code components in the SAM which are not assessed by the empaneled experts.	by any application other than that reside in SAM 5. CA provide access to subscriber for key generation & setting Authpin only after the satisfactory completion of identity verification as per IVG 6. SAM verify the authentication of subscriber before facilitating any subscriber bound functions 7. Subscriber actions such as communicating with the HSM for PKCS-10 request generation, obtaining the PKCS-10 from the HSM, and setting the Authpin is implemented in a single secure session 8. HSM receive the authentication code submitted by subscribers in an encrypted form by the public key corresponding to the private key generated in the HSM 9. No software code components aredeployed in SAM which is not assessed by the empanelled experts. 10. For authentication of end user , SAM use SHA-256 hash of Authpin and a random number of 128 bits or longer in accordance with RFC 2104 or alternative authentication protocols that offer at least as much security 11. The code to be deployed in the SAM is digitally signed by CA 12. The compliance report of authorized cert-in empanelled experts and no non-compliance are present. 13. The logs of software changes / installations made in the SAM are	Mandatory	e-authentication guidelines for eSign	
3.9.13.18	SAM shall perform authentication of end user using SHA-256 hash of Authpin and a random number of 128 bits or longer in accordance with RFC 2104. Alternative authentication protocols shall offer at least as much security		Mandatory	e-authentication guidelines for eSign	
3.9.13.19	The code to be deployed in the SAM shall be digitally signed by CA after security and software code level auditing to ensure security and reliability. The software testing shall be carried out by authorized cert-in empanelled experts. If the SAM functions are natively build in the HSM and certified , the same need not to be examined and tested by the empanelled experts.		Mandatory	e-authentication guidelines for eSign	
3.9.13.20	The logs of software changes / installations made in the SAM shall be archived.		Mandatory	e-authentication guidelines for eSign	
3.9.13.21	CA/ESP shall have dedicated Key Management Server (KMS) to interface with HSM/ SAM and the software module interfacing directly with HSM/SAM should host in KMS. All the communication to KMS server shall be in a request/response format.		Mandatory	e-authentication guidelines for eSign	

		archived. 14. CA/ESP have deployed dedicated Key Management Server (KMS) to interface with HSM/ SAM and the software module interfacing directly with HSM/SAM sis hosted in KMS. 15. All the communication to KMS server are in a request/response format.			
Key generation & management					
3.9.13.22	The CA shall facilitate key pair generation by the subscriber under subscriber's direct control after successful authentication to eKYC account. The Authpin for subsequent successful authorization should be set by the subscriber.	Check the following are implemented by CA and examine the input/out , sample testing if applicable 1. The CA generates key pair for subscriber only after successful authentication to subscriber's eKYC account. 2. The Authpin for subsequent successful authorization is set by the subscriber 3. The HSM securing the private key of subscriber is physically hosted at CA premises or application owner' s premises. 4. HSM securing the private keys of subscribers is under the sole administrative control of CA. 5. The key generation is in the FIPS 140-2 Level 3 validated/certified HSM. 6. Private keys are always be secured by HSM 7. The HSM administrator of the hosting environment cannot perform the subscriber's key authentication function	Mandatory	e-authentication guidelines for eSign	
3.9.13.23	The HSM securing the private keys of subscribers shall be physically hosted in the CA premises or application owners premises however it should be under the sole administrative control of CA.		Mandatory	e-authentication guidelines for eSign	
3.9.13.24	The key generation shall be in the FIPS 140-2 Level 3 validated/certified HSM. Private keys shall always be secured by HSM		Mandatory	e-authentication guidelines for eSign	
3.9.13.25	The HSM administrator of the hosting environment shall not be able to perform the subscriber's key authentication function.		Mandatory	e-authentication guidelines for eSign	
3.9.13.26	For any key management functions eKYC account id, eKYC account PIN and Authpin authentications shall be required.		Mandatory	e-authentication guidelines for eSign	
3.9.13.27	To ensure the centrally stored private key is bound to the subscriber, implement all subscriber actions such as communicating with the HSM for PKCS-10 generation, obtaining PKCS-10 from the HSM, and setting the Authpin in a single secure session. This secure session shall be available to the subscriber for key generation & setting Authpin only after the satisfactory completion of identity verification as per IVG		Mandatory	e-authentication guidelines for eSign	

3.9.13.28	The key management function by CA is limited only to deletion backup and restore	8. For any key management functions eKYC account id, eKYC account PIN and Authpin authentications is required 9. A single session is used for all subscriber actions such as communicating with the HSM for PKCS-10 generation, obtaining PKCS-10 from the HSM, and setting the Authpin . 10. CA provides secure session access to subscriber for key generation & setting Authpin only after the satisfactory completion of identity verification as per IVG 11. The key management function by CA is limited only to deletion backup and restore 12. The private key can be deleted by the subscriber directly or by CA as per the scenarios mentioned under CPS. i.e the private key shall be deleted after revocation. 13. The private key is retained by the HSM beyond the certificate validity period. 14. The certificate renewal, re-key suspension etc., are not allowed under this scheme	Mandatory	e-authentication guidelines for eSign	
3.9.13.29	The private key can be deleted by the subscriber directly or by CA as per the scenarios mentioned under CPS. i.e the private key shall be deleted after revocation.		Mandatory	e-authentication guidelines for eSign	
3.9.13.30	The private key shall not be retained by the HSM beyond the certificate validity period.		Mandatory	e-authentication guidelines for eSign	
3.9.13.31	The certificate renewal, re-key suspension etc., are not allowed under this scheme		Mandatory	e-authentication guidelines for eSign	
Authpin Authentication					
3.9.13.32	SAM shall perform subscriber authentication related functions	Verify the following :- 1. The subscriber authentication related functions are carried out by SAM 2. Authpin for activation of the private	Mandatory	e-authentication guidelines for eSign	
3.9.13.33	Authpin for activation of the private key shall be stored along with eKYC id		Mandatory	e-authentication guidelines for eSign	

3.9.13.34	Authpin shall be 6 characters in length	key is stored along with eKYC id 3. Authpin I of 6 characters in length 4. A secure session is used for both auth pin authentication & data submission 5. The maximum number of consecutive Authpin retries does not exceed 10 after which the account will be temporarily locked out for a period of no less than one hour or until HSM Trusted Administrator takes action. 6. Upon three consecutive lockouts, the account will be permanently locked out. 7. CA provided mechanism for resetting Authpin by the subscriber 8. The authe PIN reset is only after a successful video verification of the subscriber	Mandatory	e-authentication guidelines for eSign	
3.9.13.35	To protect the Authpin from exposure & binding to data to be signed, HSM shall use a secure session for submission of the data to be signed, once the Authpin authentication succeeds.		Mandatory	e-authentication guidelines for eSign	
3.9.13.36	The maximum number of consecutive Authpin retries shall be 10 after which the account shall be temporarily locked out for a period of no less than one hour or until HSM Trusted Administrator takes action. Upon three consecutive lockouts, the account shall be permanently locked out.		Mandatory	e-authentication guidelines for eSign	
3.9.13.37	Upon permanent locked out of account, CA should provide mechanism for resetting Authpin by the subscriber after a successful video verification of the subscriber		Mandatory	e-authentication guidelines for eSign	
Roles, privileges and access control					
3.9.13.38	The following human users or IT entity with designated roles & privileges interact with SAM	Verify the following:- CA implemented the following human users or IT entity with designated roles & privileges to interact with SAM 1. Users - the authorised and registered subscribers 2. HSM Administrator: Handling software code, initialization of subscriber 3. Administrator -security, user management and other administrative functions 4. Verification agent - establishing the identity of the signatory, providing this data to the SAM ensuring it's integrity and initiating the lifecycle of the	Mandatory	e-authentication guidelines for eSign	
3.9.13.39	Users - the authorised and registered subscribers		Mandatory	e-authentication guidelines for eSign	
3.9.13.40	HSM Administrator: Handling software code, initialization of subscriber		Mandatory	e-authentication guidelines for eSign	
3.9.13.41	Administrator -security, user management and other administrative functions		Mandatory	e-authentication guidelines for eSign	
3.9.13.42	Verification agent - establishing the identity of the signatory, providing this data to the SAM ensuring it's integrity and initiating the lifecycle of the signatory account. Signatory account creation and initialization shall not allow without verification agent's authentication.		Mandatory	e-authentication guidelines for eSign	
3.9.13.43	Auditor -The auditor is in charge of performing the audit functions		Mandatory	e-authentication guidelines for eSign	

