# MauSign CA

# Certification Practice Statement

**Version**: Release 1.3

**Date: 17 November, 2021**

| | |
|---|---|
| **Document Title** | Certification Practice Statement |
| **Document Type** | Policy |
| **Author** | MauSign Certification Authority |
| **Version No** | 1.3 |
| **OID** | |
| **Issue Date** | November 2021 |

**CPS Revision Control**

| Date | Issue No | Details of Changes |
|---|---|---|
| 4-Mar-21 | 1.0 | 1st Document |
| 28-Apr-21 | 1.1 | Updates based on the Document on the OCSP, CRL, Installation of Root CA & CA Manually, and Renewal of CA |
| 8-Aug-21 | 1.2 | Updating effective date of CPS and pricing for certificates and OIDs |
| 17-Nov-21 | 1.3 | Update with respect to downloading the CCA and CA certificates and certificate installation |

# TABLE OF CONTENTS

**1**

# Certification Practice Statement

## 1 OVERVIEW

### 1.1 Definitions and Abbreviations

#### 1.1.1 Definitions

The following definitions shall be used in the CPS:

**Access Control:** Process of granting access to information system resources only to authorized users, programs, processes, or other systems.

**Applicant:** The subscriber is called an "applicant" after applying to a Certificate Authority for a certificate, but before the certificate issuance procedure is completed.

**Audit:** Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

**Backup:** Copy of files and programs made to facilitate recovery if necessary.

**Certificate:** A digital representation of information which at least (1) identifies the Certificate Authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it

**Certificate Authority (CA):** An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.

**CA Facility:** The collection of equipment, personnel, procedures and structures that are used by a Certificate Authority to perform certificate issuance and revocation.

**Certificate Authority Software/solution:** Key management and cryptographic software used to manage certificates issued to subscribers.

**Certification Practice Statement (CPS):** A statement of the practices that a CA employs in issuing, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CPS, or requirements specified in a contract for services)

**Certificate Revocation List:** A list maintained by a Certificate Authority of the certificates that it has issued that are revoked prior to their stated expiration date.

**Compromise:** Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

**Hardware Security Module:** The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module.

**Digital Signature:** The result of a transformation of a message by means of a cryptographic system using keys such that a relying party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made

**e-Sign** means the service offered to Organisations to generate digital signatures for citizens who are holders of MauPass 2FA

**MauPass** means the National Authentication Framework which supports Two-Factor Authentication (2FA) and can also be used to generate one-time digital certificate by MauSign CA

**Object Identifier (OID)**: A specialized formatted number that is registered with an internationally recognized standards organization, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class.

**Public Key:** The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is normally made publicly available in the form of a digital certificate.

**Public Key Infrastructure (PKI):** A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public/private key pairs, including the ability to issue, maintain, and revoke public key certificates.

**Registration Authority (RA):** An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a registration authority is delegated certain tasks on behalf of an authorized CA)

### 1.1.2 Abbreviations

The following abbreviations shall be used in the CPS:

| **Abbreviation** | **Description** |
|---|---|
| CA | Certification Authority |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| DN | Distinguished Name |
| LDAP | Lightweight Directory Access Protocol |
| OCSP | Online Certificate Status Protocol |

| | |
|---|---|
| OID | Object Identifier |
| PKI | Public Key Infrastructure |
| RA | Registration Authority |
| RSA | Rivest-Shamir-Adleman (encryption algorithm) |
| SHA | Secure Hash Algorithm |
| URL | Uniform Resource Locator |

## 1.2 Introduction and Objectives

### 1.2.1 Background and Purpose of Certification Practice Statement (CPS)

This Certification Practice Statement (CPS) describes the practices of MauSign CA as a provider of digital certificates and eSign service under the National Public Key Infrastructure (PKI) to enable a secure and safe online environment for digital transactions.

MauSign digital certificates and eSign service will guarantee confidentiality, integrity, authentication and non-repudiation in electronic transaction and communication.

Besides the practices employed in issuing certificates and providing eSign services, the CPS also describes the digital certificate lifecycle including issuance, certificate management, revocation, and renewal.

### 1.2.2 Controller of Certification Authority

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

### 1.2.3 Registration Authority, SUBSCRIBERS and RELYING PARTIES

MauSign CA may delegate to Registration Authorities (RAs) duties including identity verification of subscribers applying for products and services from the MauSign CA.

### 1.2.4 NCB

The National Computer Board (NCB) was set up in 1988 by the National Computer Board Act (Act No.43) to promote the development of Information and Communication Technologies (ICT) in Mauritius. It is a para-statal body administered by a Board of Director and operates under the aegis of the Ministry of Information Technology, Communication and Innovation.

The NCB is licensed to operate the MauSign CA providing digital certificate products and eSign services

The contact information for MauSign CA is as follows:

- Address: 5th floor, Wing B, Atal Bihari Vajpayee Tower, Ebene Cyber City

- Internet URL: https://mausign.govmu.org

- Email: support@mausign.govmu.org

- Telephone: (230) 454 9955

### 1.2.5 Digital Certificate and Validity

#### 1.2.5.1 Digital Certificate

MauSign Certification Authority (MauSign CA) shall issue digital certificates after verifying the subscriber's identity matches the subscriber information submitted to the registration authority at the time of application. The digital certificates shall be digitally signed by MauSign CA.

#### 1.2.5.2 Validity

Certificate issued by NCB shall remain valid except for cases of revocation, where the validity of such certificate shall be revoked.

### 1.2.6 Scope of Use and Restrictions

By using the certificate, a subscriber agrees to use the certificate for its lawful and intended use only.

Relying parties are required to seek further independent assurances deemed reasonable and at a minimum must assess:

1) The appropriateness of the use of the certificate for any given purpose and that the use is not prohibited by this CPS.

2) The certificate is being used in accordance with its key-usage field extensions.

3) The certificate is valid at the time of reliance by performing Online Certificate Status Protocol (OCSP) or Certificate Revocation List (CRL) checks.

All certificates issued under this policy cannot be used for purposes other than what is allowed in section 2.1 and what is stipulated in the laws of the Republic of Mauritius.

