
CONTROLLER OF CERTIFICATION
AUTHORITIES OF MAURITIUS

# Controller of Certification Authorities of Mauritius

# Certificate Practice Statement (CPS)

## Document control

| | |
|---|---|
| Document name | CCA of Mauritius CPS |
| Version | 1.1 |
| Last update | 04 October 2013 |
| Document Owner | Controller of Certification Authorities of Mauritius |

## Table of Contents

## 1. Introduction

Under section 18 (z) of the Information and Communication Technologies Act 2001 (ICT Act), the ICT Authority is the Controller of Certification Authorities (CCA) in Mauritius. The CCA as the "Root" Authority certifies the technologies, infrastructure and practices of all the Certification Authorities (CA), licensed/approved/recognised, to issue Digital Signature Certificates.

It is the ICT Authority's responsibility to monitor that certification-service-providers comply with the obligations imposed on them by law. In this respect, the CCA maintains a publicly accessible database containing a CA disclosure record for each licensed/approved/recognised CA.

The Electronic Transactions Act, 2000, as amended, and its regulations, provide the required legal sanctity to digital signatures based on asymmetric cryptosystems. It also provides for the CCA to license/approve/recognise and regulate the working of CAs in Mauritius. The CAs issue digital signature certificates to users.

The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed/approved/recognised CAs.

In line with the provisions of the Electronic Transaction Act 2000, as amended, and the regulations made thereunder, the issuance of licensed/approved/recognised certificates implies the remittance of:

i. a digital licence; and
ii. a paper-based licence.

In May 2012, the technical infrastructure required for the issuance of the digital licence was installed at the premises of the Authority. This infrastructure allows the Authority to perform the following distinct exercises:

i. issuance of the key pair (public and private key) for the CCA;
ii. issuance of the self-signed root certificate for the CCA and hosting of same on the www.cca.mu website as per section 24(6) of the Electronic Transactions (Certification Authorities) Regulations 2010;
iii. affixture of the CCA digital signature on licensed/recognised/approved CA public key certificate of CAs;

The Certification Practice Statement (CPS) of the CCA states how the PKI components meet the assurance requirements, security control, operational policy, procedures and other matters relevant to obligations and responsibilities of the CCA and CAs in accordance with the Electronic Transaction Act 2000, as amended and the Regulations thereunder.

This CPS uses certain expressions. These are given below.

**Approval:** means an approval issued by the Controller, at the Minister's request, to a public sector agency under regulation 15 of the Electronic Transaction Act 2000, as amended, or renewed under regulation 16 of the Electronic Transaction Act 2000, as amended, as the case may be.

**Certifying Authority (CA):** means a person or organisation who has been granted a licence/recognition/approval to issue Digital Signature Certificates under Section 24 of the Electronic Transactions (Certification Authorities) Regulations 2010.

**Certification Practice Statement (CPS):** means the statement issued by the Controller of Certification Authorities of Mauritius to specify the practices it employs in the issuance of Digital Signature Certificates.

**Controller:** means the Controller of Certifying Authorities appointed under Section 18 (z) of the Information and Communication Technologies Act 2001.

**Controller of Certifying Authorities (CCA):** means the Office of the Controller.

**Digital Signature:** means authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 19 of the Electronic Transactions Act, 2000, as amended.

**Digital Signature Certificate (DSC):** means a Digital Signature Certificate issued under Section 24 of the Electronic Transactions (Certification Authorities) Regulations 2010.

**ICT Appeal Tribunal:** means the ICT Appeal Tribunal established under Section 36 of the ICT Act 2001.

**Licence:** means a licence issued under regulation 5 of the Electronic Transaction Act 2000, as amended or renewed under regulation 6 of the Electronic Transaction Act 2000, as amended, as the case may be.

**Recognition:** means a recognition issued to a foreign certification authority under regulation 11 of the Electronic Transaction Act 2000, as amended or renewed under regulation 12 of the Electronic Transaction Act 2000, as amended, as the case may be.

