Information Security Section
Queensland Police Service

X.509 Certificate Policy

for the

QPS PKI

Version:	1.0
Status:	Consultation draft
Last updated:	31 March 2009
Classification:	UNCLASSIFIED

Summary

1. The Queensland Police Service (QPS) Public Key Infrastructure (PKI) is a three-tier PKI hierarchy and forms part of the Queensland Government PKI (QG PKI). The root of trust for the QPS PKI is the QG Root CA (QGRCA). The QPS Policy CA (QGPCA2) is directly subordinate to QGRCA. The QPS Issuing CAs are in turn subordinate to QGPCA2.
2. Participants in the QPS PKI include the Queensland Government PKI Policy Authority, QPS PKI Policy Authority, Certification Authorities, Registration Authorities, Subscribers, Relying Parties and Trusted Roles.
3. The QPS Certificate Policy (CP) supports three different assurance levels (Basic, Medium, and High) for public key certificates. The level of assurance associated with a public key is an assertion by a Certification Authority (CA) of the degree of confidence that a Relying Party may reasonably place in the binding of a Subscriber's public key to the identity and privileges asserted in the certificate.
4. Basic Assurance is suitable for certificates issued to a device, service or process not including PKI CA/RA components and requires:

    - the Subscriber to meet IRAL-2 identity assurance as a minimum, and
    - single factor authentication.

5. Medium Assurance is suitable for authentication certificates issued for access to the QPS network or for digital signing certificates and requires:

    - the Subscriber to meet IRAL-3 identity assurance as a minimum, and
    - two factor authentication.

6. High Assurance will not be used within the initial implementation of the QPS PKI. High Assurance requires:

    - the Subscriber to meet IRAL-4 identity assurance
    - strong cryptographic authentication mechanisms, and
    - at least two factor authentication.

7. Certificates will only be issued to Subscribers who are employees of QPS or other Queensland Government entities. To be issued with a certificate, all Subscribers must meet or exceed the requirements for the relevant assurance level defined above.
8. Subscribers must submit a request for a certificate through their officer-in-charge/section head, to a Registration Authority to obtain a certificate. A request for a CA certificate must be approved by the QPSPKIPA and QGPKIPA.
9. Signing certificates issued to smart cards will have a five year validity period for permanent employees and a one year validity period for contractors. To access information on the smart card the employee or contractor will be required to enter a PIN.
10. The physical components of the QPS PKI (HSM and Servers) must be housed in a Secure location as defined in the *Queensland Government Information Security Classification Framework* (QGISCF).
11. QPS Registration Authorities must be housed in an intruder resistant location as defined in the QGISCF. This requires tamper-evident barriers, highly resistant to covert entry, an effective means of providing access control during both operational and non-operational hours, all persons to wear passes and all visitors escorted at all times.

12. The QPS PKI must undergo an initial accreditation process for the QG PKI and will be subject to an annual external audit to maintain that accreditation.

Contents

1. INTRODUCTION

This document defines the policies that apply for the use of X.509 digital public key certificates by the Queensland Police Service (QPS) to:

- facilitate internal authentication to the QPS computer network
- provide digital signing of emails
- provide encryption of data and
- secure information management and exchange between QPS and other Queensland Government entities.

This policy applies to:

- the Queensland Government Policy Certification Authority (QGPCA2)
- all QPS Issuing Certification Authorities subordinate to QGPCA2
- all Registration Authorities that have been delegated by the above QPS Issuing Certification Authorities to perform identification and registration functions for Subscribers or to request the issuance, revocation and re-keying of certificates from the CA
- all Subscribers of the QPS PKI
- all Relying Parties of the QPS PKI.

The policies represent three different assurance levels (Basic, Medium, and High) for public key certificates. The level of assurance associated with a public key is an assertion by a Certification Authority of the degree of confidence that a Relying Party may reasonably place in the binding of a Subscriber's public key to the identity and privileges asserted in the certificate.

Level of assurance depends on the registration processes for Subscribers, the mechanisms used to manage the certificate and to control the use of the private key, and the security provided by the Public Key Infrastructure (PKI) itself.