## 1.3 Name of Document

The Document shall be referred to as "MauSign CA Certification Practice Statement."

## 1.4 Parties Engaged in the Certification Practice

For the effective issuance, use, and management of digital signature certificates, parties engaged in the certification practice shall cooperate based on the principles of trust and good faith.

### 1.4.1 ICT Authority

The ICTA is the Controller of Certification Authority (CCA) and is the primary trust point for the entire National Public Key Infrastructure (PKI).

The CCA is also responsible to ensure that Certificate Authorities comply with the obligations imposed on them by law.

The Electronic Transaction Act 2000 (ETA), as amended, and its regulations, provides the necessary legal framework necessary for the proper deployment of PKI in Mauritius. This legal framework, in turn, sets the stage for a secure and pro business environment for electronic commerce in Mauritius.

### 1.4.2 MauSign CA

As a Certificate Authority, MauSign CA has the following duties:

- Operate and manage the CA system and its functions in accordance to CA policies and all applicable regulations;
- Issue and manage certificates to individual or legal entities;
- Register Application Service Providers for eSign service;
- Provide eSign service to Application Service Providers;
- Publish issued certificates and revocation information;
- Handle revocation request regarding certificates issued
- Notification of issuance, revocation, or renewal of its certificates.

### 1.4.3 Registration Authority

A registration authority shall perform several duties including processing certificate applications and verification of the identities of applicants for purposes of certificate issuance, renewal, reissuance, or revocation or ASP registration.

The Mauritius Post Limited (MPL) will be acting as the Registration Authority.

### 1.4.4 Subscriber

A subscriber is an individual or legal entity whose name appears as the subject name field in a certificate or in the case of a server certificate, the entity applying for the certificate. The subscriber

asserts that he or she uses the keys and certificate in accordance with the certificate policy, and is responsible for the following:

- Providing accurate information when submitting a certificate application;
- Protecting the subscriber's private key;
- Protecting the subscriber ASP credentials
- Using the private key and certificate in key usage and MauSign policies; and
- Notifying MauSign CA in case the subscriber's private key is compromised or in case of compromise.

### 1.4.5 Relying party

A relying party is the entity that relies on the validity of the binding of the subscriber's name to a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. A relying party may use the information in the certificate to determine the suitability of the certificate for a particular use, through the following:

- Checking the purpose for which a certificate is used;
- Performing digital signature verification;
- Checking revocation status.

### 1.4.6 Obligations of MauSign

#### 1.4.6.1 Provision of Accurate Information

Through its directory system or the MauSign CA Portal (https://mausign.govmu.org), MauSign CA shall announce to subscribers and relying parties the following information for certificate verification purposes:

- Designation of certification authority
- Suspension, or revocation of certification services
- Cancellation of the designation of certification authority
- Certification Practice Statement
- Information on certificates such as Subscriber certificates, List of suspended or revoked subscriber certificates
- Other information related to the certification service

#### 1.4.6.2 Protection of MauSign digital certificates

MauSign CA shall keep its own digital certificates including digital signature creation data secure by utilizing reliable software or hardware and manage them appropriately to prevent loss, damage, theft, or leakage.

#### 1.4.6.3 Restriction on the Use of Digital Signature Creation Data

When issuing subscriber certificates, MauSign CA shall only use Digital Signature Creation Data matching the verification information signed by the CCA.

#### 1.4.6.4 Security of Digital Signature Creation Data

MauSign CA shall notify subscribers of any event that may affect the reliability or validity of certificates including loss, damage, theft, or leakage of Digital Signature Creation Data and may revoke the subscriber certificates issued using the relevant Digital Signature Creation Data as necessary.

MauSign CA shall immediately post the corresponding notice on the MauSign CA Portal (https:// mausign.govmu.org) and update the Certificate Revocation Lists. Likewise, MauSign CA shall also allow relying parties to use the updated Certificate Revocation Lists and act appropriately to secure the reliability and validity of its certification service.

#### 1.4.6.5 Management of Registration authority

The MauSign CA shall ensure that the Registration Authorities shall comply with all registration procedures and safeguards as may be determined from time to time by MauSign and as set out in the CPS. The RA shall comply with all the registration procedures as laid down in the amended and latest version of the CPS which can be downloaded from the website (mausign.govmu.org) whenever a new version of the CPSis adopted.

#### 1.4.6.6 Verifying the Identity

MauSign CA may verify the actual identity of a subscriber and collect related subscribers documents for that purpose.

### 1.4.7 Obligations and Responsibilities of Registration Authorities

#### 1.4.7.1 Processing of Applications

Registration Authorities shall accept application for digital certificates including certificate issuance, re-issuance, renewal or revocation and application for registration as Application Service Providers in accordance with the procedures enumerated in the CPS and CCA guidelines

#### 1.4.7.2 Verifying the Identity

The Registration Authority shall process and handle the application for digital certificates or application to be registered as Application Service Provider with paramount care and diligence to ensure that the only genuine applicants are provided digital certificates and are registered as Application Service Providers.

A registration authority may demand the submission of relevant documents to check the identity of a subscriber as part of the Know Your Customer (KYC) process.

The identity verification process will depend in type of certificates and will be specific for ASP applicants.

#### 1.4.7.3 Responsibilities

In case a Registration Authority fails to comply to the policies and thus incurs material hindrances to the certification services, MauSign CA may impose proper sanctions to the relevant registration authority.

Where the registration authority has caused damages to subscribers or relying parties due to failure to verify the identity of subscriber of certificate, it shall be liable to such penalty as may be imposed at the sole discretion of MauSign.

### 1.4.8 Subscribers' Obligations

#### 1.4.8.1 Provision of Accurate Information

Subscribers shall provide accurate information to the registration authority and MauSign CA for the following:

- Application for certificate issuance
- Application for certificate re-issuance
- Application for certificate renewal
- Application for certificate revocation
- Application for Application Service Provider
- Updating of subscriber information

#### 1.4.8.2 Rational Use of Certificates

Subscribers shall use certificates fin strict compliance to the laws of Mauritius.

