Queensland Digital Licence PKI

Certificate Policy and Certification Practice Statement

April 2023

Copyright

Licence

CC BY licence summary statement

In essence, you are free to copy, communicate and adapt this work, as long as you attribute the work to the State of Queensland (Department of Transport and Main Roads). To view a copy of this licence, visit: https://creativecommons.org/licenses/by/4.0/

Translating and interpreting assistance

The Queensland Government is committed to providing accessible services to Queenslanders from all cultural and linguistic backgrounds. If you have difficulty understanding this publication and need a translator, please call the Translating and Interpreting Service (TIS National) on 13 14 50 and ask them to telephone the Queensland Department of Transport and Main Roads on 13 74 68.

Disclaimer

While every care has been taken in preparing this publication, the State of Queensland accepts no responsibility for decisions or actions taken as a result of any data, information, statement or advice, expressed or implied, contained within. To the best of our knowledge, the content was correct at the time of publishing.

Feedback

Please send your feedback regarding this document to: dlpki@qld.gov.au

Contents

1 Introduction

This document is a Certificate Policy (CP) and Certification Practices Statement (CPS), whose purpose is to describe the security and operational practices in use by the Public Key Infrastructure (PKI) supporting Queensland's electronic ID documents such as the mobile Driving Licence (mDL).

The document is structured according to RFC 3647 [5] and explains the operation, validation, issuance, management, and revocation of certificates in this PKI, as well as the requirements and responsibilities to be adopted by Subscribers and Relying Parties of this PKI. This document replaces the need for separate Subscriber and Relying Party agreements.

1.1 Overview

In a PKI, the Certification Authority's (CA) practices in creating, signing and issuing certificates, and in revoking invalid certificates, are of central utmost importance to the reliability and trustworthiness of a Public Key Infrastructure ("PKI").

This CP/CPS is specifically applicable to the Queensland IACA (Queensland Issuing Authority Certification Authority). It leverages the following standards:

- RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework [5]
- RFC 5280 - Internet X.509 PKI - Certificate and CRL Profile [2]
- ISO/IEC 18013-5:2021 - Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application [1]

These practices are valid exclusively for certificates that are issued by the IACA for signing data objects of mDL and other electronic ID documents.

This document specifies how its practices and controls are implemented, and how the IACA meets the specified requirements described in ISO/IEC 18013-5:2021.

1.2 Document Name and Identification

This document is the Queensland Digital Licence PKI Certificate Policy (CP) and Certification Practice Statement (CPS).

1.3 PKI Participants

1.3.1 Certification Authorities

The Queensland Digital Licence PKI is composed of a root CA, having a self-signed root certificate, corresponding to the Issuing Authority Certificate Authority (IACA) as defined in international standard ISO/IEC 18013-5:2021 [1]. Throughout this document, the terms PKI, CA and IACA may be used interchangeably to refer to the Certification Authority issuing certificates and CRLs.

Within this PKI, the IACA issues the following certificates:

- Document Signer (DS) certificates
- JWS Signer certificates
- TLS certificates
- IACA link certificates

- IACA CRLs

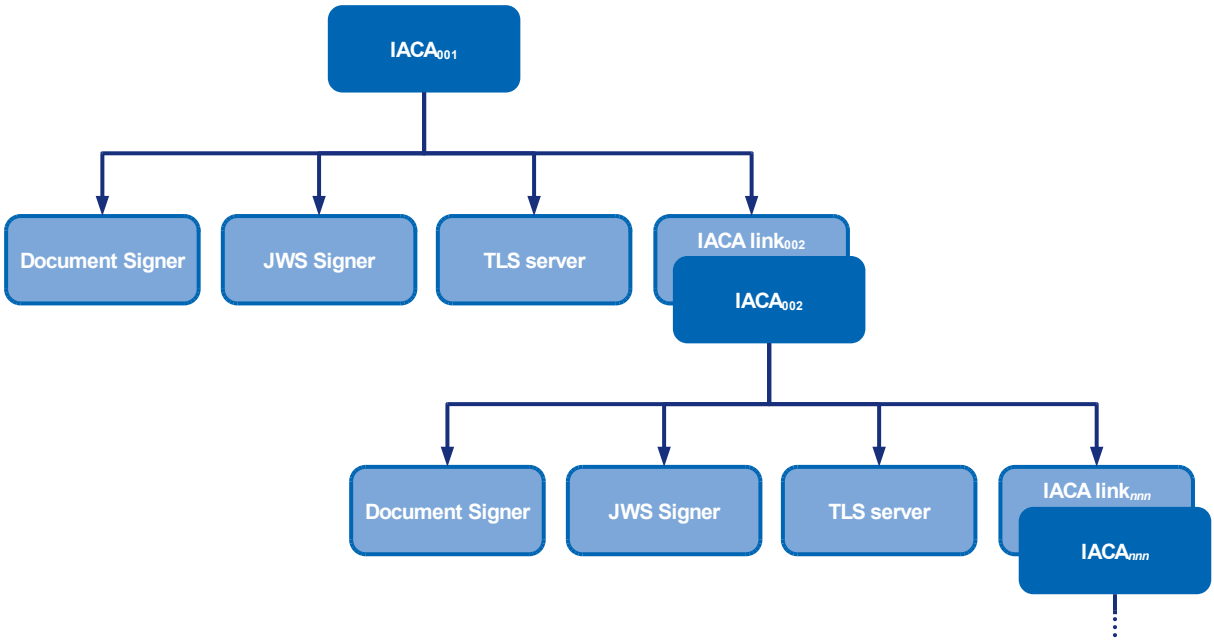

Figure 1 - PKI Hierarchy

Subject to explicit authorisation of this PKI policy administration (see section 1.5), the IACA may be signed by other Certification Authorities.

1.3.2 Registration Authorities

The IACA acts as a Registration Authority for the certificate requests required by mDL and other electronic ID systems since it validates the application data provided by the subscribers in enrolment and revocation requests.

1.3.3 Subscribers

Subscribers of this PKI are organisations authorised by the Queensland Government to operate services issuing mDLs or other similar electronic ID documents. These organisations are typically governmental agencies and departments, which in turn may delegate the operation of the issuing services to other governmental organisations or companies.

Under this policy, “Subscriber” (the entity which requests the certificate and uses it) and “Subject” (the entity to whom the credential is bound) can be used interchangeably.

1.3.4 Relying Parties

A relying party is any individual, entity or service that acts in reliance of a certificate and/or a digital signature issued under this IACA.

In this CPS, “relying parties” refer to all services and applications (including applications for mobile devices – “apps”), whether run by persons, companies or governmental bodies and agencies, requesting to verify the certificates issued by the IACA with the objective of verifying the authenticity and integrity of an mDL or other electronic ID document issued by the Queensland Government.

1.3.5 Other Participants

1.3.5.1 VICAL Providers

The IACA certificate may be distributed through VICAL (Verified issuer certificate authority list) providers.

Relying Parties may use VICALs of one of or more providers as trust anchors for the verification of the certificates.

The responsibilities and risks of assessment, selection and usage of such VICALs is entirely up to the Relying Parties.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The IACA issues its own self-signed certificate and an IACA link certificate, which binds the new key to the previous key in IACA rollovers (re-keys).

The IACA certificates are used to issue Document Signer, JWS and TLS certificates – end entity certificates, also referred herein as Subscriber certificates – in support of the mDL and other related electronic ID documents issued by the Queensland Government, as well as establishing a trust point in the certificate hierarchy.

The Subscriber certificates are intended to be used in services under the supervision of the Queensland Government to protect the integrity and authenticity of the electronic ID document (e.g. mDL) and the confidentiality of the established communication channels. Specifically:

- Document Signer certificate is used to sign and verify the integrity and authenticity of the ISO/IEC 18013-5 [1] “mdoc” object;
- JWS certificate is used to sign and verify the integrity and authenticity of the ISO/IEC 18013-5 [1] JSON Web Token (JWT);
- TLS certificate is used to verify the authenticity of the endpoint providing server retrieval (as in section 9.2 of ISO/IEC 18013-5 [1]) and protect the confidentiality of the communication channel.

Additionally, the Queensland PKI issues CRLs periodically, as well as link certificates on IACA rollovers.

1.4.2 Prohibited Certificate Uses

Certificates shall only be used to the extent the usage is consistent with applicable law, including, but not limited to, applicable cryptography import and export controls and/or laws.

IACA certificates shall not be used for any functions other than CA functions. In addition, end entity certificates (e.g. DS, JWS, TLS) issued by the IACA shall not be used as IACA certificates, or for any other function except the appropriate uses described above.

1.5 Policy administration

1.5.1 Organisation Administering the Document

The organisation responsible for this document is:

Name: Queensland Government - Department of Transport and Main Roads

Address: GPO Box 1549

Brisbane QLD 4001

1.5.2 Contact Person

The contact person is:

Name: DL PKI Policy Group

Email: dlpki@qld.gov.au

1.5.3 Person Determining CP/CPS Suitability for the Policy

The PKI Policy Management Group is responsible to verify and confirm all the information in this document and its conformance with the applicable requirements.

1.5.4 CPS Approval Procedures

Approval of this document and subsequent amendments (or updates) shall be made by the PKI Policy Management Group. Amendments (or updates) shall be published in the form of new releases of the document. Amendments and updates supersede any designated or conflicting provisions of the referenced version of this document, as described in section 9.12 Amendments (page 51).

1.6 Definitions and Acronyms

Below is a glossary of the definitions, abbreviations and acronyms used in this document.

Terms, abbreviations, and acronyms	Meaning
Authentication	The process of establishing that individuals, organisations, or things are who or what they claim to be. In the context of a PKI, authentication can be the process of establishing that an individual or organisation applying for or seeking access to something under a certain name is, in fact, the proper individual or organisation. This corresponds to the second process involved with identification, as shown in the definition of "identification" below. Authentication can also refer to a security service that provides assurances that individuals, organisations, or things are who or what they claim to be or that a message or other data originated from a specific individual, organisation, or device. Thus, it is said that a digital signature of a message authenticates the message's sender.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certification Authority (CA)	An authority trusted and authorised to issue and manage X.509 Public Key Certificates and CRLs.
Certification path	An ordered sequence of certificates that, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates, and providing access to them, in accordance with specific requirements (e.g., requirements specified in the Certificate Policy, or requirements specified in a contract for services).
Certification Revocation List (CRL)	A list maintained by a CA of the certificates which it has issued that are revoked prior to their stated expiration date.