This QPS CP is consistent with the Internet Engineering Task Force (IETF) *Public Key Infrastructure X.509 (IETF PKIX), RFC 3647, Certificate Policy and Certification Practice Statements frameworks*.

The terms and provisions of this X.509 Certificate Policy for the QPS shall be interpreted under and governed by applicable Commonwealth and Queensland state law.

1.1 OVERVIEW

The Internet Engineering Task Force (IETF) *Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Certificate Policy and Certification Practice Statement frameworks* provides a structure for certificate policy documents in the form of section headings and recommended content for each section. This document that defines the X.509 Certificate Policy for the QPS uses that framework.

1.2 DOCUMENT NAME AND IDENTIFICATION

This Certificate Policy (CP) is called the ***X.509 Certificate Policy for the QPS PKI*.**

QPS has registered three levels of assurance. Each level of assurance has been assigned an object identifier (OID) to be asserted in certificates issued by a Certification Authority (CA) that complies with the policy stipulations related to that level.

The OIDs registered by QPS for certificate policies are shown in *Table 1*. These OIDs are registered under the Queensland-Police-Service arc as:

{iso(1) member body(2) Australia(36)government (1)Queensland-government(3)Executive Branch (1)Queensland Police Service(2) Certificate Policies (1)}

Queensland Police Service -BasicAssurance ID::={id-certificate-policy 2}
Queensland Police Service -MediumAssurance ID::={id-certificate-policy 3}
Queensland Police Service -HighAssurance ID::={id-certificate-policy 4}

Table 1: QPS Policy Object Identifiers

Certificate Policy	Object Identifier (OID)	Certificate Policy URL
Queensland Police Service Basic	1.2.36.1.3.1.2.1.2	http://www.pki.qld.gov.au/QPS/cp.html
Queensland Police Service Medium	1.2.36.1.3.1.2.1.3	http://www.pki.qld.gov.au/QPS/cp.html
Queensland Police Service High	1.2.36.1.3.1.2.1.4	http://www.pki.qld.gov.au/QPS/cp.html

The stipulations presented in this CP apply to all three assurance levels (Basic, Medium, and High) unless otherwise noted.

1.3 PKI PARTICIPANTS

1.3.1 Certification Authorities

A Certification Authority (CA) is an entity authorised by the QPSPKIPA to generate, sign, and issue public key certificates.

The three tier Queensland Police Service PKI (QPS PKI) forms part of the Queensland Government PKI (QG PKI). The root of trust for the QPS PKI is the QG Root CA (QGRCA). The Queensland Government Policy CA (QGPCA2) is directly subordinate to QGRCA. The QPS Issuing CAs are in turn subordinate to QGPCA2.

CAs may register the Subscribers themselves, or may delegate that function to one or more separate Registration Authorities (RA).

QGPCA2, which hosts this CP, is jointly operated by the Queensland Government (QG) and QPS.

Each CA has a Certification Authority Manager (CAM) who is responsible for overseeing the management and operation of all components of the CA and for ensuring adherence of the CA to this CP.

1.3.2 Registration Authorities

A Registration Authority (RA) may be delegated by Certification Authorities to perform the identification and registration of Subscribers and associated certificate functions.

RAs may make requests of Certification Authorities for the issuance, revocation and re-keying of certificates but cannot sign certificates.

An RA operating under this CP shall perform its function in accordance with its respective Certification Practice Statement (CPS).

Each QPS RA has one Registration Authority Manager (RAM) who is responsible for overseeing the operations of the RA. Each RA has one or more Registration Officers (RO) who are responsible for registering Subscribers.

1.3.3 Subscribers

A Subscriber operating under this policy is the entity whose name appears as the subject in a certificate issued under this policy. A Certificate Authority is not a Subscriber.

A Subscriber may be an individual or a device or service.

Examples of individuals who are Subscribers are:

- QPS sworn member (police officer)
- QPS recruit
- QPS unsworn member (non police officer)
- QPS contractor
- QPS approved QG employee
- QPS approve QG contractor.
- QPS or Queensland Government devices such as firewalls, routers, servers or other hardware or software components used to secure QPS communications.

