Department of
eGovernment
Cayman Islands Government

eGOV

Certification Practice Statement

March 2025

gov.ky

General information

Documentary control

Security classification:	Public
Version:	1.0
Edition date:	10/03/2025
File:	CIG CPS-1.0

Formal state

Prepared by:	Reviewed by:	Approved by:
Name: Albert Borrás	Name: Donald D. Márquez	Name: Ian B. Tibbetts
Date: 29/09/2021	Date: 07/03/2025	Date: 10/03/2025

Versions control

Version	Changes	Description of change	Author of change	Date of change
1.0	Original	Document creation	Donald Márquez	07/03/2025

Contents

1. Introduction

Presentation

This document declares the Certification Practice for authentication and digital signature of the Cayman Islands Government (CIG).

The issued Certificates are the following:

- **Natural Person**
  - Natural Person Certificate for Authentication
  - Natural Person Certificate for Electronic Signature

Document name and identification

This document is the "Certification Practice Statement of CIG".

1.1.1. Certificates' identifiers

CIG has assigned an object identifier (OID) to each Certificate policy, for their identification by requests.

Number OID	Type of Certificates
	Natural Person
1.3.6.1.4.1. 58033.1.1.1.1	*Natural Person Certificate for Authentication*
1.3.6.1.4.1.58033.1.1.1.2	*Natural Person Certificate for Digital Signature*

In case of contradiction between this Certification Practice Statement and other documented practices and/or procedures, the practices established in this Practice Statement shall prevail.

Definitions and Acronyms

1.1.2. Definitions

Acceptance Sheet: agreement subscribed by the Signer accepting the obligations applicable to Signers according to this Certification Practice Statement, that may include: the use of a secure cryptographic device, consent to the keeping of a record by the TSP of information used in registration, declaration about the Signer's identity and any specific attributes placed in the Certificate, and the passing of this information to third parties under the same conditions as required in the case of the TSP terminating its services.

Applicant: The natural person that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Signer.

Certificate: An electronic document with the public key of a signer, together with signer related identity information that uses a digital signature of a Certificate Authority to bind the public key and the identity.

Certificate Policy: Set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.

Certificate Revocation List (CRL): A signed and time-stamped list of revoked Certificates that is periodically created and signed by the CA that issued the Certificates.

Certification Authority (CA): In relation to a particular Certificate, the CA that creates, issues, revokes and manages the digital Certificates. This could be either a Root CA or a Subordinate CA.

Certification Practice Statement (CPS): One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Certification Services Provider (CSP): An organization that is responsible for the creation, issuance, revocation, and management of Certificates. The CSP may use other parties to provide parts of the certification services. The Root CA and Subordinate CA perform roles in the CSP.

Compromise: A violation of a security policy that results in loss of control over sensitive information.

Digital Signature: data appended to, or cryptographic transformation of a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery.

Directory Service: Trust service related to publication of Certificate validity information.

Distinguished Name: Unique Subject name in the infrastructure of Certificates.

Key Compromise: A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.

Key Pair: The Private Key and its associated Public Key.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

Object Identifier (OID): A unique numeric identifier registered under the Internet Assigned Numbers Authority's applicable standard for a specific object or object class.

OCSP Responder: An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests.

Online Certificate Status Protocol (OCSP): An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Public Key: The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Registration Authority (RA): CIG or an affiliated organization who perform Applicants identification, registers their data, authorizes issuance of Certificates and perform the suspension, revocation and renewal procedures.

Registration Data: Information that identifies the Certificate Subject. Subject Identity Information.

Registration Operator: person in charge of performing the identification of the Signers, approving and issuing the digital certificates.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party: Any natural person or Legal Entity that relies on the information contained within a Valid Certificate.

Root CA: The top-level Certification Authority whose Root Certificate is distributed and issues Subordinate CA Certificates.

Root Certificate: The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs.

Secure Email: service for sending utilising different types of delivery, providing methods of protection to the recipient. Secure email includes a content awareness feature to shape message delivery methods.

Secure signature creation device (SSCD): a device which holds the signer's private key, protects this key against compromise and performs signing or decryption function on behalf of the signer.

Signer: natural person identified in the digital Certificate that acquires the correspondent obligations according to this Certification Practice Statement and the Acceptance Sheet.

Subject: The natural person identified in a Certificate as the holder of the private key associated with the public key given in the certificate. The Subject is the Signer.

Subordinate CA: A Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with the Certification Practice Statement.

Valid Certificate: A Certificate that passes the validation procedure specified in RFC 5280.

1.1.3. Acronyms

CA	Certification Authority.
CP	Certificate Policy
CPS	Certification Practice Statement.
CRL	Certificate Revocation List.
CSR	Certificate Signing Request.
DES	Data Encryption Standard.
DN	Distinguished Name.
DSA	Digital Signature Algorithm.
FIPS	Federal Information Processing Standard Publication
ISO	International Organization for Standardisation.
LDAP	Lightweight Directory Access Protocol.
OCSP	On-line Certificate Status Protocol.
OID	Object Identifier.

PA	Policy Authority.
PIN	Personal Identification code.
PKI	Public Key Infrastructure.
PSD2	Payment service directive
RA	Registration Authority
RSA	Rivest-Shimar-Adleman Algorithm.
SHA	Secure Hash Algorithm.
SSCD	Secure signature creation device
SSL	Secure Sockets Layer
TCP/IP	Transmission Control. Protocol/Internet Protocol
TSP	Trust Service Provider

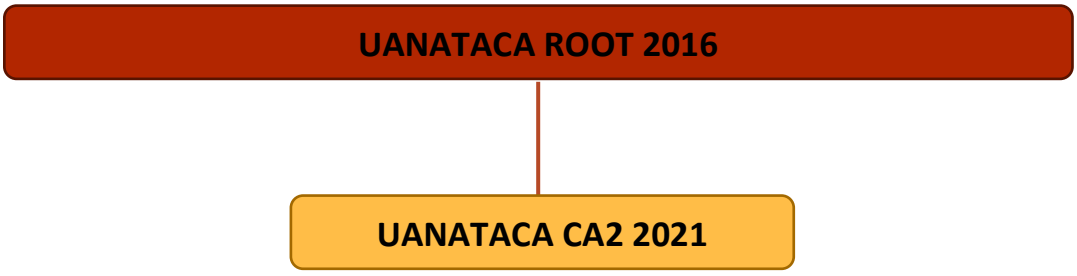
Participants in the certification services

1.1.4. Certification Service Provider

CIG is a Certification Service Provider which is the legal person that issues and manages Certificates in accordance with this CPS.

CIG relies on a public key infrastructure provider that acts in accordance with REGULATION (EU) 910/2014 OF THE EUROPEAN PARLIAMENT AND BOARD of 23rd July of 2014 as amended by REGULATION (EU) 2024/1183 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 11 April 2024, related to the electronic identification and to the relying services for electronic transactions within the domestic market and repealing Directive 1999/93/CE, as well as the technical rules of the ETSI applicable to the issuance and management of Certificates, mainly the 319 411-1, in order to facilitate the legal requirements and international recognition of its services.

To provide certification services, CIG has established a hierarchy of certification entities:



1.1.4.1. UANATACA ROOT 2016

This is an entity certification root of the hierarchy that issues Certificates to other entities of certification and whose public key Certificate has been self-signed.

Identification data:

CN:	UANATACA ROOT 2016
Digital fingerprint:	6d c0 84 50 a9 5c d3 26 62 c0 91 0f 8c 2d ce0 23 d 74 66 ad
Valid from:	Friday, 11th March 2016
Valid until:	Monday, 11th March 2041
RSA key length:	4,096 bits

1.1.4.2. UANATACA CA2 2021

This is an entity certification of the hierarchy that issues final entity Certificates and electronic timestamping Certificates, and whose public key Certificate has been digitally signed by UANATACA ROOT 2016.

Identification data:

CN:	UANATACA CA2 2021
Digital fingerprint:	2d 35 17 27 f4 5b 01 2a a4 88 03 4b db 01 1c da 4f 61 a4 2e
Valid from:	Thursday, June 3, 2021
Valid until:	Saturday, June 3, 2034
RSA key length:	4,096 bits

1.1.5. Regsitration Authority

A Registration Authority acting on behalf of CIG as the CSP, is an entity that may:

- Process Certificate applications.
- Identify the Applicant and verify that they comply with the requirements for the issuance of a Certificate
- Validate the personal data of the signatory of the Certificate.

- Manage the key generation and the issuing of the Certificate.
- Deliver the Certificate to the signer or to the means for its generation.
- Have custody of the documentation related to the identification and registry of the Signers and management for the life cycle of the Certificates.
- Suspend, revoke and cancel certificates.

The following entities will be able to act as RA of CIG:

- Any entity authorized by CIG.
- CIG directly.

CIG will formalise the relations between itself and each of the entities that act as an RA of CIG by way of a written agreement. Such agreement will include the process by which identification of Applicants will be performed.

The entity acting as an RA of CIG will be able to authorise one or more persons as Operators of the RA to perform the tasks the RA is authorised to do by CIG on behalf of the RA.

In addition, the entities appointed as RAs will execute their activities according to this Certification Practice Statement, including by maintaining authentic records regarding the subscription and identification process of all Applicants.

1.1.6. End entities

The end entities are people receiving the services of the issuance, management and use of digital Certificates, for authentication and electronic signature.

1.1.6.1. Eligible clients of the certification services

The eligible clients of the certification services are:

- Natural persons that acquire the Certificates for themselves and they have been identified in the Certificates, the Signer.

The client for the certification services acquires a license to use the Certificate, for its own use. In this case, the natural person with authority to sign is identified in the Certificate (and known as the Signer).

The signer of the certification service, is therefore, the client of the certification services provider and has the rights and obligations defined by the certification services provider, which are additional to, and do not prejudice the rights and obligations of, the Signers.

1.1.6.2. Signers

The Signers are natural persons, who possess exclusively the authentication and digital signature private keys for their identification and/or electronic signature.

The private key of a Signer cannot be recovered or deduced by the relying party or Certification Services Provider, so the natural persons identified in the relevant Certificates are solely responsible for their protection and should consider the implications of losing a private key.

Given the existence of Certificates not only for electronic signature, but also for authentication, the more generic term 'identified natural person in the Certificate', is also used, with respect to each person identified in any digital Certificate issue by CIG according to this Certification Practice Statement.

1.1.6.3. Relying parties

The Relying Parties are the persons and organizations that receive electronic records or files to which a digital signature has been applied.

To trust the associated Certificates, the Relying Parties must verify them, as it is established in the Certification Practice Statement and in the corresponding instructions available from the web page of the CIG.

Use of certificates

This section lists the requests for which each type of Certificate can be used, sets limitations to certain requests and prohibits certain requests of Certificates.

1.1.7. Uses permitted for Certificates

The permitted use specified in the various fields of the Certificate profiles should be taken into consideration, available on this Certification Practice Statement.

