SECURITY GUIDELINES FOR CERTIFICATE AUTHORITIES

Draft Version 1.0

INFORMATION NETWORK SECURITY AGENCY

2012 E.C.

Document Control

Document Name	Security Guidelines For Certificate Authority
Status	Draft
Version	1.0
Last Update	
Document Owner	Information Network Security Agency, INSA

Contents

1. Introduction

The electronic environment needs high security to and also a need to ensure that the electronic transactions are reliable and have not been tampered with.

Public key technology provides the capabilities for transacting parties in an electronic environment to authenticate each other's identities and ensure non-repudiation of electronic transactions through the use of digital signatures.

A certification authority acts as a trusted party to facilitate the confirmation of the relationship between a public key and a named entity. The certification authority issues digital certificates that can be used for authentication and digital signatures. The certification authority also performs certificate management services such as publication and revocation of digital certificates.

As certification authorities play a vital role in facilitating secure electronic transactions, there needs to be an assurance that the certification authorities perform their roles and duties with high levels of integrity and security.

This document defines the security guidelines for the management, systems, and operations of a certification authority. It is intended for use by the management, security, technical and operational personnel of a certification authority.

1.1. Purpose

The purpose of this document is to define security guidelines for the management, systems, and operations of certification authorities (CAs). The guidelines are aimed at protecting the integrity, confidentiality, and availability of certification services, data, and systems.

1.2. Scope

The scope of this document covers the basic security role and functions of RCA and Sub-CAs. This document does not address the requirements for a hierarchy of CA's, e.g. the Sub-CA's relationship with an RCA and a cross-certification entity. The security guidelines do not cover interoperability requirements across CA's, e.g. certificate formats and certificate management protocols.

2. Definition and Acronyms

2.1. Definitions

CA certification key: The CA's private key is used to sign certificates, suspension and revocation information.

CA operator: The technical personnel that operates the systems associated with the CA's function.

CA systems: The systems that perform or support the registration, certification and repository functions of a CA.

Certificate generation: The process of approving a user's registration request and the production of a certificate associated with the request.

Certificate issuance: The process of issuing a certificate whose contents have been verified and signed by the CA to the certificate applicant.

Certificate Policy: A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

Certificate Provider: The entity that issues certificates to CA applicants. In an open PKI model, the certificate provider is typically the certification authority whereas in an outsource model, the certificate provider may outsource the backend certification operations to another entity.

Certificate: an electronic data that links public key to the person named in the certificate and confirms the real identity of that person. It contains certain digitally signed information, including the identification information of the entity, the public key, purpose, and scope of the usage of the key, name of certification authority, etc.

Certification Authority (CA): The relied-upon entity that issues, publishes, suspends and revokes of end-entity (end-user).

Certification Practice Statement: A statement of the practices that a CA employs in issuing and managing certificates, and addressing its general business liability and service availability.

Certification: The process of generating/signing certificates, suspension and revocation information for individuals, corporations, equipment, etc.

Compromise: A case where the private key and related security information have been or may be stolen or leaked or where secrecy has been or may be lost by a third party's decryption. Key

custodian: A person who is entrusted to maintain custody of the secret keys for the CA operations. The person must not be directly involved in performing the CA operations.

Key generation system: The system that is used to generate cryptographic keys.

Key loading: The process by which a key is manually or electronically transferred into a secure cryptographic device.

Physical notice: Physical notices may include writing delivered by hand or certified or registered mail.

Policy Management Authority: The Policy Management Authority is the authority on policies relating to the PKI and is responsible for developing the Certificate Policy.

Registration Authority (RA): A PKI component that performs the registration functions, e.g. verification of the certificate applicant's identification information.

Registration function: Registration services consist of registering and managing individual data, and carrying out the authentication necessary for the issuance or revocation of certificates, on behalf of the CA.

Relying party: A recipient of a certificate who acts in reliance on that certificate and/or digital signature verified using that certificate.

Repository: a system for disclosing, storing and retrieving certificates or other information relating to certificates.

Signatory: a person who holds private key and signs either on his own behalf or on behalf of the person he represents.

Split control: The process of utilizing two or more persons, who are operating in concert, to protect sensitive functions or information. No single person is to be able to access or to utilize the protected entity.

Subscriber: a person who is the subject named in a certificate, accepts the authenticity of the content the certificate and owns a private key which corresponds to a public key listed in that certificate.

Suspension: The temporary invalidation of a certificate within the validity period of that certificate. Suspended certificates can be re-instated if the certificate information is validated and the secret key associated with the certificate has not been compromised.

User community: The users of the certification services. The user community typically includes the certificate subscribers and relying on parties.

Verification: The process of checking the authenticity of certificates and any data used by subscribers and relying on parties.

2.2. Acronyms

CA	Certificate Authority
CMCSRS	Critical Mass Cyber Security Requirement Standard
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
ICA	Intermediate Certificate Authority
INSA	Information Network Security Agency
IT	Information Technology
LAN	Local Area Network
PKI	Public Key Infrastructure
RA	Registration Authority
RCA	Root Certificate Authority
UPS	Uninterrupted Power Supply

3. Security Management

The CAs shall implement the following Information security Management:

3.1. Security Policy and Procedures

a) Comprehensive Information security policy for its Operation shall be developed, periodically updated and communicated to all individuals with access to the CA's information and systems and widely published throughout the organization to ensure that the person follows the policies.

b) Personnel shall be provided with the information security policy upon employment. It shall be the responsibility of each person to read and understand it. Security notices, pamphlets, posters and signs shall be used to provide updates and reminders of the security policy.

c) Information security operational procedures for installation, configurations, deployment of Information systems and other tasks shall be applied.

d) Procedures shall be documented and implemented to ensure that when personnel or contractors are transferred by appointment, assignment or deployment, all-access privileges to information systems, information and assets are reviewed, modified or revoked accordingly.

e) Procedures or a mechanism shall be established and implemented so that access rights of all registered users, their levels of access and their continued requirement for access can be checked regularly (re-authentication).

f) Procedures shall be established and implemented to actively keep track of security vulnerabilities and attacks that are reported by reputable sources and develop countermeasures or correct them promptly. The procedures should include an incident response capability to provide active defense and corrective actions against security exploits and attacks.

g) Incident response procedures shall be established for documenting an event as a basis for subsequent action including forensics where necessary.

h) A comprehensive Information security plan shall be developed by referring to the Critical Mass Cyber Security Requirements Standard Specifically the Cyber Security Planning Process.