Terms, abbreviations, and acronyms	Meaning
Digital Signature	The result of a transformation of a message by means of a cryptographic system using private/public key pairs and certificates such that the recipient of the message and signature can determine: (1) whether the transformation was created using the Private Key which complements the public key in the certificate; and (2) whether the message has been altered since the transformation was made.
DN	Distinguished Name
DS	Document Signer
End entity	User of PKI certificates and/or end user system that is the subject of a certificate.
HSM	Hardware Security Module
IACA	Issuing Authority Certificate Authority
Identification	The process of establishing the identity of an individual or organisation, i.e., to show that an individual or organisation is a specific individual or organisation. In the context of a PKI, identification refers to two processes: (1) establishing that a given name of an individual or organisation corresponds to a real-world identity of an individual or organisation, and (2) establishing that an individual or organisation applying for or seeking access to something under that name is, in fact, the named individual or organisation. A person seeking identification may be a certificate applicant, an applicant for employment in a trusted position within a PKI participant, or a person seeking access to a network or software application, such as a CA administrator seeking access to CA systems.
Intellectual Property Rights (IPR)	Includes copyright works, databases, data, designs, discoveries, inventions, improvements, know-how, confidential information, all title, rights and interests to and in all of these or arising out of them (whether such rights exist, or are of a kind which exist, at the time of this agreement or whether they or that kind only come into existence afterwards), applications for and registrations of them and the rights in them, and the right to apply for any form of protection for any of these things and rights (whether such rights exist, or are of a kind which exist, at the time of this agreement or whether they or that kind only come into existence afterwards) In each case it includes the aforesaid title, rights and interests in every part of the world for their full term, including any renewals and extensions, the right to receive any income from them, and the right to sue in respect of any past, continuing or future infringement of any of them, and to claim and receive damages (or an account of profits) and interest in respect of any such infringement.
JWS	JSON Web Signature
mDL	Mobile Driving Licence
OID	Object Identifier
Online Certification Status Protocol (OCSP)	Protocol for determining the status of a certificate, as defined by the Internet Engineering Task Force (RFC 6960).
Policy qualifier	Policy-dependent information that may accompany a CP identifier in an X.509 certificate. Such information can include a pointer to the URL of the applicable CPS or relying party agreement. It may also include text (or number causing the appearance of text) that contains terms of the use of the certificate or other legal information.

Terms, abbreviations, and acronyms	Meaning
Registration Authority (RA)	An entity that is responsible for one or more of the following functions: the identification and authentication of certificate applicants, the approval or rejection of certificate applications, initiating certificate revocations or suspensions under certain circumstances, processing subscriber requests to revoke or suspend their certificates, and approving or rejecting requests by subscribers to renew or re-key their certificates. RAs, however, do not sign or issue certificates (i.e., an RA is delegated certain tasks on behalf of a CA).
Relying Party	An individual or an organisation, who acts in reliance on a certificate and digital signatures, verified using that certificate.
Root Authority	The Certification Authority (CA) at the top of a CA hierarchy.
Subject	The holder of a private key corresponding to a public key. The term "Subject" can, in the case of an organisational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject's Certificate.
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organisational Certificate, an organisation that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorised to use, the private key that corresponds to the public key listed in the Certificate.
TLS	Transport Layer Security
TMR	Department of Transport and Main Roads
VICAL	Verified Issuer Certificate Authority List
UPS	Uninterruptible Power Supply
URI	Uniform Resource Identifiers

2 Publication and Repository Responsibilities

2.1 Repositories

The Security Officers Working Group is responsible for the repository of this PKI.

The repository is available in a publicly accessible web site at URI http://dlpki.qld.gov.au.

Further to this repository, the IACA certificate may be distributed through VICALs (refer to section 1.3.5.1 VICAL Providers, page 9).

2.2 Publication of Certification Information

The following information is published in the repository:

- IACA self-signed certificates and link certificates;
- IACA CRLs for non-expired IACA certificates;
- This CP/CPS document; and
- Contact information for this PKI.

2.3 Time and Frequency of Publication

Updates to this policy document are published in the repository after approval by the PKI Policy Management Group, in accordance with section 1.5.4.

New IACA certificates are published after they are generated on a key ceremony.

The CRLs are regularly issued and updated in the repository within an interval window of 60 to 90 days. Additional CRLs may be issued and published earlier due to exceptional circumstances (e.g. certificate revocation).

2.4 Access Controls on Repositories

Information published in the repository is available online and subject to access control mechanisms that allow reading access only. Security measures are established to prevent non-authorised parties from adding, deleting or modifying repository files and/or contents.

3 Identification and Authentication

3.1 Naming

The naming conventions adopted for the certificates in this PKI follow the rules defined in ISO/IEC 18013-5:2021 [1].

3.1.1 Types of Names

Certificates and CRLs issued under this PKI contain X.501 Distinguished Names (DN) in the Issuer and Subject fields, where applicable.

For the **IACA self-signed certificates**, the Subject and Issuer DNs are as follows:

Attribute	Value
Country (C)	`AU`
State or Province Name (ST)	`AU-QLD`
Organisation (O)	`Queensland Government`
Serial Number	`001` *(increased monotonically at each IACA renewal)*
Common Name (CN)	`IACA Digital Licence Queensland - Australia`

For the **IACA link certificates**, the Subject DN is set with the new IACA certificate and the Issuer DN with the legacy IACA being rolled over. For example, for the first IACA renewal, Issuer DN is:

`C=AU, ST=AU-QLD, O=Queensland Government, SerialNumber=`**`001`**`, CN= IACA Digital Licence Queensland - Australia`

and Subject DN is:

`C=AU, ST=AU-QLD, O=Queensland Government, SerialNumber=`**`002`**`, CN= IACA Digital Licence Queensland – Australia`

(note the difference in the `SerialNumber` component)

Document Signer certificates have the Issuer DN as in the IACA certificate and the Subject DN is set as follows:

Attribute	Value

Country (C)	AU
State or Province Name (ST)	AU-QLD
Organisation (O)	Queensland Government
Common Name (CN)	Digital Licence Document Signer Queensland – Australia

JWS certificates have the Issuer DN as in the IACA certificate and the Subject DN is set as follows:

Attribute	Value
Country (C)	AU
State or Province Name (ST)	AU-QLD
Organisation (O)	Queensland Government
Common Name (CN)	Digital Licence JWS Signer Queensland – Australia

TLS certificates have the Issuer DN as in the IACA certificate and the Subject DN is set as follows:

Attribute	Value
Country (C)	AU
State or Province Name (ST)	AU-QLD
Organisation (O)	Queensland Government
Common Name (CN)	Digital Licence Server Retrieval Queensland – Australia

TLS certificates shall also include at least one (1) dnsName in the Subject Alternative Name.

3.1.2 Need for Names to be Meaningful

Names in certificates issued by Queensland IACA are fixed and represent the organisation and/or the service where the certificate is used.

DNs may include variable components set as sequence numbers to help identifying the issuing IACA.

DNS names included in the Subject Alternative Name extension of TLS certificates correspond to hostnames under the effective control of the Subscriber.

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymous and pseudonymous certificates names are not allowed.

3.1.4 Rules for interpreting various name forms

The naming conventions for both the IACA and end entity certificates in this PKI must be processed as defined in ISO/IEC 18013-5:2021 [1].

3.1.5 Uniqueness of Names

Subject Distinguished Names of end entity certificates are unique to the respective services and reused between renewals and/or rekeys.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 Initial Identity Validation

3.2.1 Method to prove possession of private key

3.2.1.1 IACA Certificate

The possession of the IACA private key is guaranteed by the elements of the identified working groups attending the key ceremony.

3.2.1.2 End entity certificates

An end entity certificate (e.g. DS, JWS, TLS) applicant must hold the private key corresponding to the public key to be listed in the certificate. After the public and private keys are generated, a Certificate Signing Request (CSR) in PKCS#10 [6] format shall be generated, containing the public key to be certified and a signature by the correspondent private key as proof of possession.

The proof of possession signature is verified by the PKI prior to the certificate issuance. The certificate request is rejected if the proof of possession can not be correctly verified.

3.2.2 Authentication of Organisation Identity

Certificates issued under this Policy are exclusively issued to and by the Queensland Government, its agencies, departments or other internal organisation units operating issuing services of mDL documents.

3.2.3 Authentication of Individual Identity

Origin of certificate requests is limited to a list of approved certificate applicants, duly authorised and identified, acting and/or operating a service in representation or on behalf of the Subscriber.

3.2.4 Non-verified Subscriber Information

No non-verified subscriber data is included in certificates issued under this PKI.

3.2.5 Validation of Authority

End entity certificate requests are received from an approved list of individuals duly authorised and in representation of the services supporting mDL and other electronic ID documents supported by this PKI.

The authenticity and integrity of certificate requests is verified by out-of-band mechanisms.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Refer to 3.2 Initial Identity Validation (page 15).

3.3.2 Identification and Authentication for Re-key After Revocation

Refer to 3.2 Initial Identity Validation (page 15).

3.4 Identification and authentication for revocation request

Prior to the revocation of a certificate, it is verified that the revocation has been requested by an authorised entity.

The revocation request includes the DN, serial number and fingerprint of the certificate to be revoked.

The revocation request is approved and processed by a minimum of two members of the PKI Working Groups.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application?

Certificate applications are limited to the Subscribers listed in section 3.2.3 Authentication of Individual Identity (page 15).

4.1.2 Enrolment Process and Responsibilities

4.1.2.1 IACA Certificates

The process for issuing IACA Certificates is under the sole responsibility of the PKI Working Groups, in key ceremonies, following the established processes and procedures.

4.1.2.2 End Entity Certificates

Authorised certificate applicants shall submit the certificate issuance request form, and undergo an enrolment process consisting of:

1. generating the key pair (private and public key);
2. generating the corresponding CSR (PKCS#10 [6] format);
3. calculating the hash (SHA-256) of the CSR;
4. delivering the CSR and certificate issuance form to the System Operators. The Security Officers will verify the identity of the certificate applicants and return a dated and signed copy of the certificate issuance form;
5. receiving the signed certificate issuance form and the certificate issued from the System Operators;
6. returning a dated and counter signed copy of the certificate issuance form.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of all required information is performed under the terms of section 3.2 Initial Identity Validation (page 15).

4.2.2 Approval or Rejection of Certificate Applications

An end entity certificate application is approved if the following criteria is met:

1. successful identification and authentication of all required information in terms of section 3.2 Initial Identity Validation (page 15);
2. certificate issuance request form is correctly filled;

3. valid CSR.

Should any of the above criteria fail, the certificate application is rejected.

4.2.3 Time to Process Certificate Applications

A certificate application shall be processed within 7 days once the certificate request has been approved.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Issuance of the certificates is carried out according to the established procedures.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Refer to section 4.1.2.2.

4.3.3 Notification of Certificate Issuance by the CA to Other Entities

For new IACAs, the repository is updated with the new IACA and IACA-link certificates.