1.1.7.1. Certificate for Authentication of a Natural Person

The Certificate has the OID 1.3.6.1.4.1.58033.1.1.1.1. It is a Certificate issued for authentication, in accordance with the previsions of the standard ETSI EN 319 411-1. Certificates for authentication of a natural person proves the identity of the Signer. The information of uses in the Certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following function:

a. Digital Signature, for authentication
b. Key Encipherment

1.1.7.2. Certificate for Electronic Signature for a Natural Person

This Certificate has the OID 1.3.6.1.4.1.58033.1.1.1.2. It is a Certificate that is issued for creating Advanced Electronic Signatures in accordance with the previsions of the standard ETSI EN 319 411-1 . Certificates proves the identity of the Signer.

The information of uses in the Certificate's profile indicates the following:

The 'key usage' field is activated and therefore it allows us to perform the following functions:

a. Content commitment, for electronic signatures

They can also be used in requests that do not require the electronic signature equivalent to the handwritten signature, as the following requests:

a) Signature of Secure Email.
b) Other digital signature requests.

1.1.8. Limits and forbidden uses of Certificates

Certificates can only be used for the functions set out in this CPS and must not be used for other functions or other purposes.

Likewise, Certificates must be used only in accordance with the applicable law.

Certificates cannot be used for the issuance of new Certificates of any type, nor Certificate Revocation Lists (CRL).

The Certificates SHALL NOT be used for any of the following purposes:

- unlawful activity (including cyber-attacks and attempt to infringe the Certificate or the Card),
- issuance of new Certificates and information regarding Certificate validity,
- enabling other parties to use the Signer's Private Key,
- enabling the Certificate issued for electronic signing to be used in an automated way.

The Certificates have not been designed for use as control equipment for dangerous situations, such as operations that require fail-safe actions, or the operation of nuclear installations, navigation systems or air communications, or weapons control systems, where a failure could lead directly to death, personal injury or severe environmental damage.

There must be taken into account the limits indicated in the various fields of the Certificates profiles.

The use of the digital Certificates in operations that violate this Certification Practice Statement, the Acceptance Sheet, or Terms of Use, is considered to be misuse of the digital Certificate and therefore exempts CIG, from any liability arising from or related to this misuse of the Certificates made by the Signer or any third party.

CIG does not have any access to the data upon which the Certificate is applied (such as a document which is being signed). Therefore, as a result of the technical impossibility to access to the content of the data upon which the Certificate is being used, CIG cannot issue any evaluation about the mentioned content. The Signer assumes any responsibility arising from the content linked to the use of a Certificate.

Likewise, any liability that may result from the use of the Certificate out of the limits and conditions of use included in this Certification Practice Statement, the Acceptance Sheet and Terms of Use with each Certificate, or the contracts or agreements with the registration authorities or with their signers, and any other misuse thereof, will be attributable to the Signer or the person who misused the Certificate.

Policy management

1.1.9. Organization that administers the document

Cayman Islands Government
Government Administration Building
Box 138
133 Elgin Avenue,
George Town,
Grand Cayman KY1-9000
Cayman Islands

1.1.10. Contact information of the organisation

Department of eGovernment
Box 138
89 Nexus Way, Suite 8210
Camana Bay,
Grand Cayman KY1-9000
Cayman Islands

1.1.11. Document management procedures

The CIG will maintain this document in accordance with its policy management processes.

2. Publication of information and repository of Certificates

Repository(s) of Certificates

CIG has a Repository of Certificates and information related to the certification services is published.

The Repository is available 24 hours, 7 days per week and, in case of any system failure under CIG's control, it will use its best efforts to ensure that the service is back available within the time prescribed in section 5.7.4 of this Certification Practice Statement.

Publication of information of the certification services provider

CIG publishes the following information, in its Repository:

- Issued Certificates.
- Revoked Certificates list and other information about the status if the Certificates revocation.
- Applicable Certificate policies.
- Certification Practice Statement.

Frequency of publication

The information of the certification services provider, including the Certificate policies, the Certification Practice Statement and any changes thereto, are published when available.

Information as to the revocation status of the Certificates will be published in accordance with sections 4.1.24 and 4.1.25 of this Certification Practice Statement.

Access control

CIG does not limit the read access to the information listed in section 0, but establishes controls to prevent non-authorized people being able to add, modify or delete entries in the Repository, to protect the integrity and authenticity of the information, especially information about the revocation status.

CIG, via a public key infrastructure provider, uses reliable systems for the Repository, in such a way that:

- Only authorized persons can do annotations and modifications.
- The authenticity of the information can be verified.
- Any technical change affecting the security requirements can be detected.

3. Identification and authentication

Initial registration

3.1.1. Type of names

All Certificates contain a distinguished name (DN) X.501 in the field Subject including a component Common Name (CN=), relative to the identity of the signer, the natural person identified on the Certificate, as well as additional identity information in the field *SubjectAlternativeName.*

The names on the Certificates are as follows.

3.1.1.1. Certificate for Authentication for Natural Person

Country (C)	KY
Surname	Signer's Surname
Given Name	Signer's First Name
Serial Number	Cayman Islands Identification Code
Common Name (CN)	Given name and surname of the Signer

3.1.1.2. Certificate for Electronic Signature for Natural Person

Country (C)	KY
Surname	Signer's Surname
Given Name	Signer's First Name
Serial Number	Cayman Islands Identification Code
Common Name (CN)	Given name and surname of the Signer

3.1.2. Meaning of the names

The names in the fields of the Certificates *SubjectName* and *SubjectAlternativeName* are understandable in natural language, in accordance with the provisions of the previous section.

3.1.2.1. Issuance of Certificates of the set of tests and Certificates of tests in general

In case the provided data in the DN or Subject were fictitious (e.g. 'Test First Name', 'Firstname TEST', 'Lastname TEST' 'Surname1') or expressly stated words indicating its invalidity (e.g. 'TEST' 'EVIDENCE' OR 'INVALID'), the Certificate will be considered as legally invalid and therefore CIG takes no responsibility for the use of such Certificates. These Certificates are issued to undertake interoperability and other kind of tests.

3.1.3. Use of anonymous and pseudonymous

Under no circumstances can pseudonymous be used for identifying a Signer. Likewise, under no circumstances can anonymous Certificates be issued.

Anonymity or pseudonymity of Signers is not allowed.

3.1.4. Interpretation of name formats

Name formats will be interpreted in accordance with the identity document provided or the naming practice within the Cayman Islands.

The field 'country' or 'state' will refer to the Cayman Islands as the jurisdiction issuing the Certificate.

The "serial number" field must include the Signer's Cayman Islands Identification Code.

3.1.5. Uniqueness of names

The names and its related identification code of the Signer of Certificates will be unique, for each type of certificate.

CIG will not issue a Certificate to a Signer using the name and identification code that already have been used, to a different Signer.

As an exception, this Certification Practice Statement allows for the issue of a Certificate when there is an overlap with the Identification code and name of the Signer, as long the Certificates have different policy identifiers.

3.1.6. Resolution of name conflicts

Applicants are not to include names in requests that may involve infringement, by the future Signer, of third-party rights. Furthermore, CIG will not act as arbitrator or mediator, or in any other way to resolve any dispute concerning the property of names of persons.

However, in case of receiving a notification concerning a name conflict, according to the legislation of the Signer's country of citizenship or legal residence, it may take appropriate actions to suspend or revoke the Certificate issued.

In any case, the certification services provider reserves the right to reject the certification request due to names/data conflict.

Initial identity validation

The identity of the Certificate's Signer is fixed at the moment of signing the contract or Acceptance Sheet (as applicable), at which time the existence of the Signer is verified, as well as any other attribute that should be included in the Certificate information.

3.1.7. Proof of possession of private key

There is a single process flow that includes key generation, Certificate Request and issuance. The keys are generated in the SSCD during personalisation of the Card by CIG. The Certificate Request sent to CA includes a cryptographic signature created by the newly generated keys.

The possession of the private key is demonstrated under the reliable process of delivery and acceptance of the ID Card and Certificates by the Signer during the process of card issuance to the Signer.

3.1.8. Authentication of natural person identity

Upon receiving an application for a Certificate, the CIG Registration Operators will verify the identity of the Signer as applicable to whom the Certificate will be issued, as well as any specific attribute that should be included in the Certificate information.

Verification of the identity shall be done in accordance with the following methods:

A) In person in the presence of the operator or authorized personnel of the CIG Registration Authority
B) Remotely through online enrolment systems implementing collection of digital evidence of the identification process.

During this process the identity of the Signer will be properly confirmed.

The Registration Authority will verify through documents or through its own verified sources of information, any remaining data and features that need to be included in the Certificate, keeping the supporting information that proves the validity of them.

3.1.8.1. In the Certificates

The identity of the Signer is validated through the identification methods specified in section 3.2.2. In such a way that:

- (i) If the Signer is identified in person before a person authorized by the CIG Registration Authority or over video call with the permission of the Registration Authority:
  - Must present identity documents that satisfy the criteria required by the Registrar for the issuance of the Cayman Islands Identification Card
- (ii) If the Signer is identified through an online enrolment remote identification system:

- Uploading identity documents that satisfy the criteria required by the Registrar for the issuance of the Cayman Islands Identification Card Providing proof of life through the use of technical means of capturing images and/or video using facial biometric algorithms and/or artificial intelligence for the comparison of the Applicant's identity and the verification of the Applicant's proof of life, as well as the authenticity of the identity document submitted.

3.1.8.2. Identity validation

For the request of Certificates, the operator or authorized personnel of the CIG Registration Authority will verify the identity of the Applicant, acting as follows:

- When the identification has been carried out in person, through the review of:
  - Identity document provided.
- When the identification has been made through the online enrolment method, which may include an in person or video confirmation of the proof of life and likeness, by:
  - Review of the images captured from the identification document provided and the Applicant himself.
  - Review of the Applicant's proof of life, through the results provided by the identification system.
  - Review of the comparison produced by the remote identification system of the photograph of the identity document with the images obtained during the registration of the Applicant.
  - .

Utilising the above processes the identity of the Signer will be confirmed. Therefore, in all cases in which a Certificate is issued the identity of the Signer is verified.

The Registration Authority will verify through the production of documents or through its own sources of information, the remaining data and features that need to be included in the Certificate, keeping the supporting information that proves the validity of them.

3.1.9. Signer’s unverified information

CIG does not include any unverified information about the signer in the Certificates.

3.1.10. Authentication of the identity of a RA and its operators

For enabling of a new Registration Authority, CIG performs the necessary checks in order to confirm the existence of the identity or organisation involved. For that purpose, CIG will be able to use the production of documents or use its own information sources.

Likewise, CIG, directly or through its Registration Authority, verifies and validates the identity of the operators of its Registration Authorities and The Registration Authority sends CIG the relevant identification documentation of the new operator, together with its authorisation of the Operator to act in such capacity for the RA.

CIG is assured that the operators of the Registration Authority receive the proper training for the performance of their duties, which is verified with a relevant assessment. The Registration Authority previously approved by CIG can execute such training and assessment.