**Root Certificate:** CCA's self-signed certificate which is at the root of the Mauritian PKI hierarchy.

**Root Key:** CCA's key pair.

## 1.1. Overview

This CPS provides information that describes the practices employed by the CCA in operating its technical infrastructure and repository.

The CCA is responsible for:

- The issuance of X.509 Public Key Certificate containing the public key of the licensed/approved/recognised CA
- Generating CRLs
- Publishing Public Key Certificates and CRLs issued by the CCA in its repository.

The CCA issues Licenses/Approval/Recognition to Certifying Authorities, after duly processing their applications as provided for under the Electronic Transactions Act, 2000, as amended, and its regulations thereunder. This process includes examining the application and accompanying documents as provided for in Section 5 (2) of the Electronic Transactions (Certification Authorities) Regulations 2010, approving the CPS; auditing the physical and technical infrastructure of the applicants. The CCA can suspend or revoke licenses/approvals/recognitions in accordance with the provisions of Sections 18 of the Electronic Transactions (Certification Authorities) Regulations 2010. The CCA also approves changes in the CPS, if any, of the CAs.

This CPS is based on the RFC 2527- Internet X.509 PKI Certificate Policy and Certificate Practice Framework. This CPS covers the practices followed by the CCA for the procedures related to the licence/approval/recognition application, issuance, use, validation, suspension, revocation and their expiry, as well as the operational maintenance of its technical infrastructure and repository. All documents issued by the CCA including the CPS can be downloaded from http://www/cca.mu.

This CPS is subject to a regular review process that strives to take into consideration developments in international PKI standardisation initiatives, development in technology and information security, as well as other relevant issues.

### 1.2. Community and Applicability

The Mauritian PKI community comprises the CCA, licensed/approved/recognised CAs, local agents for foreign CAs & their subscribers and relying parties. This CPS is applicable to all certificates issued by the CCA. The practices described in this CPS apply to the issuance and use of certificates and Certificate Revocation Lists (CRLs) for licensed/approved/recognised CAs.

### 1.3. Contact Details

C/o ICT Authority

Level 12, The Celicourt
6, Sir Celicourt Antelme Street
Port Louis
Mauritius

Telephone: +230 211 5333
Fax: +230 211 9444
Web: www.cca.mu
E-mail: info@cca.mu

## 2. General Provisions

### 2.1. Obligations

#### 2.1.1. CCA Mauritius obligations

**CCA Mauritius shall**

- Operate as an offline Root CA.
- Operate in accordance with this CPS.
- Accept certificate signing requests from authorised representative of licensed/approved/recognised CAs
- Issue Public Key certificates to the licensed/approved/recognised CAs.
- Publish the certificates in the repository.
- Accept the revocation request from the authorised representative of licensed/approved/recognised CAs.
- Immediately publish the CRL after revocation of licensed/approved/recognised CA.
- Issue and publication of routine CRLs.
- Preserve audit logs and certificate issuance process.

#### 2.1.2. The Repository obligation

**The repository shall publish**

- Public key certificates of licensed/approved/recognised CAs
- Certificate Revocation Lists

#### 2.1.3. Licensed/Approved/Recognised CA Obligations

**The licensed/approved/recognised CA must:**

- Protect their private key in a secure manner.
- have their CPS approved by the CCA.
- perform the CA operation as per their CPS approved by the CCA.
- update their CPS in accordance with the Directives and Guidelines issued by the CCA.
- publish a name and contact information of the party responsible for the licensed/approved/recognised CA.
- Undergo and pass an audit as the CCA may, by notice in writing, require.
- Maintain a web site and publish the licence/approval/recognition, subscriber certificates and CRLs.
- Revoke all the certificates to subscribers and publish the CRL immediately in case of compromise of their signing key.

### 2.1.4. Relying Party Obligations

**Before relying on a certificate under PKI hierarchy of Mauritius, Relying parties are obligated to:**

- Read and comply with the provisions of this CPS.
- Verify the purpose of a certificate, its validity period, key usage, class of certificate and path to trust anchor.
- Ascertain from the applicable CCA CRL (available on http://www.cca.mu) that the certificate has not been revoked.
- Be bound by the liability described in the CPS upon reliance on a certificate.