The new IACA and IACA-link certificates are also distributed to TMR, which in turn may be redistributed to any VICAL providers with an established communication channel.

4.4 Certificate acceptance

4.4.1 Conduct Constituting Certificate Acceptance

IACA certificates, IACA link certificates and end certificates are validated against the certificate profiles defined in ISO/IEC 18013-5:2021 [1], and according to the parameters defined in the certificate request form.

Returning a dated and signed copy of the certificate issuance form by the Subscriber applicants, containing the certificate fingerprint (sha256) constitutes certificate acceptance.

4.4.2 Publication of the certificate by the CA

The IACA and IACA-link certificates are published in the Repository (refer to section 2.1).

End entity certificates are not published.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Refer to section 4.3.3.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The use of the private key corresponding to the public key in the certificate is only permitted after certificate acceptance and during the allowed usage period, exclusively for the purposes specified in section 1.4 Certificate Usage (page 9).

Private keys of end entity certificates shall be protected from unauthorised use and shall be erased after the permitted usage period.

4.5.2 Relying Party Public Key and Certificate Usage

Reliance on a certificate must be reasonable under the circumstances.

If the circumstances indicate a need for additional assurances, the relying party must obtain such assurances in order for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties must independently

1. verify that the certificate will be used for an appropriate purpose that is not prohibited or otherwise restricted by this policy (see section 1.4), and
2. assess the status of the certificate and all the certificates in the chain (terminating at a trust anchor accepted by the Relying Party) that issued the certificates relevant to the certificate in question.

If any of the certificates in the certificate chain have been revoked or have expired, the Relying Party is solely responsible for determining whether reliance on a digital signature to be verified by the certificate in question is acceptable. Any such reliance is made solely at the risk of the Relying Party.

If a Relying Party determines that use of the certificate is appropriate, the Relying Party must utilize appropriate software and/or hardware to perform digital signature verification as a condition of relying on the certificate. Moreover, the Relying Party must validate the certificate in a manner consistent with the ISO/IEC 18013-5:2021 certificate profiles [1].

4.6 Certificate Renewal

Certificate renewal means the issuance of a new certificate to the Subscriber without changing the Subscriber's public key or any other information in the certificate.

4.6.1 Circumstance for Certificate Renewal

Renewal of certificates under this PKI may only occur under exceptional circumstances, such as required by modified security requirements or attributes in certificate profiles.

4.6.2 Who May Request Renewal

A renewal may be requested by a minimum of two (2) Security Officers Working Group.

4.6.3 Processing Certificate Renewal Requests

The PKI Policy Management Group analyses the request and approves the renewal is deemed acceptable.

The renewal is then executed according to the documented procedures by the PKI Working Groups in a key ceremony.

4.6.4 Notification of New Certificate Issuance to Subscriber

Refer to section 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate (page 17).

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Refer to section 4.4.1 Conduct Constituting Certificate Acceptance (page 17).

4.6.6 Publication of the Renewal Certificate by the CA

Refer to section 4.4.2 Publication of the certificate by the CA (page 17).

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

Refer to section 4.4.3 Notification of Certificate Issuance by the CA to Other Entities (page 17).

4.7 Certificate Re-key

Certificate re-key is the application for the issuance of a new certificate that certifies the new public key.

4.7.1 Circumstance for Certificate Re-key

Re-key of certificates may occur under the following circumstances:

a) when the planned key usage period is about to expire (refer to section 6.3.2 Certificate Operational Periods and Key Pair Usage Periods, page 35),

b) in the event of a certificate revocation (refer to section 4.9 Certificate Revocation and Suspension, page 20),

c) a change to the certificate profile (refer to section 4.8 Certificate Modification, page 19), and

d) increase of the security parameters (e.g. longer key lengths, change of algorithm, etc).

An accompanying IACA link certificate is issued at any IACA re-key.

4.7.2 Who May Request Certification of a New Public Key

Refer to section 4.1.1 Who Can Submit a Certificate Application? (page 16).

4.7.3 Processing Certificate Re-keying requests

Refer to sections 4.1.2 Enrolment Process and Responsibilities (page 16) and 4.2 Certificate Application Processing (page 16).

In case of re-keying an IACA certificate, a correspondent IACA link certificate is issued, which binds the old key to the new key.

4.7.4 Notification of New Certificate Issuance to Subscriber

Refer to section 4.3.2 Notification to Subscriber by the CA of Issuance of Certificate (page 17).

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Refer to section 4.4.1 Conduct Constituting Certificate Acceptance (page 17).

4.7.6 Publication of the Re-keyed Certificate by the CA

Refer to section 4.4.2 Publication of the certificate by the CA (page 17).

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Refer to section 4.4.3 Notification of Certificate Issuance by the CA to Other Entities (page 17).

4.8 Certificate Modification

Certificate modification refers to the issuance of a new certificate due to changes in the information in an existing certificate, other than the subscriber's public key.

4.8.1 Circumstance for Certificate Modification

Certificate modification shall be combined with a certificate re-key and carried out during the process described in section 4.7 Certificate Re-key (page 19).

4.8.2 Who May Request Certificate Modification

Refer to section 4.7.2 Who May Request Certification of a New Public Key (page 19).

4.8.3 Processing Certificate Modification Requests

Refer to section 4.7.3 Processing Certificate Re-keying requests (page 19).

4.8.4 Notification of New Certificate Issuance to Subscriber

Refer to section 4.7.4 Notification of New Certificate Issuance to Subscriber (page 19).

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Refer to section 4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate (page 19).

4.8.6 Publication of the Modified Certificate by the CA

Refer to section 4.7.6 Publication of the Re-keyed Certificate by the CA (page 19).

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Refer to section 4.7.7 Notification of Certificate Issuance by the CA to Other Entities (page 19).

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

The IACA certificate shall be revoked in case of:

- a major incident such as a key compromise.
- weak of cryptographic obsolete keys.
- Certificate is malformed or incorrectly issued.
- IACA termination.

Any Subscriber certificate may be revoked under the following circumstances:

- Compromise of the private key is suspected or discovered.
- Loss of the private key.
- Certificate is malformed or incorrectly issued.
- Certificate was issued on the basis of false statements.
- Data in the certificate is longer considered valid.
- Termination of business.
- Any major incident or other event.

4.9.2 Who Can Request Revocation

Revocation of certificates shall be requested by two or more representatives from the authorised entities.

In case of Subscriber certificates, the revocation shall be requested by any two elements of the PKI Working Groups or representatives of the Subscribers.

Regarding IACA self-signed and link certificates, since revoking an IACA certificate is an extreme measure with sound impacts, the revocation must be requested by at least two elements from the PKI Policy Management Group.

4.9.3 Procedure for Revocation Request

The authorised individuals shall fill the certificate revocation request form, and undergo a revocation procedure consisting of the following:

- Submit the certificate revocation request form to the System Operators, who will verify it has been signed by two or more duly authorised individuals. A counter signed copy of the form is returned.

If a Subscriber certificate is revoked:

- System Operators revoke the certificate and issue an extraordinary CRL;
- The extraordinary CRL is published in the repository.

If an IACA certificate is revoked:

- System Operators issue a final CRL, signed by the private key corresponding to the certificate being revoked.
- The extraordinary CRL is published in the repository.

4.9.4 Revocation Request Grace Period

Revocation requests shall be submitted as promptly as possible.

4.9.5 Time within Which CA Must Process the Revocation Request

The revocation request is processed within 2 business days after revocation notification.

4.9.6 Revocation Checking Requirement for Relying Parties

A Relying Party is responsible for acquiring and checking the most recent, scheduled CRL, whenever the relying party validates a certificate.

4.9.7 CRL Issuance Frequency

CRLs are issued at least every 90 days, even if no certificate has been revoked.

Each CRL contains a `nextUpdate` value, and a new CRL will be published at or before that time. The IACA will set the `nextUpdate` value when it issues a CRL, to signal the next scheduled CRL will be issued and published no later than that date.

4.9.8 Maximum Latency for CRLs

A CRL will be published to the repository system (section 2.1 Repositories, page 12) within 7 days after generation.

Whenever a certificate is revoked, a new CRL is issued and distributed within a period no longer than 2 business days.

4.9.9 On-line Revocation/Status Checking Availability

On-line revocation/status checking through an OCSP service is not available for this PKI. Revocation/status checking shall be performed using the CRL mechanism as defined in sections 4.9.1 to 4.9.8.

The CRL is published in the PKI repository (section 2.1 Repositories, page 12).

4.9.10 On-line revocation checking requirements

Refer to section 4.9.6 Revocation Checking Requirement for Relying Parties (page 21).

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special Requirements Regarding Key Compromise

Subscribers and Relying Parties are responsible for any losses resulting from the use of a compromised key if they continue to use it with the knowledge that it is compromised.

4.9.13 Circumstances for Suspension

Suspension of certificates is not permitted.

4.9.14 Who Can Request Suspension

No stipulation (refer to 4.9.13 Circumstances for Suspension).

4.9.15 Procedure for Suspension Request

No stipulation (refer to 4.9.13 Circumstances for Suspension).

4.9.16 Limits on Suspension Period

No stipulation (refer to 4.9.13 Circumstances for Suspension).

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The list of revoked certificates issued by the IACA is available via the CRL published in the repository.

4.10.2 Service Availability

The CRL repository is available 24 x 7.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Any Subscriber may end the subscription by:

- Allowing its own certificate to expire without requesting a new certificate.
- Revoking its certificate prior to the certificate expiration.

The IACA may end the subscription of any Subscriber certificate by:

- Not renewing the certificate after its expiration.
- Revoking the certificate prior to the certificate expiration.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

Escrow of private keys is forbidden under this CP/CPS.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation (refer to section 4.12.1 Key Escrow and Recovery Policy and Practices).

5 Facility, Management, and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The IACA operations are conducted inside a data centre in a high security zone, within a physically protected building that prevents and detects unauthorised access, based on multiple tiers of physical security.

5.1.2 Physical Access

The IACA systems are protected by a minimum of three tiers of physical security (protected building, high-security zone), with access to the lower tier required before gaining access to the higher tier.

Progressively restrictive physical access privileges control access to each tier. Sensitive CA operational activity, creation and storage of cryptographic material, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within the high-security room. Physical access is automatically logged for audit purposes.

Cryptographic hardware and keying material are further protected through the use of locked safes, cabinets and key racks. Access to the high-security room, cryptographic hardware and keying material is limited to authorised members of the PKI Working Groups and restricted in accordance with segregation of duty requirements.

Other personnel (e.g. maintenance staff) may have access if and only if escorted by authorised personnel from the PKI Working Groups. Such access is logged.

5.1.3 Power and Air Conditioning

The IACA facilities are equipped with an air conditioning system to regulate temperature and humidity.