A device or service must have a custodian who has been identified and authenticated according to this CP and who is responsible for:

- overseeing the management and operation of the device
- ensuring adherence of the device or service to this CP.

Subscribers must agree in writing to their responsibilities under this CP prior to certificate issuance.

Subscribers shall:

- accurately represent themselves in all communications with the PKI authorities
- protect their private key(s) at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements and local procedures
- promptly notify the appropriate CA upon suspicion of loss or compromise of their private key(s)
- abide by all the terms, conditions, and restrictions levied on the use of their private key(s) and certificate(s).

1.3.4 Relying Parties

Each QPS certificate contains an OID defining the level of assurance with which QPS attests that the identity of the Subscriber using the certificate is the same as the one identified in the Subscriber field of the certificate.

With this information from the certificate the Relying Party determines whether it will continue with the transaction, or not at its own risk.

Only QPS or other Queensland Government entities are Relying Parties under this CP.

No entity external to the QPS or Queensland Government is authorised to use any certificate issued under this CP for any reason.

There is no separate Relying Party Agreement under this CP.

1.3.5 Other participants

1.3.5.1 Queensland Government PKI Policy Authority

The Queensland Government Public Key Infrastructure Policy Authority (QGPKIPA) owns the PKI Government Enterprise Architecture (GEA) Policy and QG PKI Framework and acts as the overall governance committee for the QG PKI.

The QGPKIPA is responsible for:

- the registration and maintenance of the QG Root CA
- approving all Certificate Policies and Certificate Practice Statements of the QG PKI and accrediting each CA issuing certificates under the QG PKI Framework
- ensuring that regular QG Policy audits of QG PKI processes occur no less frequently than an annual basis, and
- approving the compliance audit report for each CA issuing certificates under the QG PKI Framework.

1.3.5.2 Queensland Police Service PKI Policy Authority

The QPS Public Key Infrastructure Policy Authority (QPSPKIPA) is responsible for the QPS PKI Certificate Policy and acts as the overall governance committee for the QPS PKI.

The goal of the QPSPKIPA is to ensure that the QPS PKI:

- is implemented and maintained in accordance with the QPS PKI Certificate Policy and relevant Certificate Practice Statements.
- meets and maintains the conformance requirements set out in the QG PKI Policies, and
- can provide a level of assurance compatible with the requirements of the Queensland Government Authentication Framework (QGAF),

The QPSPKIPA is responsible for:

- joint management of the QGPCA2 Certification Authority
- management of the QPS PKI
- establishing, maintaining and publishing the policies for QGPCA2
- approving the establishment of all QPS CAs that are subordinate to QGPCA2 and approving the issuance of a CA certificate to subordinate CAs
- approving all Certificate Policies and Certificate Practice Statements issued or amended under the QPS PKI
- obtaining approval for all Certificate Policies and Certificate Practice Statements issued or amended under the QPS PKI from the QGPKIPA
- ensure Trusted Roles are resourced in accordance with this policy
- ensuring continued compliance of the QPS PKI with the requirements set out in the QG Root CP and the QPS Policy CP.

1.3.5.3 Other Participants

The QPSPKIPA reserves the right to contract for services with

- QPS internal service delivery branches and sub-branches
- other Queensland Government agencies
- external private organisations.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

This CP supports three levels of assurance:

- Basic
- Medium
- High.

Basic Assurance requires:

- the Subscriber to meet IRAL-2 identity assurance as specified in the Queensland Government Authentication Framework (QGAF) as a minimum
- single factor authentication.

Basic assurance is suitable for certificates issued to a device, service or process required to secure QPS communications not including PKI CA/RA components.

Medium Assurance requires:

- the Subscriber to meet IRAL-3 identity assurance as specified in QGAF as a minimum
- two factor authentication.

Medium assurance is suitable for authentication certificates issued for access to the QPS network or for digital signing certificates.