3.2. Risk Management

a. The components of the CA system (e.g. cryptographic algorithm and its key parameters, physical security, system security, operating system, etc.) shall be reviewed every year for new technology risks and appropriate action of the components shall be developed to manage the risks identified.

b. Risk management policies and procedures shall be reviewed periodically as part of a comprehensive risk management approach.

c. Network and system security audits shall be performed periodically using automated audit tools to help identify new security vulnerabilities.

d. Network penetration tests shall be performed periodically to help identify gaps that may have been introduced in the network perimeter defenses.

e. Intrusion detection systems shall be used to provide real-time detection of network attacks.

f. Risk analysis and protection policies shall be reviewed periodically for all incidents (real or suspected) or when the perceived threat level changes (technical, physical or personnel).

3.3. Incident Management

a) An incident management plan shall be developed and approved by the management. The plan shall include but not limited to the following areas:

- CA's Private key compromise;
- Subscriber Private Key compromise;
- Systems and network penetration;
- Breach of physical security;
- Infrastructure availability; and
- Fraudulent registration and generation of certificates, certificate suspension and revocation information.

b) An incident response action plan shall be established and periodically tested to ensure the readiness of the CA to respond to incidents. The plan shall include but not limited to 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
- Media and public relations.

c) The CA's certificate shall be revoked immediately in the event of loss or compromise of the CA's private Key or its storage device. All certificates signed using the CA's private key shall be revoked.

d) All security-related incidents must be reported. Incidents related with CAs key compromise are reported to Root CA including Root CA key compromise and incidents related subscriber key compromise are reported to the issuing CA.

e) All incidents reported, actions taken, follow-up actions, and other related information shall be documented.

f) Procedures shall be defined for dealing with all security-related incidents, including malicious software, break-ins from networks, software bugs which compromised the security of the system.

3.4. Business Continuity Planning

a) Business continuity and disaster recovery planning shall be developed and tested periodically to ensure the continued availability of critical services in the event of a disaster or computer failure.

b) The planning shall include continuity plans in the event of CA private key loss and compromise.

c) The personnel who undertake the recovery process shall be provided with adequate training to deal with the crisis.

d) Redundant systems and devices shall be available to ensure continued operation of critical services on time.

e) All recovery locations active or passive should have adequate security.

f) Business continuity plans shall be reviewed for relevance and adequacy every six months to assure the continuity of business in the event of an emergency. Evidence of the review shall be documented for management review.

g) Commitment shall be obtained in writing from computer equipment and supplies vendors to replace critical equipment and supplies within a specified period following destruction of the computing facility.

h) The business continuity plan shall be developed which inter alia includes the procedures for emergency ordering of the equipment and availability of the services.

i) The need for backup hardware and other peripherals should be evaluated in accordance with business needs.

j) Emergency response procedures for all activities connected with computer operation shall be developed and documented. These procedures should be reviewed periodically.

k) Emergency drills should be held periodically to ensure that the documented emergency procedures are effective.

3.5. Capacity Building

a) Information security capacity building shall be promoted and enhanced continually in accordance with skill and knowledge of staff, technology, and Management capacity requirements.

b) An information security awareness program shall be implemented and conducted on at least an annual basis to ensure that all personnel is informed of the potential security risks and exposures in the CA operations and systems. In particular, personnel, especially those in the frontline service, shall be informed of typical social engineering attacks and the safeguards against them.

c) All personnel shall be educated on basic IT principles and safeguards. Personnel responsible for security areas (e.g. systems and operations security administrators) shall be trained on advanced IT security principles and safeguards. The security personnel shall be trained in the security features and vulnerabilities of the systems and operations.

d) All personnel, including temporary and contract personnel, who are required to perform core CA operation should be adequately trained.

e) A CA shall ensure that all personnel performing duties concerning its operation, must receive comprehensive training in:

- relevant aspects of the Information Technology Security Policy and Security
- Guidelines framed by the CA;

- all PKI software versions in use on the CA's system;
- all PKI duties they are expected to perform; and
- disaster recovery and business continuity procedures;

f) Training kept current to accommodate changes in the CA's system. Refresher training must be conducted as and when required, and the CA must review these requirements at least once a year.