All electrical components are connected to an UPS (uninterruptible power supply) and backed by a diesel electricity generator.

5.1.4 Water Exposures

The area housing the IACA systems is equipped with water sensors. In the event of a flooding, an alarm is triggered, the power supply is automatically cut off and the appropriate personnel is alerted.

5.1.5 Fire Prevention and Protection

The IACA safe environment has all the necessary mechanisms installed to detect and extinguish fires and other flame or smoke derived incidents. These mechanisms are in compliance with local fire safety regulations:

- fire and smoke detection and alarm systems are installed in all physical security levels,
- fixed and mobile fire extinguishing equipment is positioned in strategic and accessible places,
- emergency procedures are defined in case of fire.

5.1.6 Media Storage

All media containing production software and data, audit information, archive, or backup copies are stored in safe vaults within a high-security zone in the main site, as well as in a second high-security zone in another location, with appropriate physical and logical access controls designed to restrict the access to authorised working group members and mechanisms to protect such media from accidental damage (e.g. fire).

Whenever sensitive information is transported from the high-security zone in the main site to the high-security zone in the remote site, the process is performed under the supervision of, at least, 2 (two) Working Group elements, who are required to ensure the safe transportation of the information to its final destination. The information (or the information container) shall be always under visual control of the Working Group members.

In situations requiring physical displacement of data storage hardware (for example, hard discs) outside the high security zone, for reasons other than the backup copy archive, each hardware element shall be verified to ensure that it does not hold any sensitive data. In these situations, the information must be eliminated using all necessary means (hard disc format, cryptographic hardware reset, or even the physical destruction of the storage equipment).

5.1.7 Waste Disposal

Paper documents and material holding sensitive information are shredded before disposal, in such a way that no information can be read, reproduced, or used for any purpose.

Media used to collect or transmit sensitive information are rendered unreadable (securely erased or physically destroyed) before disposal. Cryptographic devices and keying material are physically destroyed, zeroized or initialized in accordance to the manufacturer's guidance, prior to disposal. Other storage hardware (hard disks or other storage equipment) must be initialized before disposal, using whatever means necessary (secure formatting or physical destruction of the storage media/equipment).

5.1.8 Off-Site Backup

A backup copy is kept in the main site for local redundancy and quick recovery of operations in case of failure of an individual component of the IACA system.

For the purpose of disaster recovery and business continuity, another backup copy is kept in a secure environment inside a secondary site, with appropriate levels of physical security and equivalent to the controls described in section 5.1 Physical Controls.

5.2 Procedural Controls

This section describes the trusted roles, responsibilities, and segregation of duties.

5.2.1 Trusted Roles

Trusted Roles include all employees, contractors, and consultants that have access to or control of any component of the IACA system.

The IACA has five different trusted roles (named Working Groups), each with different responsibilities.

5.2.1.1 Security Officers

This group is responsible for administering the implementation of the security practices.

The responsibilities of this group are:

- Overall responsibility for administering the implementation of the security practices,
- To define security policies and guarantee their application and availability to whoever is necessary,
- To guarantee compliance of the PKI with this CP/CPS,
- Management of all the IACA documentation,
- To configure the certificate profiles,
- To configure users in the Hardware Security Module (HSM),
- To configure users in the PKI management software,
- To manage all non-personal passwords,
- To maintain an inventory of all artefacts including system passwords and storing these in a secure environment,
- To ensure that all members of the other groups have no more than the strictly needed authentication tokens and passwords used in the high-security zone to perform his/her duties,
- To register the change of authentication passwords used inside the high-security zone,
- To register the compromise of an authenticating password, used by users in the high-security zone,
- To evaluate requests for documentation replication.
- To update the repository

No member of this group is allowed to access the IACA PKI system without the presence of a System Auditor.

5.2.1.2 System Operators

This group is responsible for the IACA routine operation, including certificate and CRL issuance, backup operations and monitoring hardware and software malfunctions.

The responsibilities of this group are:

- Operation of CA trustworthy system on a day-to-day basis,
- To perform the CA's systems backup/restore ceremonies,
- To monitor, report and quantify hardware and software incidents and malfunctions.

No member of this group is allowed to access the PKI system without the presence of a System Auditor.

5.2.1.3 System Auditors

This group will audit the execution of CA processes and ceremonies, registering sensible operations and validating the security of all resources used.

The responsibilities of this group are:

- To verify the correctness of processes,

- To investigate suspicions of fraud,
- To check functionality of safety controls (alarm devices, fire detectors, etc.), when present in an environment,
- To register all security auditable procedures,
- To register all security auditable checks,

No member of this group is allowed to access the PKI system without the presence of a Security Officer or System Operator.

5.2.1.4 PKI Policy Management

This group is responsible for key PKI decisions and approvals.

The responsibilities of this group are:

- To review and approve all major PKI policies (including this CP/CPS),
- To take top management decisions (e.g. risks, IACA decommissioning),
- Request IACA certificate revocation

5.2.1.5 Service Management

This group is responsible for appointing the working group's members, as well as approving operational service policies.

The responsibilities of this group are:

- To review and approve operational PKI policies
- To appoint new members to the working groups,
- Suggest IACA certificate revocation,
- To take operational management decisions (e.g. budget approval, etc).

5.2.2 Number of Persons Required per Task

All security critical operations require the presence of two authorised persons. These operations include, but are not limited to, creation; activation; de-activation; backup and recovery of the IACA private keys.

The revocation of IACA private keys is possible only under the supervision of two authorised persons. A two-person principle is also applied when carrying out maintenance on the IACA infrastructure (e.g. when the cryptographic module is initialised).

5.2.3 Identification and Authentication for Each Role

It is the responsibility of the Service Management Group to approve appointment of members to the Working Groups. The composition of the working groups and the responsibilities is registered in the PKI Human Resources document.

Based on this document, access to environments and systems related to IACA are configured. The persons shall be identified to the IACA managing system using authentication certificates stored in cryptographic tokens or smartcards. The identification to HSMs must be performed using the

authentication tokens provided by the equipment vendor, after being initialized and distributed to each person. Login and password may be also used for some components of the IACA system.

For physical access, individual contactless cards and/or PIN codes are required to progress through the security zones up to the high-security area.

5.2.4 Roles Requiring Separation of Duties

The following matrix defines exclusivity of the working groups for segregation of duty. The X mark represents an incompatibility, meaning that a member of the Working Group in the row cannot belong simultaneously to the Working Group in the column.

	Security Officers	System Operators	System Auditors	Service Management
Security Officers		X	X	
System Operators	X		X	
System Auditors	X	X		
Service Management				

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

All personnel occupying a trusted role possess the necessary qualifications and experience to provide PKI services.

All personnel occupying a trusted role at the IACA understand the involved processes and the effects and implications of all actions taken.

All personnel of the IACA have security clearance in accordance with the regulations of the Queensland Government and the Commonwealth of Australia.

5.3.2 Background Check Procedures

Background checks include:

- Identity verification, using documentation from reliable sources,
- Employment history,
- Professional references,
- Educational qualifications, and
- Criminal records.

All personnel in trusted roles shall have no conflict of interest that might affect his/her independence when performing the PKI operations.

5.3.3 Training Requirements

Adequate training and experience is given to the members of the Working Groups in order to perform their tasks in a satisfactory and competent manner.

The Working Group elements are additionally subject to a training and experience plan, including the following topics:

a) Digital certificates and Public Key Infrastructures;

b) ISO/IEC 18013-5:2021 mDL;

c) IACA PKI components;

d) Specific training for their role inside the Working Group;

e) PKI operation and management;

f) Operation of software and/or hardware used in the CAs;

g) Operational policies and procedures (including this CP/CPS and security policy);

h) Security and personal data protection rules.

5.3.4 Retraining Frequency and Requirements

Whenever necessary, complementary training and experience is provided to the Working Group members, in order to ensure the required professional level for the competent and satisfactory performance of their responsibilities. In particular,

- Whenever there are any technological changes, introduction of new tools or structural changes in the procedures;
- Whenever there are changes introduced to the CP/CPS.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorised Actions

Sanctions are applied according to the applicable labour legislation, laws and security regulations, to all the individuals who perform unauthorised actions, unauthorised use of authority or make unauthorised use of the systems.

5.3.7 Independent Contractor Requirements

Independent contractors or consultants are permitted access to high-security zones, as long as they are escorted and directly supervised by the Working Group members, at all times, and after the notice and acceptance of a Non-Disclosure Agreement.

The hiring process shall have the same requirements described in section 5.3.1 Qualifications, Experience, and Clearance Requirements.

5.3.8 Documentation Supplied to Personnel

All adequate information is made available to the Working Group members so they can perform their tasks in a competent and satisfactory manner. This information includes:

- This CP/ CPS;

- Technical procedures and guides to perform the assigned tasks.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

Significant events generate auditable logs. These include, at least, the following:

- request, issuance, renewal, re-key and revocation of certificates;
- CRL issuance;
- security-related events, including:
    - Access attempts (successful and unsuccessful) to sensitive CA system resources;
    - Operations performed by Working Group members,
    - Entry/exit of physical security zones.

Log entries include the following information:

- Date and time of the event;
- Identity of the subject that caused the event;
- Category of the event;
- Description of the event.

5.4.2 Frequency of Processing Log

The records are analysed and reviewed regularly, and additionally every time there are suspicions or abnormal activities or threats of any kind. The actions taken, based on the records information, are also documented.

5.4.3 Retention Period for Audit Log

Audit logs are kept available onsite for at least 2 (two) years after processing, and then are archived on the terms described in section 5.5 Records Archival.

5.4.4 Protection of Audit Log

The records are exclusively analysed by authorised members belonging to the Working Groups.

The records are protected by auditable electronic mechanisms in order to detect and hinder the attempt of unauthorised data changes, removal or any other manipulation schemes.

5.4.5 Audit Log Backup Procedures

Backups of audit logs are created on a regular basis on external encrypted storage media.

5.4.6 Audit Collection System (Internal vs. External)

Audit logs are collected internally to the CA system and exported to a SIEM (Security Information and Event Management) system.

5.4.7 Notification to Event-Causing Subject

In case an event triggers an alert, the PKI Working Groups are notified for further analysis. If the event is escalated to an incident, the subject causing it is notified and further actions are determined.

5.4.8 Vulnerability Assessments

The auditable records are regularly assessed in order to minimize and eliminate potential attempts to break the system security.

5.5 Records Archival

5.5.1 Types of Records Archived

All audit data (as mentioned in section 5.4.1 Types of Events Recorded), certificate issuance forms, public key certificates and documentation supporting lifecycle operations, are archived.

5.5.2 Retention period for archive

Records are retained for 7 (seven) years.