For the delivery of services, CIG ensures that the operators of the Registration Authority have access to the system via strong authentication with digital Certificate.

Identification and authentication of renewal requests

Once revoked, a certificate cannot be reactivated. The renewal of a certificate in this section means the creation of a new certificate that replaces the revoked one.

3.1.11. Validation for Certificates routine renewal

Before renewing a Certificate, the operator or the authorized personnel of CIG's Registration Authority verifies that the information used to verify the identity and the remaining signer data of the natural person identified in the Certificate remain valid.

The acceptable methods for such verifications are:

- In order to verify the identity of the natural person, the operator asks for the revocation code (CRE or ERC). If the provided code is correct, the operator can proceed with the revocation of the certificate.

- The use of the current certificate for its renewal as long as it has not exceeded any deadline legally established for this possibility.

If any information of the Signer identified in the Certificate has changed, the new information must be properly registered so a complete authentication is done, in accordance with section 0.

3.1.12. Identification and signer of renewal request

Before generating a Certificate for a signer whose Certificate is going to be renewed, the operator or the authorized personnel of CIG's Registration Authority will verify that the information used that day to verify the identity and the rest of the data of the Signer is still valid, in which case previous section shall apply.

The renewal of the Certificates after their revocation will not be possible in the following cases:

- The Certificate was revoked due to erroneous issuance to a person different than the one identified in the Certificate.
- The Certificate was revoked due to a non-authorised issuance in circumstances where by the natural person identified in the Certificate had not authorised the Certificate
- The Certificate revoked may contain misleading or fake information.
- Access to the Certificate has been lost or stolen

If any information of the Signer has changed, the new information must be properly registered so a complete authentication is done, in accordance with section 0.

Identification and authentication of revocation, suspension or reactivation request

CIG, operator or authorised personnel of the Registration Authority authenticate the requests and reports relative to revocation, suspension or reactivation of a Certificate verifying that they come from the Signer or an authorised person. In the event of a

compromise, circumstance e.g. violation of contractual obligations warranting revocation reported by a third party, CIG will use its reasonable endeavours to seek confirmation from the Signer.

The identification of the Signers during the process of revocation suspension or reactivation of the Certificates can be performed by:

- The Signer:
  - Identifying and authenticating through the Revocation Code (ERC or RC) via CIG's web page in 24x7 schedule.
  - Other media, such as telephone, e-mail, etc. when there is reasonable assurance of the identity of the Applicant for suspension or revocation in the judgement of CIG and/or Registration Authorities.

CIG'S registration authorities will identify the Signer upon a revocation, suspension or reactivation request using the methods they consider appropriate. The following shall be deemed to have been correctly identified:

- By request sent by the signatory, signed with the certificate itself.
- By request signed by the signer or his representative, proving his identity and powers.

When the signer seeks to initiate a revocation request, and there are doubts as to their identification his/her Certificate will be suspended

4. Certificate life-cycle operational requirements

Certificate issuance request

4.1.1. Who can submit an application for the issuance of a Certificate

The Applicant for a Certificate, who must agree to:

(1) This Certification Practice Statement;

(2) Acceptance Sheet; and

(3) Terms of Use.

Likewise, before the issuance and delivery of a Certificate, there must exist a request of a Certificate from the Signer to whom the Certificate will relate. Such request may be made in the same contract, in a specific Certificate request form or in writing directly to the Registration Authority Operator.

4.1.2. Registration procedure and responsibilities

The Certificate requests are processed either in paper or electronic format, individually or in batches, through external databases or securely via interface of *Web Services* whose addressee is CIG.

The request will go together with the supporting documentation of the identity and other information in relation to the Signer, in accordance with section 3.1.8. Along with contact details for the Signer in the Certificate.

Processing the certification request

4.1.3. Implementation of identification and authentication functions

Once the Certificate request has been received, Registration Authority ensures that the request for the Certificate is complete and accurate.

If so, the Registration Authority verifies the information provided, verifying the aspects described in section 0

For each Certificate, the documentation which was relied upon to approve the request and issue the Certificate will be preserved and properly registered with security and integrity for the period of time legally required from the expiration of the Certificate or in cases of early revocation (for whatever reason) from the date that the Certificate would have expired if it had not been revoked.

4.1.4. Approval or rejection of the request

Where the CIG is satisfied that the Applicant has provided sufficient information to confirm his or her identity and to confirm that he or she qualifies for a Certificate under the terms of this Certification Practice Statement and/or the Terms of Use, CIG will approve the request of the Certificate, submit an applicable Certificate request to the CA and proceed with its issuance and delivery.

The CA shall only accept Certificate requests from the CIG RA. The CA shall not accept Certificate requests if not received securely from the CIG RA.

If the verification indicates that the information is not correct or that the Applicant does not meet the criteria to be issued a Certificate, or if it is suspected that it is not correct or it may affect the reputation of the Certification Authority, the Registration Authority or the signers, CIG will deny the request, or will hold back its approval up to having made the additional checks that it considers appropriate.

CIG will definitely deny the request in any case where additional checks won't help to verify the information provided. CIG notifies the approval or denial of the request to the Applicant.

CIG, may automate:

- the verification procedures in relation to verifying the identity of an Applicant and the relevant information that will be in the Certificates; and
- the approval of the requests.

4.1.5. Time to process Certificate requests

CIG attends to requests in the order of receipt by CIG, and within a reasonable time.

In cases of urgency CIG will endeavour to expedite the request for a Certificate.

A request remains active until its approval or rejection.

Certificate issuance

4.1.6. CA actions during Certificate issuance

After approving the certification request, the CIG proceeds to issue the Certificate in a safe way and make it available to the Signer for their acceptance.

The established procedures in this section are applicable in case of certification renewal, taking into consideration that the same involves the issuance of a new Certificate.

During the process, CIG, via a public key infrastructure provider where necessary:

- Protects the confidentiality and integrity of the Registration Data that it receives.
- Uses reasonable measures including reliable systems and products to provide technical security and to protect against disturbance. This includes cryptographic security of the processes of certification to which they support.
- Generates a pair of keys, through a procedure of generation of Certificates bound in a safe way with the procedure of generation of keys.
- Uses a procedure of generation of Certificates that links in a safe way the Certificate with the registration information, including the certified public key.
- Ensures that the Certificate is issued by systems using protection against counterfeiting and guarantees the confidentiality of the keys during the process of generation of the mentioned keys.
- Indicates the date and hour in which a Certificate was issued.
- Ensures the exclusive control of the keys by Signer, and that neither CIG nor its Registration Authorities can deduce or use them in any way.

4.1.7. Notification to the Certificate issuance Applicant

The Registration Authority notifies the issuance of the Certificate to the Signer identified in the Certificate.

Certificate delivery and acceptance

4.1.8. CA Responsibilities

During this process, the operator or authorised personnel of the CIG's Registration Authority must perform the following actions:

- Definitively confirm the identity of the natural person to be identified in the Certificate as the Signer, in accordance with section 3.1.8.
- Deliver to the natural person identified in the Certificate the Acceptance Sheet in relation to the Certificate with the following minimum contents:
    - Basic information about the use of the Certificate, especially including information about the Certification services provider (CIG) and this Certification Practice Statement, as his/her obligations and responsibilities.
    - Information about the Certificate.
    - Information on the responsibility of the Signer in accordance with section 4.5.2.1.
    - Information on the Signer's liabilities in accordance with section 4.5.2.2.
    - Method of exclusive linkage to the Signer, of its private key and its Certificate activation data, in accordance with sections 6.2 and 6.4.
    - Confirmation from the Signer, of receiving the Certificate and the acceptance of the mentioned elements.
    - The date of the act of delivery and acceptance.
- Obtain the signature of the person identified in the Certificate.

The Registration Authority completes these processes as set out above, and preserves the original delivery and Acceptance Sheets, referring to CIG the electronic copy as well as the original when CIG requires access to them.

4.1.9. Certificate acceptance

The acceptance of the Certificate by the natural person identified in the Certificate occurs when they sign the Acceptance Sheet.

When the generation and delivery of the Certificate is carried out through the automated procedure defined by CIG, the acceptance of the Certificate by the natural person identified in it, is achieved by using the Certificate itself for signing.

4.1.10. Publication of the Certificate

CIG publishes the Certificate in the Repository referred in section 0, with the proper safety controls immediately after the Signer has accepted it, OCSP will start responding with "GOOD". For every Certificate that is accepted, the CIG will have received the authorisation of the natural person identified in the Certificate to publish the Certificate in the Repository.

4.1.11. Notification of the Certificate issuance to third parties

CIG does not notify any issuance to third parties.

Key pair and Certificate usage

4.1.12. Use by the Signer

CIG requires every Signer to:

- Provide to CIG complete and proper information, in accordance with the requirements of this Certification Practice Statement, especially during the registering procedure.
- Express his/her consent prior the Certificate issuance and delivery.

- Use the Certificate in accordance with this Certification Practice Statement.
- Recognise the capacity for production of electronic signatures with the Certificate in conjunction with a Secure Signature Creation Device; that is, equivalent to handwritten signatures, as well as other types of electronic signatures and information encryption mechanisms.
- Be especially diligent in the custody of his/her private key, in order to prevent unauthorised uses, in accordance with this Certification Practice Statement.
- Communicate to CIG, Registration Authorities and anyone who the Signer believes may trust or is acting in reliance upon the Certificate, without unjustifiable delays:
    - The loss, theft or potential compromise of his/her private key.
    - The loss of control over his/her private key, due to the compromise of the activation data (i.e. PIN) or any other reason.
    - The inaccuracies or changes in the content of the Certificate that the signer knows or could know.
    - When there is a loss, alteration, unauthorised use, theft or compromise of any cryptographic device holding private keys linked to the Certificate (such as a National ID card).
- Stop using the private key once the period specified in section 6.3.2 has elapsed.
- Not monitor, manipulate or perform reverse engineer acts on the technical implantation of the certification services of CIG, without previous written permission.
- Not compromise the safety of the certification services of the certification services provider of CIG.

CIG requires the Signer to take responsibility to ensure:

- All the information in the Certificate, provided by the Signer, is correct.
- The Certificate is used exclusively for legal and authorised uses, in accordance with this Certification Practice Statement.
- No unauthorised person ever has access to the private key of the Certificate, and that the Signer is solely responsible for any damage caused by his/her failure to protect the private key.

- The Signer is an end entity and not a certification services provider and will not use the private key corresponding to the public key listed in the Certificate to sign any Certificate (or any other format of certified public key), nor Certificate Revocation List, nor certification services provider title, nor any other case that implies providing certification services to third parties.