		signatory account. Signatory account creation and initialization are not allowed without verification agent's authentication. 5. Auditor -The auditor is in charge of performing the audit functions			
Software Modules					
3.9.13.44	CA shall implement the following software components in the CA systems for interfacing with HSM for management of eKYC account synchronization, key management, certificate management, Authpin management , and signature as per eSign Remote API 1.X	Verify the following 1. CA has implemented the following software components in the CA systems for interfacing with HSM for management of eKYC account synchronization, key management, certificate management, Authpin management , and signature as per eSign Remote API 1.X a) CHI- eKYC account synchronization, key management, certificate management, Authpin management shall be managed by CA-HSM Interface (CHI) software module b) SHI- The Signing-HSM interface (SHI) module shall interface with HSM for signature functionalities. The SHI module may be hosted in the CA or at trusted third party site. c) AI- CA shall implement Authentication Interface(AI) software component as per eSign API 1.x for interfacing with subscriber and HSM for authentication. 2. All communication between CHI, SHI and AI is signed & encrypted through	Mandatory	e-authentication guidelines for eSign	
3.9.13.45	CHI- eKYC account synchronization, key management, certificate management, Authpin management shall be managed by CA-HSM Interface (CHI) software module		Mandatory	e-authentication guidelines for eSign	
3.9.13.46	SHI- The Signing-HSM interface (SHI) module shall interface with HSM for signature functionalities. The SHI module may be hosted in the CA or at trusted third party site.		Mandatory	e-authentication guidelines for eSign	
3.9.13.47	AI- CA shall implement Authentication Interface(AI) software component as per eSign API 1.x for interfacing with subscriber and HSM for authentication.		Mandatory	e-authentication guidelines for eSign	
3.9.13.48	All communication between CHI, SHI and AI shall be signed & encrypted through secure channel		Mandatory	e-authentication guidelines for eSign	
3.9.13.49	CHI, SHI and AI modules shall be digitally signed by CA.				

		secure channel 3. CHI, SHI and AI modules are digitally signed by CA.			
CA Requirements					
3.9.13.50	The procedure to be followed for issuance of crypto token based certificates and eSign services are described/referred in the CPS. The following section will be used as a reference point in the CPS for certificate life cycle & signature service based on remote-key storage	Check the reference points in CPS in respect of certificate life cycle & signature service based on remote-key storage.	Mandatory	e-authentication guidelines for eSign	
CA INFRASTRUCTURE					
3.9.13.51	The CA system used for issuance of crypto token based DSC can be integrated with remote key storage based DSC issuance.	Verify the CA system used for issuance of crypto token based DSC is integrated with remote key storage based DSC issuance.	Mandatory	e-authentication guidelines for eSign	
DSC Application Form					
3.9.13.52	The DSC application form for long term validity DSC issuance on remote key-storage of a subscriber shall be as per the CPS and Schedule IV of IT Act.	Validate the DSC application form for long term validity DSC issuance on remote key-storage of a subscriber is as per the CPS and Schedule IV of IT Act.	Mandatory	e-authentication guidelines for eSign	
3.9.13.53	Response code shall be generated by ESP on eKYC user authentication request for certificate generation and should be a part of DSC & DSC application form. The Response Code should be of length 32.	Validate the response code is generated by ESP on eKYC user authentication request for certificate generation and the same is a part of DSC & DSC application form. The Response Code should be of length 32	Mandatory	e-authentication guidelines for eSign	
3.9.13.54	eSign signer can have one or more eKYC user account	Verify the CA has implemented the option for one or more eKYC user account for the same user.	Mandatory	e-authentication guidelines for eSign	
Key Life cycle & Signature requirements					

3.9.13.55	The key life cycle should be able to handle the following functions : 1. Creation of account in the protected storage area of HSM 2. Enrolment for authentication and signature service 3. Key pair and certificate generation 4. Activation of signature service 5. Use of signature service 6. Deactivation of signature service 7. Deletion of the account created in the SAM	Verify the key life cycle is able to handle the following functions : 1. Creation of account in the protected storage area of HSM 2. Enrolment for authentication and signature service 3. Key pair and certificate generation 4. Activation of signature service 5. Use of signature service 6. Deactivation of signature service 7. Deletion of the account created in the SAM	Mandatory	e-authentication guidelines for eSign	
3.9.13.56	For the certificate life cycle functions which involve HSM interaction, upon successful authentication to eKYC account by subscriber, CA redirect subscriber to HSM environment through CHI.	Verify the following In the case of remote key storage based option implementation by CA, upon successful authentication to eKYC account by subscriber, CA redirect subscriber to HSM environment through CHI.	Mandatory	e-authentication guidelines for eSign	
3.9.13.57	The request/response between CA system and HSM environment shall be as per the eSign Remote API 1.X	Validate that the request/response between CA system and HSM environment is as per the eSign Remote API 1.X	Mandatory	e-authentication guidelines for eSign	
3.9.13.58	eKYC account is pre-requisite for remote key storage. After success authentication to eKYC account by subscriber, CA redirect user to HSM environment for key generation, setting of Authpin, CSR generation, and verification of certificate details and download of certificate through CHI. CA shall ensure that all these actions are happening in a single secure session.	Verify the following 1. eKYC account is created for each remote key storage based option to subscriber. 2.After success authentication to eKYC account by subscriber, CA redirect user to HSM environment for key generation, setting of Authpin, CSR generation, and verification of certificate details and download of certificate through CHI 3.The functions mentioned in 2 are happening in a single secure session	Mandatory	e-authentication guidelines for eSign	
3.9.13.59	Subscriber requesting for revocation shall be redirected to HSM environment through CHI for revocation of certificate. For self-revocation, the authentication to eKYC account is mandatory.	Check the following 1. Subscriber requesting for certificate revocation is redirected to HSM environment through CHI.	Mandatory	e-authentication guidelines for eSign	

		2. CA system allows self-revocation, only after the successful authentication to eKYC account.			
3.9.13.60	The CA trusted persons are also be allowed to revoke after due verification as per the conditions and procedure specified under CPS	Verify CAtrusted persons revoke certificate after due verification per the conditions and procedure specified under CPS	Mandatory	e-authentication guidelines for eSign	
3.9.13.61	The Signing HSM Interface (SHI) module for subscriber signature function can reside at CA premises or trusted third party premises.	Verify the Signing HSM Interface (SHI) module for subscriber signature function is hosted at CA premises or trusted third party premises only	Mandatory	e-authentication guidelines for eSign	
3.9.13.62	The user shall authenticate to eKYC account in the case of SHI is hosted at CA and trusted third party application access account if it is hosted at trusted third party premises	Validate the Signing HSM Interface (SHI) module for subscriber signature function is hosted at CA premises or trusted third party premises only	Mandatory	e-authentication guidelines for eSign	
3.9.13.63	The SHI software component shall redirect subscriber to HSM environment as per the eSign API .1.X	Check the SHI software component redirect subscriber to HSM environment as per the eSign API .1.X	Mandatory	e-authentication guidelines for eSign	
Audit Trail of Account Creation and Maintenance					
3.9.13.64	The audit trail of certificate issuance, key generation, Authpin setting/reset , signature request/response etc should be maintained by CA. The date/time stamp, requested source details etc. also should be accessible for audit.	Check the following 1. The audit trail of certificate issuance, key generation, Authpin setting/reset , signature request/response etc are maintained by CA. 2. The date/time stamp, requested source details etc. are also accessible for audit.	Mandatory	e-authentication guidelines for eSign	
3.9.13.65	A monthly audit of ten percent (subjected to maximum of 5000) of the certificate issuance, signature functions shall be carried out by an IS Auditor in the following month and the report shall be made available during Annual CA compliance Audit.	Check the following 1. A monthly audit of ten percent (subjected to maximum of 5000) of the certificate issuance, signature functions is carried out by an IS Auditor in the following month 2. The report is to auditors of Annual	Mandatory	e-authentication guidelines for eSign	