## 2.2. Liability

The Government of Mauritius disclaims any liability that may arise from use of any certificate issued by the CCA Mauritius, or by the CCA's decision to revoke a certificate issued by it. In no event will the CCA or the Government of Mauritius be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued by the CCA Mauritius.

The CCA has no responsibility for any delays or damages due to force majeure such as warfare or a natural disaster or reasons beyond provisions of the Electronic Transaction Act 2000, as amended, ICT Act 2001 and the regulations made thereunder.

## 2.3. Financial responsibility

The CCA disclaims all liability due to the use of any certificates issued by the CCA Mauritius which certify public keys of CAs. The CCA is not the agent, fiduciary, trustee or any other representative of any of the licensed/approved/recognised CAs and must not be represented by the licensed/approved/recognised CAs in that form. licensed/approved/recognised CAs have no authority to bind the CCA, by contract or otherwise of any obligation or financial implication.

## 2.4. Interpretation and Enforcement

### 2.4.1. Governing Law

The governing laws are the ICT Act 2001 and the Electronic Transaction Act 2000, as amended, and the regulations made thereunder.

### 2.4.2. Dispute Resolution procedures

The CCA is competent under the ICT Act 2001 and the Electronic Transaction Act 2000, as amended, and the regulations made thereunder, to resolve any dispute between CAs and subscribers. The ICT Appeal Tribunal, under the ICT Act 2001, is the competent court to decide on appeals filed by individuals aggrieved by the order of the CCA.

The CCA can mediate between CAs and subscribers directly or through an arbitrator. For this purpose, it can request any information or materials from both parties in line with their CPS, and the provisions of the Electronic Transactions Act 2000, as amended. The CCA will endeavour to facilitate the resolution of conflicts between CAs and subscribers that may arise as a result of the use of certificates.

## 2.5. Fees

### 2.5.1. Certificate Issuance fees

Certificates are issued to CAs as part of the licence/approval/recognition granted to them. The fee for issuance of licence/approval/recognition shall be as prescribed under the Second Schedule of the Electronic Transactions (Certification Authorities) Regulations 2010.

### 2.5.2. Certificate Access Fee

CCA does not levy any fee for accessing certificates through its web site.

### 2.5.3. Revocation or status information access fees

CCA does not levy any fees for accessing the suspension and revocation list of certificates.

### 2.5.4. Fees for other services such as policy information

CCA can charge for printed documents, CD-ROMs etc., if required.

## 2.6. Publication and Repository

### 2.6.1. Publication of information on services offered by CCA

The CCA publishes the following information to the repository on its website.

- Self-signed certificates of CCA Mauritius
- Certificates issued to all licensed/approved/recognised CAs
- CPS of CCA Mauritius and CAs
- CRLs issued by the CCA

### 2.6.2. Frequency of publication

Certificates will be published in the repository immediately after issuance and it will be available to public through website http://www.cca.mu

CRLs will be published in the repository immediately after revocation.

## 2.7. Audit

The CCA technical infrastructure is audited annually by an auditor appointed by the Office of the CCA. Compliance audit results are communicated to the CCA.

### 2.7.1. Actions taken as a result of deficiency

The CCA shall take appropriate action on the deficiencies pointed out by the audit so as to secure the technical operations of the CCA.

## 2.8. Confidentiality

The CCA collects information about the CAs as part of the licence/approval/recognition application. These data are processed in a way that ensures protection of their private information and in line with the Data Protection Act 2004 of Mauritius. The information published in the website, their digital signature certificate, and in the CRL are not confidential.

## 2.9. Intellectual Property Rights

No right or interest in any intellectual property rights are granted to any licensed/approved/recognised CAs or any relying party. All rights in intellectual property are reserved. Any content copied from this document should include reference to this source.

Intellectual property rights on the items listed below belong to the CCA:

- Software and hardware developed by CCA
- Certification Practice Statement of CCA
- Common name of Root Certificates
- Internet Domain Name
- Key pairs created by CCA

## 3. Identification and Authentication

### 3.1. Initial Registration

All CA applicants shall fill the form for application to become licensed/approved/recognised, supported by such documents and information as required by the CCA.