4.1.13. Use by the signer

See 4.5.1

4.1.14. Use by the Relying third party on Certificates

4.1.14.1. Obligations of the Relying third parties on Certificates

CIG informs a third party Relying in Certificate of the following obligations he must assume:

- Considering whether the Certificate is appropriate for the intended use, in an independent way.
- Verify the validity, suspension or revocation of the issued Certificates, for which Certificates status information will be used.
- Verify all Certificates of the Certificates hierarchy, before trusting the digital signature or any of the Certificates of the hierarchy.
- Recognise that the verified electronic signatures and authentication actions, are legally binding.
- Consider any limitation on the use of the Certificate, regardless of whether in the Certificate, this Certification Practice Statement or in the Relying third party in Certificates contract if applicable.
- Consider any caution established in any relating instrument, regardless of its legal nature.
- Not monitor, manipulate or perform reverse engineer acts about the technical implementation of the certification services of CIG, without previous written permission.
- Not compromise the safety of the Certification services of CIG.

4.1.14.2. Civil liability of the Relying Parties in Certificates

Relying Parties in Certificates assume the following responsibilities:

- Ensuring they have enough information to make an informed decision in order to trust or not the Certificate.
- Recognising that they are solely responsible for trusting or not the information of the Certificate.
- Being solely responsible if they breach their obligations as a third party that has trusted the Certificate.

Certificate renewal

Certificate renewal requires the renewal of keys, and therefore must comply with section 0.

Key and Certificate renewal

4.1.15. Circumstances for Certificate and key renewal

Certificate renewal refers to the issuance of a new certificate to the signer without changing the signer or the other information in the certificate.

Existing Certificates can be renewed through a specific and simplified procedure of request, in order to keep the continuity of the certification service.

There are at least two ways for Certificate renewal:

a) Face to face renewal process – it will be carried out the same way as a new Certificate issuance.

b) Online renewal process (via internet) – as detailed below.

4.1.16. Online renewal process

4.1.16.1. Circumstances for online renewal

The online renewal of the Certificate will take place only if the following conditions are met:

- The Registration Authority and/or CIG have access to the online renewal service.
- The Certificate that is used for the renewal is valid, in other words, it is not expired, revoked or suspended.
- No more than 5 years have passed since the last accreditation of identity by CIG or a Registration Authority in accordance with this Certification Practice Statement

4.1.16.2. Who can request an online renewal Certificate

Any Signer will be able to request an online renewal Certificate if all the circumstances described in section 4.7.2.1 are fulfilled.

The Signer will be able to formalise his/her request by accessing the online renewal service Certificate on CIG's website.

4.1.16.3. Approval or rejection of the request

In cases where the request is verified as meeting the requirements of Sections 4.7.1 and 4.7.2 and, where necessary for those with an outdated accreditation of identity, sections 3.2, 3.3 and 3.4, CIG should approve the request of the Certificate and proceed with its issuance and delivery.

CIG notifies the approval or denial of the request to the Applicant.

CIG may automate the verification procedures of the information that will be in the Certificates, and the approval of the requests.

4.1.16.4. Procedure for online renewal request

The renewal request of a Certificate will be performed as follows:

- When the digital Certificate of the Signer is about to expire, CIG will be able to send one or more notifications over time, inviting the Signer to renew.
- The Signer will connect to the renewal service on CIG's webpage and they will proceed with the renewal request.
- The Signer will sign his/her valid Certificate renewal.

- Creation of a new pair of keys and generation and import of the Certificate taking into account the following constraints:
  - Protects the confidentiality and integrity of the information within the Certificate.
  - Uses reliable systems, products and measures that reasonable protected against disturbance and provide technical security and, in its case, cryptographic security of the processes of certification to which they support.
  - Generates a pair of keys, through a procedure of generation of Certificates bound in a safe way with the procedure of generation of keys.
  - Uses a procedure of generation of Certificates that links in a safe way the Certificate with the registration information, including the certified public key.
  - It ensures that the Certificate is issued by systems using protection against counterfeiting and guarantees the confidentiality of the keys during the process of generation of the mentioned keys.
  - Indicates the date and hour in which a Certificate was issued.
  - It ensures the exclusive control of the keys by the user, and CIG or its Registration Authorities cannot deduce or use them in any way.

4.1.16.5. Notification of the renewed Certificate issuance

CIG notifies the Signer of the Certificate issuance.

4.1.16.6. Way in which the Certificate is accepted

The acceptance of the Certificate occurs when signing the renewal electronically.

4.1.16.7. Publication of the Certificate

CIG publishes the renewed Certificate in the Repository to which refers in the section 0, with the proper safety controls.

4.1.16.8. Notification of Certificate issuance to third parties

CIG does not make any notification of the issuance to third parties.

Certificate modification

The modification of Certificates, except the modification of the certified public key, which is considered renewal, will be treated as a new issue of Certificate applied as described in sections 0, 0, 0 and 0.

Revocation, suspension or reactivation of Certificates

The revocation of a Certificate means the definitive withdrawal of the Certificate. Any such revocation is itself irreversible.

The suspension of a Certificate means the temporary withdrawal of it and it is reversible. Only end entity Certificates will be able to be suspended.

The reactivation of a Certificate is the transition from a suspended status to an active one.

4.1.17. Causes of Certificate revocation

CIG will revoke a Certificate when any of the following instances occur:

1) Circumstances affecting the information contained in the Certificate:
   a) Modification of any of the data contained in the Certificate, after the corresponding issue of the Certificate including amendments.
   b) Discovery that any of the data contained in the Certificate application is incorrect.
   c) Discovery that any of the data contained in the Certificate is incorrect.

2) Circumstances affecting the security of the key or Certificate:
   a) Compromise of the private key, infrastructure or systems Certification Service Provider that issued the Certificate, provided that it affects the reliability of the Certificates issued from that incident.

b) Infringement by CIG, of the requirements of the Certificate management procedures established in this Certification Practice Statement.
c) Commitment or suspected compromise of the private key or Certificate issued.
d) Unauthorised access or use, by a third party of the private key corresponding to the public key contained in the Certificate.
e) Unlawful or improper use of the Certificate by the natural person identified in the Certificate or lack of diligence in the custody of the private key.

3) Circumstances affecting the natural person identified in the Certificate:
   a) Completion of the legal relationship between CIG provision of services and the signer.
   b) Modification or termination of the underlying legal relationship or what caused the issuance of the Certificate to the natural person identified in the Certificate.
   c) Infringement by the Signer of the Certificate Application requirements.
   d) Violation by the person identified in the Certificate, of their obligations, responsibilities and guarantees established in this Certification Practice Statement, the Acceptance Sheet and/or the Terms of Use.
   e) Death of key holder.
   f) Request by the signer for Certificate revocation in accordance with the provisions of section 0.

4) Other circumstances:
   a) The CIG ceasing to be a Certification Service Certification Entity.
   b) The use of the Certificate that is harmful to CIG. Whether use is harmful will be determined by CIG, taking into account the following criteria:
      - The nature and number of complaints received.
      - The identity of the entities filing complaints.
      - The relevant legislation in force at all times.
      - The response of the of the person identified in the Certificate to complaints received.

4.1.18. Reasons for suspension of Certificates

CIG Certificates may be suspended in the following instances:

- When so requested by the Signer.
- When there is a request for revocation which requires further identification confirmation before being actioned.
- If the private key is suspected to have been compromised until it is confirmed. In this case, CIG will make sure that the Certificate is not suspended for longer than necessary to confirm whether or not the private key has been compromised.
- When the Certificate allows for electronic signature and the Signer becomes incapacitated.

4.1.19. Reason for reactivation of Certificates

CIG Certificates may be reactivated from the following causes:

- When the Certificate is in suspended status, and
- When so requested by the natural person identified in the Certificate.

4.1.20. Who can request the revocation, suspension or reactivation of a certificate

The Certificate may be requested to be revoked, suspended or reactivated by:

- The person identified in the Certificate.
- The signer of the Certificate through an authorized representative.
- CIG for one of the limited reasons set out at 4.9.2.

4.1.21. Procedures for revocation, suspension or reactivation request

The natural person that requires to revoke, suspend or reactivate a Certificate must apply to CIG or the Registration Authority via the online service available in the CIG's website, help desk or in person. The revocation, suspension or reactivation request shall include the following information:

- Date of application for the revocation, suspension or reactivation.
- Identity of the Signer.
- Name and title of the person requesting the revocation, suspension or reactivation.
- Contact information for the person requesting the revocation, suspension or reactivation.

- Detailed reason for the request.

The application must be authenticated by CIG or RA, in accordance with the requirements of section 0 of this policy, prior to the revocation, suspension or reactivation.

The revocation, suspension or reactivation service can be found in the CIG website at: https://certs.egov.ky.

The revocation, suspension or reactivation request will be processed upon receipt. The CIG or Registering Authority may inform the signer once the change of status of the Certificate is complete.

The revocation, suspension and reactivation management service are considered critical services and thus contained in the contingency and business continuity planning of CIG through its public key infrastructure provider.

The Signer may make request for reactivation at their discretion.

4.1.22. Period for revocation, suspension or reactivation application processing

The revocation, suspension or reactivation will occur immediately when received. If it takes place with an operator, it will be executed within the regular hours of operation CIG or the Registration Authority. If it is carried out via the online service, it will happen immediately.

4.1.23. Obligation of Relying Parties to check Certificate revocation or suspension information

Third parties should check the status of those Certificates upon which they wish to rely.

A method by which you can check the Certificate status is by consulting the latest Certificate Revocation List issued by the Certification of CIG.

The Certificate Revocation Lists are published in the Repository of the Entity Certification, as well as the following web addresses indicated in Certificates:

- http://crl1.uanataca.com/public/pki/crl/CA1subordinada.crl
- http://crl2.uanataca.com/public/pki/crl/CA1subordinada.crl

The status of the Certificate validity can also be checked by the Online Certificate Status Protocol Service.

- http://ocsp1.uanataca.com/public/pki/ocsp/
- http://ocsp2.uanataca.com/public/pki/ocsp/

4.1.24. Frequency of issuance of Certificate Revocation Lists (CRLs)

CIG issues a CRL at least every 24 hours.

The CRL indicates the scheduled time of issuance of a new CRL, although it may issue an CRL before the deadline stated in the previous CRL, to reflect revocations.

The CRL will include all revoked Certificates. It will also include the suspended Certificates until the date of expiry of the respective Certificate.

4.1.25. Maximum period of publication of CRLs

The CRLs are published in the Repository within a reasonable period immediately after being issued, which in any case is no more than a few minutes.

4.1.26. Availability of the service checking in line with the state of the Certificates

Alternatively, third parties who rely on Certificates may consult CIG repository Certificates, which is available 24 hours 7 days a week on the web:

- https://www.uanataca.com/public/pki/crtlist

To check the latest CRL issued in each CA, the following may be downloaded:

- *Certification Authority (CA) ROOT (Uanataca ROOT 2016):*
  - http://crl1.uanataca.com/public/pki/crl/arl_uanataca.crl
  - http://crl2.uanataca.com/public/pki/crl/arl_uanataca.crl

- *Certification Authority (CA) Intermediate 2 (Uanataca CA2 2021):*
  - http://crl1.uanataca.com/public/pki/crl/CA2subordinada.crl
  - http://crl2.uanataca.com/public/pki/crl/CA2subordinada.crl

In case of failure of the systems for checking Certificate status due to reasons beyond the control of CIG, it must make its best efforts to ensure that this service remains inactive for the minimum possible time, which may not exceed one day.