		CA compliance Audit.			
Account Monitoring facility to eKYC user					
3.9.13.66	The history of certificate issuance, setting PIN, & signature of documents shall be made available to subscribers.	Verify the history of certificate issuance, setting PIN, & signature of documents are available to subscribers.	Mandatory	e-authentication guidelines for eSign	
3.9.13.67	CA shall provide access to the signed transaction details to subscribers	Check the access to the signed transaction details to subscribers is provided by CA	Mandatory	e-authentication guidelines for eSign	
3.9.13.68	ASP should provide mechanism for viewing the signed documents to eSign users.	Verify audit report of ASP and check whether ASP provided mechanism for viewing the signed documents to eSign users	Mandatory	e-authentication guidelines for eSign	

3.10. Other Business and Legal Matters

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)

Fees					
3.10.1.1	The application for the grant of a licence shall be accompanied by a nonrefundable fee of twenty-five thousand rupees payable by a bank draft or by a pay order drawn in the name of the Controller.	1. Verify the required fee was paid along with the application for the grant of a license 2. For renewal of CA's license validate a non-refundable fee of five thousand rupees was paid in the name of controlled 3. Verify the process stats refund will not be done in case license is suspended or revoked 1. Check the following: a. licensed CAs don't charge for access to any certificates b. there is no charge for revocation status information c. CA charges a reasonable fee for access to archived records and key recovery. d. CA has a documented refund process for other than cases where license is suspended or revoked	Mandatory	IT CA Rules 11	
3.10.1.2	The application submitted to the Controller for renewal of Certifying Authority's licence shall be accompanied by a non-refundable fee of five thousand rupees payable by a bank draft or by a pay order drawn in the name of the controller.		Mandatory	IT CA Rules 11	
3.10.1.3	Fee or any part thereof shall not be refunded if the license is suspended or revoked during its validity period		Mandatory	IT CA Rules 11	
3.10.1.4	Licensed CAs may not charge for access to any certificates		Recommended	X.509 Policy 9.1.2, CA Browser Forum 9.1.2	
3.10.1.5	Licensed CAs may not charge for access to any revocation status information		Recommended	X.509 Policy 9.1.3, CA Browser Forum 9.1.3	
3.10.1.6	Licensed CAs may set any reasonable fees for any other services such as access to archive records or key recovery.		Recommended	X.509 Policy 9.1.4, , CA Browser Forum 9.1.4	
3.10.1.7	Licensed CAs may, but are not required to, have a documented refund process.		Recommended	X.509 Policy 9.1.5, CA Browser Forum 9.1.5	
Financial Responsibility					

3.10.1.8	Every Certifying Authority shall comply with all the financial parameters during the period of validity of the licence, issued under the Act Licensed CAs shall also maintain reasonable levels of insurance coverage to address all foreseeable liability obligations to PKI Participants	1. Validate CA complies with all the financial parameters during the period of validity of the licence, issued under the Act 2. Verify the CA Insurance coverage addresses all foreseeable liability obligations to PKI Participants 3. Check that the CA has reasonable and sufficient financial resources sufficient to maintain operations fulfill duties, and address commercially reasonable liability obligations to PKI Participants. 4. Check whether the CA provides protection to end entities that are not covered in the CP (optional)	Mandatory	IT Regulations 3, X.509 Policy 9.2.1, CA Browser Forum 9.2.1	
3.10.1.9	Licensed CAs shall also maintain reasonable and sufficient financial resources to maintain operations, fulfill duties, and address commercially reasonable liability obligations to PKI Participants. Any loss to the subscriber, which is attributable to the Certifying Authority, shall be made good by the Certifying Authority.		Mandatory	X.509 Policy 9.2.2, IT Regulations 3, CA Browser Forum 9.2.2	
3.10.1.10	Licensed CAs may, but are not required, to offer protection to end entities that extends beyond the protections provided in this CP. Any such protection shall be offered at commercially reasonable rates.		Recommended	X.509 Policy 9.2.3, CA Browser Forum 9.2.3	
Confidentiality of Business Information					
3.10.1.11	Each licensed CA shall maintain the confidentiality of confidential business information that is clearly marked or labeled as confidential, or by its nature should reasonably be understood to be confidential, and shall treat such information with the same degree of care and security as the licensed CA treats its own most confidential information.	1. Verify the maintains the confidentiality of confidential business information that is clearly marked or labeled as confidential	Mandatory	X.509 Policy 9.3, CA Browser Forum 9.3	
Privacy of Personal Information					
3.10.1.12	Licensed CAs may store, process, and disclose personally identifiable information in accordance with the privacy policy of that licensed CA.	1. Obtain the privacy policy of the CA 2. Check that the past PII data disclosed by the CA was in accordance with its privacy policy	Recommended	X.509 Policy 9.4, CA Browser Forum 9.4	

Intellectual Property Rights					
3.10.1.13	Licensed CAs shall not knowingly violate any intellectual property rights held by others	1. Validate that CA has established processes to ensure it knowingly does not violate any intellectual property rights held by others	Mandatory	X.509 Policy 9.5, CA Browser Forum 9.5	
Representations and Warranties					
3.10.1.14	Licensed CAs represent and warrant that: • Their CA signing private key is protected and that no unauthorized person has ever had access to that private key; • All representations made by the licensed CA in any applicable agreements are true and accurate, to the best knowledge of the applicable CA; and • 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. • Only verified information appears in the certificate	1. Validate that the CA warrants the elements mentioned in the control	Mandatory	X.509 Policy 9.6.1, CA Browser Forum 9.6.1	
3.10.1.15	A Subscriber shall be required to sign a document (e.g., a subscriber agreement) containing the requirements the Subscriber shall meet respecting protection of the private key and use of the certificate before being issued the certificate In signing the document described above, each Subscriber shall agree to the following: • Subscriber shall accurately represent itself in all	1. Obtain the copies of subscriber agreements which contain controls on protection of private key 2. Validate that the agreement between subscriber and CA contains the elements mentioned in the control	Mandatory	X.509 Policy 9.6.2, CA Browser Forum 9.6.3	

	communications with the PKI authorities. • The data contained in any certificates issued to Subscriber is accurate. • The Subscriber shall protect its private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures • The Subscriber lawfully holds the private key corresponding to public key identified in the Subscriber's certificate. • The Subscriber will abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates. • Subscriber shall promptly notify the appropriate CA upon suspicion of loss or compromise of their private keys. Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS.				
3.10.1.16	Parties who rely upon the certificates issued under a policy defined in this document shall: • Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension); • Check each certificate for validity, using procedures described in RFC 5280, prior to reliance; • 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.	1. Validate that the Parties who rely upon the certificates issued follow the elements in the control	Mandatory	X.509 Policy 9.6.3, CA Browser Forum 9.6.4	
Disclaimers of Warranties					

3.10.1.17	To the extent permitted by applicable law and any other related agreements, licensed CAs may disclaim all warranties (other than any express warranties contained in such agreements or set forth in the licensed CA's CPS).	1. Obtain logs of CA disclaiming warranties in the past 2. Check that this was done in accordance with the local laws	Recommended	X.509 Policy 9.7, CA Browser Forum 9.7	
Limitations of Liabilities					
3.10.1.18	Licensed CAs may limit liabilities as long as they meet the liability requirements stated in [ITACT 2000].	1. Obtain logs of past liabilities limited by the CA 2. Validate that this took place in accordance with the IT ACT 2000 3.	Recommended	X.509 Policy 9.8, CA Browser Forum 9.8	
Indemnities					
3.10.1.19	Licensed CAs includes indemnification clauses as long as the clauses are consistent with [IT ACT 2000].	1. Check the contracts for indemnification clauses 2. Validate that these clauses are in accordance with the IT ACT 2000	Mandatory	X.509 Policy 9.9, CA Browser Forum 9.9	
Term and Termination					
3.10.1.20	The CP becomes effective upon ratification by the Controller. Amendments to this CP become effective upon ratification by the Controller and publication at http://www.cca.gov.in/resource/CP.pdf	1. Verify the CP became effective upon ratification by the Controller 2. Validate the CP became effective upon ratification by the Controller and publication at CCA website under mentioned link 3. Check the following: a. CP remains in force until replaced by newer version or explicitly terminated by Controller b. Upon termination of CA,	Mandatory	X.509 Policy 9.10, CA Browser Forum 9.10	
3.10.1.21	While this CP may be amended from time to time, it shall remain in force until replaced by a newer version or explicitly terminated by the Controller.		Mandatory	X.509 Policy 9.10, CA Browser Forum 9.10	
3.10.1.22	Upon termination of this CP, licensed CAs are nevertheless bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates		Mandatory	X.509 Policy 9.10, CA Browser	