#### 1.4.8.3 Safekeeping of Certificates

Subscribers shall manage certificates using reliable software or hardware and shall keep and manage them securely to prevent loss, damage, theft, or leakage. Subscribers shall either keep or manage certificates safely or completely delete all certificates if they do not wish to keep them.

Subscribers shall assume full responsibility for all damages arising from failure to protect the private key associated with their digital certificates.

#### 1.4.8.4 Safekeeping of ASP Credentials

Subscribers shall manage the credentials associated with their ASP accounts using reliable software or hardware and shall keep and manage them securely to prevent loss, damage, theft, or leakage.

Subscribers shall assume full responsibility for all damages arising from failure to protect the credentials associated with their ASP accounts.

#### 1.4.8.5 Security Measures for Certificates and ASP credentials

To enable MauSign CA to revoke the relevant certificates or ASP credentials, subscribers shall immediately notify MauSign CA or the registration authority in case the certificate or ASP credential is lost, damaged, stolen, or leaked or otherwise believed to be unsecure.

#### 1.4.8.6 Guarantee of MauSign CA's Exemption from Liability

Subscribers shall agree to free MauSign CA from any liability as well as all responsibilities and obligation to reimburse any expenses for a period of 10 years after the expiration (including revocation) of the relevant certificates or ASP credentials in the event of the following:

- Incorrect information provided by subscribers
- Alteration to information that have been provided by subscribers
- Careless management of Certificates or ASP credentials (exposure, loss, or alteration of certificates or ASP credentials)

#### 1.4.8.7 Liability for Compensation

Subscribers shall indemnify MauSign CA or relying parties for any damage arising from the improper use of certificates or ASP credentials intentionally or otherwise.

### 1.4.9 Relying Parties' Obligations

#### 1.4.9.1 Understanding the Purpose of Certificates and eSign service

Relying Parties' shall explain the purpose and scope (including limitations) of the use of the certificates issued by MauSign CA and eSign service to subscribers and shall assume full responsibility for any damage due to their own fault.

#### 1.4.9.2 Validation of Certificates

Relying parties shall use the information contained in a digital certificate to:

- To verify the validity of certificates
- To verify the revocation of certificates
- To verify restrictions on the application scope or uses of certificates

#### 1.4.9.3 Liability for Compensation

Relying parties shall indemnify MauSign CA or subscribers for any damage arising from the improper use of certificates intentionally or otherwise.

### 1.4.10 Management of Certification Practice Statement (CPS)

#### 1.4.10.1 Contact Information

The contact information of the National Computer Board are as follows:

- Address: 5th floor, Wing B, Atal Bihari Vajpayee Tower, Ebene Cyber City
- Internet URL: https://mausign.govmu.org
- - Email: support@mausign.govmu.org
- - Telephone: (230) 454 9955

#### 1.4.10.2 Amendment of Certification Practice Statement

MauSign CA shall establish or amend its Certification Practice Statement as instructed by the ICT Authority or as deemed necessary by the Chief Executive Officer of NCB to improve its services.

Only the Chief Executive Officer of NCB may establish or amend the CPS. Whenever this CPS is amended, NCB shall maintain records containing the following:

- CPS versions
- Application scope and outline
- Records related to the establishment and amendment of CPS
- Existing provisions of CPS prior to its amendment
- Particulars of amendment
- Reasons for amendment

#### 1.4.10.3 Reporting and Application of Certification Practice Statement

NCB shall submit CPS or amended CPS to the Controller of Certification Authorities of Mauritius (CCA) 15 days before its application.

#### 1.4.10.4 Publication of Certification Practice Statement

NCB shall immediately publish the amended CPS as listed in the following URL of Information.

- URL of Certification Practice Statement: https://mausign.govmu.org/terms/cpAndCPS.sg

### 1.4.11 Consent of Subscribers

Unless subscribers raise their objections in writing (or through electronic documents digitally signed using Digital Signature Creation Data) within 30 days (including the date of publication) of the day the amended CPS is published, NCB shall assume that they have agreed to the amended CPS.

## 2 APPLICATION FEES AND PURPOSE

### 2.1 Fees for digital certificates and purpose

| Certificate Type | Object Identifier (OID) | Purpose and Price |
|---|---|---|
| Corporate | 2.16.480.100.3.1.3<br>2.16.480.100.3.1.4 | - Digital Signature<br>- 1 year validity period / RSA 2,048 bit – Rs1000<br>- 2 years validity period / RSA 2,048 bit – Rs1800 |
| Citizen | 2.16.480.100.3.1.1<br>2.16.480.100.3.1.2 | - Digital Signature<br>- 1 year validity period/RSA 2,048 bit – Rs500<br>- 2 years validity period/RSA 2,048 bit – Rs900 |
| Server | 2.16.480.100.3.1.5<br>2.16.480.100.3.1.6 | - Digital Signature<br>- 1 year validity period / RSA 2,048 bit – Rs1000<br>- 2 years validity period / RSA 2,048 bit – Rs1800 |

### 2.2 ASP fees

| Type | Object Identifier (OID) | Purpose and price |
|---|---|---|
| E-sign | 2.16.480.100.3.1.8 | - To provide eSign service<br>- 1 year validity period / RSA 2,048 bit -Rs10000 |

### 2.3 Fees for digital certificate issuance, renewal and reissue

MauSign CA shall impose fees for certificate issuance, renewal and reissue by way of regulations.

MauSign CA shall impose fees for application to become an Application Service Provider.

#### 2.3.1 Fees for access to digital certificates

MauSign shall not impose fees on users who inspect and verify certificates.

#### 2.3.2 Fees for Verification of Validity of Certificate

NCB shall not impose fees on users who intend to verify the validity of Certificate.

# 3 OPERATIONS

## 3.1 Registration of application for digital certificates

### 3.1.1 Application for digital certificate

An individual applicant or authorized representative of an organization who reside within Mauritius may apply for a digital certificate. An application for a digital certificate shall be made through a Registration Authority and shall fulfill the application requirements as mentioned in the CPS.