High Assurance requires:

- the Subscriber to meet IRAL-4 identity assurance as specified in QGAF
- strong cryptographic authentication mechanisms
- at least two factor authentication.

1.4.2 Prohibited Certificate Uses

Certification Authorities operating under this policy must not issue certificates for the use in applications by entities external to the Queensland Government.

Certification Authorities operating under this policy may issue Subscriber certificates to members of other Queensland Government Organisations but not to the Organisational entity itself.

Certification Authorities operating under this policy must not issue rudimentary level assurance certificates. Rudimentary assurance is suitable for a certificate issued when there is no registration process or the Subscriber has self registered for the certificate and no evidence of identity is required.

Certification Authorities operating under this policy must not issue basic level assurance certificates for:

- individual subscribers to authenticate to the QPS network
- email signing and
- encryption.

1.5 POLICY ADMINISTRATION

1.5.1 Organisation Administering the Document

The QPSPKIPA is responsible for all aspects of this CP. CAs operating under this policy are required to meet all facets of this CP. The QPSPKIPA will not issue waivers.

1.5.2 Contact Person

Questions regarding this CP should be directed to:

The Manager Information Security Section Information & Communications Technology Queensland Police Service 200 Roma Street GPO Box 1440 BRISBANE QLD 4001	Telephone: (07) 3008 4750 Facsimile: (07) 3221 4060 Email: ISS Manager@police.qld.gov.au

1.5.3 Person Determining CPS Suitability for the Policy

The QPSPKIPA and QGPKIPA shall jointly approve the CPS for each CA that issues certificates under this policy.

1.5.4 CPS Approval Procedures

All Certification Authorities to which this policy applies must have their respective Certification Practice Statements approved by the QPSPKIPA and QGPKIPA before issuing any certificates.

All Certification Authorities to which this policy applies must have any amendments to their respective Certification Practice Statements approved by the QPSPKIPA and QGPKIPA before issuing any certificates under the amendments.

The procedure for both new and amended Certification Practice Statements is:

- The QPSPKIPA may appoint a delegate to draft the CPS.
- The QPSPKIPA shall consider the CPS for approval.
- The QPSPKIPA will, subject to the CPS meeting the requirements of the Certificate Policy, approve the CPS for consideration by the QGPKIPA.
- The QGPKIPA will consider the CPS and notify the QPSPKIPA if approval or otherwise, has been granted.

1.6 DEFINITIONS AND ACRONYMS

See ss. 11 and 12.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The QPS Enterprise Directory may operate as the authoritative repository for:

- public signing keys issued to Subscribers
- public encryption keys
- keys required for archival and recovery

QGPCA2 will operate the authoritative repository for:

- all certificates issued to QPS Issuing Certification Authorities
- all Certificate Revocation Lists relating to certificates issued to QPS Issuing Certification Authorities.

QPS Issuing Certification Authorities may operate as repositories for:

- public signing keys issued to Subscribers
- Certificate Revocation Lists relating to Subscriber certificates
- private encryption keys
- keys required for archival and recovery.

The repositories for this CP are:

- the URL http://pki.qld.gov.au
- the URL http://pki.police.qld.gov.au .

All repositories shall implement access controls to prevent unauthorised modification or deletion of information.

The CAM is responsible for the repository functions of the CA

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The QPSPKIPA, or its delegate, is responsible for publishing:

- the QPS Issuing CA Certificate at:
  - http://pki.qld.gov.au by the QGPKIPA and http://pki.police.qld.gov.au by the QPSPKIPA
  - The AIA container within the QPS Enterprise Directory
- Certificate Revocation Lists (CRL) at
  - http://pki.police.qld.gov.au
  - The CDP container within the QPS Enterprise Directory
- this CP at http://pki.police.qld.gov.au and for providing this CP to the QGPKIPA for publication at http://pki.qld.gov.au
- information on the location of any Certification Practice Statement for CA's operating under this CP at http://pki.police.qld.gov.au

2.3 TIME OR FREQUENCY OF PUBLICATION

Certificates are published on creation. The frequency with which CAs publish CRLs is defined in s. 4.9.7.