CIG provides information to third parties who rely on Certificates on the operation of the service Certificate status information.

4.1.27. Obligation to check the consultation Certificate status service

It is mandatory to check the status of Certificates before relying on them.

4.1.28. Special requirements in case of compromise of the private key

The compromise of the CIG's private key is notified to all participants in certification services, by posting information in the CIG website and, if necessary, in other media.

4.1.29. Maximum period of suspension of digital Certificate

The maximum suspension of a digital Certificate is the period until its expiration date.

Completion of the subscription

After the period of validity of the Certificate, the service subscription ends.

As an exception, the signer can maintain the existing service, for the sole purpose of requesting Certificate renewal, in time determined by this Certification Practice Statement.

Escrow and recovery of keys

4.1.30. Policies and practices of storage and key recovery

CIG does not provide escrow services and key recovery. Storage of the Key in the SSCD is not considered a key escrow service.

4.1.31. Policy and practices of encapsulation and recovery of key session

No stipulation.

5. Physical security controls, management and operations

Physical security controls

CIG, via a public key infrastructure provider where necessary, has established physical and environmental security controls to protect the resources of the facilities where the systems, the systems themselves and the equipment used for operations of the provision of relying electronic services.

Specifically, the security policy applicable to the relying electronic services has established requirements for the following contingencies:

- Physical access controls.
- Protection against natural disasters.
- Protective measures against fires.
- Failure of the support systems (electronic energy, telecommunications, etc.)
- Collapse of the building.
- Flooding.
- Antitheft protection.
- Unauthorized removal of equipment, information, media and applications relating to components used for the services of the service provider certification.

These measures are applicable to installations where the Certificates are produced under the full responsibility of CIG, both in the production and contingency environments. High security installations that are properly audited periodically.

Facilities include preventive and corrective maintenance systems with assistance 24/7 all year round.

5.1.1. Location and construction of facilities

Physical protection is achieved by creating clearly defined security perimeters around services. The quality and strength of building materials facility ensures adequate levels of protection against intrusion by brute force and located in an area of low risk of disasters and allows quick access.

The room where the cryptographic operations are performed in the Data Processing Centre has redundancy in its infrastructure, as well as several alternative sources of power and cooling in an emergency.

CIG has facilities to physically protect the provision of services including approval of applications for Certificates and revocation management and to limit compromise caused by unauthorised access to systems or data access and disclosure thereof.

5.1.2. Physical access

CIG, via a public key infrastructure provider, has three levels of physical security (building entrance where the CPD is found, access to the room of the CPD and access to the rack) for service of protecting the Certificate generation and must be accessed from the lower to the upper levels.

Physical access to the premises, where certification is processed, is limited and protected by a combination of physical and procedural measures are carried out as such:

- Limited to expressly authorised persons, with identification at the time of access and registration thereof, including filming by CCTV.
- Access to the rooms is done with ID card readers and managed by a computer system that keeps a log of inputs and outputs automatically.
- To access the rack where the cryptographic processes are located, prior authorisation from administrators hosting service is necessary to have the key to open the cage.

5.1.3. Electrical power and air conditioning

Facilities have current-stabilising equipment and power system doubled with generator equipment.

The rooms housing IT equipment have temperature control systems with air conditioners.

5.1.4. Exposure to water

The facilities are located in an area of low risk of flooding.

The rooms where computers are housed have a moisture detection system.

5.1.5. Fire prevention and protection

The facilities and assets have automatic detection and firefighting systems.

5.1.6. Backup storage

Only authorised individuals have access to support storage.

The most sensitive data is stored in a safe offsite Data Processing Centre.

5.1.7. Waste management

The elimination of media, both paper and magnetic, is made by mechanisms that guarantee the impossibility of retrieving information.

In the case of magnetic media, it proceeds to formatting, permanent deletion, or physical destruction of the support. For paper documents, paper shredders or specially arranged bins for later destruction are used, under supervision.

5.1.8. Offsite backup

Secure external storage is used for the safekeeping of documents, magnetic and electronic devices that are independent of the operations centre.

Procedure controls

CIG endeavours that its systems are operated safely, for which it has established and implemented procedures for the functions which affect the supply of its services.

Administrative and management procedures are run according to the security policy procedures.

5.1.9. Trusted Roles

CIG has identified, in accordance with its security policy, the following trusted roles (some of the below functions and roles are performed by a public key infrastructure provider)

- **Internal Auditor**: Responsible for compliance with operating procedures. This is an external person to the System Administrator team. The tasks of Internal Auditor are incompatible with the other trusted roles defined in this section. This role is managed by the PKI provider.
- **System Administrator**: Responsible for the proper functioning of hardware and software support platform certification
- **Certification Authority Administrator**: Responsible for the actions to be executed with the cryptographic material or performing any function involving the activation of private keys of certification authorities described in this document, or any of its elements.
- **Certification Authority Operator**: Responsible, in conjunction with CA Administrator, for the custody of material activation of cryptographic keys, and responsibility for backup operations and maintenance of Certification Authority.
- **Registration Officer**: Person responsible for approving the certification requests made by the signer and issuing digital Certificates.
- **Revocation officer**: Person responsible for making the changes in the status of a Certificate, mainly proceed with the suspension and revocation of the same.
- **Security Manager**: Responsible for coordinating, monitoring and enforcing security measures as defined by the security policies applicable to this

Certification Practice Statement. This individual should be responsible for aspects related to information security: logistics, physical environment, networking, organization, etc.

Persons holding the above posts are subject to procedures of investigation and specific control. Additionally, CIG applies policy criteria for the segregation of duties, as preventive measure to fraudulent activities.

5.1.10. Number of individuals per task

CIG, via a public key infrastructure provider, guarantees at least two people to perform tasks related to the generation, recovery and back up of the private key of the Certification Authorities. Same criteria applies to the implementation of issuance tasks and activation of the Certificates and private keys of the Certification Authorities and in general in handling the device custody of the keys of the Authority root and intermediate certification.

5.1.11. Identification and authentication for each role

The individuals assigned for each role are identified by the internal auditor who will ensure that each person performs the operations for which they are assigned.

Each person only controls the assets required for their role, ensuring that no person can access unauthorised resources.

Access to resources is performed depending on the asset through cryptographic cards and activation codes.

5.1.12. Roles requiring separation of tasks

The following tasks are performed by at least two people:

- The tasks of the Auditor role will be incompatible with the operation and management of systems, and in general, with those roles related to the direct provision of relying electronic services.
- Issuance and revocation of Certificates will be incompatible tasks with the Management and systems operation.
- The management and systems operation and the Certification Authorities, will be mutually incompatible.

5.1.13. PKI management system

The PKI system is composed of the following modules:

- Component/module for Subordinate Certificate Authority management.
- Component/module for Registration Authority management.
- Component/module for solicitation management
- Component/module for key management (HSM)
- Component/module for databases
- Component/module for CRL management.
- Component/module for OCSP service management.

Personnel controls

5.1.14. History, qualification, experience and authorisation requirements

All staff members have been properly trained to perform operations that they have been assigned.
Staff in positions of trust have no personal interests that conflict with the development of the role that has been entrusted.

CIG ensures that an accurate personnel record is held in relation to each staff member.

In general, an employee is withdrawn from their duties when knowledge of the existence of the commission of any criminal act that could affect the performance of its functions come to the attention of CIG or any of its contracted providers.

Reliable site management will not be assigned to a person who is not suitable for the position, especially for having been convicted of a crime affecting their suitability for the position. For this reason, due diligence in carried out in accordance with and **to the extent permitted by applicable law**, including in relation to the following:

- Qualifications.
- Previous work history.
- Professional and other references.

In any case, the Registration Authorities will be able to establish checking procedures of different backgrounds, always preserving CIG's policies, who remains responsible for the actions of the persons who authorise the operations.

5.1.15. Procedures for personnel history investigation

CIG, or the sub-contractor directly employing a person to operate under the Certification Practice Statement, obtains the consent of candidates for employment to undertake relevant background checks. The CIG, or their sub-contractor, processes and protects all personal data in accordance with the Data Protection Act (2021 Revision) and/or any relevant data protection legislation in the jurisdiction in which the employee will be employed.

Candidates will not be employed where the relevant background checks indicate that they are unsuitable for the position.

5.1.16. Training requirements

CIG, via a public key infrastructure provider where necessary, trains the staff in trusted roles and management jobs, until they reach the required qualification, keeping reports of the training.

Training programs are updated and improved periodically.

At a minimum, training includes the following contents:

- Principles and mechanisms of security of the certification hierarchy, and the user environment of the person to train.
- Tasks the person must do.
- Policies and security procedures of CIG (and the public key infrastructure provider where necessary). Use and operation of machinery and installed applications.
- Management and processing of incidents and security incidents.
- Procedures of business continuity and emergency.
- Process management and security regarding the processing of personal data.

CIG ensures the Registration Officers have completed a course of preparation for the tasks of validation requests.

5.1.17. Retraining frequency and requirements

Staff training is updated in accordance with the needs of staff, and with enough frequency to ensure their functions can be completed in a competent and satisfactory way, especially when doing the substantial modifications in the certification tasks.

5.1.18. Job rotation frequency and sequence

Not applicable.

5.1.19. Sanctions and unauthorized actions

There are disciplinary systems, to enforce the sanctions arising from unauthorised actions, appropriate to the applicable labour legislation.

Disciplinary actions may include suspension and loss of employment of the person responsible for the harmful action, proportionate to the gravity of the unauthorised action.

Where the employee is employed by the CIG directly such actions will be in compliance with the Public Service Management Act and Personnel Regulations.

5.1.20. Professionals contracting requirements

The staff hired to perform trusted roles sign a confidentially agreement and agree to the operational requirements used by CIG. Any action that may compromise the security of the accepted processes could, once evaluated in accordance with applicable legislation, lead to the termination of the employment contract.

In cases where all or part of the certification services are performed by a third party, the provisions and controls performed in this section, or other parts of the Certification Practice Statement, will be applied and complied by the third party who performs the operation functions of the certification services, notwithstanding, the Certification Authority will be responsible in any case for the effective implementation. These aspects are reflected in the legal instrument used to arrange the certification services provision by a third party.

5.1.21. Documentation supplied to personnel

The certification services provider will provide only the documentation strictly needed by the staff at any moment, to perform their job in a competent and satisfactory form.

Security audit procedures

5.1.22. Types of recorded events

CIG, via a public key infrastructure provider where necessary, produces and maintains a record of, at least, of the following events related to the entity security:

- Booting and shutting down of systems.
- Attempts to create, delete, set passwords or change privileges.
- Attempts to login and logout.
- Unauthorised attempts to enter the CA network.
- Unauthorised attempts to access system files.
- Physical access to logs.
- System configuration maintenance and changes.