### 3.1.2 Application to become an Application Service Provider

An authorized representative of an organization who reside within Mauritius may apply for an Organisation to be registered as an Application Service Provider so that they can offer digital signing services to citizens of Mauritius using the eSign service.

### 3.1.3 Procedure for Issuance

- The applicant shall submit the application online through the MauSign CA Portal and upload requested documents
- The applicant shall visit the Registration Authority in person and undergo the identity verification process
- An online identity verification process shall be provided for those outside Mauritius or those citizens who cannot have the face to face identity verification
- The applicant undergoing identity verification should have their original identity document together with other documents which may be required
- The applicant shall download the digital certificate issued by MauSign CA.

### 3.1.4 Restrictions on Issuance

MauSign CA and the Registration Authority may not procced with an application for digital certificate or an ASP application for the following reasons:

- Application made or suspected to have been made illegally using a fake identity
- Entering or suspected to have entered false information in application or attaching a fake
- document
- Failing to effect payment in respect of application
- Failing to complete identity verification.

## 3.2 Identity Verification and Validation

### 3.2.1 Verification of Identity

The Registration Authority shall verify the identity of the applicant. The Registration Authority verifies the identity by verifying the application, the documents submitted and performing the face-to-face verification with the applicant

### 3.2.2 Issuance through Face-to-Face Identity Verification

When the Registration Authority verifies the identity of the individual applicant, it verifies:

- the civil data including the National Identity Number, names with the original identity documents.

- The photograph of the applicant against the facial of the live applicant

For an individual applicant, the documents requested are as follows:

- Applicant National Identity Card (original)

- Soft copy of photograph

Where an organization files an application for a corporate certificate through a representative, the requested documents are as follows:

- Applicant's National Identity Card (original)

- Business Registration Certificates

- Copies of Identity Card and Passport of authorized signatory (if the applicant is not the Managing Director of the company)

- A notarized Board resolution appointing the MD, if the authorized signatory is not the owner of the company

- A signed and notarized power of attorney authorizing the applicant to apply for the certificate

Where an application for server certificate is made, the documents required for identity verification purposes shall be as follows:

- Applicant's National Identity Card (original)

- Business Registration Certificates

- Copies of Identity Card and Passport of authorized signatory (if the applicant is not the Managing Director of the company)

- A notarized Board resolution appointing the MD, if the authorized signatory is not the owner of the company

- A signed and notarized power of attorney authorizing the applicant to apply for the certificate

### 3.2.3 Application for Certificate Issuance

#### 3.2.3.1 Application for Certificate Issuance by applicant

The applicant shall connect to the MauSign CA Portal within 7 days (including the date of application) of certificate application to create digital signature data using subscriber information including the authentication code and reference number received following approval of certificate application.

The certificate application shall then be digitally signed using the Digital Signature Creation Data to verify whether the digital signature verification data included in the certificate application matches the Digital Signature Creation Data owned by the subscription applicant. To prevent the exposure of the authentication code and the reference number and to guarantee the validity of verifying the identity, an application for certificate issuance shall be submitted within 7 days (including the date of request) of registering the application. After 7 days, however, an applicant must register the certificate application again.

#### 3.2.3.2 Certificate Issuance by MauSign CA

Upon receiving a certificate application, MauSign CA shall check the following items prior to issuing a certificate and then confirm the digital signature key exclusively belonging to the subscription applicant:

- Whether the applicant has entered forged or altered information through the use of authentication code, reference number, and application details

- Uniqueness of the digital signature verification data submitted by the applicant

- Whether the applicant holds the Digital Signature Creation Data matching the digital signature verification data he/she submitted

- Accuracy of the information to be registered in the certificate

After verifying the information contained in the certificate application, MauSign CA shall issue and transmit a certificate containing the following items to the rightful applicant, and MauSign CA shall also make the corresponding announcement through its directory system.

- Subscriber's name

- Subscriber's digital signature verification data

- Method of digital signature used by the subscriber and MauSign CA

- Serial number of the certificate

- Validity of the certificate
- Name of MauSign CA as a certificate issuer
- Scope of use of the certificate and restrictions, if any

Certificates issued by MauSign CA may be classified with one another by DN. DN shall include the real name and ID of subscribers. Subscriber IDs shall be exclusively given according to the registration authority, subscribers, and the usages of certificates under the practice statement of the registration authority.

Using the name registered by the applicant in registering a certificate application, MauSign CA shall set the names to be used in the basic domains within certificates, CRL. The composition method of such names shall follow international standards.

#### 3.2.3.3 Applicant's Acceptance of Certificates

Upon receiving the certificate issued by MauSign CA, the applicant shall select a location to store, and safely save and preserve the certificate and his/her Digital Signature Creation Data.

#### 3.2.3.4 Applicant's Acceptance of ASP credentials

Upon receiving the ASP credentials issued by MauSign CA, the applicant shall select a location to store, and safely save and preserve the credentials.

#### 3.2.3.5 Sending Subscriber Information

All subscriber information between MauSign CA and a Registration Authority shall be sent through a secure communication link. All subscriber information sent between MauSign CA and a Registration Authority through the communication network shall be checked for forgery and/or alteration in verifying the digital signature of the subscriber and shall be safely sent by encoding, and thus the confidentiality and integrity of subscriber information shall be guaranteed.

## 3.3 Certificate Renewal and ASP renewal

### 3.3.1 Certificate Renewal and ASP renewal

Certificate renewal pertains to the case wherein a new certificate of the same type but with updated digital signature data and extended term of validity is issued during the period beginning 1 month before the expiration of a certificate to the day the validity of the certificate expires. The renewed certificate shall assume the term of validity of the existing certificate and remain effective from the day the existing certificate expires to the duration of the term of validity.