2.4 ACCESS CONTROLS ON REPOSITORIES

The QPSPKIPA shall ensure access controls are applied to all repositories in accordance with QPS policy.

The X.509 Certificate Policy for QPS (this document) must only be created or modified by authorised QPS personnel.

The QPS Certification Practice Statements operating under this policy must only be created or modified by authorised QPS personnel.

Only those QPS personnel in Trusted Roles (see s. 5.2.1) are permitted to publish Certificates and Certificate Revocation Lists generated in accordance with this policy.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

This subcomponent prescribes the naming and identification of the Subscribers within the QG PKI.

3.1.1 Types of Names

Each entity must have a clearly distinguishable and unique X.501 Distinguished Name (DN) in the certificate subject name field.

All certificates issued by QPS Certificate Servers use the X.501 DN name format for issuer name fields constructed using DN keywords and attribute values listed below:

- Country (C)
- Organisation (O)
- Organisational Unit (OU), and
- Common Name (CN).

All CA Certificate subject names use the X.501 DN name format for subject name fields constructed using DN keywords and attribute values listed below:

- Country (C)
- Organisation (O)
- Organisational Unit (OU), and
- Common Name (CN).

Subscriber certificate subject name fields use the X.501 DN name format constructed from the Common Name (CN) only.

QPS certificates may include an alternate name form in the subjectAltName field. Smart card logon certificates must include the User Principal Name (UPN) in the subjectAltName field. Encryption Certificate must include both the UPN and the subject's email address in the subjectAltName field.

Certificates shall not use RFC-822 names or X.400 names, except in Alternate Name fields.

3.1.2 Need for Names to Be Meaningful

Certificates issued by CAs operating under this CP must identify in a meaningful way the Subscriber to which they are assigned.

3.1.3 Anonymity or Pseudonymity of Subscribers

CAs operating under this CP shall not issue anonymous certificates. Pseudonymous certificates may be issued by CAs to Subscribers to support internal operations.

CA certificates under this CP shall not contain anonymous or pseudonymous identities.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names shall be interpreted in accordance with the X.501 standard.

The QPSPKIPA is the authority responsible for QPS CA name space control.

3.1.5 Uniqueness of Names

Distinguished names must be unique for all Certification Authorities and Subscribers.

The QPSPKIPA reserves the right to make decisions about the validity, or otherwise, of all assigned certificates.

A party requesting a certificate may be required to demonstrate its right to use a particular name.

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

The CA and/or RA and the Subject of the certificate or certificate request must confirm the Subject's possession of the associated private key in a secure manner before the certificate is issued.

3.2.2 Authentication of Organisation Identity

Certification Authorities operating under this policy may issue Subscriber certificates to members of other Queensland Government Organisations but not to the Organisational entity itself.

Applicants from other Queensland Government Organisations must meet the Identity requirements for the certificate assurance level as defined in s. 1.4.1.prior to the certificate request being processed.

3.2.3 Authentication of Individual Identity

QPS Issuing CAs must issue certificates to Subscribers that are single entities. Certificates shall not be issued that contain a public key whose associated private key is shared.

All identification processes for Subscribers must meet the requirements for the assurance level sought as defined in s. 1.4.1.

3.2.4 Non-verified Subscriber Information

Prior to certificate issuance all information required in a certificate must be verified to meet the requirements of the assurance level sought as defined in s. 1.4.1.

3.2.5 Validation of Authority

Prior to issuing CA certificates, the QPSPKIPA shall verify that the applicant has the authority to act in the name of the CA by validating that the person submitting the request is the CAM for the applicant CA.

3.2.6 Criteria for Interoperation

The QPSPKIPA may make decisions about interoperability with another PKI subject to the policies defined in this CP and with the approval of the QGPKIPA.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication for Routine Re-key

Policies relating to re-key requests are defined in s. 4.7.

High Assurance certificates and any certificates asserting an IRAL-4 shall not be re-keyed on the basis of a current valid certificate and the Initial Identity Validation shall be undertaken each time.