		licensed CAs are bound by its terms for all Certificates issued for the remainder of the validity periods of such Certificates		Forum 9.10	
Individual Notices and Communications with Participants					
3.10.1.23	Unless otherwise specified by agreement between the parties, licensed CAs shall use commercially reasonable methods to communicate, taking into account the criticality and subject matter of the communication	1. Identify and verify licensed CAs uses commercially reasonable methods to communicate, taking into account the criticality and subject matter of the communication	Mandatory	X.509 Policy 9.11, CA Browser Forum 9.11	
Amendments					
3.10.1.24	The Controller shall review this at least once every year. Additional reviews may be enacted at any time at the discretion of the Controller	1. Verify the controller reviews amendments at least once every year 2. Validate that the amendments recommended by the Controller have been inculcated 3. Verify the most up to date copy of the CP is uploaded at http://www.cca.gov.in 4. Validate errors, and anticipated changes to CP resulting from reviews have been published online at http://www.cca.gov.in 5. Check CP and subsequent changes were made publicly available within seven days of approval	Mandatory	X.509 Policy 9.12, CA Browser Forum 9.12	
3.10.1.25	If the Controller wishes to recommend amendments or corrections to the CP, such modifications shall be circulated to the licensed CAs. Comments from the licensed CAs shall be collected and adjudicated by the Office of CCA. Controller shall use commercially reasonable efforts to immediately notify licensed CAs of changes		Mandatory	X.509 Policy 9.12, CA Browser Forum 9.12	
3.10.1.26	Errors, and anticipated changes to this CP resulting from reviews are published online at http://www.cca.gov.in. The most up to date copy of the CP can be found at http://www.cca.gov.in This CP and any subsequent changes shall be made publicly available within seven days of approval.		Mandatory	X.509 Policy 9.12, CA Browser Forum 9.12	
Dispute Resolution Provisions					

3.10.1.27	Provisions for resolving disputes between a licensed CA and its Customers shall be set forth in the applicable agreements between the parties. Dispute resolution procedures shall be consistent with [IT ACT 2000].	1. Verify provisions have been made for resolving disputes between licensed CA and its customer 2. Check provisions have been covered in applicable agreements between the parties	Mandatory	X.509 Policy 9.13, CA Browser Forum 9.13	
Governing Law					
3.10.1.28	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 Information Technology shall govern the construction, validity, enforceability and performance of actions per this CP.	1. Validate the regulations and guidelines mentioned in control description govern the construction, validity, enforceability and performance of actions per the CP	Mandatory	X.509 Policy 9.14, CA Browser Forum 9.14	
Compliance with Applicable Law					
3.10.1.29	This CP 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.	1. Validate that the CA is compliant to the applicable to 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.	Mandatory	X.509 Policy 9.15, CA Browser Forum 9.15	
Miscellaneous Provisions					
3.10.1.30	If any provision of this CP is held to be invalid by a court of competent jurisdiction, then the remaining provisions will nevertheless remain in full force and effect.	1. Verify the CA is aware if any provision of this CP is held to be invalid by a court of competent	Mandatory	X.509 Policy 9.16, CA Browser	

		jurisdiction, then the remaining provisions will nevertheless remain in full force and effect		Forum 9.16	
3.10.1.31	Licensed CAs shall not be liable for any failure or delay in its performance under this CP 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, failure of equipment, failure of telecommunications lines, lack of Internet access, sabotage, and governmental action.	2. Verify the CA is aware it shall not be liable for any failure or delay in its performance under this CP due to causes that are beyond their reasonable control	Mandatory	X.509 Policy 9.16, CA Browser Forum 9.16	

3.11. CA website, Application software , CA software requirements

3.11.1 Compliance Requirements for the Application system.

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
The applicant software provides external access to users. The compliance requirements for the software are below.					
3.11.1.1	The verification requirements shall be as per CCA-IVG. The applicant software should have strictly implemented the functions as mentioned in the Guidelines issued by CCA	Verify the following w.r.t controls 1. RA software specifications	Mandatory	CCA-CALIC 2.1 **Annexure VI**	
Application Interface Software					

3.11.1.2	The verification requirements shall be as per CCA-IVG. The applicant software should have strictly implemented the functions as mentioned in the Guidelines issued by CCA.	Verify the following 1. VA-PT by Cert-in empanelled auditor and Its closure 2. Internal VA-PT report and its closure	Mandatory	CCA-CALIC 2.1 **Annexure VI**	
Audit Logs and Evidence Requirements					
3.11.1.3	The applicant software must generate audit logs for user actions, user failures, and modifications to the configuration	Verify the following 1. Roles defined in the RA software and its privilege given. As this is critical , the the corresponding software, schema and interaces may be checked to verify the practices followed by CA against the procedure mentioned in IVG 2. Whether role based access implemented 3. subscriber and RA roles maintained 4. RA's access to applicants' information is limited only up to the approval by CA 5. RA's page view shall be restricted to RA who facilitated the DSC application form submission only	Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.1.4	The audit logs shall be secured in the CA facility with physical and system access controls as required for CA operations.		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.1.5	The audit logs should be stored in the CA facility.		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.1.6	The audit logs are to be protected for data integrity preferably using Syslog servers		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.1.7	The applicant interface access shall be periodically reviewed.		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
Session Time-out					
3.11.1.8	In the eKYC account creation process, inactivity time limits shall be enforced. The activity time limits shall be as per the following 1. eSign-based Signature - Immediate 2. eKYC account Information submission - 20 minutes 3. OTP authentication - 5 minutes	1. Check whether inactivity time limits are enforced.	Mandatory	CCA-CALIC 2.1 **Annexure VI**	

	4. DSC applicant Login - 20 Minutes 5. Exit upon inactivity - 5 minutes				

3.11.2 Compliance Requirements for the CA system.

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
3.11.2.1	1. The CA management software is expected to be certified as CC EAL4 or higher in consistent with the Certificate Issuing and Management Components Protection Profile, Version 1.5. (NIST) or Protection Profile for Certification Authorities or both. 2. The CAs are encouraged to obtain Common Criteria EAL4+ certification ASAP. In case the CA software does not have certification at present, as an interim measure, a security audit of the CA software shall be carried out as per "4. Security Evaluation Requirements for CA". The compliance report in this regard should be made available to the empanelled auditors. The broad areas to be covered but not limited to the security audit of CA software are below:	Verify w.r.t controls 1. Verify the certificate scope, validity etc.& consistency with the profiles 2. If not certified verify "Security Evaluation Requirements for CA" report till the specified period.		CCA-CALIC 2.1 Annexure VI	
3.11.2.2	Security Policy	1. The compliance report in this regard should be made available to the empanelled auditors. The broad areas to be covered but not limited to the Software Application Testing & Evaluation scope are below : • Security Policy • Roles (Administration Officers,	Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.3	Roles (Administration Officers, Registration Officers, Authentication Officers)		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.4	Access Control and Authorization		Mandatory	CCA-CALIC 2.1 **Annexure VI**	

3.11.2.5	Identification and Authentication	Registration Officers, Authentication Officers) • Access Control and Authorization • Identification and Authentication • Remote Data Entry and Export • Key Management: Key Generation, Key Storage, Key Destruction, and Key Export • Cryptographic module requirements • Profile Management(Certificate, CRL, OCSP) • Certificate applicant data registration • Certificate Registration • Certificate Preparation • Certificate approval • Certificate Signing • Certificate Activation • Certificate storage & delivery • Certificate Publication • Certificate Revocation • Certificate Status Information Provision – OCSP, CRL • CA Policy Administration • Key Archiving and Recovery • PIN Management • Audit and Log Review	Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.6	Remote Data Entry and Export		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.7	Key Management: Key Generation, Key Storage, Key Destruction, and Key Export		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.8	Cryptographic module requirements		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.9	Profile Management(Certificate, CRL, OCSP)		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.10	Certificate applicant data registration		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.11	Certificate Registration		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.12	Certificate Preparation		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.13	Certificate approval		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.14	Certificate Signing		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.15	Certificate Activation		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.16	Certificate storage & delivery		Mandatory	CCA-CALIC 2.1 **Annexure VI**	