3.6. Personnel Security Controls

a) The management should set out clear policies on the recruitment, assessment, training and dismissal of operative personnel.

b) All job applicants shall be subjected to a security screening before being employed. The screening shall ensure that the applicant does not have any criminal records that may jeopardize the trustworthiness of the CA functions.

c) All personnel shall be required to sign a confidentiality agreement as part of their initial terms and conditions of employment before being given access to the CA services and processes facilities.

d) Confidentiality or non-disclosure agreements shall be reviewed when there are changes to the terms of employment or contract, particularly when employees are due to leave the organization or contracts are due to end.

e) Personnel performing trusted roles or security-sensitive functions shall be subjected to stringent security screening.

f) Dual control and segregation of duties shall be implemented for critical CA services and processes.

g) Security-related roles shall be given to dedicated personnel who are adequately trained to perform the job without any conflict of interest.

h) Job responsibilities and access rights shall be designed and reviewed yearly to ensure proper segregation of duties and alignment of access rights to business functions, i.e. certificate registration, issuance, suspension, and revocation. Besides, periodic cross-checks on personnel performing trusted roles or security-sensitive functions for incompatible duties or interests (internal or external) shall be conducted.

i) All personnel shall be adequately trained in their designated tasks and functions. Personnel who have not been adequately trained shall not be allowed to independently operate the CA functions without the presence or supervision of trained personnel.

j) CA must make available to his personnel the Digital Signature Certificate policies it supports, its Certification Practice Statement, policies or contracts relevant to their position.

4. Certificate Management

The certificate management processes include certificate registration, generation, issuance, renewal, suspension, and revocation, as well as the publication of certificates, certificate suspension and revocation information. The objective is to establish the integrity and accountability of the certificate management processes and certificates.

4.1. Certificate Attributes

a) A certificate shall be uniquely identifiable within its user community.

b) A certificate shall indicate certificate policy and usage parameters to allow relying parties to check the acceptable use of a certificate.

c) A certificate shall indicate expiration parameters to allow relying parties to verify the validity of the certificate.

d) The certificate should include parameters declaring the policy mapping as well as any constraints to policy maps.

e) Certificate extensions may be labeled as critical. The relying party shall be provided with the applications to verify and process any critical certificate extensions or reject the certificate.

4.2. Registration

a) The authentication method to verify the identity of the certificate applicant shall commensurate with the level of assurance accorded by the certificate. Where possible, faceto-face authentication of the applicant should be employed. A pre-existing trust relationship between the RA and the applicant may also be employed.

b) The authenticity of attribute information of an applicant shall be verified against official documents issued by authorized organizations.

c) Adequate documents and logs for each registration shall be maintained to enable post verification of the certificate applications.

4.3. Generation

a) Procedures shall be defined to ensure that the subscribers' certificates generated are in accordance with the Certificate Policy.

b) The accuracy (e.g. the information in the certificate is correct) and integrity (e.g. the correct association of the key pair with the certificate information) of the certificate shall be ensured.

4.4. Issuance

a) The CA shall require the subscriber to explicitly acknowledge the receipt and acceptance of the certificate upon issuance.

b) After the CA verified the source of the request, Certificates shall be checked to ensure that all fields and extensions are properly populated. After generation, verification, and acceptance, a CA shall post the certificate as outlined in applicable CPSs.

c) The CA shall notify the Subscriber of the issuance of a Certificate conveniently and appropriately based on information submitted during the enrolment process.

4.5. Publication

a) The CA shall publish its certificate and the location(s) of its CPS and repository to its user community using a reliable and trustworthy channel

b) Publication of the subscribers' certificate information in the repository shall be subject to the subscribers' explicit consent.

c) The contents in the repository shall be protected from unauthorized modification, insertion and deletion. Strong authentication mechanisms shall be used to validate identity of parties amending the repository contents. Where required, appropriate access controls to the contents of the repository shall be implemented to restrict access solely to the user community or to protect subscribers' privacy.

d) Adequate backup and redundancy measures shall be implemented to ensure that the availability of the certificate repository conforms to the service level guaranteed to the user community.

4.6. Renewal

a) The CA shall provide prior notice to the subscribers on the expiry date of their certificates so that they have sufficient time to apply for renewal or termination.

b) Certificate renewal requests shall be submitted using a secure communication channel. A secure channel may include the use of an online renewal request that is digitally signed by the subscriber as long as the certificate is still valid.

c) The certificate generation and issuance guidelines in this section shall apply in the generation and issuance of a new certificate to replace an expired certificate.

4.7. Certificate Suspension

a) A certificate shall be suspended fully or partially for a time not exceeding 6 months by the circumstances listed on the CP section 4.9.13.

b) Certificate suspension requests shall be submitted using a secure communications channel to verify the identity of the requester to minimize the risk of sabotage with unauthorized disruption of service or with malicious requests for suspension.

c) Certificate suspension information in the certificate revocation list shall include the reason and time of the suspension so that relying parties can determine the point at which the certificate ceases to be valid.

d) Certificate suspension information in the certificate revocation list shall be digitally signed by the CA to enable the relying parties to verify the authenticity and integrity of the information.

e) Certificate suspension information in the certificate revocation list shall be published once the suspension request has been verified to be valid.

f) Certificate suspension information in the certificate revocation list shall be protected from unauthorized modification and deletion.

g) The subscriber whose certificate has been suspended shall be notified once the suspension takes effect.

4.8. Certificate Revocation

a) A certificate shall be revoked in accordance with the circumstances listed on the CP section 4.9.13.

b) Revoked certificates shall be included on all new publications of the certificate status information until the certificates expire.

c) A revoked certificate shall appear on at least one CRL.

d) Certificate revocation requests shall be submitted using a secure communication channel to verify the identity of the requester to minimize the risk of sabotage with unauthorized revocation.

e) The certificate revocation information shall at least contain the following: □

- Reason code for revocation; and
- Revocation date and time.

f) Certificate revocation information shall be digitally or manually signed by the subject to enable the relying party to verify the authenticity and integrity of the information.

g) Certificate revocation information shall be published once the revocation request has been verified to be valid. It should include provisions for:

- Online certificate revocation checking; and
- Distribution points certificate revocation information.

h) Certificate revocation information shall be protected from unauthorized modification and deletion.

