ICTA
INFORMATION & COMMUNICATION TECHNOLOGIES AUTHORITY

CONTROLLER OF CERTIFICATION AUTHORITIES (CCA)

Level 12, The Celicourt 6, Sir Celicourt Antelme Street Port Louis Mauritius
Tel.: (230) 211 5333/4 Fax: (230) 211 9444 email: info@cca.mu

CCA
CONTROLLER OF CERTIFICATION AUTHORITIES OF MAURITIUS

THE CCA DIRECTIVE 3 OF 2010

Ref: ICTA/CCA/CCAD/3/2010 **10 December 2010**

The Information and Communication Technologies Authority in the exercise of its function as the Controller of Certification Authorities and in pursuance of Section 18 (1) (z) of the Information and Communication Technologies Act 2001 (as amended), Section 37 of the Electronic Transactions Act 2000 (as amended) and Regulation 3 (3) of the Electronic Transactions (Certification Authorities) Regulations 2010, hereby issues the following Directive.

1. Short title and Commencement

(i) This Directive shall be called "The CCA Directive 3 of 2010 - (CCAD 3 of 2010)"

(ii) The CCA Directive 3 of 2010 shall come into effect on 13 December 2010.

2. Scope and objective

This Directive pertains to security measures for the management and operation of licensed, recognised and approved Certification Authorities (CAs).

The objective of this directive is aimed at protecting the integrity, confidentiality and availability of their services, data and systems.

Information & Communication Technologies Authority
Level 12
The Celicourt
6, Sir Celicourt Antelme St
Port Louis

Mr. T. Dwarka
Chairman

Dr. M. K. Oolun
Executive Director

To: All Licensed, Recognised and Approved Certification Authorities

DIRECTIVE - III

Security Directives for Certification Authorities

Index

Security Directives for Certification Authorities

1. Introduction

This document prescribes security directives for the management and operation of Certification Authorities (CAs) and is aimed at protecting the integrity, confidentiality and availability of their services, data and systems. These directives apply to Certification Authorities that perform all the functions associated with generation, issue and management of Digital Signature Certificate such as:

(1) Verification of registration, suspension and revocation request;

(2) Generation, issuance, suspension and revocation of Digital Signature Certificates; and

(3) Publication and archival of Digital Signature Certificates, suspension and revocation of information.

2. Security Management

The Certification Authority shall define Information Technology security policies for its operation on the lines defined in Directive-II and Directive-III. The policy shall be communicated to all personnel and widely published throughout the organization to ensure that the personnel follow the policies.

3. Physical controls – site location, construction and physical access

(1) The site location, design, construction and physical security of the operational site of Certification Authority shall be in accordance with para 4 of the Information Technology Security Directives given at Directive-II.

(2) 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 para 4.5 of the Information Technology Security Directives given at Directive-II.

(3) A Certification Authority must:

(i) ensure that the operational site housing PKI servers, communications and networks is protected with fire suppression system in accordance with para 4.3 of the Information Technology Security Directives given at Directive-II.

(ii) ensure that power and air-conditioning facilities are installed in accordance with para 4.2 of the Information Technology Security Directives given at Directive-II.

(iii) ensure that all removable media and papers containing sensitive or plain text information are listed, documented and stored in a container properly identified.

(iv) ensure unescorted access to Certification Authority's server is limited to those personnel identified on an access list.

(v) ensure that the exact location of Digital Signature Certification System shall not be publicly identified.

(vi) ensure that access security system is installed to control and audit access to the Digital Signature Certification System.

(vii) ensure that dual control over the inventory and access cards/keys are in place.

(viii) ensure that up-to-date list of personnel who possess the access cards/keys is maintained at the Certification Authority's operational site. Loss of access cards/keys shall be reported immediately to the Security Administrator; who shall take appropriate actions to prevent unauthorised access.

(ix) ensure personnel not on the access list are properly escorted and supervised.

(x) ensure a site access log is maintained at the Certification Authority's operational site and inspected periodically.