- Records of the CA applications.
- Booting and shutting down of CA application.
- Changes of the CA and/or keys details.
- Changes in Certificate issuing policies.
- Generation of own keys.
- Creation and revocation of Certificates.
- Records of destruction of materials containing key information or activation data.
- Events related to the Certificate's lifecycle of the cryptographic module, as lobby, use and uninstalling of it.
- Generation keys ceremony and keys management databases.
- Physical access records.
- System configuration maintenance and changes.
- Staff changes.
- Commitments and disagreements reports.
- Records of destruction of materials containing key information, activation data or personal information of the signer, in case of individuals Certificates, or the natural person identified in the Certificate, in case of organisation Certificates.
- Possession of activation information for operations with the private key of the Certification Authority.
- Complete reports of the physical intrusion attempts in the infrastructures that support the Certificates issuance and management.

Log entries include the following elements:

- Login date and time.
- Serial number or entry sequence, in the automatic records.
- Identity of the entity entering in the register.
- Type of entrance.

5.1.23. Frequency of processing audit logs

CIG, via a public key infrastructure provider, reviews its logs when a system alert motivated by the existence of any incident occurs.

Processing audit logs is a review of the records including the verification that confirm they have not been tampered, a brief inspection of all log entries and a deeper investigation of any alert or irregularities in the logs. The actions from the audit review are documented.

CIG , via a public key infrastructure provider, keeps a system that ensures:

- Enough space for logs storage.
- Logs files are not rewritten.
- Information held includes, at least: type of event, date and time, user running the event and result of the operation.
- Logs files will be held in structured files susceptible to incorporate into a data base for further exploration.

5.1.24. Period of retention of audit logs

CIG, via a public key infrastructure provider, holds the logs information for a period of time as required by the National Archive and Public Records Act.

5.1.25. Audit logs protection

The systems logs:

- Are protected from manipulation by signing the files that contain them.
- Are stored in fireproof devices.
- Availability is protected through its storage in facilities out of the centre where the CA is located.

Access to logs files is reserved only to authorised persons. Also, devices are handled at all times by authorised personnel.

There is an internal procedure where management processes devices containing the data of the audit logs are detailed.

5.1.26. Audit log backup procedures

CIG, via a public key infrastructure provider, has a proper backup procedure so that, in case of loss or destruction of relevant files, corresponding backups will be available in a short period of time.

CIG , via a public key infrastructure provider, has implemented a secure backup procedure of audit logs, making a copy of all logs weekly in an external source. Additionally, a copy is held in an external custody centre.

5.1.27. Location of the audit logs storage system

The information of the audit events is collected internally and in an automated way by the operating system, network communications and software Certificate management, in addition to the data generated manually, will be stored by the authorised personnel. All this composes the storage system of audit logs.

5.1.28. Notification of the audit event to the Subject that caused the event

When the log audit accumulation system records an event, it is not necessary to send a notification to the individual, organisation, device or application that caused the event.

5.1.29. Vulnerability analysis

The audit processes of CIG, via a public key infrastructure provider, cover vulnerability analysis.

Vulnerability analysis must be run, reviewed and revised by an examination of these monitored events. This analysis must be run daily, monthly and annually in accordance with the internal procedure intended for this purpose.

Audit data systems are stored in order to be used in the investigation of any incident and to locate vulnerabilities.

Information files

CIG, via a public key infrastructure provider where necessary, endeavours to ensure that all information relating to the Certificates is held for an appropriate period of time as established in section 5.1.31 of this policy.

5.1.30. Types of records archived

The following documents involved in the life cycle of the Certificate are stored by CIG directly or via a public key infrastructure provider or registration authorities:

- All audit data system.
- All data relating to Certificates, including contracts with the Signers and the data relating to their certification and location.
- Requests of issuance and revocation of Certificates.
- Type of document presented in the Certificate request.
- Identity of the Registration Authority that accepts the Certificate request.
- Unique identification code provided by the previous document.
- All Certificates issued or published.
- CRLs issued or logs of the status of the generated Certificates.
- The history of generated keys.
- Communications between the elements of the PKI.
- Policies and Practices Certification.
- All audit data identified in section 0.
- Information of requests certification.
- Documentation provided to justify the certification requests.
- Life cycle Certificate information.

CIG and/or the Registration Authorities accordingly are responsible for archive records about certificate applications, signed Signer agreements, registration information (including evidences of Signer identity verification) and requests or applications for suspension, termination of suspension and revocation are retained and the correct filing of all this material.

The records maybe physical or digital.

5.1.31. Retention period for the files

CIG saves the mentioned logs above for the period required by the National Archives and Public Records Act as informed by the Data Protection Act.

5.1.32. Protection of the files

CIG protects the files so only the duly authorised persons can access to them. The files are protected against visualisation, modification, erasure or any other manipulation through its storage in a reliable system.

CIG ensures proper protection of the digital files by implementing technical measures to ensure secure storage.

5.1.33. File backup procedures

CIG has an external storage centre to ensure the availability of the file backups of electronic files. The physical documents are stored in safe places restricted to authorised personnel.

CIG, at least, makes incremental daily backups of support of all its electronic documents and makes weekly full backups for data recovery cases.

In addition, CIG (or the organisations that undertake the registration functions) keeps a copy of the paper documents in a safe place different from the Certification Authority.

5.1.34. Location of the file system

CIG via a public key infrastructure provider has a centralised system of gathering information of the activity of the equipment involved in the Certificate management service.

CIG or its Registration Authorities has a centralised system of gathering information of the activity of the equipment involved in the Registration processes.

5.1.35. Procedures to obtain and verify file information

CIG has a procedure to verify that the stored information is correct and reachable. CIG provides the information and means of verification to the auditor.

Keys renewal

The CA keys will be changed before the use of the private key expires. The former CA and its private key will only be used for signing CRLs while there are active Certificates issued by that CA. A new CA will be generated with a new private key and a new DN. The key change of the signer is done by a new issuing process.

Alternatively, in the case of the Subordinated Certification Authorities, you will be able to renew the Certificate with or without key change, not applying the procedure described earlier.

Compromised key and recovery of disaster

5.1.36. Management procedures of incidents and compromises

CIG via a public key infrastructure provider has security policies and business continuity, which allows the management and recovery of the systems in case of compromise or disaster of its operations, ensuring critical services of revocation and publication of the condition of the Certificates can continue uninterrupted.

5.1.37. Computing resources, applications or data corruption

When computer resources, applications or data corruption events happen, the incidences will be communicated to security, and the proper management procedures will begin, which contemplate scaling, investigation and response to the incident. CIG will initiate procedures for the handling of compromised keys, or disaster recovery, if necessary.

5.1.38. Compromised private key of the entity

In case of suspicion or knowledge of the compromise of CIG's public key infrastructure provider's, private key compromise procedures will be activated in accordance to the security policies, incident management and business continuity, which allow the recovery of the critical systems, and if necessary in an alternative data centre.

5.1.39. Business continuity capabilities after a disaster

CIG, via a public key infrastructure provider where necessary, will restore critical services (suspension and revocation, and publication of the information of the Certificates status) in accordance with the contingency and business continuity plan, restoring the normal operation of the previous services within 24 hours of the disaster.

CIG, via a public key infrastructure provider, has an alternative centre for the operation of certification schemes described in the business continuity plan, if necessary.

Service termination

CIG, via a public key infrastructure provider, ensures that potential disruptions to signers and third parties are minimal as a result of the cessation of the certified services provider and, especially, ensures a continuous maintenance of the records required to provide certified evidence for regulatory or criminal investigation, by transfer to a trustworthy repository.

Before the services cessation, CIG's public key infrastructure provider will develop a termination plan, with the following provisions:

- To inform all Signers, Relying Parties and other CA's with which it has agreements or another type of relation of the cessation with a minimum of 6 months' notice.
- To revoke any authorisation to outsourced entities to act on behalf of the CA in the process of Certificates issuance.
- To transfer its obligations regarding the maintenance of the registry information and logs for the period of time indicated to signers and users.

- To destroy or disable for use the private keys of the CA.
- To keep active the Certificates and verification system to expiration and revocation of all Certificates issued.
- To run all necessary tasks to transfer the maintenance obligations of registration information and the files of events log during the respective time periods indicated to the signer and Relying Parties in Certificates.

6. Technical security controls

CIG uses reliable systems and products, protected against any alteration and via its PKI Infrastructure Provider ensures the technical and cryptographic security of the certification, which are used as support.

Generation and installation of the pair of keys

6.1.1. Generation of the pair of keys

The Certification Authority Root "UANATACA ROOT 2016" in accordance with the ceremony procedures of CIG via its PKI Infrastructure Provider created the pair of keys of the intermediate Certification Authority "UANATACA CA2 2021", within the high security perimeter addressee to this area.

The activities performed during the keys generation ceremony have been registered, dated and signed for all the individuals participating in it, with the presence of an Auditor CISA. Such records are securely retained for audits and for an appropriate period determined by CIG.
For the Certification Authorities Root and intermediate key generation, devices with the certification FIPS 140-2 level 3 and Common Criteria EAL4+ are used.

UANATACA ROOT 2016	4.096 bits	25 years
UANATACA CA2 2021	4.096 bits	13 years
- Final entity Certificates	2.048 bits	Up to 5 years

The PKI Disclosure Statement (PDS) of all the electronic Certificate profiles indicated in this document, are accessible under the link: https://certs.egov.ky/public/pds/

6.1.1.1. Generation of the Signer pair of keys

The Signer can create the Signer keys through hardware and/or software devices authorized by CIG. The keys are created using public key algorithm RSA, with a minimum length of 2048 bits.

6.1.2. Delivering the private key to the Signer

The private key of the Signer is created in the signature creation device and stored, properly protected, in the interior of such a device.

6.1.3. Sending of the public key to the Certificate issuer

The Signer's 'Public key' is computed inside the SSCD and then transmitted to Certificate Issuer inside the PKCS#10 Certificate Signing Request (CSR). The CSR is signed by the Signer for authenticity. The transmission is protected by TLS communication channel for additional confidentiality and authenticity or other equivalent secure channel or any other method approved by CIG.

6.1.4. Public key distribution of the certification services provider

CIG's public keys are communicated to third parties who trust in Certificates, ensuring the integrity of the key and authenticating its origin, through its publication in the Repository.

Users can access to the Repository to obtain the public keys, and additionally, in applications S/MIME, the data message may contain a chain of Certificates, which are distributed to the users in this way.

The Certificate of the CA Root and Subordinates will be available on the CIG web page.

6.1.5. Key sizes

- The length of the Certification Authority Root keys is 4096 bits.
- The length of the Certification Authority Subordinated keys is 4096 bits.
- The length of the end Entity Certificates keys are 2048 bits.

6.1.6. Generation of public key parameters

The CA Root, CA Subordinates and the signer Certificates public key are encrypted in accordance with RFC 5280.

6.1.7. Quality check of the public key parameters

- Module Length= 4096 bits
- Algorithm of keys generation: rsagen1
- Cryptographic functions of Summary: SHA256.