i) The subscriber who certificate has been revoked shall be notified once the revocation takes effect

4.9. Archival

a) Digital Certificates stored and generated by the CA must be retained for at least ten years after the date of its expiration. This requirement does not include the backup of private signature keys.

b) The second copy of all information retained or backed up must be stored at three locations within the country including the CA 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 a few hours.

c) All information about CA operation, Subscriber's application, verification, identification, authentication, and Subscriber agreement shall be stored within the country.

d) The CA should verify the integrity of the backups at least once every six months.

e) Information stored off-site must be periodically verified for data integrity.

f) Record archives shall be indexed, stored, preserved and reproduced to be accurate, complete, legible and accessible to authorized persons. The integrity and availability of the record archives shall be ensured

4.10. Audit Trails

a) Audit trails of certificate registration, generation, issue, renewal, suspension, and revocation shall be maintained.

b) The integrity and availability of the audit trails shall be ensured.

c) Audit trails shall be archived for a minimum period of 10 years or longer, in accordance with the applicable regulatory requirements.

d) Transactions that meet exception criteria shall be completely and accurately highlighted and reviewed by personnel independent of those that initiate the transaction. 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 shall be analyzed.

e) The security audit logs should be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanisms shall be used to monitor and promptly report all significant security events.

f) 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. Further, there shall be a procedure that checks and corrects drift in the real-time clock.

5. Key Management

This section defines the guidelines to manage risk at each phase of key management to ensure the confidentiality and integrity of cryptographic keys. It covers technical and administrative security requirements to manage the risk of cryptographic key compromise. The scope includes cryptographic keys used by the CA (including registration functions) and the user community.

The principle of split control is to be applied to the handling of CA keys.

5.1. Generation

a) The CA keys shall be generated and stored under split control by parties who are not involved in the set-up and maintenance of the CA systems and operations.

b) Separate key pairs for digital signature and encryption should be generated.

c) The key generation process shall generate statistically random key values for the generation of a strong (unique) key.

d) The integrity of the CA private key is vital. It shall, therefore, be strong and shall be generated using unpredictable random number generators preferably hardware-based.

5.2. Distribution of Keys

a) 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 end-toend confidentiality and integrity.

5.3. Storage

a) CA keys shall be stored in tamper-proof devices and can only be activated under split control by parties who are not involved in the set-up and maintenance of the LCP systems and operations.

b) The CA key may be also stored in a tamper-proof cryptographic module or split into subkeys stored in tamper-proof devices under the custody of the key custodians.

c) The CA's key custodians shall ensure that the CA key component or the activation code is always under his sole custody. Change of key custodians shall be approved by the CA management and documented. If the key custodian is unavailable, CA should put in place a system of checks to ensure that there is no single point of failure.

5.4. Usage

a) A system and software integrity check shall be performed before CA's key loading.

b) Custody of and access to the CA's keys shall be under split control. In particular, CA's key loading shall be performed under split control.

5.5. Backup

a) CA private keys shall be backed up to prevent a CA's operation from stopping due to accidental deletion or corruption of keys.

b) CA private key backups shall be protected with the same guidelines as required for CA private key storage.

c) Separate key custodians shall be assigned to protect each component of the backup key.

d) CA private key backups should be stored in a separate secure storage facility, at a different location from where the original key is stored.

5.6. Key Change

a) CA and subscriber keys shall be changed or recertified periodically.

b) A key change shall be processed as per Key Generation guidelines.

c) The validity period of Keys shall be defined.

d) The CA shall provide reasonable notice to the subscriber's relying parties of any change to a new key pair used by the CA to sign certificates.

e) The CA shall define a CA key change process that ensures the 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.

f) The CA shall notify the subscriber or the owner of the digital certificates of any type of key change that is performed automatically either through a secure application program.

5.7. Destruction

a) Private keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked.

b) To destroy a Private Key stored on software cryptographic modules, the subscriber can overwrite the data.

c) To destroy a Private Key stored on hardware cryptographic modules, the subscriber will need to execute a "zeroize" command.

5.8. Key Compromise

a) A procedure shall be pre-established to handle cases where a compromise of the CA certification key has occurred.

b) The CA shall immediately revoke all affected subscriber certificates in the case of a CA certification private key compromise.

c) The CA shall immediately revoke the affected keys and certificates in the case of subscriber private key compromise.

5.9. CA Key and Subscriber Encryption Key Archival

a) CA Public keys shall be archived permanently to facilitate audit or investigation requirements.

b) All subscriber encryption keys should be archived for a reasonable period to safeguard users from any compromise or misplacement of keys that may result in their denial of service.

c) Archives of CA public keys and subscriber encryption keys shall be protected from unauthorized modification.

5.10. CA's Public Key Delivery to Users

a) The CA'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.

6. Systems and Operations Guidelines

6.1. Physical Security

6.1.1. Site location

The site location, design, construction and physical security of the operational site of Certificate Authority shall be in accordance with the following requirements:

a) The site location, design, construction and physical security of the operational Site of Certificate Authority shall be in accordance physical security process of CMCSRS.

b) The site shall not be in locations that are prone to natural or man-made disasters, like flood, fire, chemical contamination and explosions

c) As per the nature of the operations, suitable floor structuring, lighting, power, and water damage protection requirements shall be provided.

d) Construction shall comply with all applicable building and safety regulations of the Ethiopian government.

e) Materials used for the construction of the operational site shall be fire-resistant and free of toxic chemicals.

f) Air-conditioning system, power supply system and uninterrupted power supply Unit with proper backup shall be installed depending upon the nature of Operation.

g) All ducting holes of the air-conditioning system must be designed to prevent intrusion of any kind.

h) Any facility that supports mission-critical and sensitive applications must be located and designed for repair ability, relocation, and reconfiguration. The ability to relocate, reconstitute and reconfigure these applications must be tested as part of the business continuity/disaster recovery plan.