(4) Multi-tiered access mechanism must be installed at the Certification 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. Each security zone must be separated from the other by floor to ceiling concrete reinforced walls. 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. Electrical/Electronic circuits to external security alarm monitoring service (if used) must be supervised. No single person must have complete access to PKI Server, root keys or any computer system or network device on his/her own.

(5) Entrance to the main building where the Certification Authority's facilities such as Data Centre, PKI Server and Network devices are housed and entrance to each security zone must be video recorded round the clock. The recording should be carefully scrutinized and maintained for at least one year.

(6) A Certification Authority site must be manually or electronically monitored for unauthorised intrusion at all times in accordance with the Information Technology Security Directives given at Directive-II.

(7) Computer System/PKI Server performing Digital Signature Certification function shall be located in a dedicated room or partition to facilitate enforcement of physical access control. The entry and exit of the said room or partition shall be automatically locked with time stamps and shall be reviewed daily by the Security Administrator.

(8) Access to infrastructure components essential to operation of Certification Authority such as power control panels, communication infrastructure, Digital Signature Certification system, cabling, etc. shall be restricted to authorized personnel.

(9) By-pass or deactivation of normal physical security arrangements shall be authorised and documented by security personnel.

(10) Intrusion detection systems shall be used to monitor and record physical access to the Digital Signature Certification system during and after office hours.

(11) 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.

(12) System software shall be verified for integrity in accordance with para 15 of the Information Technology Security Directives given at Directive-II.

4. Media Storage

A Certification Authority must ensure that storage media used by his system are protected from environment threats such as temperature, humidity and magnetic and are transported and managed in accordance with para 8.3 and para 8.4 of the Information Technology Security Directives given at Directive-II.

5. Waste Disposal

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.

6. Off-site Backup

A Certification Authority must ensure that facility used for off-site backup, if any, shall be within the country and shall have the same level of security as the primary Certification Authority site.

7. Change and Configuration Management

(1) The components of the Certification Authority infrastructure (e.g. cryptographic algorithm and its key parameters, operating system, system software, computer system, PKI server, firewalls, physical security, system security etc.) shall be reviewed every year for new technology risks and appropriate action plan shall be developed to manage the risks identified for each component.

(2) The application software, system software and hardware, which are procured from questionable sources, shall not be installed and used for any function associated with generation and management of Digital Signature Certificate.

(3) Software updates and patches shall be reviewed for security implications before being implemented on Certification Authority's system.

(4) Software updates and patches to rectify security vulnerability in critical systems used for Certification Authority's operation shall be promptly reviewed and implemented.

(5) Information on the software updates and patches and their implementation on Certification Authority's system shall be clearly and properly documented.

8. Network and Communications Security

(1) Certification Authority's systems shall be protected to ensure network access control to critical systems and services from other systems in accordance with para 17, para 18, para 19 and para 20 of the Information Technology Security Directives given at Directive-II.

(2) Network connections from the Certification Authority's system to external networks shall be restricted to only those connections which are essential to facilitate Certification Authority's functional processes and services. Such

network connections to the external network shall be properly secured and monitored regularly.

(3) 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) shall be implemented to protect the systems performing the function of generation and management of Digital Signature Certificate from potential attacks.

(4) 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.

(5) Communication between the Certification Authority systems connected on a network shall be secure to ensure confidentiality and integrity of the information. For example, communications between the Certification Authority's systems connected on a network should be encrypted and digitally signed.

(6) 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.

9. System Security Audit Procedures

9.1 Types of event recorded

(1) The Certification 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:

(i) System start-up and shutdown;

(ii) Certification Authority's application start-up and shutdown;

(iii) Attempts to create, remove, set passwords or change the system privileges of the PKI Master Officer, PKI Officer, or PKI Administrator;

(iv) Changes to keys of the Certification Authority or any of his other details;

(v) Changes to Digital Signature Certificate creation policies, e.g. validity period;

(vi) Login and logoff attempts;

(vii) Unauthorised attempts at network access to the Certification Authority's system;

(viii) Unauthorised attempts to access system files;

(ix) Generation of own keys;

(x) Creation and revocation of Digital Signature Certificates;

(xi) Attempts to initialize remove, enable, and disable subscribers, and update and recover their keys;

(xii) Failed read-and-write operations on the Digital Signature Certificate and Certificate Revocation List (CRL) directory.