5.5.3 Protection of archive

The archive:

- Is protected so that only authorised members of the Working Groups may access and consult its contents,
- Is protected against any change or attempt to remove it,
- Is protected against the deterioration of the media where it is stored, through the regular migration to a new media, and
- Is protected against obsolescence of the hardware, operating systems and other software, through the conservation of the hardware, operating systems and other software which then make part of the archive itself, in order to allow the access and use of the stored records in a timeless manner.

5.5.4 Archive backup procedures

Backup copies of the archives are performed in full and stored in appropriate devices onsite and offsite.

All paper based documentation supporting certificate issuance and lifecycle operations is archived in a secure cabinet, with restricted access to the elements of the Working Groups.

5.5.5 Requirements for time-stamping of records

All records contain date and time information based on a trusted time source.

Paper based documentation is dated and signed-off before being archived.

5.5.6 Archive collection system (internal or external)

Archive collection systems are internal.

5.5.7 Procedures to obtain and verify archive information

The archived Information may only be retrieved by authorised members of the Working Groups and under the supervision of a System Auditor and authorised by the Service Management Group.

5.6 Key changeover

The procedures to provide a new IACA public key after a re-key operation are the same as for the current IACA. Refer to section 4.7 Certificate Re-key (page 19).

5.7 Compromise and Disaster Recovery

This section describes requirements relating to notification and recovery procedures in the event of compromise or disaster of the IACA.

5.7.1 Incident and Compromise Handling Procedures

Whenever a potential incident occurs, it is analysed to determine the impact and take the necessary measures.

Backups of CA private keys (generated and maintained in accordance with section 6.2.4 Private Key Backup, page 34) and archived records (section 5.5 Records Archival, page 30) are kept in a high-security zone in a secondary site and are made available in case of compromise or disaster.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

In the event computing resources, software, and/or data are corrupted or suspected to be corrupted, the backup of the CA private key and archived records can be obtained and the integrity of the original data can be verified.

If it is confirmed that computer resources, software and/or data are corrupted, appropriate measures shall be taken to respond to the incident. The response to the incident shall include the recovery of the corrupted equipment/data, using similar equipment and/or recovering stored backup copies and records. It may also include the activation of IACA services in the secondary site, until the conditions in the main site are restored.

5.7.3 Entity Private Key Compromise Procedures

In the event of the IACA private key being compromised or suspicion of its compromise, appropriate measures shall be taken to respond to the incident, which may include:

- Investigation, analysis, and impact estimation,
- Revocation of the IACA certificate and communication to Relying Parties, in accordance to section 4.9 Certificate Revocation and Suspension (page 20),
- Revocation of the Subscriber certificates signed by the IACA private key that was compromised or suspected to be compromised, in accordance with section 4.9 Certificate Revocation and Suspension,
- Generation of a new key pair for the IACA, in accordance with section 4.7 Certificate Re-key (page 19).

In the event of the private key of a Subscriber certificate being compromised, the responses to the incident may include:

- Investigation, analysis, and impact estimation,
- Revocation of the Subscriber certificate corresponding to the private key compromised,
- Issuance of a new CRL and publishing in the repository,
- Generation of a new key pair and issuance of a new Subscriber certificate,
- Notification of the Subscriber.

5.7.4 Business Continuity Capabilities After a Disaster

Replicas of computing resources, software, backup copies and records are stored in the secondary site facilities. These resources are necessary to restore or recover essential operations (certificate issuing, revocation, CRL publication) after a natural disaster or other major incident that may render the main site unusable.

5.8 CA or RA termination

IACA may terminate activity, ceasing issuance of Subscriber certificates. In that case, the IACA will wither:

a) continue to issue CRLs until all Subscriber certificates issued have expired, or

b) transfer the responsibility to other entity/provider which will continue to issue the CRL. The transfer process shall include all archives.

In case this is not possible, all Subscriber certificates will be revoked and the corresponding private keys shall be destroyed.

6 Technical Security Controls

This section defines the security measures taken by the IACA to protect the cryptographic keys and related activation data. Secure key management is critical to ensure that all secret and private keys and activation data are protected and accessed only by duly authorised personnel.

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The IACA key pair generation is performed by Working Group members, in a planned and audited Key Ceremony, in accordance with written procedures. The activities performed in each key generation process are registered, dated and signed by all Working Group members involved.

The IACA key pair is generated and stored in an offline HSM, compliant with FIPS 140-2 level 3. All cryptographic operations involving the IACA key pair are performed exclusively in the HSM. Usage of the keys in the HSM is protected by security policies, access controls, segregation of duty of Working Groups, multifactor authentication, and m-of-n activation.

6.1.2 Private Key Delivery to Subscriber

Private keys to be certified by the IACA shall be generated at the Subscriber's premises and shall not be transferred.

6.1.3 Public Key Delivery to Certificate Issuer

The certificate applicant provides a Certificate Signing Request (CSR) in PKCS#10 [6] format, containing the public key, and the certificate issuance form to the System Operators. This form must contain the SHA256 hash of the CSR.

6.1.4 CA public key delivery to relying parties

IACA public keys are available in the repository as self-signed and link certificates. If the IACA is subordinate and/or cross certified to other PKIs, the certificates may also be published in the repository.

The IACA certificates may also be distributed:

- through trust lists such as VICAL, provided by third parties, and
- bilateral exchange, through secure out-of-band mechanisms.

6.1.5 Key Sizes

Key pairs shall be of sufficient length to prevent others from determining the private key using cryptanalysis during the period of expected utilization of such key pair. The expected key size strength is:

- IACA key pairs – 384 bits, based on secp384r1.
- Subscriber key pairs – 256 bits, based on prime256v1.

6.1.6 Public Key Parameters Generation and Quality Checking

Key pairs are based in elliptic curve cryptography and generated in an HSM certified FIPS 140-2 Level 3, operating according to the evaluated security target.

The cryptography algorithms are referenced as named curves within the subset defined in ISO/IEC 18013-5:2021 [1].

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

IACA private keys are used to sign Subscriber certificates, IACA link certificates and CRLs. IACA certificates have X.509 v3 key usage bits `keyCertSign` and `cRLSign` enabled.

Subscriber private keys for DS and JWS certificates are used to sign ISO/IEC 18013-5:2021 [1] “mdoc” data objects (or equivalent) for the purpose of integrity and authenticity. Those certificates have the X.509 v3 key usage bit `digitalSignature` enabled.

Subscriber private keys for TLS certificates are used for establishing the TLS protocol in the online retrieval service. Those certificates have the X.509 v3 key usage bit `digitalSignature` enabled.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

IACA key pair generation and private key storage are performed in certified hardware security modules (HSM) that meet or exceeds the following requirements:

Security certifications:

- FIPS 140-2 Level 3

Cryptography:

- Full Suite B support
- Asymmetric: RSA (1024-8192), DSA (1024-3072), Diffie-Hellman, Elliptic Curve Cryptography (ECDSA, ECDH, ECIES) with named, user-defined and Brainpool curves
- Symmetric: AES
- Hash/Message Digest/HMAC: SHA-2 (224-512)
- Random Number Generation: FIPS 140-2 approved DRBG (SP800-90 CTR mode)

API support:

- PKCS#11

Safety and Environmental Compliance:

- UL, CSA, CE
- FCC, VCCI, CE
- RoHS, WEEE
- TAA

6.2.2 Private Key (n out of m) Multi-Person Control

Technical and procedural mechanisms, which require the participation of multiple Working Group members to perform sensitive CA cryptographic operations, are implemented.

The activation data is needed to allow the use of the IACA private key. A threshold number of separate parts, with a minimum of two (2), is required to activate the IACA private key stored on the hardware cryptographic module. Backup and restore of the IACA private key require an additional part, in control of a different Working Group for the purposes of segregation of duty.

6.2.3 Private Key Escrow

Escrow of private keys is forbidden under this CP/CPS.

6.2.4 Private Key Backup

IACA private keys have at least two backup copies with the same security level as the original key.

Two backups of the private keys are generated in the key ceremony. Each backup uses a HSM with two-factor multi-person authentication (m-of-n authentication is required before the backup can be performed).

One of the backups is collocated with the original copy in the main site for local redundancy, subject to the same security controls. The second backup is stored in the secondary site, with equivalent security controls.

IACA private keys may be recovered in case of malfunction of the original copy.

6.2.5 Private Key Archival

IACA private keys are permanently erased from all cryptographic modules copies under the following circumstances:

- after the expiration date of the IACA certificate,
- if the IACA certificate is revoked.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Transferring of the IACA private key is only possible for backup purposes to similar HSM certified FIPS 140-2 level 3 and initialized with the same activation data.

6.2.7 Private Key Storage on Cryptographic Module

IACA private keys are stored in encrypted form on HSMs certified FIPS 140-2 level 3 and operating according to the security target.

6.2.8 Method of Activating Private Key

Since the IACA is offline and usually powered off, the private key must be activated in the cryptographic module at every system boot. This activation of the private key requires multi-person

control (refer to section 6.2.2 Private Key (n out of m) Multi-Person Control, on page 34) with two factor authentication.

6.2.9 Method of Deactivating Private Key

Since the IACA is an offline CA, the private key is deactivated when not in use.

To deactivate the IACA's private key, the HSM crypto token must be deactivated in the system and disconnected from the server and from the power supply. Once the key is deactivated, it will remain inactive until a new activation process is executed.

6.2.10 Method of Destroying the Private Key

Private keys are destroyed according to documented procedures to permanently erase all copies in all cryptographic modules. The process follows the HSM manufacturer instructions to ensure irrecoverable deletion of the private key, in part or full.

The destruction process follows a documented procedure and a report is created and archived.

6.2.11 Cryptographic Module Rating

Refer to section 6.2.1 Cryptographic Module Standards and Controls (page 33).

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The IACA public keys are archived in association with the corresponding certificates as defined in section 5.5 Records Archival (page 30).

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The operational period of a certificate corresponds to the time between the `notBefore` and `notAfter` fields. If a certificate is revoked before its term, the end of the operational period is anticipated and coincides with the effective revocation time.

The following table summarizes the certificate operational and key usage periods.

	Operational Period	Full Usage Period		
		Usage period	Lead time (up to)	Total
IACA self-signed	2,370 days	1,825 days	90 days	1,915 days
IACA link	up to 2,370 days	N/A	N/A	N/A
Subscriber Certificates				
Document Signer	455 days	365 days	90 days	455 days
JWS Signer	455 days	365 days	90 days	455 days
TLS	397 days	365 days	32 days	397 days

Further details are provided in the following sub-sections.