6.1.2. Fire Protection

a) Inflammable and explosive materials shall not be stored within a hundred meters of the Operational site.

b) Automatic FDAS (fire detection and alarming system) shall be designed in accordance with requirements of ES ISO 7240 as prescribed by the Fire Brigade or any other agency of the Central or State Government shall be installed at the operational site.

c) Automatic as well as portable fire extinguishers shall be installed at the operational site and their Locations clearly marked with appropriate signs.

d) Periodic testing and inspection of fire protection control equipment shall be conducted according to ES ISO 7240 and maintenance of FPCE and fire suppression systems shall be carried out.

e) Procedures for the safe evacuation of personnel in an emergency shall be visibly fixed/ displayed at prominent places at the operational site. Periodic training and fire drills shall be conducted.

f) There shall be no eating, drinking or smoking in the operational site. The work areas shall be kept clean at all times.

6.1.3. Environmental Protection

a) Water detectors shall be installed under the raised floors throughout the operational site and shall be connected to audible alarms.

b) The temperature and humidity condition in the operational site shall be monitored and controlled periodically.

c) Personnel at the operational site shall be trained to monitor and control the various equipment and devices installed at the operational site for fire and environment protection.

d) Periodic inspection, testing, and maintenance of the equipment and systems shall be scheduled.

6.1.4. Physical Access

Physical access to the operational site housing computer servers, PKI server, communications, and network devices shall be controlled and restricted to the authorized individuals only in accordance with the following requirements:

a) Responsibilities round the clock, seven days a week, three hundred sixty-five days a year for the 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.

b) Biometric physical access security systems shall be installed to control and audit access to the operational site.

c) Physical access to the operational site at all times shall be controlled and restricted to authorized personnel only. Personnel authorized for limited physical access shall not be allowed to gain unauthorized access to a restricted area within an operational site.

d) Dual control over the inventory and issue of access cards/keys during normal business hours to the Data Centre shall be in place. An up-to-date list of personnel who possess the cards/keys shall be regularly maintained and archived for three years.

e) Loss of access cards/keys must be immediately reported to the security supervisor of the operational site who shall take appropriate action to prevent unauthorized access.

f) All individuals, other than operations staff, shall sign in and sign out of the operational site and shall be accompanied by operations staff.

g) Emergency exits shall be tested periodically to ensure that the access security systems are operational.

h) All opening of the Data Centre should be monitored round the clock by surveillance video cameras.

6.2. Change and Configuration Management

a) Executables of questionable sources or where trustworthiness cannot be ascertained shall not be installed or run on CA systems.

b) Software updates and patches shall be reviewed, thoroughly tested and proven for security implications before being implemented

c) Software updates and patches to rectify security vulnerabilities in critical systems shall be promptly reviewed and implemented.

d) The information on the software updates and patches and their implementation shall be clearly and properly documented.

6.3. Network and Communications Security

6.3.1. Network Administrator

a) Each organization shall designate a properly trained "Network Administrator" who will be responsible for the operation, monitoring security and functioning of the network.

b) 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 follow up of any unusual activity or pattern of access on the computer network shall be investigated promptly by the Network Administrator.

c) The system must include a mechanism for alerting the Network Administrator of possible breaches in security, e.g., unauthorized access, virus infection, and hacking.

d) Secure Network Management System should be implemented to monitor the functioning of the computer network. Broadcast of network traffic should be minimized.

e) Only authorized and legal software shall be used on the network.

6.3.2. Connectivity

a) The organization shall establish a procedure for allowing connectivity of their computer network or computer system to a non-organization computer system or networks. The permission to connect other networks and computer systems shall be approved by the Network Administrator and documented.

b) CA systems shall be protected to ensure network access control to critical systems and services from other systems.

c) Network connections to external networks (if required) from the CA's systems shall be restricted to only the connections that are essential to facilitate CA's function processes and services.

d) Network connections (if required) should be initiated by the systems performing the certification function to those performing the registration and repository functions but not vice versa. If this is not possible, compensating controls (e.g. use of proxies) shall be implemented to protect the systems performing the certification function from potential attacks

e) Security testing and evaluation of the network access control of the CA's systems shall be reviewed by a suitably qualified independent party before allowing connections to the external network to be made. Mitigating controls shall be put in place for the risks that have been identified.

f) Systems performing the certification function should be isolated to minimize exposure to attempts to compromise the confidentiality, integrity, and availability of the certification function.

g) The CA's certification key shall be protected from unauthorized access to ensure its confidentiality and integrity.

h) Communication between the CA systems over a network shall be secure to ensure confidentiality, integrity, and authenticity. For example, communications between the CA systems over a network should be encrypted and digitally signed.

i) Intrusion detection tools shall be deployed to monitor critical networks and perimeter networks and alert administrators of network intrusions and penetration attempts in a timely manner.

j) All unused connections and network segments should be disconnected from active networks. The computer system/personal computer or outside terminal accessing an organization's host system must adhere to the general system security and access control guidelines.

k) The suitability of new hardware/software particularly the protocol compatibility should be assessed before connecting the same to the organization's network.

l) As far as possible, no Internet access should be allowed to database server/file server or server hosting sensitive data.

m) The level of protection for communication and network resources should be commensurate with the criticality and sensitivity of the data transmitted.