(2) Monitoring and Audit Logs

(i) A Certification 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:

(a) Registration;

(b) Certification;
(c) Publication;
(d) Suspension; and
(e) Revocation.

(ii) Records and log files shall be reviewed regularly for the following activities:
(a) Misuse;
(b) Errors;
(c) Security violations;
(d) Execution of privileged functions;
(e) Change in access control lists;
(f) Change in system configuration.

(3) 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.

(4) A Certification Authority should also collect and consolidate, either electronically or manually, security information which may not be generated by his system, such as:
(i) Physical access logs;
(ii) System configuration changes and maintenance;
(iii) Personnel changes;
(iv) Discrepancy and compromise reports;
(v) Records of the destruction of media containing key material, activation data, or personal subscriber information.

(5) To facilitate decision-making, all agreements and correspondence relating to services provided by Certification Authority should be collected and consolidated, either electronically or manually, at a single location.

9.2 Frequency of Audit Log Monitoring

The Certification 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.

9.3 Retention Period for Audit Log

The Certification Authority must retain its audit logs onsite for at least twelve months and subsequently retain them in the manner described in para 10 of the Information Technology Security Directives as given in Directive-II.

9.4 Protection of Audit Log

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.

9.5 Audit Log Backup Procedures

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

9.6 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. The Certification Authority must ensure that a vulnerability assessment is performed, reviewed and revised, if necessary, following an examination of these monitored events.

10. Records Archival

(1) Digital Signature Certificates stored and generated by the Certification Authority must be retained for at least seven years after the date of its expiration. This requirement does not include the backup of private signature keys.

(2) Audit information as detailed in para 9, subscriber agreements, verification, identification and authentication information in respect of subscriber shall be retained for at least seven years.

(3) A second copy of all information retained or backed up must be stored at three locations within the country including the Certification 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.

(4) All information pertaining to Certification 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 properly constitutional warrant or such other legally enforceable document is produced.

(5) The Certification Authority should verify the integrity of the backups at least once every six months.

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

11. Compromise and Disaster Recovery

11.1 Computing Resources, Software and/or Data are corrupted

The Certification 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 Certification Authority, the Certification Authority must ensure that any agreement with the repository provides for business continuity procedures.

11.2 Secure facility after a natural or other type of disaster

The Certification 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 Certification Authority, the Certification Authority must ensure that any agreement with the repository provides that a disaster recovery plan be established and documented by the repository.

11.3 Incident Management Plan

An incident management plan shall be developed and approved by the management. The plan shall include the following areas:

(i) Certification Authority's certification key compromise;
(ii) Hacking of systems and network;
(iii) Breach of physical security;
(iv) Infrastructure availability;
(v) Fraudulent registration and generation of Digital Signature Certificates; and
(vi) Digital Signature Certificate suspension and revocation information.

An incident response action plan shall be established to ensure the readiness of the Certification Authority to respond to incidents. The plan should include the following areas:

(i) Compromise control;
(ii) Notification to user community; (if applicable)
(iii) Revocation of affected Digital Signature Certificates; (if applicable)
(iv) Responsibilities of personnel handling incidents;
(v) Investigation of service disruption;
(vi) Service restoration procedure;
(vii) Monitoring and audit trail analysis; and
(viii) Media and public relations.

12. Number of Persons Required Per Task

The Certification 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 Certification 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 Certification Authority.

13. Identification and Authentication for Each Role

All Certification Authority personnel must have their identity and authorization verified before they are:

(i) included in the access list for the Certification Authority's site;
(ii) included in the access list for physical access to the Certification Authority's system;
(iii) given a certificate for the performance of their Certification Authority role;
(iv) given an account on the PKI system.

Each of these certificates and accounts (with the exception of Certification Authority's signing certificates) must:

(i) be directly attributable to an individual;
(ii) not be shared;
(iii) be restricted to actions authorized for that role; and
(iv) procedural controls.