#### 3.1.1. Types of names

Each CA Applicant must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate subjectName field.

#### 3.1.2. Need for names to be meaningful

The Subject name contained in a CA certificate must be meaningful in the sense that the CCA is provided with proper evidence of the association existing between the name and the entity to which it belongs.

#### 3.1.3. Uniqueness of names

The CCA shall ensure that the set of names is unambiguous. The name shall conform to X.500 standards for name uniqueness.

#### 3.1.4. Name claim dispute resolution procedure

The CCA may, by reasonable endeavours; resolve disputes that may arise over the allocation of names and in its discretion may reject, change, re-issue or revoke certificates in relation to any Distinguished Name.

#### 3.1.5. Method to prove possession of private key

To establish that the applicants possess valid functioning key pairs, the CCA would require applicants to submit a Certificate Signing Request (CSR) in accordance with the PKCS#10 standard. The signing key pair of the licensed/approved/recognised CAs shall be stored in FIPS 140-1 level 3 or higher level device. An independent verification may be performed as a part of the auditing process.

#### 3.1.6. Authentication of organisation identity

The documents mentioned in 4.1 ensure the authentication of organisation identity.

#### 3.1.7. Authentication of individual identity

The documents mentioned in 4.1 ensure the authentication of individual identity.

### 3.2. Revocation Request

Licensed/approved/recognised CAs can request the revocation of its certificate(s). The Controller of Certifying Authorities can also decide to revoke a CA certificate.

## 4. Operational Requirements

### 4.1. Certificate Application

An application for a licence/approval/recognition public key certificate is made by filling out the application supported by relevant information which can be obtained directly from the Office of the CCA or downloaded from the web site of the CCA - www.cca.mu or use the PKI enabled application form for online application.

### 4.2. Certificate Issuance

Once grant of license to the CA is approved by CCA, the public key certificate is issued after checking the following criteria:

- A certificate request is generated by the applicant in PKCS # 10 format and submitted to the CCA. The CCA establishes that the public key corresponds to a functioning key pair.

- The CCA establishes the uniqueness of the DN submitted by the applicant.
- The certificate request is used by the CCA to generate the certificate.
- All certificates issued are published in the Repository and are accessible through the web site of the CCA Mauritius.

## 4.3. Certificate Acceptance

The certificate issued by the CCA to the CA applicant will be deemed to have been accepted on its receipt by the CA applicant.

## 4.4. Certificate Revocation

The CCA can order, or an authorised signatory of the licensed/approved/recognised CAs can request, that a public key certificate be revoked when any of the information it contains is known or suspected to be inaccurate, or when the private key associated with the certificate is compromised or suspected to have been compromised.

The CCA shall revoke a public key certificate when it considers revocation necessary or expedient.

### 4.4.1. CRL issuance frequency

The CCA shall update the CRL after a valid revocation request is processed.

### 4.4.2. CRL checking requirements

A relying party may check the CCA's CRL for determining the CA's certificate status before relying on any certificate issued by the CA.

### 4.4.3. Revocation/status checking availability

The CCA shall provide CA certificate status checking through publication of the CRL on the web site

### 4.4.4. Special requirements regarding key compromise

In case of key compromise, the concerned CA shall notify the CCA immediately for revocation of the CA certificate.

## 4.5. Licence Revocation

The CCA can revoke a licensed/approved/recognised CA's licence only under the circumstances defined in regulation 18 of the Electronic Transaction Act 2000, as amended.