For Medium and Basic Assurance certificate re-key requests the Subscriber's identity:

- may be established through use of the current signing key, and
- must meet the criteria defined in s. 1.3.3 at the time the re-keyed certificate becomes valid

3.3.2 Identification and Authentication for Re-key after Revocation

Issuance of a new certificate after certificate revocation shall be undertaken using initial identity validation in accordance with s. 3.2 of this CP.

3.4 Identification and Authentication for Revocation Request

The parties who can make a request for the revocation of a certificate are identified in s. 4.9.2.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

All applicants must successfully complete the Initial Identity Validation in accordance with s. 3.2 of this CP.

4.1.1 Who Can Submit a Certificate Application

An application for a CA certificate must be submitted to the QPSPKIPA by the CAM of the applicant CA.

An application for a RA certificate must be submitted to the QPSPKIPA by one of:

- the CAM of the CA that will generate the certificate for the applicant RA
- the RAM of the applicant RA

An application for an individual Subscriber certificate must be submitted by one of:

- the Registration Officer for an RA with the approval of the Subscriber's officer-in-charge / section head
- the Subscriber's officer-in-charge / section head
- the Subscriber with the approval of their officer-in-charge / section head.

An application for a Subscriber certificate for a device or service shall be submitted by the custodian of the device or service.

4.1.2 Enrolment Process and Responsibilities

Certification Authorities

To enrol an Issuing Certification Authority in the QPS PKI the applicant must:

- be identified to the same assurance level as the highest level of certificate that will be issued by the CA
- complete and submit an application to the QPSPKIPA, supported by the documentation identified in the Queensland Government PKI Framework.

The QPSPKIPA must

- arrange an Accreditation Audit of the QPS CA as part of the enrolment process,
- approve the enrolment of the CA in the QPS PKI before any certificates are issued
- submit the enrolment request to the QGPKIPA for accreditation of the CA to the QG PKI.

Registration Authorities

To enrol a Registration Authority in the QPS PKI the applicant must

- be identified to the same assurance level as the highest level of certificate that can be issued by the parent CA
- complete and submit an application to the QPSPKIPA with

    - documented Operational and Security Controls for the RA
    - Disaster Recovery and Business Continuity Plans for the RA

  The QPSPKIPA must:

- arrange an Accreditation Audit of the RA as part of the enrolment process,
- approve the enrolment of the RA in the QPS PKI before any certificates are requested by the RA
- provide the enrolment request and Accreditation Audit Report to the QGPKIPA with the next accreditation audit of the QPS PKI.

Subscribers

The enrolment process for Subscribers in the QPS PKI shall require the Subscriber to:

- complete the Evidence of Identity processes required under s. 1.4.1 of this CP prior to enrolment
- have a valid record in the QPS Enterprise Directory at the time of the enrolment request

Enrolment of a Subscriber in the QPS PKI occurs when a Subscriber certificate is issued to, and accepted by the Subscriber.

4.2 CERTIFICATE APPLICATION PROCESSING

Information in certificate applications must be verified before certificates are issued.

The procedures for verifying information in certificate applications must be described in the approved CPS for the CA.

4.2.1 Performing Identification and Authentication Functions

The QPS Policy CA QGPCA2 will only issue CA certificates to QPSPKIPA Certification Authorities.

The identification and authentication of a CA shall be the responsibility of the QPSPKIPA.

QPS Issuing Certification Authorities will only issue certificates to QPSPKIPA Registration Authorities and Subscribers.

The identification and authentication of a Subscriber shall be performed by the CA or the delegated RA and must meet the requirements specified for Subscriber authentication in ss. 3.2 and 3.3 of this CP.

4.2.2 Approval or Rejection of Certificate Applications

Approval or rejection of CA certificate applications operating under this policy must be authorised by the QPSPKIPA.

Rejection of a Subscriber certificate application that has been approved by an OIC / Section Head must be authorised by the CAM, RAM or Authorising Officer for the Issuing CA.

4.2.3 Time to Process Certificate Applications

There is no time limit for the QPSPKIPA or its delegates to consider a certificate application.