### 3.3.2 Procedure for Certificate Renewal

#### 3.3.2.1 Subscriber's Application for Certificate Renewal and Verification of Identity

The subscriber shall forward the details of application of renewal of the certificate by accessing the MauSign CA Portal. The details of renewal of the certificate shall include as follows:

- Newly created digital signature verification data

- Digitally signed data with newly created digital signature creation data

- Data digitally signing the above content with existing created digital signature creation data

- Existing certificate data

Since a subscriber may apply for certificate renewal only when his/her existing digital signature is valid, MauSign CA shall identify the subscriber based on the digital signature shown in the application for certificate renewal. In case the existing registration information of the subscriber is changed at the time of applying for certificate renewal, MauSign CA or the registration authority concerned may request the subscriber to submit documents related to the change(s).

#### 3.3.2.2 MauSign CA's Issuance of Certificate Renewal

Prior to renewal of certificates, upon receiving a certificate renewal application, MauSign CA shall check the following items contained in the details of the certificate renewal application, and then confirm the digital signature key exclusively belonging to the subscriber:

- To verify the uniqueness of the digital signature verification data submitted by the subscriber

- To verify whether the subscriber holds the Digital Signature Creation Data matching the digital

- signature verification information he/she has submitted,

- To verify the identity of the subscriber by checking the digital signature created with the existing

- Digital Signature Creation Data

After verifying the information contained in the details of certificate renewal application, MauSign CA shall renew the certificate where it finds that the subscriber is the rightful one. MauSign CA shall transmit the renewed certificate to the subscriber and make the corresponding announcement through its directory system.

#### 3.3.2.3 Subscribers' Acceptance of Certificates

With respect to procedures through which a subscriber accepts a newly issued certificate, the procedure of Section 3.2.2.3 Subscription Applicant's Acceptance of Certificates shall apply.

#### 3.3.2.4 Sending Subscriber Information

With respect to methods to send subscriber information, Section 3.2.2.4 Sending Subscriber Information shall apply.

## 3.4 Certificate Reissuance

### 3.4.1 Certificate Reissuance

Certificate reissuance pertains to the case wherein the subscriber requests for reissuing his/her certificate when the subscriber has revoked or lost his/her certificate or is worried over the exposure of or damage to Digital Signature Creation Data. The reissued certificate is valid from the date of reissuance until the expiration date of the original certificate.

### 3.4.2 Procedure for Certificate Reissuance

With respect to reissuance of certificates, Section 3.2.1 Verification of Identity and Section 3.2.2 Procedure of New Issuance shall apply.

## 3.5 Updating of Subscriber Information

### 3.5.1 Updating Requirements of Subscriber Registration Information

Updating of subscriber registration information refers to the case wherein MauSign CA changes the registered information as requested by a subscriber in case the subscriber registration information (email address, address, telephone numbers, etc.) other than those reflected in the certificate is changed.

### 3.5.2 Application for Updating Subscriber Information and Verification of Identity

MauSign CA may be requested to update subscriber information

In particular, MauSign CA shall confirm the subscriber's identity using the digital signature shown in the application for updating subscriber information. With respect to methods to send subscriber information, Section 3.2.2.4 Sending Subscriber Information shall apply.

## 3.6 Revocation of Certificate

Certificate revocation refers to the case wherein the validity of a certificate is compulsorily terminated during the term of validity at the request of the subscriber or as deemed necessary by MauSign CA to maintain safety, security, and reliability in carrying out certification practice.

### 3.6.1 Reasons for Certificate Revocation

MauSign CA shall revoke a certificate for any of the following reasons pursuant to Section 1.3.7 (Obligations of MauSign CA) of this CPS:

- An application for certificate revocation has been filed by the subscriber.
- In case of death of subscriber, dissolution, etc.
- If the certificate is issued to the minor without consent of his/her legal representative
- If the certificate is expired

- If subscriber received or is suspected to have received the certificate by unfair means

- If the digital signature creation information of subscriber is lost, damaged or stolen or leaked

- If it is necessary to maintain and improve the security of MauSign CA service.

- The subscriber failed to observe his/her major obligations or other matters stipulated in this CPS.

### 3.6.2 Application for Certificate Revocation and Verification of Identity

The procedure for applying for certificate revocation and verifying the identity is the same as that in Section 3.2.1 (Identity Verification).

#### 3.6.2.1 Measures for Application for Certificate Revocation

The application for certificate revocation or suspension shall be made to MauSign CA through the Registration Authority, and verification of the identity shall be applied to Section 3.2.1 (Identity Verification). When the application for certificate revocation has been filed, then MauSign CA shall immediately take the required measures.

#### 3.6.2.2 Measures for Receipt of Report of Loss

When MauSign CA has received the report of loss, MauSign CA shall verify the subscriber identity. If the reporter of the loss is the subscriber of MauSign CA, MauSign CA shall, without delay, verify the subscriber identity; immediately perform revocation at the request of subscriber. Time of receipt of report of loss through MauSign CA shall be the one that is filed in the MauSign CA system.

### 3.6.3 Updating and Announcement of Certificate Revocation Lists (CRL)

MauSign CA shall update the Certificate Revocation Lists periodically to a maximum of 24 hours after reflecting the results of revoking subscribers' certificates and immediately publish the updated lists on the MauSign CA Portal (https://mausign.govmu.org) or on its directory system. The CA shall support the generation and publishing of a CRL. The CA shall include the Uniform Resource Identifier (URI) of the published CRL to the CRL Distribution Point extension in CA issued certificates.

### 3.6.4 Notice of Compulsory Certificate Revocation

MauSign CA shall notify the subscriber through email or by telephone in case of revocation of his/her certificate without his/her consent for reasons stipulated in Section 3.6.2 (Reasons for Certificate Revocation).

## 3.7 Online Certificate Status Protocol (OCSP) Service

Online Certificate Status Protocol (OCSP) service refers to one whereby if a subscriber presents his/her certificate by connecting with a relying party, the relying party transmits the serial number of the certificate to MauSign's OCSP system. MauSign CA verifies the validity of the certificate and send the verification results to the user. With this service, a relying party may verify the validity of the MauSign CA certificates. OCSP stapling with a caching time of 30 minutes is being applied.