## 4.6. Security Audit Procedures

### 4.6.1. Types of event recorded

The minimum audit records of CCA Mauritius to be kept include:

SECURITY AUDIT

- Any changes to the Audit parameters, e.g. audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs

IDENTITY-PROOFING

- Successful and unsuccessful attempts to assume a role
- The value of maximum number of authentication attempts is changed
- The number of unsuccessful authentication attempts exceeds the maximum authentication attempts during user login
- An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
- An Administrator changes the type of authenticator, e.g., from a password to a biometric

ROOT KEY GENERATION

- Whenever the Component generates a key

ROOT CA CREATION

- All CA creation parameters including trusted roles

LICENSED/APPROVED/RECOGNISED CA CERTIFICATE SIGINING

- All certificate PKCS#10 requests signing

CERTIFICATE REVOCATION

- All certificate revocation requests

ACCOUNT ADMINISTRATION

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

CERTIFICATE PROFILE MANAGEMENT

- All changes to the certificate profile

REVOCATION PROFILE MANAGEMENT

- All changes to the revocation profile

CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT

- All changes to the certificate revocation list profile

MISCELLANEOUS

- Creation of a Trusted Role
- Designation of personnel for multiparty control
- Installation of the Operating System
- Installation of the PKI Application
- Installation of hardware cryptographic modules
- Removal of hardware cryptographic modules
- Destruction of cryptographic modules
- Logon attempts to PKI Application
- Receipt of hardware / software
- Attempts to set passwords
- Attempts to modify passwords
- Restoration from back up of the internal CA database
- Posting of any material to a PKI Repository
- Access to the internal CA database
- All certificate compromise notification requests
- Zeroizing Tokens

CONFIGURATION CHANGES

- Hardware
- Software
- Operating System
- Patches
- Security Profiles

PHYSICAL ACCESS / SITE SECURITY

- Personnel Access to room housing Component
- Access to the Component
- Known or suspected violations of physical security

ANOMALIES

- Software error conditions
- Software check integrity failures
- Equipment failure
- Electrical power outages
- Uninterruptible Power Supply (UPS) failure

### 4.6.2. Frequency of processing log

The CCA's audit logs are regularly reviewed by the trusted personnel of Office of CCA and all significant events are detailed in an audit log summary. Such reviews verify that the log has not been tampered with, and then briefly inspect all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken following these reviews are documented.

### 4.6.3. Retention period for audit log

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

### 4.6.4. Protection of audit log

The electronic audit log system includes mechanisms to protect the log files from unauthorised viewing, modification, and deletion.

Manual audit information will be protected from unauthorised viewing, modification and destruction.

### 4.6.5. Audit log backup procedures

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

### 4.6.6. Audit collection system

The CCA audit collection system is a combination of automated and manual processes. The system is maintained through access control mechanisms and role separations with regard to the software and hardware and through documented operational procedures known and followed by CCA personnel. The control measures of both the automated and the manual processes are audited in accordance with section 2.7 of this CPS.

### 4.6.7. Notification to event-causing subject

Operations personnel notify the security administrator when a process or action causes a critical security event or discrepancy.

### 4.6.8. Vulnerability assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities.

## 4.7. Records Archival

### 4.7.1. Types of event recorded

Audit information as detailed in section 4.6 are recorded.

### 4.7.2. Retention period for archive

All CCA records concerning the operation of its certification services are archived and are retained for a period of 10 years.

### 4.7.3. Protection of archive

Archived information is stored in a restricted access facility.

### 4.7.4. Requirements for correct source of time

The real time clock of the computer or communications device shall be set to Mauritian Time. Further there shall be a procedure that checks and corrects drift in the real time clock.

### 4.7.5. Archive collection system

Only authorised and authenticated staffs are allowed to handle archive.

#### 4.7.6. Procedures to obtain and verify archive information

The integrity of the backups is verified immediately after backup. Information stored off-site is also periodically verified for data integrity.

### 4.8. CCA Key changeover

On key changeover, a new public key will be made available via the web.

### 4.9. Compromise and Disaster Recovery

#### 4.9.1. Computing resources, software, and/or data are corrupted

The CCA has established business continuity procedures that outline the steps to be taken in the event of the corruption or loss of computing and networking resources, software and/or data.

#### 4.9.2. Entity key is compromised

In the event of the CCA private signature key being compromised, the CCA shall revoke and re-issue all certificates in use at that instant.

#### 4.9.3. Secure facility after a natural or other type of disaster

In the event of a natural or other type of disaster, the operation of the CCA and the repository will be re-established on an independent disaster recovery site.