6.4. Monitoring Audit Logs

a) The CA should consider the use of automated security management and monitoring tools providing an integrated view of the security situation at any point in time.

b) Records of the following application transactions shall be maintained:

- Registration;
- Certification;
- Publication;
- Suspension; and

- Revocation.

c) Records and log files shall be reviewed periodically for the following activities:

- Misuse;
- Errors;
- Security violations;
- Execution of privileged functions;
- Change in access control lists;
- Change in system configuration; and
- Change in software modules.

d) A review of audit trails shall be performed by personnel tasked specifically with the oversight function.

e) Audit logs shall be adequately protected from unauthorized access, modification, and deletion and backed up periodically on time for archival purposes.

f) Audit trail retention for system access records (e.g. Syslog, security-related logs) shall be kept for a minimum of twelve months or longer, in either hard copy or electronic form. Records that are necessary to support litigation or investigation of criminal activities shall be retained permanently or as stipulated by relevant legislation.

g) Records of application transactions and significant events shall be retained for a minimum of twelve months or longer, in accordance with the applicable regulatory requirements.

6.5. Information Management

6.5.1. System Administration

a) CA's shall designate a properly trained "System Administrator" who will ensure that the protective security measures of the system are functional and who will maintain its security posture. Depending upon the complexity and security needs of a system or application, the System Administrator may have a designated System Security Administrator who will assume security responsibilities and provide physical, logical and procedural safeguards for the information.

b) CA's shall ensure that only a properly trained System Security Administrator is assigned the system security responsibilities.

c) The responsibility to create, classify, retrieve, modify, delete or archive information must rest only with the System Administrator.

d) Any password used for the system administration and operation of trusted services must not be written down (in paper or electronic form) or shared with anyone. A system for password management should be put in place to cover the eventualities such as forgotten passwords or changeover to another person in case of System Administrator (or System Security Administrator) leaving the organization. Every instance of usage of administrator's passwords must be documented.

e) A periodic review of the access rights of all users must be performed.

f) The System Administrator must 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).

g) The System Administrator must take steps to safeguards classified information as prescribed by its owner.

h) 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.

i) Criteria for the review of audit trails/access logs, reporting of access violations and procedures to ensure timely management action/response shall be established and documented.

j) All security violations must be recorded, investigated, and periodic status reports compiled for review by the management.

k) The System Administrator together with the system support staff, shall conduct a regular analysis of problems reported to and identify any weaknesses in the protection of the information.

l) 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.

m) The System Administrator should ensure that no generic user is enabled or active on the system.

6.5.2. Sensitive Information Control

a) Information assets shall be classified and protected according to their sensitivity and criticality to the organization in accordance with CMSCRS.

b) Procedures must be in place to handle the storage media, which has sensitive and classified information.

c) All sensitive information stored in any media shall bear or be assigned an appropriate security classification.

d) All sensitive material shall be stamped or labeled accordingly.

e) Storage media (i.e. floppy diskettes, magnetic tapes, portable hard disks, optical disks, etc.) containing sensitive information shall be secured according to their classification.

f) Electronic communication systems, such as a router, switches, network devices, and computers, used for transmission of sensitive information should be equipped or installed with suitable security software and if necessary with encryption software. The appropriate procedure in this regard should be documented.

g) 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. Preferably such affected/corrupted/damaged media both internal and external to the system shall be destroyed.

6.5.3. Sensitive Information Security

a) Highly sensitive information assets shall be stored on secure removable media and should be in an encrypted format to avoid compromise by unauthorized persons.

b) 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.

c) Removable electronic storage media must be removed from the computer and properly secured at the end of the work session or workday.

d) Removable electronic storage media containing sensitive information and data must be clearly labelled and secured.

e) Hard disks containing sensitive information and data must be securely erased before giving the computer system to another internal or external department or for maintenance.

6.5.4. Prevention of Computer Misuse

a) 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.

b) CA's shall provide adequate information to all persons, including management, systems developers and programmers, end-users, and third party users warning them against the misuse of computers.

c) Effective measures to deal expeditiously with breaches of security shall be established within each organization. Such measures shall include:

- Prompt reporting of a suspected breach;
- Proper investigation and assessment of the nature of the suspected breach;
- Secure evidence and preserve the integrity of such material as relates to
- the discovery of any breach;
- Remedial measures.

6.6. System integrity and security measures

6.6.1. Use of Security Systems or Facilities

a) 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.

b) Any system software or resource of the computer system should only be accessible after being authenticated by an access control system.

6.6.2. System Access Control

a) Access control software and system software security features shall be implemented to protect resources. Management approval is required to authorize the issuance of user identification (ID) and resource privileges.

b) Access to information system resources like memory, storage devices, etc., sensitive utilities and data resources and program files shall be controlled and restricted based on a "needtouse" basis with proper segregation of duties.

c) 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" shall be avoided. All passwords used must be resistant to dictionary attacks.

d) Appropriate approval for the request to access system resources shall be obtained from the System Administrator. Guidelines and procedures governing access authorizations shall be developed, documented and implemented.

e) An Access Control System manual documenting the access granted to a different level of users shall be prepared to guide the System Administrator for grant of access.

f) 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.

g) Stored passwords shall be encrypted using internationally proven encryption techniques to prevent unauthorized disclosure and modification.

h) Stored passwords shall be protected by access controls from unauthorized disclosure and modification.

i) Automatic time-out for terminal inactivity should be implemented.

j) Audit trail of security-sensitive access and actions taken shall be logged.

k) All forms of audit trail shall be appropriately protected against unauthorized modification or deletion.

l) Where second-level access control is implemented through the application system, password controls similar to those implemented for the computer system shall be in place.

m) Activities of all remote users shall be logged and monitored closely.

n) The facility to log in 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, an administrator in Windows NT or Windows 2000). This means that there must be a user account configured for the trusted administrator. The system requires trusted users to change their effective username to gain access to root and to re-authenticate themselves before requesting access to privileged functions.

o) The start-up and shutdown procedure of the security software must be automated.

p) 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 the System Administrator.