6.3.2.1 IACA Certificate

The IACA certificate will be re-keyed every 5 years approximately. The private key will be used to issue end entity certificates for the period of 5 years. The validity period of the IACA certificate is approximately 6 years and 6 months, being determined by adding the following periods:

- the length of time the IACA private key is used to issue end entity certificates: 5 years,
- the longest validity period of any end entity certificate issued under that key: 1 year and 3 months, and
- a lead in time, which includes the period of time necessary to disseminate the IACA certificate: 3 months.

An accompanying IACA link certificate is issued at any IACA re-key.

6.3.2.2 Document Signer Certificate

A new Document Signer certificate shall be issued approximately every 6 months. The private key will be used to sign “mdoc” objects as defined in ISO/IEC 18013-5:2021 [1] for the period of approximately 6 to 9 months. The validity period of the Document Signer certificate is approximately 1 year and 3 months, being determined by adding the following periods:

- the length of time the key will be used to sign mdoc objects: 6 months,
- the longest validity period of any mDL mdoc signed under that key: 6 months,
- a period of tolerance, which includes the time necessary to process end-to-end Document Signer certificate re-keys: 3 months.

6.3.2.3 JWS Certificate

A new JWS certificate shall be issued approximately every 12 months. The private key will be used to sign “mdoc” objects as defined in ISO/IEC 18013-5:2021 [1] for the period of approximately 12 months. The validity period of the JWS certificate is approximately 1 year and 3 months, being determined by adding the following periods:

- the length of time the key will be used to sign mdoc objects: 12 months,
- the longest validity period of any mDL mdoc signed under that key: not applicable, JWS signed mdoc objects are ephemeral,
- a period of tolerance, which includes the time necessary to process end-to-end JWS certificate re-keys: 3 months.

6.3.2.4 TLS Certificate

A new TLS certificate shall be issued approximately every 12 months. The private key will be used for the TLS protocol, to protect the Internet domain of the endpoint hosting the online retrieval method as defined in ISO/IEC 18013-5:2021 [1] for the period of approximately 12 months. The validity period of the TLS certificate is approximately 1 year and 1 month, being determined by adding the following periods:

- the length of time the key will be used for TLS: 12 months,
- a period of tolerance, which includes the time necessary to process end-to-end TLS certificate re-keys: 1 month.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The activation data necessary for using the IACA private key in the cryptographic module – the HSM – is split into several parts, imprinted in physical electronic tokens, assigned to different members of Working Groups for segregation of duty. The activation data is generated during the first key ceremony, according with the document procedures, and witnessed by the members of the Working Groups, including the System Auditors.

Activation of the HSM requires a minimum number of parts (m) out of the total number of split parts (n) – *m-of-n* mechanism.

6.4.2 Activation Data Protection

The split secret parts of the activation data associated with the IACA private key are imprinted in physical electronic tokens and cannot be extracted in clear. Cloning of the tokens can only be performed through the HSM using the original set of tokens and following the mechanisms provided by the HSM manufacturer.

The tokens are kept in safes and key racks with a combination of access controls that requires individual authentication of the Working Group members.

6.4.3 Other Aspects of Activation Data

If activation data for private keys needs to be transmitted, the transmission is protected against loss, theft, modification and unauthorised disclosure.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Access to the IACA production servers is limited to the Working Group members.

IACA components include the following functionalities:

- require authenticated logins for trusted roles;
- provide access control;
- provide a security audit capability (protected in integrity);
- use of cryptography for session communication and database security;
- trusted path for identification and authentication.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Security Controls

6.6.1 System Development Controls

The CA management systems are developed and implemented by third parties in accordance with defined rules for system development and change management.

All software configurations and changes are performed and audited by authorised members of the Working Group.

6.6.2 Security Management Controls

The infrastructure has mechanisms and/or Working Groups in place to control and monitor the configuration of the CA systems. The CA management system, when first started, is verified to ensure that the software used is reliable, not forged and was not modified after its installation.

6.6.3 Life Cycle Security Controls

Any system modification and software upgrade must be audited and controlled by authorised persons.

Unauthorised modifications in the IACA software or configuration are detected

6.7 Network Security Controls

The IACA is an offline “air gapped” system, with no network connection to any other system.

6.8 Time-stamping

As the IACA is offline with no network connectivity, all date/times used are from the local clock. Accuracy is verified when the system is started and synchronized if necessary, using a trusted time source as reference.

7 Certificate and CRL Profiles

7.1 Certificate profile

The IACA and Subscriber certificate profiles conform to the ISO/IEC 18013-5:2021 [1] specification.

7.1.1 Version Number(s)

According to ISO/IEC 18013-5:2021 [1], the version number of the certificates is `3` (three).

7.1.2 Certificate extensions

The extensions defined for X.509 v3 certificates provide methods for associating additional attributes with users or public keys and for managing a certification hierarchy.

The certificate extensions present in IACA and Subscriber certificates are compliant with ISO/IEC 18013-5:2021 [1].

7.1.2.1 IACA Certificate Profile/Extensions

Certificate Component	RFC 5280	Value	Present	Critical
Version	4.1.2.1	`3`	M	
Serial Number	4.1.2.2	16 bytes octet, positive, random, minimum 64 bits of entropy	M	
Signature	4.1.2.3	`1.2.840.10045.4.3.3` (ECDSA with SHA-384)	M	
Issuer	4.1.2.4		M	
countryName (C)		`AU`	M	
stateOrProvinceName (ST)		`AU-QLD`	M	
organizationName (O)		`Queensland Government`	M	
serialNumber		*nnn* (incremented at each IACA re-key, starting in `001`)	M	
commonName (CN)		`IACA Digital Licence Queensland – Australia`	M	
Validity	4.1.2.5		M	
Not Before		Issuance date	M	
Not After		Issuance date + 2 370 days	M	

Subject	4.1.2.6	Same as Issuer	M	
Subject Public Key Info	4.1.2.7		M	
algorithm		`1.2.840.10045.2.1` (elliptic curve public key)	M	
parameters		`1.3.132.0.34` (secp384r1)	M	
subjectPublicKey		384 bits	M	
X.509v3 Extensions	4.2		M	
Subject Key Identifier	4.2.1.2	160-bit SHA-1 hash of the subject public key `BIT STRING` value (excluding tag, length, and number of unused bits)	M	NC
Key Usage (bits)	4.2.1.3		M	C
Digital Signature		`0`	M	
Non Repudiation		`0`	M	
Key Encipherment		`0`	M	
Data Encipherment		`0`	M	
Key Agreement		`0`	M	
Key Certificate Signature		`1`	M	
CRL Signature		`1`	M	
Encipher Only		`0`	M	
Decipher Only		`0`	M	
Issuer Alternative Name	4.2.1.7		M	NC
rfc822Name		`dlpki@qld.gov.au`	M	
uniformResourceIdentifier		`http://dlpki.qld.gov.au`	M	
Basic Constraints	4.2.1.9		M	C
CA		`TRUE`	M	
pathLenConstraint		`0`	M	
CRL Distribution Points	4.2.1.13		M	NC
distributionPoint		`http://dlpki.qld.gov.au/crl/au-qld-iaca-dl-001.crl`	M	

7.1.2.2 IACA link Certificate Profile/Extensions

Certificate Component	RFC 5280	Value	Present	Critical
Version	4.1.2.1	`3`	M	
Serial Number	4.1.2.2	16 bytes octet, positive, random, minimum 64 bits of entropy	M	
Signature	4.1.2.3	`1.2.840.10045.4.3.3` (ECDSA with SHA-384)	M	
Issuer	4.1.2.4		M	
countryName (C)		`AU`	M	
stateOrProvinceName (ST)		`AU-QLD`	M	
organizationName (O)		`Queensland Government`	M	
serialNumber		*nnn*	M	
commonName (CN)		`IACA Digital Licence Queensland – Australia`	M	
Validity	4.1.2.5		M	
Not Before		Issuance date	M	
Not After		Same `notAfter` date of the previous IACA signing this certificate	M	

Subject	4.1.2.6		M	
countryName (C)		AU	M	
stateOrProvinceName (ST)		AU-QLD	M	
organizationName (O)		Queensland Government	M	
serialNumber		*nnn + 1*	M	
commonName (CN)		IACA Digital Licence Queensland – Australia	M	
Subject Public Key Info	4.1.2.7		M	
algorithm		1.2.840.10045.2.1 (elliptic curve public key)	M	
parameters		1.3.132.0.34 (secp384r1)	M	
subjectPublicKey		384 bits	M	
X.509v3 Extensions	4.2		M	
Authority Key Identifier	4.2.1.1		M	NC
keyIdentifier		Same value as the subject key identifier of the previous IACA signing this certificate	M	
Subject Key Identifier	4.2.1.2	160-bit SHA-1 hash of the subject public key BIT STRING value (excluding tag, length, and number of unused bits)	M	NC
Key Usage (bits)	4.2.1.3		M	C
Digital Signature		0	M	
Non Repudiation		0	M	
Key Encipherment		0	M	
Data Encipherment		0	M	
Key Agreement		0	M	
Key Certificate Signature		1	M	
CRL Signature		1	M	
Encipher Only		0	M	
Decipher Only		0	M	
Issuer Alternative Name	4.2.1.7		M	NC
rfc822Name		dlpki@qld.gov.au	M	
uniformResourceIdentifier		http://dlpki.qld.gov.au	M	
Basic Constraints	4.2.1.9		M	C
CA		TRUE	M	
pathLenConstraint		0	M	
CRL Distribution Points	4.2.1.13		M	NC
distributionPoint		http://dlpki.qld.gov.au/crl/au-qld-iaca-dl-001.crl	M	

7.1.2.3 Document Signer Certificate Profile/Extensions

Certificate Component	RFC 5280	Value	Present	Critical
Version	4.1.2.1	3	M	
Serial Number	4.1.2.2	16 bytes octet, positive, random, minimum 64 bits of entropy	M	
Signature	4.1.2.3	1.2.840.10045.4.3.2 (ECDSA with SHA-256)	M	
Issuer	4.1.2.4		M	

countryName (C)		AU	M	
stateOrProvinceName (ST)		AU-QLD	M	
organizationName (O)		Queensland Government	M	
serialNumber		*nnn*	M	
commonName (CN)		IACA Digital Licence Queensland – Australia	M	
Validity	4.1.2.5		M	
Not Before		Issuance date	M	
Not After		Issuance date + 455 days	M	
Subject	4.1.2.6		M	
countryName (C)		AU	M	
stateOrProvinceName (ST)		AU-QLD	M	
organizationName (O)		Queensland Government	M	
commonName (CN)		Digital Licence Document Signer Queensland – Australia	M	
Subject Public Key Info	4.1.2.7		M	
algorithm		1.2.840.10045.2.1 (elliptic curve public key)	M	
parameters		1.2.840.10045.3.1.7 (prime256v1)	M	
subjectPublicKey		256 bits	M	
X.509v3 Extensions	4.2		M	
Authority Key Identifier	4.2.1.1		M	NC
keyIdentifier		Same value as the subject key identifier of the IACA signing this certificate	M	
Subject Key Identifier	4.2.1.2	160-bit SHA-1 hash of the subject public key BIT STRING value (excluding tag, length, and number of unused bits)	M	NC
Key Usage (bits)	4.2.1.3		M	C
Digital Signature		1	M	
Non Repudiation		0	M	
Key Encipherment		0	M	
Data Encipherment		0	M	
Key Agreement		0	M	
Key Certificate Signature		0	M	
CRL Signature		0	M	
Encipher Only		0	M	
Decipher Only		0	M	
Issuer Alternative Name	4.2.1.7		M	NC
rfc822Name		dlpki@qld.gov.au	M	
uniformResourceIdentifier		http://dlpki.qld.gov.au	M	
Extended Key Usage	4.2.1.9		M	C
Key Purpose		1.0.18013.5.1.2 (mdlDS)	M	
CRL Distribution Points	4.2.1.13		M	NC
distributionPoint		http://dlpki.qld.gov.au/crl/au-qld-iaca-dl-001.crl	M	