### 4.10. CA Termination

In the event of change in government policies, and/or Acts, as a result of which if the CCA is terminated, the CCA shall:

- Provide no less than 6 months' notice to all current licensed/approved/recognised CAs of its intent to cease operations
- Ensure the secure preservation and maintenance of all relevant databases, archives, records and documents with an independent custodian and/or designated government body. The archives will be retained in the manner and for the time indicated in 4.7.
- Provide access to Repository maintained by the CCA, for a maximum period of 12 months following cessation of services
- Revoke all valid certificates at the end of the notice period.
- Ensure availability and access to relevant CRLs for a period of 12 months following cessation of operations.

## 5. Physical, Procedural and Personnel Security Controls

### 5.1. Physical Security Controls

#### 5.1.1. Physical access

Physical access to the CCA for performing operations is controlled and restricted to the authorised individuals only.

##### *5.1.1.1 By-pass or deactivation*

The By-pass or deactivation of normal physical security arrangements are authorised and documented.

##### *5.1.1.2 Trespass detection and alarm system*

Access to the site is controlled through access cards. In addition, a biometric access system is used for access to the server room, of the authorised personnel.

*5.1.1.3 Sensing and preventive measures.*

The site is monitored using appropriate equipment for surveillance based on various sensors.

The security guard of the site takes the suitable escalation procedures.

*5.1.1.4 DVR (Digital Video Recorder) system*

The site is constantly monitored using a CCTV system to detect any unusual activities. Round-the-clock Digital video Recording is also carried out

#### 5.1.2. Power Supply and Air Conditioning

a. Continuous power supply has been ensured by suitable deployment of UPS.
b. The air conditioning system installed equipped with temperature and humidity control.

#### 5.1.3. Fire prevention and protection

Fire alarm system has been installed to handle any emergent situation arising out of fire.

#### 5.1.4. Media storage

Storage media are protected from environment threats such as temperature, humidity and magnetic field.

#### 5.1.5. Waste disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal.

#### 5.1.6. Backup

Routine backups of the system data, audit log data, and other sensitive information are performed and stored in a secure place at the CCA.

### 5.2. Procedural controls

#### 5.2.1. Trusted roles

The following roles have been identified in connection with the operation of the CCA:

a. System Engineer
b. System Administrators
c. Auditor

### 5.3. Personnel Controls

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

The background, qualifications, and experience of the technical personnel are verified as per employment procedures.

#### 5.3.2. Employees Verification/Investigation

CCA has followed appropriate government procedures for appropriate investigation of all personnel

#### 5.3.3. Training Requirements

CCA has provided comprehensive training to all the technical personnel performing duties.

#### 5.3.4. Re-training frequency and requirements

Refresher training of technical personnel is conducted as and when required, and CCA reviews these requirements on a regular basis.

#### 5.3.5. Sanctions for unauthorised actions

In the event of actual or suspected unauthorised actions by a person performing duties with respect to the operations of the CCA, access to site is denied to him/her, with immediate effect. Further actions will be initiated as per ICT Authority administrative procedures.

#### 5.3.6. Contracting personnel requirements

Contractors are allowed access to the Server Room only under the supervision and presence of at least two trusted persons.

#### 5.3.7. Documentation supplied to personnel

Officers/staff operating site have been provided with comprehensive user manuals detailing the procedure of certificate creation, update, renewal, suspension, and revocation, and software functionality.

### 5.4. Compliance with Security Service Regulations

Office of CCA observes and adheres strictly to defined Security procedures which are not shown in the Certification Practice Statement.

## 6. Technical Security Controls

### 6.1. Key Pair Generation and Installation

#### 6.1.1. Key Pair Generation

Key pair for the CCA is generated in a hardware security module (HSM) which is minimum FIPS 140-1 level 3 certified.

#### 6.1.2. Public Key Delivery from CA (applicant) to CCA

CAs' Public keys are delivered to the CCA as a PKCS#10 certificate request. The signature on the PKCS#10 request is verified to confirm that the CA is in possession of the private key associated with each public key delivered. A certificate is then signed by the CCA and issued to the CA in the format as specified in 7.1.