## 3.8 Renewal of Digital Signature Key of Certification Authority

Once a digital signature key of MauSign CA is renewed, MauSign CA shall disclose the renewed certificate on its directory system and thus distribute it to the relying party. In issuing, renewing, or reissuing a certificate of a subscriber, MauSign CA shall make it possible for the subscriber to download the certificate of MauSign CA and thus distribute it to the subscriber.

## 3.9 Suspension and Revocation of Certification Services

### 3.9.1 Suspension of Certification Services

When MauSign CA intends to suspend certification services because of unavoidable circumstances other than natural disasters or acts of god, it shall set a period of suspension, notify subscribers thereof within thirty (30) days before the expected date of suspension, and report the suspension to the ICT Authority.

A period of suspension shall not exceed six (6) months.

### 3.9.2 Revocation of Certification Services

When MauSign CA intends to revoke certification services because of unavoidable circumstances other than natural disasters or god of acts, it shall notify subscribers thereof within sixty (60) days before the expected date of revocation, and report the revocation to the ICT Authority.

In this case, MauSign CA shall transfer to other certification authorities the certificate of the subscriber and records on the suspension and revocation (hereinafter referred to as "Subscriber Certificates"). However, where unavoidable circumstances make it impossible to transfer subscriber certificates, MauSign CA shall without delay notify the ICT Authority thereof.

### 3.9.3 How to Delete and Destroy Digital Signature Creation Keys

If MauSign CA's certificate expires, or if its electronic signature creation keys are damaged and/or leaked, MauSign CA shall delete the electronic signature creation keys in accordance with the standards procedure.

### 3.10 Downloading and installing the CCA certificate and CA certificate

The Root certificate of CCA Mauritius and the Mausign CA certificate can be downloaded at the following location:https://mausign.govmu.org/about/rootCAandCA.sg . The instructions for installing the CCA certificate and CA certificates as well as end user certificates can be found at the following location: https://mausign.govmu.org/resourceroom/aplyDownload/list.sg

# 4 PUBLICATION

## 4.1 Repositories

MauSign CA is responsible for the publication of this CPS which is publicly accessible on the MauSign CA portal.

MauSignCA shall post its CRL in a directory that is publicly accessible through the Lightweight Directory Access Protocol (LDAP). To promote consistent access to certificates and CRLs, the repository shall implement access controls and communication mechanisms to prevent unauthorized modification or deletion of information.

## 4.2 Publication of certification information

### 4.2.1 Publication Location of Major Information

The following is the publication location of information related to the certification service such as the revocation list of the certificates.

- Publication Location: ldap://ldap.govmu.org:389/
- Effectiveness Status Information of Certificate: http:// ocsp.govmu.org:9020

### 4.2.2 Frequency of Publication

Information on certificate issuance and management shall be promptly published after each processing. The CRL shall be updated and published periodically to a maximum of 24 hours. Note, however, that the period may be changed, in which case MauSign CA shall publicly announce the change on the MauSign CA Portal (https://mausign.govmu.org). In case damages have incurred to the subscriber or user from omission of publication of certificate revocation, MauSign CA shall be liable for such damages.

# 5 PHYSICAL, PROCEDUAL AND PERSONAL CONTROL RELATED TO SECURITY

## 5.1 Physical Protective Measures

### 5.1.1 Control of Physical Access

NCB shall safeguard the site of the core certification systems from physical risks such as intrusion by outsiders, illegal access, or fires as follows:

- NCB shall install and operate the core certification systems in a secured and controlled area.

- The access control system of MauSign CA shall control access to the controlled area using a combination of identification cards, fingerprinting system.

- NCB shall install the core certification systems in a secure cabinet to control physical access.

- In case of a need for an outsider to gain access to the core certification system to repair

- hardware, NCB shall ask a manager in charge to accompany the outsider.

- NCB shall maintain and review regularly the record of entry to the controlled area in connection

- with the access control system.

- NCB shall install the following monitoring systems in order to activate alarm systems and

- communicate with adjacent facilities in case of an abnormal situation through wired and wireless

- reporting functions:

    - CCTV camera and other monitoring systems

- - NCB shall ensure that the person in charge of maintenance accompanies any outsider when the certification operation system rooms, etc., is accessed by the outsider for some maintenance works such as the repair of hardware.

### 5.1.2 Prevention of Flood Damage

NCB shall install the certification systems at least 30cm above the floor in order to safely protect the certification systems from flood, and shall use a water leakage alarm in order to detect and promptly cope with water leakages.

### 5.1.4 Prevention of Fire Damage

NCB shall install fire detectors, portable fire extinguishers, and automatic fire extinguishing facilities in order to prevent the fires in the certification system operation rooms.

### 5.1.5 Power Source

NCB shall use UPS in order to prevent serious system damages due to unexpected power failures and shall securely provide power sources by installing separate independent power generators.

### 5.1.6 Protection

The outer walls of certification system operation rooms shall be designed to protect the certification systems from external invasions as required to provide certification services.

- The materials of outer walls shall be erected with bricks or ferroconcrete, or shall be welded to steel-frame structures with iron plates of more than 3T
- Outer walls shall be perfectly finished from the floors to the ceilings
- The inner walls of the certification systems shall be designed as separated from the operation room

### 5.1.7 Constant Temperature and Humidity, Ventilation

Proper quantities of devices for constant temperature and humidity shall be installed and managed at certification system operation rooms,

### 5.1.8 Storage of Media

NCB shall store major media in a fireproof vault installed in a controlled area to control physical access.

### 5.1.9 Waste Disposal

Sensitive media and documentation that are no longer needed for operations shall be destroyed in a secure manner. For example, sensitive paper documentation shall be shredded, burned or otherwise rendered unrecoverable.

### 5.1.10 Offsite back ups

NCB shall perform weekly system backups sufficient to recover from system failure and shall store the backups, including at least one full backup copy, at an offsite location that has procedural and physical controls that are commensurate with its operational location.

## 5.2 Procedural Protective Measures

### 5.2.1 Division of Certification Services

MauSign CA shall manage certification service personnel, by classifying them according to their roles, thus ensuring the safety and reliability of its certification services, and such personnel shall meet qualification and experiences set forth in “Section 5.4.1 Required Qualifications, Experiences of Certification Service Providers”.