3.11.2.17	Certificate Publication	• Batch Processing • Communication with RA Software • Initial Boot Process Threats(Authorised user threats, System related threats, Cryptography related threats, External attacks)	Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.18	Certificate Revocation		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.19	Certificate Status Information Provision – OCSP, CRL		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.20	CA Policy Administration		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.21	Key Archiving and Recovery		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.22	PIN Management		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.23	Audit and Log Review		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.24	Batch Processing		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.25	Communication with RA Software		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.26	Initial Boot Process		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.2.27	Threats(Authorised user threats, System related threats, Cryptography related threats, External attacks)		Mandatory	CCA-CALIC 2.1 **Annexure VI**	

3.11.3 Compliance Requirements for the CA Website

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
3.11.3.1	CA website shall display current past versions of CPS		Mandatory	CCA-CALIC 2.1 Annexure VI	
3.11.3.2	The repository of CA shall be made available to the public		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.3.3	CA website shall provide Interface to the RA portal. CA website shall make available the direct payment options to the DSC applicants.		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.3.4	CA website shall publish CRL and CA certificate details		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.3.5	A help desk for subscribers and application owners shall be provided and the details should be available on the website of CA		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.3.6	Contact details & email shall be published on the CA website		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.3.7	The website shall provide Grievance & Redressal interface		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.3.8	The certificate fees shall be made available on the website		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.3.9	The list of empanelled token providers shall be published by CA on their website.		Mandatory	CCA-CALIC 2.1 **Annexure VI**	

3.11.3.10	CA shall provide a certificate search option for a subscriber based on authentication		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.3.11	The website shall provide eKYC account-related information access as mentioned in the IVG		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.3.12	Provision for submitting the certificate revocation request by a subscriber shall be provided		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.3.13	The website should display the list of directors and the authorised representative details		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.3.14	Ensure that no confidential information is available publically through the CA website		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.3.15	Ensure high availability of the CA website at all levels		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.3.16	If outsourced, CA shall maintain all agreements related to development and hoisting.		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.3.17	Role-wise access control mechanism implemented for the access to the website for updation and administration		Mandatory	CCA-CALIC 2.1 **Annexure VI**	
3.11.3.18	CA shall record the non-availability/hacking/other failure-related incidents and the same shall be made available to auditors.		Mandatory	CCA-CALIC 2.1 **Annexure VI**	

3.11.4 Security Evaluation Requirements for CA

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
3.11.4.1	The overall scope of this security evaluation shall include System architecture, Design, Network, operating system and Software applications (internal & external). Software application audit includes all the software hosted by the organisation such as CA software, website, eSign Application, OCSP, Time Stamping, external eKYC interface (UID, Banking, PAN, GST etc), Mobile Apps, DLL, etc. The only exception is in case CA software and any of the software is already CC EAL 4+ certified. In case of any change, CA should analyse the impact due to change(s) and get a security evaluation concerning the applicable area where there is a significant impact due to the change.	Verify the scope of the security evaluation		CCA-CALIC 2.1 Annexure VI	
3.11.4.2	1. Architecture, Design, Network & Firewall Access Rules (FAR) Review: Evaluation of existing network security architecture, Design, HLDs, LLDs, including topology/configuration, and security components/features, network segmentation inspection of single point of failure, high availability etc.	**1.** Verify the report submitted by the Cert-In empanelled auditor. **2.** Attach the Security audit reportwith the overall audit report	Mandatory	CCA-CALIC 2.**1** Annexure VI	
3.11.4.3	2. Secure Configuration of OS, servers, Network equipment and Database: Evaluation of security practices and their implementation, passwords, Patches, service packs, open ports, unused services, permission, authentication, additional security measures implemented, encryption etc. as per the best practices and security standards.		Mandatory	CCA-CALIC 2.**1** Annexure VI	
3.11.4.4	3. Source Code Review: Testing of the source code of a software application to identify vulnerabilities, security weaknesses, coding errors, and potential areas for improvement. The scope includes all software applications hosted and distributed by CA except CC EAL certified. In case of unavailability of source code, the self-signed certificate from OEM with the present status of vulnerability should be reviewed.		Mandatory	CCA-CALIC 2.**1** Annexure VI	

3.11.4.5	4. Application Security Testing: The active analysis of all the CA applications for any weakness(es), technical flaws, or vulnerabilities as per OWASP Application Security Verification Standard 4.0.3			CCA-CALIC 2.1 Annexure VI	
3.11.4.6	5. Vulnerability Assessment/PT: The vulnerability assessment should cover the Network devices, OS, Applications etc. The vulnerability assessment and penetration testing should cover OWASP Top 10 and SANS Top 25 guidelines for all the applications.			CCA-CALIC 2.1 Annexure VI	
3.11.4.7	6. Functional Testing with reference to the Guidelines issued by CCA: The checklist for the functional testing should be as per CCA-FT			CCA-CALIC 2.1 Annexure VI	
3.11.4.8	7. Mobile APP: The mobile APP shall be tested in accordance with the OWASP- Mobile Application Security Verification Standard v2.1.0			CCA-CALIC 2.1 Annexure VI	
3.11.4.9	8. Digital Forensics Readiness Assessment: The CA shall collect, preserve, protect (temper evident) and analyze digital evidence so that this evidence can be effectively used in any legal matters or court of law. The security audit team should include a forensic expert and should cover tamper-evident logs of devices, applications and operation systems. The final audit report shall contain the status of every round of testing/audit and also the final status after the remedial action taken by CAs. These remedial actions shall be verified and accepted by the auditor. A maximum of 10 calendar days shall be permitted for remedial action. The auditor shall submit its report within 30 days of the initiation of the audit. Any subsequent closure of the audit observation shall be verified by the auditor before submitting it to the Office of CCA.			CCA-CALIC 2.1 Annexure VI	
3.11.4.10	The final audit report shall contain the status of every round of testing/audit and also the final status after the remedial action taken by CAs. These remedial actions shall be verified and			CCA-CALIC 2.1 Annexure VI	

	accepted by the auditor. A maximum of 10 calendar days shall be permitted for remedial action. The auditor shall submit its report within 30 days of the initiation of the audit. Any subsequent closure of the audit observation shall be verified by the auditor before submitting it to the Office of CCA.				

3.11.5 Conditions for Appointment of Auditor

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
3.11.5.1	For annual audits, CAs shall not be allowed to engage the same auditor in consecutive years. However, there is no restriction in other types of audits related to pre-licence audit, Site shifting, enabling new eKYC mode, ESP empanelment, Infrastructure change(hardware, software, application, new DR site) etc 2. In the case of a special audit, CCA will decide the auditor. 3. Cert-in/STQC empanelled auditors shall carry out the annual security audit as per the scope mentioned in Annexure VI 4. The annual audit and security audit shall not be carried out by the same audit agencies. **5.** In case the auditor firm is engaged in any manner in respect of the set-up of CA, then the same auditor shall not audit the CA for the next 3 years. 6. In the case of the CA internal audit by an empanelled auditor, the same auditor shall not be allowed to perform the annual audit of that CA in the same year. **7.** The auditor should provide an undertaking for compliance with these conditions at the time of submitting the annual audit report.	Verify the conditions for the appointment of auditor is complied with.		CCA-CALIC 2.1 Annexure VII	

3.11.6 Financial Status Verification

Control No.	Control	Audit Checks	Control Type	References	Compliance ((Yes/No/NA)
3.11.6.1	The financial status verification shall be carried out by the qualified resource of the empanelled auditor or the agency nominated by CCA The scope includes the following 1. Validate the source of paid-up capital & net-worth 2. Assessment of Business Process and Financial Practices related to DSC issuance 3. Invoice and Tax Evasion 4. Advance payment resulting in financial liability. 5. Any loss to the subscriber which is attributable to the CA. 6. Overall Financial sustainability 7. Latest Audited Balance sheet	Verify the Financial Report.		**CCA-CALIC 2.1** Annexure VIII	

3.12. Instructions for submission of Audit Report

3.12.1 Mode of Submission

Auditor may submit the audit report either physically accompanying the forwarding letter as per 3.11.2 on their letter head duly signed or digitally signed audit report with the forwarding letter as per 3.11.2 may be submitted at email id cca@cca.gov.in and info@cca.gov.in.