6.1.8. Key generation in IT applications or in equipment goods

All keys are generated in secure devices, in accordance with the device certifications indicated in section 6.1.1.

6.1.9. Key usage purposes

Key usage for the CA Certificates is exclusively for signing Certificates and CRLs.

Key usage for the end entity is exclusively for the digital signature, non-repudiation and data encryption.

Private key protection

6.1.10. Cryptographic modules standards

In relation to the modules that manage the keys of the CA and the signers of the electronic signature Certificates, the required level by the standards indicated in the above sections is ensured.

6.1.11. Private key multi-person (n of m) control

A multi-person control is required for activating the private key of the CA. In the case of this Certification Practice Statement, in detail there is a policy of **3 of 6** persons for the keys activation.

Cryptographic devices are physically protected, as determined in this document.

6.1.12. Signer Private key retention

CIG doesn't store usable copies by any means of the private key of the Signers.

6.1.13. CA Private key backup

CIG's PKI infrastructure provider makes backup copy of the CAs private key that enables their recovery in case of disaster, loss or deterioration thereof. Both generation of the copy and the recovery thereof need at least two people participation.

These recovery files are stored in fireproof cabinets and in the external custody centre.

6.1.14. Private key storage

The CA private keys are archived for a period of **10 years** after the issuance of the last Certificate. They will be stored in secure fireproof files and in the external custody centre. At least the collaboration of two people will be needed to recover the CA private key in the initial cryptographic device.

6.1.15. Private key transfer into a cryptographic module

Certification Authorities' private keys are directly generated in the cryptographic modules of production of CIG.

6.1.16. Private Key Storage on Cryptographic Module

The Certification Authority private keys are encrypted and stored in the production cryptographic modules of CIG.

6.1.17. Method of activating the private key

CIG private key is activated by the running of the corresponding safe boot procedure of the cryptographic module, by the indicated persons in section 6.1.11.

The CA keys are activated by a process m of n (3 of 6).
The activation of the private keys of the Intermediate CA is managed with the same process of m of n of the CA keys.

6.1.18. Method of deactivating the private key

For deactivation of CIG private key, the same steps outlined in the corresponding manual of the cryptographic equipment are followed.

6.1.19. Method of destroying the private key

Before destroying the keys, a revocation of the Certificate of the public keys associated with them will be issued.

Devices that have stored any part of CIG private keys are physically destroyed or reset to low level. For disposal, the same steps outlined in the corresponding manual of the cryptographic equipment are followed.

Finally, the backups will be destroyed in a safety way.

The Signer keys on software may be destroyed by deleting them following the instructions of the application.

The Signer keys in hardware may be destroyed by a special computer application at the offices of the RA or CIG.

6.1.20. Cryptographic modules classification

See Section 6.2.1

Other aspects of key pair management

6.1.21. Public key Archival

CIG archives its public keys routinely, according to the practices established in this document.

6.1.22. Public and private key usage periods

Periods of use of the keys are determined by the duration of the Certificate, after which they cannot continue to be used, except that public key may continue to be used for signature verification.

CIG does not recommend use of the certificates for encryption.

Activation data

6.1.23. Activation data generation and installation

Activation data of the devices that protect CIG private keys are generated in accordance with the established practices in section 6.1.11 and key procedures ceremony.

The creation and distribution of such devices is recorded.

Likewise, CIG generates the activation data in a safe way.

6.1.24. Activation data protection

Activation data devices that protect the private keys of the Certification Authority Root and Subordinates, are protected by the holders of cards managers of the cryptographic modules, as stated in the document of the keys ceremony.

The Signer is responsible for protecting his/her private key, with a password or Personal Identification Number (PIN) as complete and complex as possible. The Signer must remember the password or PIN.

ATechnical security controls

CIG's PKI infrastructure provider uses reliable systems to provide certification services. CIG's PKI infrastructure provider has made controls and computer audits to establish its

proper computer activity management with the level of security required in the system management of electronic certification.

Regarding the information security, CIG's PKI infrastructure provider applies the certification scheme controls on management systems ISO 27001.

Equipment used are initially configured with appropriate security profiles by CIG's PKI infrastructure provider staff, in the following aspects:

- Setting up the operating system.
- Setting up the application security.
- Correct sizing of the system.
- User and permissions settings.
- Setting event Log.
- Backup and recovery plan.
- Antivirus settings.
- Requirements of network traffic.

6.1.25. Specific computer security technical requirements

Each of CIG's PKI infrastructure provider's server includes the following functionalities:

- Access control of the Subordinate CA services and privilege management.
- Imposition of separation of duties for managing privileges.
- Identification and authentication of roles associated to identities.
- Archive of the signer and Subordinate CA history and audit data.
- Audit events related to security.
- Self-diagnosis of safety related with the Subordinate CA services.
- Recovery mechanisms of keys and Subordinate CA system.

The stated functionalities are performed through a combination of operating system, PKI software, physical protection and procedures.

6.1.26. Computer security rating

The CA and RA used by CIG are reliable.

Life cycle technical controls

6.1.27. System development controls

The applications are developed and implemented by CIG (via a public key infrastructure provider) in accordance with the development and change control standards.

The applications have methods for verifying the integrity and authenticity, as well as the correction of the version to use.

6.1.28. Security management controls

CIG (partially via a public key infrastructure provider) develops the precise activities for training and employee awareness of security. The materials used for training and descriptive documents processes are updated after approval by a group for security management. An annual training plan is used.

CIG requires by contract equivalent security measures be applied to any external provider involved in the certification tasks of the relying electronic service.

6.1.28.1. Classification and management of information and goods

CIG's public key infrastructure provider maintains an inventory of assets and documentation and a procedure for the management of this material to guarantee its use.

CIG's public key infrastructure provider security policy details the procedures of information management where it is classified according to its level of confidentiality.

The documents are classified into three levels: UNCLASSIFIED, INTERNAL USE and CONFIDENTIAL.

6.1.28.2. Management operations

CIG's public key infrastructure provider has an appropriate process management and incident response, by implementing a warning system and the generation of periodic reports.

In CIG's public key infrastructure provider security document the incident management process is developed in detail.

CIG's public key infrastructure provider has documented all the procedure relative to the roles and responsibilities of the staff involved in the control and manipulation of elements contained in the certification process.

6.1.28.3. Treatment of supports and safety

All documents are treated safely in accordance with the requirements of the classification of information. The documents that contain sensitive information are destroyed safely if they are not going to be required again.

Planning system

CIG's PKI infrastructure provider's Systems department keeps track of the capabilities of the equipment. In conjunction with the implementation of resources' control, each system can provide a possible re-sizing.

Reports of incidents and response

CIG's public key infrastructure provider has a procedure for follow-up of incidents and its resolution, where the answers and an economic evaluation are registered, which supposes the resolution of the incident.

Operational procedures and responsibilities

CIG via its PKI infrastructure provider appoints persons responsible for performing daily operations in addition to those appointed with trusted roles.

6.1.28.4. Access system management

CIG's PKI infrastructure provider makes all efforts that are reasonable available to confirm that the system access is limited to authorised persons.

In particular:

CA General

- Controls based on firewalls, antivirus and IDS high availability are available.
- Sensitive data is protected by cryptographic techniques or controls with strong identification.
- CIG's PKI infrastructure provider has a documented procedure for managing the users' authorisations and cancellations and access policy, detailed in its policy of security.
- CIG's PKI infrastructure provider has procedures to ensure that operations are performed in accordance with policy roles.
- Each person has associated a role to perform the certification operations.
- CIG's PKI infrastructure provider staff is responsible for its actions by the confidentiality agreement signed with the Company in accordance with it's contractual obligations to CIG.

Certificate generation

Authentication for Issuance process is performed through a system of m of n operators for activating CIG private key.

Revocation management

Revocation will be performed by strong authentication to the applications of an authorised administrator. Logs systems will generate the tests that guarantee non-repudiation of the action taken by CIG's public key infrastructure provider administrator.

Revocation status

The application for the status of the revocation offers access control based on the authentication with Certificates or dual factor identification to avoid the attempt to change of the status information of the revocation.

6.1.28.5. Life cycle management of cryptographic hardware

CIG via its PKI infrastructure provider ensures that the cryptographic hardware used for signing Certificates is not tampered with during its transport by inspecting the delivered material.

The cryptographic hardware moves on prepared supports to prevent any manipulation.

CIG via its PKI infrastructure provider records all relevant device information to add to the catalogue of assets.

The use of cryptographic hardware for signature Certificates requires the use of at least two trusted employees of CIG's PKI infrastructure provider.

CIG via its PKI infrastructure provider makes periodic tests to ensure the correct functionality of the device.

Only reliable personnel manipulate the cryptographic hardware device.

CIG's signature private key stored in the cryptographic hardware will be erased once the device is removed.
CIG system configuration, as well as its modifications and updates are documented and controlled.

Changes or updates are authorised by the security officer and they are reflected in the corresponding team's working minutes. At least, two reliable persons of CIG's PKI infrastructure provider perform these settings.

Network security controls

CIG via its PKI infrastructure provider protects the physical access to network management devices and has an architecture that directs the traffic generated based on

its features of security, creating clearly defined network sections. This division is performed with firewalls.

Confidential information is NOT transferred through unsecured networks; it is performed in an encrypted way using SSL protocols or VPN system with dual factor authentication.

Engineering controls of cryptographic modules

Cryptographic modules are subject to engineering controls provided in the standards indicated along this section.

The key generation algorithms used are commonly accepted for the use of the key to which they are intended.

All cryptographic operations for CIG are performed in modules with FIPS 140-2 level 3 certification.

7. Certificates profiles and CRLs

Certificate profile

All Certificates issued under this policy comply the X.509 standard version 3, RFC 3739 and ETSI 101 862 “Certificate Profile”. The documentation relating to the profiles of the policy EN 319 412 can be requested from CIG.

7.1.1. Version number

CIG issues Certificates X.509 Version 3

7.1.2. Certificate extensions

Certificates extensions are detailed in the profiles documents, which are accessible from CIG’s web (https://myeid.egov.ky).

In this way, it is allowed to keep more stable versions of the Certification Practice Statement and decouple them from frequent adjustments in the profiles.

7.1.1. Object identifier (OID) of the algorithms

The object identifier of the signature algorithm is:

- 1.2.840.113549.1.1.11 sha256WithRSAEncryption
- The object identifier of the public key algorithm is:
- 1.2.840.113549.1.1.1 rsaEncryption

7.1.2. Names format

Certificates must contain the required information for its use, as determined by the appropriate policy.

7.1.3. Names restriction

Names contained in the Certificates are restricted as “Distinguished Names” X.500, which are unique and not ambiguous.

7.1.4. Object identifiers (OID) of Certificates types

All Certificates include an identifier of the Certificates policy under which they have been issued, in accordance with the indicated in this document.

CRL profile

7.1.5. Version number

CRLs issued by CIG are from version 2.

7.1.6. OCSP profile

According to standard IETF RFC 6960.