- NCB shall designate a system administrator to plan, supervise, and control all protective measures

- NCB shall designate a developer to provide technical support to application service providers

- NCB shall arrange a CA and RA Administrator to perform services in establishing, managing, certification systems that support the function to create, issue, and manage certificates

- NCB shall arrange a Registration Authority to perform services in establishing and managing, certification systems that support the function to subscriber registration information

- NCB shall arrange an OCSP and LDAP operators to perform services in establishing and managing certification systems that support the function to check the validity of subscriber certificate

## 5.3 Technical Security Control

### 5.3.1 Creation of Digital Signature Data

- Only authorized persons shall be allowed by Mausign CA to create digital signature data.

- MauSign CA shall create digital signature data using a secure key creation system that is not connected to any internal and external communications network and is consequently protected from physical intrusion.

### 5.3.2 Size and Hash Value of Digital Signature Data

To use a safe and reliable digital signature algorithm, Mausign CA shall use information of the following sizes and hash value:

- In case of RSA: 2048 bits or higher

- In case of SHA-256 : 256 bits

### 5.3.3 Storage of Digital Signature Creation Data

Mausign CA shall store Digital Signature Creation Data safely in Hardware Security Module (HSM). The HSM carries the function of signing and access control and also prevents the exposure or change of Digital Signature Creation Data.

### 5.3.4 Destruction of Digital Signature Creation Data

A Digital Signature Creation Data shall be destroyed when no longer needed or when the certificate to which it corresponds is already expired or is revoked or in case of leakage. The private key of the Digital Signature Creation Data shall be destroyed in a way that prevents its loss, theft, modification, unauthorized disclosure or unauthorized use. Such destruction shall be documented, and will be done following the procedures that meet the corresponding process

### 5.3.5 Validity of Digital Signature Creation Data

Digital signature creation data of Mausign CA and subscribers may be used during the validity of the relevant certificate.

## 5.4 Personal Security

NCB shall conduct the background check upon hiring its employees and periodically examine the qualifications and qualities of operation personnel for MauSign CA

### 5.4.1 Required Qualifications, Experiences of Certification Service Providers

As personnel of facilities and equipment necessary for certification services, NCB shall have at least five (5) persons who meet the following requirements.

- Degree or Diploma in computer engineering, computer science or information and communications technology and any other related fields;
- Having knowledge of the functionalities of the CA
- Not an undischarged bankrupt person in the country or elsewhere, or has arranged with his creditors;
- Has not been convicted, whether in the country or elsewhere, of an offense, or fraudulent or dishonest act;

### 5.4.2 Matters on Education, Service Circulation of Certification Services

- NCB shall take necessary measures for training its employees to understand relevant matters for security measures.
- NCB shall get a System Administrator who will be the security staff in charge of managing certification systems to provide training related to information protection more than once per year.

- NCB shall ensure that personnel managing certification systems sign a non-disclosure agreement for confidential matters acquired while performing their duties.

- NCB shall take supplementary measures without delay where it is necessary to amend or add protective measures due to changes in working environments.

- NCB shall take appropriate measures of deactivating accounts in case of personnel shifts or retirement of personnel that manage certification systems.

### 5.4.3 Disciplinary Matters on Unauthorized Activities

- With respect to unauthorized activities of its employees, NCB shall take measures in line with the terms and conditions prescribed by its internal rules.

## 5.5 Audit and System Recovery Measures

### 5.5.1 Types of Incidents Included in Audit Records

NCB shall include on the inspection records details of the following events that have occurred on certification systems for more than ten (10) years:

- Entry of, access to, change in, or deletion of subscriber registration information

- Creation of, access to, or deletion of digital signature data

- Certificate issuance, renewal, or revocation

- Registration and management of subscriber certificates

- Start up and shut down of core certification systems

- Addition and deactivation of accounts

- Login and log out

- Other major activities of core certification system operators

### 5.5.2 Review and Protection of Audit Records

The System Administrator of MauSign CA shall check and manage audit records of certification systems. The System Administrator shall generally manage audit records of each system, and the System Administrator may only read audit records.

### 5.5.3 Backup Period and Procedure of Inspection Records

NCB shall back up and preserve audit records in storage media other than hard disk on a daily basis.

## 5.6 Storage of Records

### 5.6.1 Types of Records for Storage

NCB shall record and preserve details of the following services for ten (10) years from the date when the relevant certificate is revoked.

- Certification services including issuance and management of certificates
- Operation services of certification system of MauSign CA

### 5.6.2 Safekeeping of Stored Records

To prevent forgery, tampering, or damage, NCB shall protect the stored records as follows:

- Electronic documents shall be safely stored with digital signatures.

- General documents shall be stored in cabinets equipped with locking devices.

### 5.6.3 Backup Period and Procedure of Stored Records

NCB shall back up and preserve stored records on a daily basis.

## 5.7 Restoration of Failure and Disaster

NCB shall take prompt measures and establish restoration systems in preparation for discontinuance of certification services due to a failure of certification systems, leakage of Digital Signature Creation Data or equivalent accidents, and disasters of earthquake, flood, or fire.

### 5.7.1 Reporting and Restoration by Type of Failures and Disasters of Certification Services

NCB shall notify the ICT Authority of failures and disasters against Certification Services.

### 5.7.2 Type of Failures of Certification Services

The following types of failures shall be classified into an emergent condition of "Caution."

- Outflows of Digital Signature Creation Information of some subscriber due to infringing accidents of hacking, etc.
- Failures due to failures or malfunctions of certification systems
- Failures due to a worm, virus, Operating System attack, etc.

The following types of failures shall be classified into an emergent condition of "Alert."

- Damages of Digital Signature Creation Information (including backups)
- A large quantities of outflows of subscriber's Digital Signature Creation Information due to

- infringing accidents of hacking, etc.

- Failure of certificate issuance services

The following types of failures shall be classified into an emergent condition of "Serious."