4.3 CERTIFICATE ISSUANCE

The CA must verify the requester and confirm the Subscriber's possession of the private key before generating, issuing and publishing the certificate and notifying the recipient or delegate.

4.3.1 CA Actions during Certificate Issuance

Upon receiving a request for a CA or Subscriber certificate the CA must:

- verify the bone fides of the certificate requester
- authenticate the request
- confirm Subject's possession of the private key
- generate and issue the certificate
- publish the certificate in accordance with s. 4.4.2.

4.3.2 Notification to Subscriber of Issuance of Certificate

The Subscriber or the custodian of a device or service shall be informed of the creation of a certificate and its availability.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct constituting certificate acceptance

The QPSPKIPA, or an authorised delegate, will provide the QGPKIPA with written or digitally signed acceptance of the QGPCA2 certificate.

The QPSPKIPA or an authorised delegate will provide the QGPKIPA with written or digitally signed acceptance of all QPS Issuing CA certificates.

First use of a private key by an RA will constitute acceptance of the certificate.

First use of a private key by a Subscriber will constitute acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

Certificate publication must occur prior to certificate usage. Certificate publication is defined in s. 2.2.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

The QPSPKIPA must be notified by the CAM whenever a CA operating under this policy issues a CA certificate.

The QPSPKIPA, or an authorised delegate, must notify the QGPKIPA whenever any CA operating under this CP issues a CA certificate.

The individual Subscriber, the individual Subscriber's officer-in-charge / section head, or a device or service custodian must be notified when a Subscriber or device or service certificate has been issued. The person or entity responsible for notification will be detailed in the CPS for the Issuing CA.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

The Subscriber's private key must:

- never leave the device on which it is stored. (for individual as opposed to device or service Subscribers under this CP, for QPS Medium Assurance certificates or higher, the associated private keys must be secured by hardware (smart card or Hardware Security Module)
- not be used after the expiration or revocation of the certificate
- be used in accordance with the terms and conditions in this policy
- only be used for QPS approved applications consistent with the certificate content.

No copy of any High Assurance or Medium Assurance Authentication/Signature Private Key shall be held by any entity other than the Subscriber.

4.5.2 Relying Party Public key and Certificate Usage

A Relying Party:

- must only use the certificate for the purpose for which it was issued, as indicated in the certificate content
- must only perform public key operations using a valid certificate
- is responsible for verifying the status of the certificate prior to use.

4.6 CERTIFICATE RENEWAL

Renewing a certificate means creating a new certificate with the same name, key, and other information as the old one, but with a new, extended validity period and a new serial number.

4.6.1 Circumstance for Certificate Renewal

Renewal of certificates is not supported by this CP. Certificates can only be re-keyed.

4.6.2 Who May Request Renewal

No stipulation.

4.6.3 Processing Certificate Renewal Requests

No stipulation.

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6 Publication of the Renewal Certificate by the CA

No stipulation.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 CERTIFICATE RE-KEY

4.7.1 Circumstance for Certificate Re-key

A certificate may be re-keyed only if:

- the certificate to be re-keyed is valid at the time the re-key operation is conducted
- the certificate is issued with either Basic or Medium level assurance
- the Subject of the certificate meets the criteria in:

  - s. 1.3.1, or
  - s. 1.3.2, or

- s. 1.3.3

- all the Subject information in the certificate is to be exactly the same in the new certificate
- the officer-in-charge / section head certifies that the Subscriber will meet the criteria defined in s. 1.3.3 at the time the re-keyed certificate becomes valid
- for individual Subscribers, for Medium Assurance certificates, all private keys used to sign re-key requests are secured on hardware devices such as smart cards.
- a new public key will be used in the new certificate to be issued. Specifically an existing public key must not be used.

A re-key of a CA certificate may be considered if:

- the certificates that are to be issued by a CA will have an expiry date later than that of the CA certificate's expiry date, or
- a CA updates its private key resulting in a new public key to be added to a certificate.

Certificates may undergo the re-key operation only once.