8. Compliance audit

Frequency of compliance audit

CIG's public key infrastructure provider conducts a compliance audit annually, in addition to internal audits carried out at its own discretion or at any time, due to a suspected breach of any security measure.

Identification and qualification of the auditor

An external independent audit consultancy firm performs the audits, demonstrating technical competence and experience in computer security, information systems security and compliance audits of public key certification services and related elements.

Auditor relationship to audited entity

Audit firms are of renowned prestige, with specialized departments in conducting IT audits, so there is no conflict of interest that could undermine its performance in relation to CIG.

Topics covered by audit

The audit verifies that:

a) The entity has a management system, which ensures the quality of service.
b) The entity complies with the requirements of the Certification Practice Statement and other documentation related to the issuance of the various digital Certificates.
c) The Certification Practice Statement and other related legal documentation comply with the agreed with CIG and the established in the current regulation.
d) The entity properly manages its information systems.

Specially, the topics covered by audit are as follows:

a) CA, RA's and related elements processes.
b) Information systems.
c) Protection of the data processing centre.
d) Documents.

Actions taken as a result of lack of conformity

Once the management has received the auditor's compliance report, the deficiencies and non-conformities found are analysed with the auditing entity. This report also develops and implements the corrective policies that tackle these deficiencies.

If CIG's public key infrastructure provider is unable to develop and/or implement the corrective measures or if the deficiencies found pose an immediate threat to the system security or integrity, it shall immediately inform CIG, which can perform the following actions:

- Cease operation temporarily.
- Revoke the CA key and regenerate the infrastructure.
- Terminate the CA service.
- Other complementary actions needed.

Treatment of audit reports

Audit reports results are delivered to CIG within a maximum period of 15 days after completion of the audit.

9. Business and legal requirements

Fees

9.1.1. Fees

9.1.2. CIG can establish a fee for: Certificate issuance, Certificate renewal, certificate access, Certificate status information access, and other services associated with Certificates. If such fee is established details will be published and signers will be notified.

Financial capacity

CIG and its public key infrastructure provider each have enough economic resources to continue its operations, to comply with its obligations and to confront the risk of liability for claim and damages, in relation to the management of the services finalisation and termination plan.

Insurance coverage for signers and Relying Parties in Certificates

CIG's public key infrastructure provider has a warranty coverage of its civil liability, through an insurance of professional liability, for relying electronic services.

Confidentiality

9.1.3. Confidential information

CIG, and its public key infrastructure provider where relevant, keeps in confidence the following information:

- Certificate requests, approved or rejected, and all other personal data obtained for issuance and maintenance of Certificates, except the information indicated in next section.

- Private keys generated and/or stored by the certification services provider.
- Transaction record, including full records and audit records of the transactions.
- Internal and external transaction records created and/or kept by the Certification Authority and its auditors.
- Sensitive aspects of business continuity and emergency plans.
- Security plans.
- Documentation of operations, archiving, automatisation and other analogous matters.
- All other information identified as 'Confidential'.

9.1.4. Non confidential information

The following information is considered non-confidential:

- Certificates issued or in the process of issuance.
- Information linking the signers to a Certificate issued by CIG.
- Name and surname of the natural person identified on the Certificate, as well as any other related or personal information of the holder, in the event that it is important according to the purpose of the Certificate.
- Email of the natural person identified on the Certificate, or email assigned to the signer, in case it is important according to the purpose of the Certificate.
- Economic uses and limits outlined in the Certificate.
- Validity period of the Certificate, as well as date of issue and expire date of the Certificate.
- Serial number of the Certificate.
- The different status or conditions of the Certificate and starting date for each, specifically: pending of generation and/or delivery, valid, revoked, suspended or expired and the reason that caused the change of status.
- The Certificate Revocation Lists (CRLs), and the remaining revocation status information.
- The information contained in the Certificate repository.
- Any other information not indicated in section 9.3.1.

9.1.5. Information disclosure of suspension and revocation

See previous section.

9.1.6. Legal disclosure of information

Records that support the reliability of the data contained in the Certificate will be disclosed if required to prove the evidence of the certification in legal proceedings, even without the consent of the Certificate Signer.

CIG will indicate these circumstances in the privacy notice under section 0.

9.1.7. Information disclosure on request of the owner

Will be in accordance with Subject access requests under the Data Protection Act (2021 Revision), or otherwise in accordance with the Data Protection Act (2021 Revision).

9.1.8. Other information disclosure circumstances

Not stipulated.

Personal data protection

Personal data collected and processed by the CIG under this CPS will be treated in accordance with the Privacy Notice which can be found at https://myeid.gov.ky/app/privacy .

Intellectual property rights

9.1.9. Property of Certificates and revocation information

CIG exerts any and all intellectual property rights in relation to the Certificates it issues, without any prejudice of the rights of the signers, key holders and third parties, to which it grants non-exclusive license to reproduce and distribute Certificates, free of charge, as long as the reproduction is full and does not alter any element of the Certificate, and is necessary in relation to digital signatures and/or encryption systems within the scope of the Certificate use, and according to the documentation that links them.

The same rules are applicable to the use of the information as to Certificate revocation.

9.1.10. Property of the Certification Practice Statement

CIG exerts all intellectual property rights in relation to this Certification Practice Statement.

9.1.11. Property of information relating to names

The natural person identified on the Certificate, preserves all rights in relation to any brand, product or trade name included on the Certificate.

The signer owns the distinguished name of the Certificate, consisting of the information specified in this document.

9.1.12. Property of keys

The signers of the Certificates are the owners of the key pair.

When a key is divided in parts, all parts of the key are property of the owner of the key.

Obligations and liability

9.1.13. CIG obligations

CIG endeavours to ensure, that it complies with all requirements established in the Certification Practice Statement, and it is responsible for ensuring compliance with the procedures described, according to the instructions contained in this document.

CIG provides certification services in accordance with this Certification Practice Statement.

Prior to issuance and delivery of the Certificate to the signer, CIG informs the signer of the terms and conditions related to the use of the Certificate, price and use limitations, through policies included in this document.

CIG binds all the parties involved in the certification service provision through this certification practices statement, at least with the following:

- Indication of the applicable policy, indicating that the Certificates are not issued to the public.
- Demonstration that the information contained in the Certificate is accurate.
- Consent for the publication of the Certificate in the Repository and third-party access.
- Consent for storing information used for the Signer registration and the termination of such information to third parties, in case of termination of operations of the Certification Authority without revocation of valid Certificates.
- Limits of use of the Certificate, including those established in section 1.1.8.
- Information about how to validate a Certificate, including the requirement to check the Certificate status and the conditions under which it can reasonably trust the Certificate, which applies when the signer acts as a Relying Party in the Certificate.
- The extent to which the liability of CIG is guaranteed.
- Limitations of liability, including the uses for CIG accepts or excludes its liability.
- Certificate request information file period.
- Audit registry file period.
- Applicable procedures of dispute settlement.

- Applicable Law and competent jurisdiction.

9.1.14. Representations and warranties offered to signers and Relying Parties in Certificates

CIG warrants to the signer, at least:

- It uses reasonable endeavours to ensure the correctness of information in Certificate signing requests to prevent factual errors in the information in the Certificates, known or made by the Certification Authority.
- No factual errors in the information in the Certificates, due to lack of due diligence of the Certificate request or to its creation.
- The Certificates comply with all the material requirements established in the Certification Practice Statement.
- Revocation services and the use of the Repository comply with all material requirements established in the Certification Practice Statement.

CIG warrants to the third party that trusts in the Certificate it has used its uses reasonable endeavours to ensure, at least:

- The information contained or incorporated by reference in the Certificate is accurate, except when the opposite is indicated.
- In case of Certificates published in the Repository, that the Certificate has been issued to the identified signer and the Certificate has been accepted, in accordance with section 0.
- The approval of the Certificate request and in the Certificate issuance all the material requirements established in the Certification Practice Statement have been complied with.
- Speed and assurance with the services provision, especially with revocation services and Repository.

In addition, CIG represents to the signer and the Relying Party in the Certificate:

- The Certificate has the information that a Certificate must have, in accordance with Electronic Transactions Act (2003 Revision).

- Confidentiality is preserved during the process if private keys are generated by the signer or, where appropriate, the natural person identified on the Certificate.

9.1.15. Rejection of other warranties or guarantees

CIG rejects any other warranties or guarantee, except the ones covered in section 9.1.14.

9.1.16. Limitation of liability

CIG limits its responsibility to the issuance and management of Certificates and key pairs of signers supplied by the Certification Authority.

9.1.17. Indemnity clauses

9.1.17.1. Signer indemnity clause

CIG includes in the contract with the signer, a clause whereby the signer agrees to indemnify the CIG of any damage from any action or omission that results in liability, damage or loss, expenses of any kind, including judicial and legal representation that may be incurred by the publication and use of the Certificate, due to any of the following causes:

- False or inaccurate statements made by the Signer.
- Applicant error when providing enrolment request data, if there was fraud, negligence or omissions in providing de data upon their enrolment.
- Private key protection negligence, when using a system or by failure to maintain necessary precautions to avoid its compromise, loss, disclosure, modification or unauthorised use.
- Use of a name (including names, email address and domain names), or other Certificate information that infringes intellectual or third party industrial property of others by the signer.

9.1.17.2. Relying Party in the Certificate indemnity clause

CIG informs the Relying third parties, that they agree that CIG is not responsible for any damage from any action or omission that results in liability, damage or loss, expenses of any kind, including court and legal representation that may be incurred by the reliance on the certificate, due to any of the following causes:

- Breach of the obligations of the relying third party in the certificate.
- Reckless trust in a certificate.
- Lack of checking of the certificate status, to determine that it is not suspended or revoked.

9.1.18. Force majeure

The CIG shall not be deemed to be in breach of this Certification Practice Statement nor liable for delay in performing, or failure to perform, any of its obligations under it if such delay or failure results from events, circumstances or causes beyond its reasonable control and which could not have been avoided by the use of reasonable diligence.

9.1.19. Applicable law

CIG informs that the applicable law in relation to functions carried out under, or in relation to, this Certification Practice Statement including the policy and practices of certification, is the law of the Cayman Islands.

9.1.20. Severability, survival, entire agreement and notification clauses

CIG informs the severability, survival, entire service agreement and notification clauses:

- Severability: the invalidity of a clause will not affect the rest of the contract.
- Survival: certain rules will remain in force after the completion of the regulatory service of the legal relationship between the parties including: requirements of sections 9.6.1 (Obligations and liability), 8 (Compliance audit) and 9.3 (Confidentiality).
- Entire agreement: This CPS, the Acceptance Sheet and the Terms of Use collectively form the entire agreement between the parties.

- Under the notification clause, it will be established the procedure by which the parties mutually report incidents.

9.1.21. Competent jurisdiction clause

The competent jurisdiction in relation to any matter arising in connection with this Certification Practice Statement that involves the CIG, is the Cayman Islands.

9.1.22. Resolution of conflicts

The Registrar has a complaints procedure at https://myeid.egov.ky