6.6.3. Password Management

a) Certain minimum quality standards for passwords 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 sixty days; for the sensitive system, a password shall be changed at least once every thirty days; and
- Shall not be shared, displayed or printed.

b) Password retries shall be limited to a maximum of three attempted logins 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.

c) Easy-to-guess passwords (e.g. user name, birth date, month, standard words, etc.) should be avoided.

d) Initial or reset passwords must be changed by the user upon first use.

e) Passwords shall always be encrypted in storage to prevent unauthorized disclosure.

f) All passwords used must be resistant to dictionary attacks and all known password cracking algorithms.

6.6.4. Privileged User's Management

a) System privileges shall be granted to users only on a need-to-use basis.

b) Login privileges for highly privileged accounts should be available only from Console and terminals situated within the Console room.

c) An audit trail of activities conducted by highly privileged users shall be maintained for two years and reviewed periodically at least every week by an operator who is independent of System Administrator.

d) Privileged user shall not be allowed to log in to the computer system from a remote terminal. The usage of the computer system by the privileged user shall be allowed during a certain period.

e) Separate user IDs shall be allowed to the user for performing privileged and normal (nonprivileged) activities.

f) The use of user IDs for emergency use shall be recorded and approved. The passwords shall be reset after use.

6.6.5. User's Account Management

a) Procedures for user account management shall be established to control access to application systems and data. The procedures shall include the following:

- Users shall be authorized by the computer system owner to access the computer services.
- A written statement of access rights shall be given to all users.
- All users shall be required to sign an undertaking to acknowledge that they understand the conditions of access.
- Where access to computer services is administered by service providers, ensure that the service providers do not provide access until the authorization procedures have been completed. This includes the acknowledgment of receipt of the accounts by the users.
- A formal record of all registered users of the computer services shall be maintained.
- Access rights of users who have been transferred, or left the organization shall be removed immediately.
- A periodic check shall be carried out for redundant user accounts and access rights that are no longer required.
- Ensure that redundant user accounts are not re-issued to another user.

b) User accounts shall be suspended under the following conditions:

- When an individual is on extended leave or inactive use of over thirty days. In the case of a 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 one month. In the case of protected computer systems, the limit of one month may be reduced to two weeks.

6.6.6. Data and Resource Protection

a) 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.

b) 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, program) or groups of named objects, and the type of access allowed.

c) For networked or shared computer systems, system users shall be limited to a profile of data objects required to perform their needed tasks.

d) Access controls for any data and/or resources shall be determined as part of the systems analysis and design process.

e) Application Programmer shall not be allowed to access the production system.

6.7. Sensitive Systems Protection

a) Security tokens/smart cards/bio-metric technologies such as Iris recognition, fingerprint verification technologies, etc., shall be used to complement the usage of passwords to access the computer system.

b) For computer systems processing sensitive data, access by other organizations shall be prohibited or strictly controlled.

c) For sensitive data, encryption of data in storage shall be considered to protect its confidentiality and integrity.

6.8. Data Centre Operations Security

6.8.1. Job Scheduling

a) 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.

b) As far as possible, automated job scheduling should be used. Manual job scheduling should require prior approval from the competent authority.

6.8.2. System Operations Procedure

a) Procedures shall be established to ensure that only authorized and correct job stream and parameter changes are made.

b) 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.

c) Procedures shall be established to ensure that people other than well-trained computer operators are prohibited from operating the computer equipment.

d) 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.

6.8.3. Media Management

a) Responsibilities for media library management and protection shall be clearly defined and assigned.

b) All media containing sensitive data shall be stored in a locked room or cabinets, which must be fire resistant and free of toxic chemicals.

c) Access to the media library (both on-site and off-site) shall be restricted to authorized persons only. A list of personnel authorized to enter the library shall be maintained.

d) The media containing sensitive and back up data must be stored at three different physical locations in the country, which can be reached in a few hours.

e) A media management system shall be in place to account for all media stored on-site and offsite.

f) All incoming/outgoing media transfers shall be authorized by management and users.

g) An independent physical inventory check of all media shall be conducted at least every six months.

h) All media shall have external volume identification. Internal labels shall be fixed, where available.

i) Procedures shall be in place to ensure that only authorized addition/removal of media from the library is allowed.

j) Media retention periods shall be established and approved by management in accordance with legal/regulatory and user requirements.

6.8.4. Media Movement

a) Proper records of all movements of computer tapes/disks between on-site and off-site media library must be maintained.

b) There shall be procedures to ensure the authorized and secure transfer to media to/from external parties and the off-site location. A means to authenticate the receipt shall be in place.

c) 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.

6.9. Data Backup and Off-site Retention

a) Back-up procedures shall be documented, scheduled and monitored.

b) Up-to-date backups of all critical items shall be maintained to ensure the continued provision of the minimum essential level of service. These items include:

- Data files
- Utilities programmers
- Databases
- Operating system software
- Applications system software
- Encryption keys
- Pre-printed forms
- Documentation (including a copy of the business continuity plans)

c) 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.

d) Backups of the system, application, and data shall be performed regularly. Backups should also be made for application under development and data conversion efforts.

e) Data backup is required for all systems including personal computers, servers, and distributed systems and databases.

f) Critical system data and file server software must have full backups taken weekly.

g) The backups must 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 must be rotated periodically to an off-site storage location.

h) Critical system data and file server software must have incremental backups taken daily.

i) Completely static systems may not require periodic backup, but shall be backed up after changes or updates in the information.

j) Each LAN/system should have a primary and backup operator to ensure continuity of business operations.

k) The business recovery plan should be prepared and tested on an annual basis.