7.1.2.4 JWS Certificate Profile/Extensions

Certificate Component	RFC 5280	Value	Present	Critical
Version	4.1.2.1	3	M	
Serial Number	4.1.2.2	16 bytes octet, positive, random, minimum 64 bits of entropy	M	
Signature	4.1.2.3	1.2.840.10045.4.3.2 (ECDSA with SHA-256)	M	
Issuer	4.1.2.4		M	
countryName (C)		AU	M	
stateOrProvinceName (ST)		AU-QLD	M	
organizationName (O)		Queensland Government	M	
serialNumber		*nnn*	M	
commonName (CN)		IACA Digital Licence Queensland – Australia	M	
Validity	4.1.2.5		M	
Not Before		Issuance date	M	
Not After		Issuance date + 455 days	M	
Subject	4.1.2.6		M	
countryName (C)		AU	M	
stateOrProvinceName (ST)		AU-QLD	M	
organizationName (O)		Queensland Government	M	
commonName (CN)		Digital Licence JWS Signer Queensland – Australia	M	
Subject Public Key Info	4.1.2.7		M	
algorithm		1.2.840.10045.2.1 (elliptic curve public key)	M	
parameters		1.2.840.10045.3.1.7 (prime256v1)	M	
subjectPublicKey		256 bits	M	
X.509v3 Extensions	4.2		M	
Authority Key Identifier	4.2.1.1		M	NC
keyIdentifier		Same value as the subject key identifier of the IACA signing this certificate	M	
Subject Key Identifier	4.2.1.2	160-bit SHA-1 hash of the subject public key BIT STRING value (excluding tag, length, and number of unused bits)	M	NC
Key Usage (bits)	4.2.1.3		M	C
Digital Signature		1	M	
Non Repudiation		0	M	
Key Encipherment		0	M	
Data Encipherment		0	M	
Key Agreement		0	M	
Key Certificate Signature		0	M	
CRL Signature		0	M	
Encipher Only		0	M	
Decipher Only		0	M	
Issuer Alternative Name	4.2.1.7		M	NC
rfc822Name		dlpki@qld.gov.au	M	

uniformResourceIdentifier		http://dlpki.qld.gov.au	M	
Extended Key Usage	4.2.1.9		M	C
Key Purpose		1.0.18013.5.1.3 (mdlJWS)	M	
CRL Distribution Points	4.2.1.13		M	NC
distributionPoint		http://dlpki.qld.gov.au/crl/au-qld-iaca-dl-001.crl	M	

7.1.2.5 TLS Server Certificate Profile/Extensions

Certificate Component	RFC 5280	Value	Present	Critical
Version	4.1.2.1	3	M	
Serial Number	4.1.2.2	16 bytes octet, positive, random, minimum 64 bits of entropy	M	
Signature	4.1.2.3	1.2.840.10045.4.3.2 (ECDSA with SHA-256)	M	
Issuer	4.1.2.4		M	
countryName (C)		AU	M	
stateOrProvinceName (ST)		AU-QLD	M	
organizationName (O)		Queensland Government	M	
serialNumber		*nnn*	M	
commonName (CN)		IACA Digital Licence Queensland – Australia	M	
Validity	4.1.2.5		M	
Not Before		Issuance date	M	
Not After		Issuance date + 397 days	M	
Subject	4.1.2.6		M	
countryName (C)		AU	M	
stateOrProvinceName (ST)		AU-QLD	M	
organizationName (O)		Queensland Government	M	
commonName (CN)		Digital Licence Server Retrieval Queensland – Australia	M	
Subject Public Key Info	4.1.2.7		M	
algorithm		1.2.840.10045.2.1 (elliptic curve public key)	M	
parameters		1.2.840.10045.3.1.7 (prime256v1)	M	
subjectPublicKey		256 bits	M	
X.509v3 Extensions	4.2		M	
Authority Key Identifier	4.2.1.1		M	NC
keyIdentifier		Same value as the subject key identifier of the IACA signing this certificate	M	
Subject Key Identifier	4.2.1.2	160-bit SHA-1 hash of the subject public key BIT STRING value (excluding tag, length, and number of unused bits)	M	NC
Key Usage (bits)	4.2.1.3		M	C
Digital Signature		1	M	
Non Repudiation		0	M	
Key Encipherment		0	M	
Data Encipherment		0	M	
Key Agreement		0	M	

Key Certificate Signature		0	M	
CRL Signature		0	M	
Encipher Only		0	M	
Decipher Only		0	M	
Subject Alternative Name	4.2.1.6			
dNSName		Internet domain name of the server. Can have up to 10 dNSName entries.		
Issuer Alternative Name	4.2.1.7		M	NC
rfc822Name		dlpki@qld.gov.au	M	
uniformResourceIdentifier		http://dlpki.qld.gov.au	M	
Extended Key Usage	4.2.1.9		M	C
Key Purpose		1.3.6.1.5.5.7.3.1 (serverAuth)	M	
Key Purpose		1.3.6.1.5.5.7.3.2 (clientAuth)	O	
CRL Distribution Points	4.2.1.13		M	NC
distributionPoint		http://dlpki.qld.gov.au/crl/au-qld-iaca-dl-001.crl	M	

7.1.3 Algorithm Object Identifiers

The following signature algorithms are used in the IACA:

- IACA self-signed and link certificates: ecdsa-with-SHA384 (OID 1.2.840.10045.4.3.3).
- Subscriber certificates: ecdsa-with-SHA256 (OID 1.2.840.10045.4.3.2).

The following key types are permitted in the IACA:

- IACA self-signed and link certificates: secp384r1 (OID 1.3.132.0.34)
- Subscriber certificates: prime256v1 (OID 1.2.840.10045.3.1.7)

7.1.4 Name Forms

Refer to section 3.1.1 Types of Names (page 13).

7.1.5 Name Constraints

Name Constraints shall not be used.

7.1.6 Certificate Policy Object Identifier

The certificate policy OID is omitted in the certificates, in compliance with the certificate profiles defined in ISO/IEC 18013-5:2021 [1].

7.1.7 Usage of Policy Constraints Extension

Policy Constraints shall not be used.

7.1.8 Policy Qualifiers Syntax and Semantics

Policy Constraints shall not be used.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

A Relying Party shall reject a certificate if it encounters a critical extension it does not recognize or a critical extension that contains information that it cannot process.

7.2 CRL profile

When a certificate is issued, it is expected to be in use for its entire validity period. However, various circumstances may cause a certificate to become invalid prior to the expiration of the validity period (refer to section 4.9.1 Circumstances for Revocation, page 20).

The CRL in this PKI conforms to the profile defined in ISO/IEC 18013-5:2021 [1].

7.2.1 Version number(s)

The “version” CRL field describes the version of the encoded CRL. In this profile, the version is 2 (two).

7.2.2 CRL and CRL entry extensions

The extensions defined for X.509 v2 CRLs provide methods for associating additional attributes with CRLs.

The IACA CRL contains the list of unexpired revoked certificates.

CRL Component	RFC 5280	Value	Present	Critical
Version	5.1.2.1	2	M	
Signature	4.1.2.3	1.2.840.10045.4.3.3 (ECDSA with SHA-384)	M	
Issuer	4.1.2.4		M	
countryName (C)		AU	M	
stateOrProvinceName (ST)		AU-QLD	M	
organizationName (O)		Queensland Government	M	
serialNumber		*nnn*	M	
commonName (CN)		IACA Digital Licence Queensland – Australia	M	
This Update	5.1.2.4	Issuance date	M	
Next Update	5.1.2.5	Issuance date + 90 days	M	
Revoked Certificates	5.1.2.6	Conditional, shall not be present if there are no revoked certificates. If present, shall not be empty. Each CRL entry in the revoked certificates list shall contain the serial number of the revoked certificate and the revocation date. CRL entry extensions shall not be used.	M	
CRL Extensions	5.1.2.7		C	
Authority Key Identifier	5.2.1		M	NC
keyIdentifier		Same value as the subject key identifier of the IACA signing this CRL	M	
CRL number	5.2.2	Sequential CRL number, increased monotonically at each new CRL issued, starting in 1	M	NC

7.3 OCSP profile

Not applicable. The IACA does not provide an OCSP service.

8 Compliance Audit and Other Assessments

8.1 Frequency or Circumstances of Assessment

The IACA systems are subject to periodic compliance audits which are no less frequent than once every 3 years and after each significant change to the deployed procedures and techniques.

Moreover, the Queensland Government may at any time require an audit of the IACA to validate that it is operating in accordance with this document.

8.2 Identity/Qualifications of Assessor

Compliance audits or other assessments are performed by personnel with:

- know-how in public key infrastructure technology, information security tools and techniques,
- security auditing.

8.3 Assessor's Relationship to Assessed Entity

Regular examination of compliance will be performed by System Auditors.

When the compliance audits or other assessments are performed by third party auditors, those auditors must be independent of the staff operating the IACA.

The auditor shall maintain a high standard of ethics required to ensure impartiality and the exercise of independent professional judgment.

8.4 Topics Covered by Assessment

The IACA assessment shall prove the adherence of the IACA to this CP/CPS.

8.5 Actions Taken as a Result of Deficiency

In case deficiencies are found during the assessment, the IACA shall undertake the necessary corrections to comply with this document.

The Service Management Group, together with input from the auditor and Working Group members, is responsible for approving a corrective action plan in case deficiencies are found during the assessment.