Certification Authority's operations must be secured using techniques of authentication and encryption, when accessed across a shared network.

14. Personnel Security Controls

The Certification Authority must ensure that all personnel performing duties with respect to its operation must:

(i) be appointed in writing;

(ii) be bound by contract or statute to the terms and conditions of the position they are to fill;

(iii) have received comprehensive training with respect to the duties they are to perform;

(iv) be bound by statute or contract not to disclose sensitive Certification Authority's security related information or subscriber information;

(v) not be assigned duties that may cause a conflict of interest with their Certification Authority's duties; and

(vi) be aware and trained in the relevant aspects of the Information Technology Security Policy and Security Directives framed for carrying out Certification Authority's operation.

15. Training Requirements

A Certification Authority shall ensure that all personnel performing duties with respect to its operation, must receive comprehensive training in:

(i) relevant aspects of the Information Technology Security Policy and Security Directives framed by the Certification Authority;

(ii) all PKI software versions in use on the Certification Authority's system;

(iii) all PKI duties they are expected to perform; and

(iv) disaster recovery and business continuity procedures.

16. Retraining Frequency and Requirements

The requirements of para 15 must be kept current to accommodate changes in the Certifiying Authority's system. Refresher training must be conducted as and when required, and the Certification Authority must review these requirements at least once a year.

17. Documentation Supplied to Personnel

A Certification 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.

18. Key Management

18.1 Generation

(1) The subscriber's key pair shall be generated by the subscriber or on a key generation system in the presence of the subscriber.

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

18.2 Distribution of Keys

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.

18.3 Storage

(1) Certification 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 Certification Authority. The key of the Certification 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.

(2) The Certification Authority's key custodians shall ensure that the Certification Authority's key component or the activation code is always under his sole custody. Change of key custodians shall be approved by the Certification Authority's management and documented.

18.4 Usage

(1) A system and software integrity check shall be performed prior to Certification Authority's key loading.

(2) Custody of and access to the Certification Authority's keys shall be under split control. In particular, Certification Authority's key loading shall be performed under split control.

18.5 Certification Authority's Public Key Delivery to Users

The Certification 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.

19. Private Key Protection and Backup

(1) The Certification Authority must protect its private keys from disclosure.

(2) The Certification 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.

(3) The Certification Authority's private key backups should be stored in a secure storage facility, away from where the original key is stored.

20. Method of Destroying Private Key

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.

21. Usage Periods for the Public and Private Keys

21.1 Key Change

(1) Certification Authority and Subscriber keys shall be changed periodically.

(2) Key change shall be processed as per directive I.

(3) The Certification Authority shall provide reasonable notice to the Subscriber's relying parties of any change to a new key pair used by the Certification Authority to sign Digital Signature Certificates.

(4) The Certification 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. All keys must have validity periods of no more than five years.

Suggested validity period:

(a) Certification Authority's root keys and associated certificates – five years;

(b) Certification Authority's private signing key - two years;

(c) Subscriber Digital Signature Certificate key – three years;

(d) Subscriber private key – three years.

Use of particular key lengths should be determined in accordance with departmental Threat-Risk Assessments.

21.2 Destruction

Upon termination of use of a Certification Authority signature private key, all components of the private key and all its backup copies shall be securely destroyed.

21.3 Key Compromise

(1) A procedure shall be pre-established to handle cases where a compromise of the Certification Authority's Digital Signature private key has occurred. In such case, the Certification Authority shall immediately revoke all affected Subscriber Digital Signature Certificates.

(2) The Certification Authority should immediately revoke the affected keys and Digital Signature Certificates in the case of Subscriber private key compromise.

(3) The Certification Authority's public keys shall be archived permanently to facilitate audit or investigation requirements.

(4) Archives of Certification Authority's public keys shall be protected from unauthorised modification.

22. Confidentiality of Subscriber's Information

(1) Procedures and security controls to protect the privacy and confidentiality of the subscribers' data under the Certification 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.

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

(3) A secure communication channel between the Certification 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.