6.10. Measures to Handle Computer Virus

a) 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.

b) Virus detection software must be used to check storage drives both internal and external to the system periodically.

c) 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.

d) A team shall be designated to deal with reported or suspected incidents of computer virus. The designated team shall ensure that the latest version of antivirus software is loaded on all data, files, PKI servers and personal computers.

e) 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
- An incident report must be documented and communicated per established procedures.

f) Awareness and training program shall be established to communicate virus protection practices, available controls, areas of high risk to virus infection and responsibilities.

6.11. Relocation of Hardware and Software

a) 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 a 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.

6.12. Hardware and Software Maintenance

Whenever the hardware and software maintenance of the computer or computer network is being carried out, the following should be considered:

a) Proper placement and installation of Information Technology equipment to reduce the effects of interference due to electromagnetic emanations.

b) Maintenance of an inventory and configuration chart of hardware.

c) Identification and use of security features implemented within the hardware.

d) Authorization, documentation, and control of change made to the hardware.

e) Identification of support facilities including power and air conditioning.

f) Provision of an uninterruptible power supply.

g) Maintenance of equipment and services.

h) An organization must make proper arrangements for maintenance of computer hardware, software (both system and application) and firmware installed and used by them. It shall be the responsibility of the officer in charge of the operational site to ensure that the contract for the annual maintenance of hardware is always in place.

i) An organization must enter into maintenance agreements, if necessary, with the supplier of computer and communication hardware, software (both system and application) and firmware.

j) Maintenance personnel will sign non-disclosure agreements.

k) The identities of all hardware and software vendor maintenance staff should be verified before allowing them to carry out maintenance work.

l) All maintenance personnel should be escorted within the operational site/computer system and network installation room by the authorized personnel of the organization.

m) After maintenance, any exposed security parameters such as passwords, user IDs, and accounts will be changed or reset to eliminate any potential security exposures.

n) If the computer system, computer network or any of its devices are vulnerable to computer viruses as a result of performing maintenance, system managers or users shall scan the computer system and its devices and any media affected for viruses as a result of maintenance.

6.13. Purchase and Licensing of Hardware and Software

a) 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 this Security Guideline for CA before the signing of any contract, purchase or lease.

b) 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 this Security Guideline for CA. 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.

c) 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.

d) 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.

e) Illegally acquired or unauthorized software must not be used on any computer, computer network or data communication equipment. If any illegally acquired or unauthorized software is detected by the System Administrator or Network Administrator, the same must be removed immediately.

6.14. System Software

a) All system software options and parameters shall be reviewed and approved by the management.

b) System software shall be comprehensively tested and its security functionality validated before implementation.

c) All vendor-supplied default user IDs shall be deleted or password changed before allowing users to access the computer system.

d) Versions of system software installed on the computer system and communication devices shall be regularly updated.

e) All changes proposed in the system software must be appropriately justified and approved by an authorized party.

f) A log of all changes to system software shall be maintained, completely documented and tested to ensure the desired results.

g) 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.

h) System Programmers shall not be allowed to have access to the application system's data and program files in the production environment.

i) Procedures to control the use of sensitive system utilities and system programs 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 person independent of System Administrator for dubious activities.

6.15. Documentation Security

a) All documentation about 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.

b) All documentation and subsequent changes shall be reviewed and approved by an independent authorized party before the issue.

c) Access to application software documentation and sensitive system software documentation shall be restricted to authorized personnel on a "need-to-use" basis only.

d) Adequate backups of all documentation shall be maintained and a copy of all critical documentation and manuals shall be stored off-site.

e) Documentation shall be classified according to the sensitivity of its contents/implications.

f) Organizations shall adopt a clean desk policy for papers, diskettes and other documentation to reduce the risks of unauthorized access, loss of and damage to information outside normal working hours.

6.16. Firewalls

a) Intelligent devices generally are known as "Firewalls" shall be used to isolate the organization’s data network with the external network. A firewall device should also be used to limit network connectivity for unauthorized use.

b) 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.

c) All firewalls shall be subjected to a thorough test for vulnerability before being put to use and at least half-yearly thereafter.

d) All web servers for access by Internet users shall be isolated from other data and host servers.

6.17. Problem Management and Reporting

a) Procedures for identifying, reporting and resolving problems, such as non-functioning 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.

b) A help desk shall be set up to assist users in the resolution of problems.

c) 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.

6.18. Maintenance of Subscriber’s Data

a) 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 court order.

b) Data on the usage of the Digital Signature Certificates by the subscribers and other transactional data relating to the subscribers' activities generated by the Certificate Authority in the course of its operation shall be protected to ensure the subscribers' privacy.

c) A secure communication channel between the Certificate Authority and its subscribers shall be established to ensure the authenticity, integrity, and confidentiality of the exchanges (e.g. transmission of Digital Signature Certificate, password, private key) during the Digital Signature Certificate issuance process.

7. Reference

1. Critical Mass Cybersecurity Requirement Standard. INSA September 2009 E.C
2. Electronic Signature Proclamation, Proclamation No.1072/2018, FEDERAL NEGARIT GAZETTE, ADDIS ABABA, 16th February 2018.
3. Security guidelines for certification authorities. Singapore, September 2003
4. Public Key Infrastructure (PKI) Regulations. National Information Technology Development Agency (NITDA), Nigeria, September 2014.

5. Indian Security Guidelines for Certifying Authorities
6. Indian Information Technology (IT) Security Guidelines