8.6 Communication of results

An audit compliance report, including identification of corrective measures taken or being taken by the audited party, shall be provided to:

- Queensland Government
- Service Management Group
- PKI Policy Management Group
- PKI Working Group members

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fee

No stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following information is considered confidential and shall be protected against disclosure by the participants using a reasonable degree of care:

- Private keys;
- Activation data used to access private keys or to gain access to the CA system;
- Contents, equipment and layout on the location of the CA's environments;
- Composition of the working groups and identification of its members;
- Business continuity, incident response, contingency, and disaster recovery plans;
- Other security practices used to protect the confidentiality, integrity, or availability of information;
- Audit logs and archive records;
- Transaction records, and external or internal audit trail records and any audit; and
- Any other information not expressly deemed public shall be considered confidential.

9.3.2 Information Not within the Scope of Confidential Information

The following information is not considered confidential:

- IACA certificates;
- IACA CRLs;
- Subscriber certificates;
- This CPS/CP document; and
- Contents of the web repository.

9.3.3 Responsibility to Protect Confidential Information

All participants shall be responsible for protecting the confidential information they possess in accordance with the Government Information Security Classification Framework and applicable laws.

The CA may disclose confidential information to the extent required under any law, including under the *Right to Information Act 2009* (Qld).

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Not applicable. The IACA does not process any personal information about individuals.

9.4.2 Information Treated as Private

Not applicable. Refer to section 9.4.1 Privacy Plan.

9.4.3 Information Not Deemed Private

Not applicable. Refer to section 9.4.1 Privacy Plan.

9.4.4 Responsibility to Protect Private Information

Not applicable. Refer to section 9.4.1 Privacy Plan.

9.4.5 Notice and Consent to Use Private Information

Not applicable. Refer to section 9.4.1 Privacy Plan.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Not applicable. Refer to section 9.4.1 Privacy Plan.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

This CP / CPS does not impact, whether by way of licence, transfer or assignment, the ownership of the Intellectual Property Rights of any party.

The party which already holds existing Intellectual Property Rights or which first creates any new Intellectual Property Rights will own and continue to own those Intellectual Property Rights.

If a party seeks the right to use or exploit any Intellectual Property Rights owned by another party, then those parties must enter into a separate agreement governing the grant of a licence to use the Intellectual Property Rights.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

The IACA will warrant and agree to:

- Provide the operational infrastructure and certification services;
- Provide certification and repository services consistent with this CP/CPS and operating policies and procedures;
- Use its private signing key only to sign certificates and CRLs and for no other purpose;

- Perform authentication and identification procedures in accordance with operational policies and procedures;
- Provide certificate and key management services including certificate issuance, publication, revocation and key renewal and update in accordance with the IACA CP/CPS; and
- Ensure that CA personnel use private keys issued for the purpose of conducting CA duties only for such purposes.

9.6.2 RA Representations and Warranties

RA tasks are performed under the scope of the CA operations. Refer to section 9.6.1 CA Representations and Warranties.

9.6.3 Subscriber Representations and Warranties

Subscribers warrant and agree that:

- Each digital signature created using the private key corresponding to the public key listed in the certificate is the digital signature of that corresponding certificate, and the certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created;
- The private key is protected and no unauthorised person has ever had access to it;
- All information contained in the certificate is true;
- The certificate is being used exclusively for authorised and legal purposes, consistent with this CP/CPS;
- The certificate is an end-user certificate and not a CA certificate, and therefore is not using the private key corresponding to any public key listed in the certificate for purposes of digitally signing any certificate (or any other format of certified public key) or CRL, as a CA or otherwise;
- They will sign the CSR before submitting to the IACA;
- They will promptly request revocation of the certificate, and cease using it and its associated Private Key, if any of the revocation circumstances defined in section 4.9.1 Circumstances for Revocation (page 20) happens; and
- They will promptly cease all use of the private key corresponding to the public key included in the Certificate upon revocation of that certificate for reasons of key compromise.

9.6.4 Relying Party Representations and Warranties

Relying Parties warrant and agree that they will:

- Obtain the IACA certificates to be set as trust anchors through the established dissemination mechanisms, defined in section 6.1.4 CA public key delivery to relying parties (page 32);
- Establish trust in the IACA who issued a certificate by verifying the certificate path in accordance with the guidelines set in standards X.509 [3] and RFC 5280 [2];
- Use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage and extended key usage extensions);

- Check each Certificate for validity, using the procedures described in X.509 [3], prior to reliance;
- Verify the validity by ensuring that the certificate has not expired;
- Ensure that the Certificate has not been suspended or revoked by accessing current revocation status information available at the location specified in the Certificate to be relied upon; and
- Determine that such Certificate provides adequate assurances for its intended use.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

The IACA disclaims and excludes, to the maximum extent permissible by law, all warranties and conditions, express or implied, including any warranty or condition as to:

- the accuracy of any information in a Certificate; or
- the status of any Certificate.

If any warranties or conditions implied by law are unable to excluded by the IACA, then the IACA's liability for any breach of the warranty or condition is limited to re-performing the services to which the warranty or condition applied.

The IACA disclaims and excludes, to the maximum extent permissible by law, any terms or conditions implied by law relating to any loss or damage that may be suffered by any PKI participant as a result of participating in the certificate application process, or using any certificate or associated keys issued under the IACA.

This section is subject always to section 9.8 Limitations of Liability (page 50).

9.8 Limitations of Liability

Each PKI participant releases the IACA from all liability in contract, or in tort, or pursuant to any other common law or statutory cause of action whatsoever arising under this document or in connection with the CA, for any loss or damage whether or not reasonably foreseeable, including but not limited to liability for:

- An entity described in this document under which certificates are issued carrying out, or failing to carry out, any activity described in, or contemplated by, any document published by the IACA; or
- The carrying out of, or failure to carry out, any activity related to the accreditation process.

If any term or condition implied by law is unable to be excluded by the IACA, then the liability of the IACA and any of its officers, employees, agents, and contractors (including sub-contractors), for any breach of the implied term or condition is limited to re-performing the services to which the term or condition applies.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

The CA-related documents (including this CP/CPS and further amendments) become effective upon publication in the repository and are only terminated or changed by their ruling or in accordance with section 9.10.2 Termination (page 50).

9.10.2 Termination

This IACA CP/CPS is valid until:

- it is replaced by a newer revised version; or
- the IACA is forced to end its certification services.

In the case of the IACA ending its certification services, this CP/CPS remains valid at least until the expiry of the validity period of the last certificate issued by IACA.

9.10.3 Effect of Termination and Survival

Upon termination of this CP/CPS, participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

Termination of this CP/CPS will not affect any provision of this CP/CPS which is expressly or by implication intended to remain in effect on or after termination. For clarity, sections 9.3, 9.5, 9.6, 9.7, 9.8 and 9.10.3 survive the termination of this CP/CPS.

9.11 Individual Notices and Communications with Participants

The repository described in section 2.1 Repositories (page 12) is the main communication channel for all IACA public information.

Additional communication channels are securely established bilaterally between participants for individual notices.

Each PKI participant acknowledges that they are responsible for keeping themselves informed of any notices and communication as set forth in this section.

9.12 Amendments

9.12.1 Procedure for Amendment

In order to amend this CP/CPS, it's necessary to submit a formal request to the contact person defined in section 1.5.2 Contact Person (page 10), indicating as a minimum:

- the requester's identification;
- the request reason; and
- the requested amendments.

The Security Officers will review the request and, in case of acceptance, will proceed to the necessary document updates, resulting in a new draft version of the document. The new draft document is then made available to all Working Group members and to affected parties (if any) for their review. From that date, the different parties have 15 business days to submit their comments. When that period ends, the Security Officers have 15 business days to analyse all the received comments and, if relevant, incorporate them on the document, after which the document is submitted to the PKI Policy

Management Group for ratification and publishing, following which the amendments will become final and effective.

9.12.2 Notification Mechanism and Period

Amendments of this policy come into effect as soon as a new version is published by the IACA and PKI participants are notified in accordance with section 9.11 Individual Notices and Communications with Participants.

9.12.3 Circumstances Under Which OID Must be Changed

This CP/CPS does not define or uses proprietary OIDs. Only OIDs from standard ISO/IEC 18013-5 [1] are used.

9.13 Dispute Resolution Provisions

Disputes arising out of this document that the Certificate is issued under shall be resolved using the following processes:

- The parties shall use their best endeavours to resolve any problem that arises by negotiating with each other;
- If the dispute is not resolved by the parties by negotiation, the dispute is to be referred to mediation. The mediation will be conducted in Brisbane, Queensland in accordance with the Resolution Institute's Mediation Rules. All other details concerning the mediation will be as agreed between the parties; and
- If the dispute is not resolved by the parties through mediation, then any party may commence any other form of action to resolve the dispute, including court proceedings.

9.14 Governing Law

This document is governed by, and are to be construed in accordance with, the laws from time to time in force in the State of Queensland.

The parties agree to submit to the courts having jurisdiction in the State of Queensland.

9.15 Compliance with applicable law

All parties agree to abide by the provisions of all applicable Commonwealth of Australia, State, Territory, or Local Government laws that relate to the subject matter of this document.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No party may assign or delegate this CP/CPS or any of its rights or duties under this CP/CPS, without the prior written consent of the CA.

9.16.3 Severability

If any section of this CP/CPS is determined to be incorrect, invalid or unenforceable, the other sections of this CP/CPS shall validly remain in effect. The parties may agree to amend the CP/CPS to replace the unenforceable section with a valid and enforceable section in accordance with section 9.12 Amendments (page 51).

In the event of a conflict between these CP/CPS requirements and a law, regulation or government order of any jurisdiction defined in section 9.14 Governing Law, IACA may modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

The failure of a party to enforce, at any time, any provision of this CP/CPS will not be construed to be a continuing waiver of that provision.

9.16.5 Force Majeure

Events considered to constitute a "force majeure" may include so-called "Acts of God," wars, terrorism, strikes, natural disasters, fire, failures of suppliers or vendors to perform, or failures of the Internet or other infrastructure.

The IACA is not liable for any delay or failure to perform an obligation under this CP/CPS to the extent that the delay or failure is caused by an occurrence beyond the IACA's reasonable control, including, but not limited to, any force majeure event.

9.17 Other provisions

No stipulation.

10 Bibliography

[1] ISO/IEC 18013-5:2021 - Personal identification — ISO-compliant driving licence — Part 5: Mobile driving licence (mDL) application

[2] RFC 5280 – Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

[3] ITU-T Recommendation X.509 (10/19): Information Technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, October 2014.

[4] RFC 5480 – Elliptic Curve Cryptography Subject Public Key Information

[5] RFC 3647: Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework

[6] RFC 2986 – PKCS#10: Certification Request Syntax Specification, version 1.7

11 Version History

Version	Date	Comments
1.0	2023-04-26	Public release revision