3.12.2 Format of Forwarding letter

To

Controller of Certifying Authorities
Ministry of Electronics & Information Technology
Electronics Niketan, 06, CGO Complex, Lodhi Road
New Delhi- 110 003.

Sir/Madam

We have audited the assertion by the management of **<ABC>** Certifying Authority that its CA services as established at **<XYX>** Location, **(as on dd/mm/yyyy for the pre-operations audits/ for the period dd/mm/yyyy to dd/mm/yyyy in the case of an existing CA)** include effective controls over its operations in conformity with the Information Technology Act, 2000, the Rules and Regulations there under, and Guidelines issued, as relating to:

- Security policy and planning;
- Physical security;
- Technology evaluation;
- Certifying Authority's services administration;
- Relevant Certification Practice Statement;
- Compliance to relevant Certification Practice Statement;
- Contracts/agreements;
- Regulations prescribed by the Controller;
- Policy requirements of Certifying Authorities Rules, 2000.
- WebTrust Requirements for Certification Authorities

As part of the above, we have audited the CA services at **[ABC CA, Location(s)]** for compliance as per Rule 31 notified vide Gazette Notification GSR 789(E) dated 17.10.2000 under the Information Technology (IT) Act. Under this, we have specifically checked for compliance to the Rules under Information Technology Act, Regulations & guidelines/documents issued by the Office of CCA as per Audit Criteria for Certifying Authorities published on the CCA website at http://cca.gov.in/sites/files/pdf/guidelines/ CCA-CAAC.pdf, and any other instruction(s) given by the Office of CCA.

The audit was conducted during the period **dd/mm/yy to dd/mm/yyyy.**

ABC-CA's management is responsible for its assertion. Our responsibility is to express an opinion on management's assertion based on our audit.

In our view, ABC-CA's management's assertion is fairly stated, in all materials respect in accordance with Information Technology Act, 2000, the Rules and Regulations thereunder and guidelines till the period during which the audit was done. As part of Audit, following is submitted:

a) Detailed Audit report as per the Audit Criteria for Certifying Authorities, Ver…..
b) Summary of non-compliances as per the format at Annexure-A1
c) The details of <ABC> CA as Annexure-A2
d) Audit Schedule completed as per Annexure A4
e) Additional pages of Auditors Notes as Annexure A3
f) The report of DSC compliance of as Annexure A5(in the case of annual audit)
g) The compliance to eSign API request/response format as Annexure A6(in the case of ESP empanelment Audit)
h) Verify and submit reports as per Annexure VI-Security Evaluation Requirements for CA & CCA-FT of CCA-CALIC
i) Verify and submit reports as per VIII-Financial Status Verification of CCA-CALIC
j) Verify and submit reports as per Annexure VIII-Financial Status Verification of CCA-CALIC
k) Undertaking by Auditor in respect of Annexure VIII-Financial Status Verification

The projection of any conclusions, based on our finding, to future periods is subject to risk that (1) changes may have been made to the system or controls (2) changes may have been made in processing requirements (3) changes may have been required because of the passage of time, or (4) degree of compliance with the policies or procedure may have altered the validity of such conclusions.

The relative effectiveness and significance of specific controls at ABC-CA and their affect on assessment of control risk for subscribers and relying parties are dependent on their interaction with the controls, and other factors present at individual subscriber and relying party locations.

This report is issued for the limited purpose of **[award of CA licence or renewal of CA licence or annual audit in accordance with Rule 31- choose, whichever applicable]** solely for the information and use of the Controller of Certifying Authorities and management of ABC-CA. The audit report is not intended to be and should not be used for any other purposes without the prior express consent of both, the Controller and the Auditor.

[Name of Empanelled Auditor firm]

[City]

[Date of report]

Annexure-A1

Audit Criteria for Certifying Authorities, Ver…...

Summary of non-compliances observed

S. No.	Control No	Reference(s)	Non-compliance observed	Action taken by CA, if any	Remarks

Auditor's Opinion on CA's worthiness for Fresh Licence/Renewal/Continued operation

Annexure-A2

Details of CA (To be filled by CA &Verified by the Auditor)

1. Annual Audit period details

S. No.	Description	From	To	Brief details of open observation (max 50 words)
1	Audit period of last Annual Audit			
2	Audit period of this Annual Audit			
3	Audit period of next Annual Audit			
Verification by Auditor:				

2. Internal Audit Details

S. No.	Description	From	To	Brief details of open observation (max 50 words)	Details of Auditors
1	Date of Last Internal Audit				
2	Date of next Internal Audit				
Verification by Auditor:					

3. eKYC account Audit Details of last one year-Month wise -– during the annual audit period

S. No.	Month	From	To	Summary of Observations	Details of Auditors
1					
2					
Verification by Auditor:					

4. eKYC account-based verification enabled by CA- Details of the audit Period

S. No.	Option	Date of Approval by CCA	No DSCs issued During the audit period	Associated External service	Details of external services
1	Offline Aadhaar eKYC				
2	Online Aadhaar eKYC			KUA Licence date:	
3	PAN eKYC			PAN KYC service details:	
4	CA eKYC				
5	Organisational eKYC			GST Service Details	
6	Banking eKYC			Name of Banks	
Verification by Auditor:					

5. RA audit details – during the annual audit period

S. No.	Description	Details
1	Number of RAs	Total RAs, (b) Active RAs
2	Dates of RA Audit	
3	Details of Non-Compliance reported by RAs	
4	Action Taken by CAs	

Verification by Auditor:

6. No of Court Cases /Police Complaints

S. No.	Description	Details
1	Number of active court cases related to verification prior to issuance of DSC Exists before the audit period	
2	Number of court cases related to verification prior to issuance of DSC Registered during the audit period	
3.	No of police complaints against CA on DSC issuance/verification related Activities.	
Verification by Auditor:		

7. No of revocation of DSC during the audit period

S. No.	Description	Details
1	Number of DSCs revoked	
2	Number of revocation requests received from subscriber/organizations& reasons	
3.	Number of DSCs revoked by CAs & reasons	
Verification by Auditor:		

8. Empanelment of crypto Token

S. No.	Brand Name of Token	Details of OEM	Make In India Percentage	FIPs certification up to	Details of security Audit of Crypto token
1					
2					
3					
Verification by Auditor:					

9. Details of CA software/Website

S. No.	Description	Developed by	Database Used	Certification	Last security Audit
1	CA Software				
2	OCSP				
3.	TSA				
4	RA Software				
5	eSign service software				
6	Website				
Verification by Auditor:					

10.Details of DC & DR Site

S. No.	Description	Location	No of CA administrators	No of System administrators	No of CA Operators	No of Verification Officers	Total CA Manpower
1	Main Site						
2	DR Site						
3	Any other location						
Verification by Auditor:							

11.Details of CA Services

S. No.	Description	Internal Only	External service	No of ASPs/ Organizations
1	eSign service based on Aadhaar			
	eSign service based on CA eKYC service			
2	Timestamping			
Verification by Auditor:				

12.Details of ASP

S. No.	Description	Details
1	No of ASPs	
2	No of ASPs whose audit exceed more than One year	
Verification by Auditor:		

13.Public Information maintained at the website of CA

S. No.	Description	Website Link
1	CA certificates	
2	CA CRLs	
3	Repository	
4	CA help desk	
5	DSC price List	
6	Interface for DSC applicants to apply for DSC	
7	CA Licensing Details	
8	CA current CPS & earlier versions	
Verification by Auditor:		

14.Cost of Certificates issued during audit period.

S. No.	Name	
1.	Average expenditure for issuance of one DSC and maintenance of the Details for a period of 7 years after expiry of DSC	
2	Average fee charged for one DSC by CA	
3.	Detailed explanation , sustainability plan if the average fee charged is less than average cost of certificates.	
Verification by Auditor:		

15. CA Self-assessment for audit period.

S. No.	Name	
1.	No of DSC issued without any DSC application Forms, if any & reason for non-compliance.	
2	No of DSC issued without charging fee, if any & details.	
3.	No DSC issued without having physical verification(video/Biometric Aadhaar) if any	
4.	No of DSC issued(except for foreign nationals) whose name is not matching with as that of in Aadhaar or PAN, if any & reason for noncompliance.	
5	Whether CA system allows sending common OTP to many customers? If Yes, reason for such non-compliance?	
6.	Whether access to CA system is based on single URL-point or allows Link based access. If link-based access allowed, provide details in respect of coverage of such access in the security audit, annual audit & int audit. The details of vulnerabilities and non-compliance noted for each type of links.	
7	The effort taken by CA to find out the own-noncompliance and action Taken during the audit period	
Verification by Auditor:		

16.CA Software and external connectivity.