#### 6.1.3. Root CA Public Key Delivery to Users

The self-signed Certificate of the CCA is available to End-Users for Certificate validation purposes. The certificate hash (thumbprint) and the Root CA certificate are available on the web site of each licensed/approved/recognised CAs as well as CCA's Web site (www.cca.mu). Relying parties must confirm the validity of their copy of the CCA certificate using this thumbprint. The CCA's self-signed certificate, along with this CPS and other documentation such as the acts, regulations, and directives are available on CCA's website.

This certificate shall also be made available by each CA on its website to enable verification by relying parties.

#### 6.1.4. Key Sizes

The modulus of the CCA Root CA and the keys of CCA as well as the hash algorithm used by the CCA for signing are as per the CCA Directive 1 - Standards for Certification Authorities.

#### 6.1.5. Key Usage Purposes

The key of the CCA will be used for:

- The issuance of certificates to the Certification Authorities that have been licensed/approved/recognised
- Issuance of Certificate Revocation Lists

### 6.2. Private Key Protection

#### 6.2.1. Standards for Cryptographic Module

The cryptographic module used by the CCA is certified to FIPS 140-1 level 3.

#### 6.2.2. Private Key (n out of m) Multi-person Control

Use of the private key for signing will require multi-person (minimum two) authorisations

#### 6.2.3. Private Key Backup

The Private Key of the CCA is backed up multi person control and kept in a secure manner.

#### 6.2.4. Method of Destroying Private Key

Private signature keys will be deleted or zeroised when they are no longer needed, or when the certificates to which they correspond expire or are revoked. Prior to disposal, the Hardware cryptographic modules will be physically destroyed.

### 6.3. Other Aspects of Key Pair Management

#### 6.3.1. Public Key Archival

All public keys of the CCA will be archived.

### 6.4. Computer Security Controls

#### 6.4.1. Specific Computer Security Technical Requirements

CCA has established and documented all computer security technical controls implemented for the Root CA.

### 6.5. Life Cycle Technical Controls

#### 6.5.1. Security management controls

Security management controls are enforced by rigid separation of operator roles.

- System Engineer
- System Administrator

### 6.6. Network Security Controls

The CCA's Root is maintained and operated off-line and is not networked with any external components.

### 6.7. Cryptographic Module Engineering Controls

The cryptographic module used by the CCA is certified to FIPS 140-1 level 3.

## 7. Certificate, Certificate Suspension and Revocation List Profile

### 7.1. Certificate Profile

CCA issues certificates in conformance with the CCA Directive 1 - Standards for Certification Authorities

### 7.2. CRL Profile / Certificate Suspension and Revocation List Profile

The CCA issues CRLs in conformance with the CCA Directive 1 - Standards for Certification Authorities

# 8. Specification Administration

## 8.1. Specification change procedures

CCA will periodically review the CPS in light of policy and/or infrastructure technology change. The CPS will be revised if required.

The revision-related record of the Certification Practice Statement will be maintained.

## 8.2. Publication and notification policies

The revised Certification Practice Statement will be made available by the CCA to the user community through publication on CCA's website.

CCA also notifies the CAs about the revised Certification Practice Statement. The revised Certification Practice Statement is in force from the date and time of publication on CCA's website.

## 8.3. CPS approval procedures

### 8.3.1. Items that can change without notification

Editorial, typographical corrections or changes to the contact details shall be made to this Certification Practice Statement without notification.

### 8.3.2. Changes with notification

The CCA shall give a minimum of 45 days notice to the certificate holders of any substantial changes made to the certification practice statement.

Changes to items, which in the judgment of the CCA will not materially impact a substantial majority of certificate holders may be changed on a minimum 30 days notice. While changes required by law, or those in the judgment of the CCA required to be implemented for the benefit of certificate holders may be made with a reasonable notice period. Notice of all changes made under section 8.3.2 of this certification practice statement will be published on the website of the CCA at http://www.cca.mu