- Outflows of Digital Signature Creation Information used in issuance of subscriber certificates

- Occurrence of wrongful uses due to a large quantity of outflows of subscriber's Digital Signature

- Creation Information due to infringing accidents of hacking, etc.

- Failures of certification validity verification services

### 5.7.3 Restoration by Type of Failures of Certification Services

- In case of a failure due to a worm, virus, or Dos attack, NCB shall disconnect relevant IPs and ports by using an invasion blocking system and take measures to strengthen monitoring through an invasion blocking system.

- In case of leakage of subscriber certificates due to hacking, NCB shall revoke the subscriber's flown-out certificates and notify the subscriber thereof.

- In preparation for a worm, virus, Dos attack, and hacking, NCB shall manage firewall, an

- invasion detection system, security S/W, ID, Password and take protective measures with the latest patch of S/W, and restore damages with backup data.

- NCB shall compose and operate certification systems into a high availability system, and prepare for disasters and failures of earthquake, flood, or fire in operating the backup center.

- Upon the occurrence of a logical failure, NCB shall use the function to restore the failure to the prior conditions.

- NCB shall compose an access control and a restoration system for main resources by system accessible IP control, server security S/W installation

### 5.7.4 Measures to Secure Continuity: Prevention of Failure of Certification Services

- NCB shall compose the certification system into a highly available system, establish a nonstop operation system, and use best efforts to prevent a failure by operating a backup center.

- Upon the occurrence of tampering or damage of main data in subscriber certificates, NCB shall

- maintain continuity of services by prompt restoration with backup materials.

# 6 AUDIT AND SYSTEM RECOVERY MEASURES

## 6.1 Warranty

### 6.1.1 Warranty

NCB shall guarantee the following items regarding the certificates it has issued:

- The details shown in the certificates are based on facts registered with NCB (existing facts when the subscriber applied for certificates).
- Subscribers' certificates shall be in accordance with this CPS.
- The accuracy of the list of revoked certificates shall be ensured.

### 6.1.2 Limitation on Warranty

NCB shall not guarantee matters other than those prescribed in Section 6.1.1 (Warranty Liability) of this CPS, i.e., subscribers' credit and integrity of information related to subscribers.

## 6.2 Liability

### 6.2.1 Liability for Compensation

Where NCB has caused damages to subscribers or users who have trusted and utilized certificates in violation of the provisions of the CPS, it shall indemnify the damages within the limit of liability.

### 6.2.2 Limitation on Liabilities

NCB shall not be held liable for damages other than that arising from the certificates it has issued and the certification services. Also NCB shall be exempted from liability where it has been proven that NCB was not negligent.

## 6.3 Interpretation and Enforcement

### 6.3.1 Applicable Laws

This Certification Practice Statement (CPS) shall be interpreted and applied pursuant to the laws of the Republic of Mauritius.

### 6.3.2 Legal Jurisdiction

Disputes related to the certification services shall be handled by a district court having jurisdiction over NCB or headquarters of the relevant registration authority.

### 6.3.3 Procedure Regarding the Settlement of Disputes

In case of a dispute related to the certification services between NCB and subscribers or relying parties, the ICT Authority may investigate related matters to determine whether NCB has violated the Act, its Decree, and its Regulation and this CPS and settle the disputes in a prompt way pursuant to the procedures of relevant laws. In such case, NCB may provide the relevant information to the parties concerned as requested in writing.

## 6.4 Protection of Personal Information

### 6.4.1 Scope of Protection and Liability of Information related to Certification Services

NCB and Registration Authorities shall comply with relevant laws with respect to the following materials acquired in the course of performing certification services, and they shall be liable for non-compliance of the above pursuant to the terms prescribed by the relevant laws. However, where a third party requests for the disclosure of information in accordance with the requirements and procedures prescribed by laws, NCB may accede to such request:

- Private information of subscribers (excluding information whose release was authorized by the
- subscriber or information disclosed in the certificate and directory system)
- Records related to certification
- Data related to the audit of certification services generated or kept by NCB
- Security measures for the operation of MauSign CA's certification services

### 6.4.2 Measures for Protection of Personal Information

Personal information shall be thoroughly managed through password after designation of administrators with the minimum personnel necessary for access and control; and MauSign CA shall take the following measures to prevent loss, damage, theft, alteration or leakage of personal information:

- to ensure security of storage of personal information and in-and-out network by application of encoding algorithm.
- to link to the vaccine program to prevent any damages or harms by computer virus.

### 6.4.3 The purpose of collection and use of personal information

To provide the certification service, the following personal information is collected to the minimum extent required for the purpose of certificate issuance and management.

- Items of personal information collected: name, e-mail address, address, phone number, cell phone number

- Items of unique identifying information collected: National Identity Card Number and Business Registration Number

- Items of equipment information collected: IP address and Domain name

### 6.4.4 Policies on the privacy of personal information

NCB establishes and enforces the policies on the privacy of personal information for the NCB service, and the details of these policies can be found on the MauSign website.

## 6.5 Inspection and Examination

### 6.5.1 Review of Facilities and Equipment

NCB shall perform certification services by using the facilities and equipment that have been subjected to reviews at the time when it was designated as a Certificate Authority.

Where it is necessary to change facilities or equipment for NCB's performance of certification services, NCB shall notify ICT Authority thereof, receive confirmation of appropriateness of the change(s), and then apply the changes to certification services.

However, where it is necessary to take urgent measures due to infringing accidents, natural disasters, or system failures, NCB may apply the change(s) in advance and report the application within seven (7) days thereafter.

### 6.5.2 Regular Audit

NCB shall be subjected to annual regular audits with respect to safe operations of facilities and equipment for performance of certification services.

Examinations shall be made with respect to the following matters:

- Certification services

- Management of digital signature keys

- Other certification services

- Management of facilities and equipment

- Management of documents and records

- Test operations and provision of information for certification services

- Network and system security

- Physical security

- Disaster prevention

- Managerial security and emergent plans

## 6.6 Validity of CPS

Once the CPS is amended, the content prior to the amendment shall become void from the date when the amended CPS comes into effect. The CPS as amended shall come into effect from August 8, 2021.