S. No.	Name	
1.	Type of each type of external connectivity allowed and details such as access location person etc Also reference to the coverage under the audit, risk assessment etc	
2.	Frequency of backup synchronization with DR Site	
3	Data loss occurred during the audit period?	
4.	If data loss occurred, how it was addressed?	
Verification by Auditor:		

17.Down time during the Audit period.

S. No.	Name	
1.	Total service down time during the audit period, if any.	
2.	Reason for non-availability of service and remedial measures taken.	
Verification by Auditor:		

18. List of CA trusted persons

S. No.	Name	Designation	Location of Posting DC/DR	Role in CA	ID Card No & Mobi	Identification Details in the CA Payroll	Employed Since	Training details	Date of last background verification
Verification by Auditor:									

3.13. Annexure A

3.13.1. Supporting Documents accompanying the Application

Category	Document to be submitted
Government Organization	1. Application form. 2. KYC documents: No documents are required. 3. Audit report. 4. Go Live checklist.
Authority Constituted under Central Act	1. Application form. 2. KYC documents a. Copy of the act under which the organization is constituted. 3. Audit report. 4. Go Live checklist
Not for Profit Organization/Special Purpose	1. Application form. 2. KYC documents a. Letter of authority, authorizing the signatory to sign documents on behalf of the organization. b. Documentary proof for Not-for-profit company/ special purpose organization of National importance. 3. Audit report. 4. Go Live checklist.
Bank/ Financial Institution/ Telecom Company	1. Application form. 2. KYC documents a. Letter of authority, authorizing the signatory to sign documents on behalf of the organization. b. License issued by competent authority to run a bank / financial institution / telecom company in India. 3. Audit report. 4. Go Live checklist
Legal entity registered in India	1. Application form. 2. KYC documents a. certificate of incorporation, partnership deed or any other document in support of the Agency being a legal entity registered in India b. List of names of CEO/CFO/directors/partners/ trustees/person-in-charge of the agency along with the organization chart c. Letter of authority authorizing the signatory to sign documents on behalf of the organization 3. Additional documents a. Self-declaration stating that the entity has not been blacklisted by any State Government, Central

	Government, PSUs, Statutory, Autonomous, or Regulatory body in last five years. 4. Audit report. 5. Go Live checklist.

3.13.2. RFC 2119

Note that the force of these words is modified by the requirement level of the document in which they are used.

1. MUST

This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.

2. MUST NOT

This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.

3. SHOULD

This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.

4. SHOULD NOT

This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.

5. MAY

This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

6. Guidance in the use of these Imperatives

Imperatives of the type defined in this memo must be used with care and sparingly. In particular, they MUST only be used where it is actually required for interoperation or to limit behavior which has potential

for causing harm (e.g., limiting retransmissions) For example, they must not be used to try to impose a particular method on implementors where the method is not required for interoperability.

7. Security Considerations

These terms are frequently used to specify behavior with security implications. The effects on security of not implementing a MUST or SHOULD, or doing something the specification says MUST NOT or SHOULD NOT be done may be very subtle. Document authors should take the time to elaborate the security implications of not following recommendations or requirements as most implementors will not have had the benefit of the experience and discussion that produced the specification.

8. Acknowledgments

The definitions of these terms are an amalgam of definitions taken from a number of RFCs.

3.13.3. Business Practices Disclosure Topics

The CA maintains controls to provide reasonable assurance that it's Certificate Policy and Certification Practice Statement address the topics from RFC 3647 or RFC 2527 listed below.

3.13.3.1. RFC 3647

Section No.	*RFC 3647 Section*
1	Introduction
1.1	Overview
1.2	Document Name and Identification
1.3	PKI Participants
1.3.1	Certification Authorities
1.3.2	Registration Authorities
1.3.3	Subscribers
1.3.4	Relying Parties
1.3.5	Other Participants
1.4	Certificate Usage
1.4.1	Appropriate Certificate Uses
1.4.2	Prohibited Certificate Uses
1.5	Policy Administration
1.5.1	Organization Administering the Document
1.5.2	Contact Person
1.5.3	Person Determining CPS Suitability for the Policy
1.5.4	CPS Approval Procedures
1.6	Definitions and Acronyms
2	Publication and Repository Responsibilities
2.1	Repositories

2.2	Publication of Certification Information
2.3	Time or Frequency of Publication
2.4	Access Controls on Repositories
3	Identification and Authentication
3.1	Naming
3.1.1	Type of Names
3.1.2	Need for Names to be Meaningful
3.1.3	Anonymity or Pseudonymity of Subscribers
3.1.4	Rules for Interpreting Various Name Forms
3.1.5	Uniqueness of Names
3.1.6	Recognition, Authentication, and Role of Trademarks
3.2	Initial Identity Validation
3.2.1	Method to Prove Possession of Private Key
3.2.2	Authentication of Organization Identity
3.2.3	Authentication of Individual Identity
3.2.4	Non-Verified Subscriber Information
3.2.5	Validation of Authority
3.2.6	Criteria for Interoperation
3.3	Identification and Authentication for Rekey Requests
3.3.1	Identification and Authentication for Routine Rekey
3.3.2	Identification and Authentication for Rekey After Revocation
3.4	Identification and Authentication for Revocation Request
4	Certificate Life Cycle Operational Requirements
4.1	Certificate Application
4.1.1	Who Can Submit a Certificate Application
4.1.2	Enrolment Process and Responsibilities
4.2	Certificate Application Processing
4.2.1	Performing Identification and Authentication Functions
4.2.2	Approval or Rejection of Certificate Applications
4.2.3	Time to Process Certificate Applications
4.3	Certificate Issuance
4.3.1	CA Actions During Certificate Issuance
4.3.2	Notifications to Subscriber by the CA of Issuance of Certificate
4.4	Certificate Acceptance
4.4.1	Conduct Constituting Certificate Acceptance
4.4.2	Publication of the Certificate by the CA
4.4.3	Notification of Certificate Issuance by the CA to Other Entities
4.5	Key Pair and Certificate Usage
4.5.1	Subscriber Private Key and Certificate Usage
4.5.2	Relying Party Public Key and Certificate Usage
4.6	Certificate Renewal
4.6.1	Circumstances for Certificate Renewal
4.6.2	Who May Request Renewal
4.6.3	Processing Certificate Renewal Requests
4.6.4	Notification of New Certificate Issuance to Subscriber

4.6.5	Conduct Constituting Acceptance of a Renewal Certificate
4.6.6	Publication of the Renewal Certificate by the CA
4.6.7	Notification of Certificate Issuance by the CA to Other Entities
4.7	Certificate Rekey
4.7.1	Circumstances for Certificate Rekey
4.7.2	Who May Request Certification of a New Public Key
4.7.3	Processing Certificate Rekeying Requests
4.7.4	Notification of New Certificate Issuance to Subscriber
4.7.5	Conduct Constituting Acceptance of a Rekeyed Certificate
4.7.6	Publication of the Rekeyed Certificate by the CA
4.7.7	Notification of Certificate Issuance by the CA to Other Entities
4.8	Certificate Modification
4.8.1	Circumstances for Certificate Modification
4.8.2	Who May Request Certificate Modification
4.8.3	Processing Certificate Modification Requests
4.8.4	Notification of New Certificate Issuance to Subscriber
4.8.5	Conduct Constituting Acceptance of Modified Certificate
4.8.6	Publication of the Modified Certificate by the CA
4.8.7	Notification of Certificate Issuance by the CA to Other Entities
4.9	Certificate Revocation and Suspension
4.9.1	Circumstances for Revocation
4.9.2	Who Can Request Revocation
4.9.3	Procedure for Revocation Request
4.9.4	Revocation Request Grace Period
4.9.5	Time Within Which CA Must Process the Revocation Request
4.9.6	Revocation Checking Requirements for Relying Parties
4.9.7	CRL Issuance Frequency
4.9.8	Maximum Latency for CRLs
4.9.9	Online Revocation/Status Checking Availability
4.9.10	Online Revocation Checking Requirements
4.9.11	Other Forms of Revocation Advertisements Available
4.9.12	Special Requirements re Key Compromise
4.9.13	Circumstances for Suspension
4.9.14	Who Can Request Suspension
4.9.15	Procedure for Suspension Request
4.9.16	Limits on Suspension Period
4.10	Certificate Status Services
4.10.1	Operational Characteristics
4.10.2	Service Availability
4.10.3	Operational Features
4.11	End of Subscription
4.12	Key Escrow and Recovery
4.12.1	Key Escrow and Recovery Policy and Practices
4.12.2	Session Key Encapsulation and Recovery Policy and Practices
5	Facility, Management, and Operational Controls

5.1	Physical Controls
5.1.1	Site Location and Construction
5.1.2	Physical Access
5.1.3	Power and Air Conditioning
5.1.4	Water Exposures
5.1.5	Fire Prevention and Protection
5.1.6	Media Storage
5.1.7	Waste Disposal
5.1.8	Off-Site Backup
5.2	Procedural Controls
5.2.1	Trusted Roles
5.2.2	Number of Persons Required per Task
5.2.3	Identification and Authentication for Each Role
5.2.4	Roles Requiring Separation of Duties
5.3	Personnel Controls
5.3.1	Qualifications, Experience, and Clearance Requirements
5.3.2	Background Check Procedures
5.3.3	Training Requirements
5.3.4	Retraining Frequency and Requirements
5.3.5	Job Rotation Frequency and Sequence
5.3.6	Sanctions for Unauthorised Actions
5.3.7	Independent Contractor Requirements
5.3.8	Documentation Supplied to Personnel
5.4	Audit Logging Procedures
5.4.1	Types of Events Recorded
5.4.2	Frequency of Processing Log
5.4.3	Retention Period for Audit Log
5.4.4	Protection of Audit Log
5.4.5	Audit Log Backup Procedures
5.4.6	Audit Collection System (Internal vs. External)
5.4.7	Notification to Event-Causing Subject
5.4.8	Vulnerability Assessments
5.5	Records Archival
5.5.1	Types of Records Archived
5.5.2	Retention Period for Archive
5.5.3	Protection of Archive
5.5.4	Archive Backup Procedures
5.5.5	Requirements for Time-Stamping of Records
5.5.6	Archive Collection System (Internal or External)
5.5.7	Procedures to Obtain and Verify Archive Information
5.6	Key Changeover
5.7	Compromise and Disaster Recovery
5.7.1	Incident and Compromise Handling Procedures
5.7.2	Computing Resources, Software, and/or Data Are Corrupted
5.7.3	Entity Private Key Compromise Procedures

5.7.4	Business Continuity Capabilities After a Disaster
5.8	CA or RA Termination
6	Technical Security Controls
6.1	Key Pair Generation and Installation
6.1.1	Key Pair Generation
6.1.2	Private Key Delivery to Subscriber
6.1.3	Public Key Delivery to Certificate Issuer
6.1.4	CA Public Key Delivery to Relying Parties
6.1.5	Key Sizes
6.1.6	Public Key Parameters Generation and Quality Checking
6.1.7	Key Usage Purposes (as per X.509 v3 Key Usage Field)
6.2	Private Key Protection and Cryptographic Module Engineering Controls
6.2.1	Cryptographic Module Standards and Controls
6.2.2	Private Key (n out of m) Multi-Person Control
6.2.3	Private Key Escrow
6.2.4	Private Key Backup
6.2.5	Private Key Archival
6.2.6	Private Key Transfer Into or From a Cryptographic Module
6.2.7	Private Key Storage on Cryptographic Module
6.2.8	Method of Activating Private Key
6.2.9	Method of Deactivating Private Key
6.2.10	Method of Destroying Private Key
6.2.11	Cryptographic Module Rating
6.3	Other Aspects of Key Pair Management
6.3.1	Public Key Archival
6.3.2	Certificate Operational Periods and Key Pair Usage Periods
6.4	Activation Data
6.4.1	Activation Data Generation and Installation
6.4.2	Activation Data Protection
6.4.3	Other Aspects of Activation Data
6.5	Computer Security Controls
6.5.1	Specific Computer Security Technical Requirements
6.5.2	Computer Security Rating
6.6	Life Cycle Technical Controls
6.6.1	System Development Controls
6.6.2	Security Management Controls
6.6.3	Life Cycle Security Controls
6.7	Network Security Controls
6.8	Time-Stamping
7	Certificate, CRL, and OCSP Profiles
7.1	Certificate Profile
7.1.1	Version Number(s)
7.1.2	Certificate Extensions
7.1.3	Algorithm Object Identifiers
7.1.4	Name Forms

7.1.5	Name Constraints
7.1.6	Certificate Policy Object Identifier
7.1.7	Usage of Policy Constraints Extension
7.1.8	Policy Qualifiers Syntax and Semantics
7.1.9	Processing Semantics for the Critical Certificate Policies Extension
7.2	CRL Profile
7.2.1	Version Number(s)
7.2.2	CRL and CRL Entry Extensions
7.3	OCSP Profile
7.3.1	Version Number(s)
7.3.2	OCSP Extensions
8	Compliance Audit and Other Assessments
8.1	Frequency and Circumstances of Assessment
8.2	Identity/Qualifications of Assessor
8.3	Assessor's Relationship to Assessed Entity
8.4	Topics Covered by Assessment
8.5	Actions Taken as a Result of Deficiency
8.6	Communications of Results
9	Other Business and Legal Matters
9.1	Fees
9.1.1	Certificate Issuance or Renewal Fees
9.1.2	Certificate Access Fees
9.1.3	Revocation or Status Information Access Fees
9.1.4	Fees for Other Services
9.1.5	Refund Policy
9.2	Financial Responsibility
9.2.1	Insurance Coverage
9.2.2	Other Assets
9.2.3	Insurance or Warranty Coverage for End-Entities
9.3	Confidentiality of Business Information
9.3.1	Scope of Confidential Information
9.3.2	Information Not Within the Scope of Confidential Information
9.3.3	Responsibility to Protect Confidential Information
9.4	Privacy of Personal Information
9.4.1	Privacy Plan
9.4.2	Information Treated as Private
9.4.3	Information Not Deemed Private
9.4.4	Responsibility to Protect Private Information
9.4.5	Notice and Consent to Use Private Information
9.4.6	Disclosure Pursuant to Judicial or Administrative Process
9.4.7	Other Information Disclosure Circumstances
9.5	Intellectual Property Rights
9.6	Representations and Warranties
9.6.1	CA Representations and Warranties
9.6.2	RA Representations and Warranties

9.6.3	Subscriber Representations and Warranties
9.6.4	Relying Party Representations and Warranties
9.6.5	Representations and Warranties of Other Participants
9.7	Disclaimers of Warranties
9.8	Limitations of Liability
9.9	Indemnities
9.10	Term and Termination
9.10.1	Term
9.10.2	Termination
9.10.3	Effect of Termination and Survival
9.11	Individual Notices and Communications with Participants
9.12	Amendments
9.12.1	Procedure for Amendment
9.12.2	Notification Mechanism and Period
9.12.3	Circumstances Under Which OID Must be Changed
9.13	Dispute Resolution Provisions
9.14	Governing Law
9.15	Compliance with Applicable Law
9.16	Miscellaneous Provisions
9.16.1	Entire Agreement
9.16.2	Assignment
9.16.3	Severability
9.16.4	Enforcement (Attorney's Fees and Waiver of Rights)
9.17	Other Provisions

ANNEXURE A4

Audit Schedule
RCAI Annual Audit – by <<Auditor>> Team
<<Date>>

Auditors Team (Name)

Agenda

Day 1 – <<Date>>, Location

Time	Auditee	Auditor	Activity Details	Remarks

Day 2– <<Date>>, Location

Time	Auditee	Auditor	Activity Details	Remarks

• • • • • • • • • • •

Day n – <<Date>>, Location

Time	Auditee	Auditor	Activity Details	Remarks