4.7.2 Who May Request Certification of a New Public Key

Subject to the requirements of s. 3.3, a re-key request can be made by:

- a Subscriber who is the Subject of the certificate
- the Subscriber's officer-in-charge / section head
- the custodian of a device or service
- a RAM
- a CAM.

All requests to re-key RA/CA certificates must be approved by the QPSPKIPA.

4.7.3 Processing Certificate Re-keying Requests

The procedure for processing re-key requests must ensure that the policies in s. 4.7.1 are implemented.

4.7.4 Notification of New Certificate Issuance to Subscriber

Notification will occur according to s. 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

Refer to s. 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

Refer to s. 4.4.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Refer to s. 4.4.3

4.8 CERTIFICATE MODIFICATION

Subscriber certificates shall not be modified under this CP.

4.8.1 Circumstance for Certificate Modification

A CA operating under this policy may modify the information in a CA certificate if:

- the certificate to be modified is valid at the time the modification is conducted
- the certificate is issued with Medium or High level assurance.
- the information to be changed does not include:

    - subject name
    - the assurance level.

4.8.2 Who May Request Certificate Modification

Subject to the requirements of s. 3.3, a certificate modification request can be made by:

- the CAM
- the QPSPKIPA
- the QGPKIPA for the QPS Policy CA QGPCA2.

The QPSPKIPA must approve modification of a CA certificate.

4.8.3 Processing Certificate Modification Requests

The CAM or QPSPKIPA must verify all changes to certificate information before a modified certificate is issued.

4.8.4 Notification of New Certificate Issuance to Subscriber

No Stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Refer to s. 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

Refer to s. 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Refer to s. 4.4.3.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

CAs operating under this policy shall issue CRLs covering all unexpired certificates issued by the CA.

Suspension of certificates is not allowed under this policy.

4.9.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the Subscriber identified in the Subject Name field and the public key defined within the certificate is no longer considered valid.

Examples of circumstances that invalidate the binding are:

- the certificate is modified
- a change in any identifying information or affiliation components that necessitate a change in DN
- the Subscriber's keys or certificate are no longer required by the Subscriber, for example, on termination of employment
- privilege attributes asserted in the certificate are reduced
- the certificate information is inaccurate, for whatever reason
- the Subscriber or CA identified in the Subject Name field can be shown to have violated the terms and conditions of this policy
- there is reason to believe the private key or media holding the private key has been compromised
- the Subscriber identified in the Subject Name field or other authorised party (as defined in the CPS) asks for his/her certificate to be revoked
- the device or service identified in the Subject Name field is decommissioned.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL.

4.9.2 Who Can Request Revocation

A request to revoke a CA Certificate must be made by one of the following:

- the CAM of the CA whose certificate is to be revoked
- the QPSPKIPA
- the QGPKIPA.

A request to revoke a RA Certificate must be made by one of the following:

- the RAM of the RA whose certificate is to be revoked
- the CAM of the CA that issued the certificate
- the QPSPKIPA.

A request to revoke a Subscriber certificate may be made by one of the following:

- the individual Subscriber identified in the Subject Name field of the certificate
- the OIC / Section Head of the individual Subscriber identified in the Subject Name field of the certificate
- the Manager, HR or his/her delegate when the period of employment of a staff member or contractor with QPS is terminated.
- the custodian of a device or service
- a Registration Officer or RAM on behalf of the QPSPKIPA
- the CAM of the CA that issued the certificate
- a member of the QPSPKIPA.

All requests to revoke a CA certificate must be approved by the QPSPKIPA prior to the revocation occurring.

All requests to revoke a RA certificate must be approved by the CAM of the relevant CA prior to the revocation occurring. The CAM must inform the QPSPKIPA when revocation occurs.

All requests to revoke an individual Subscriber certificate must be approved prior to the revocation occurring by one of:

- the officer-in-charge or section head of the individual Subscriber
- the Manager, Information Security Section or an authorised delegate
- the Manager, Human Resource Management Branch or an authorised delegate
- the Assistant Commissioner, Ethical Standards Command or an authorised delegate.

A QPS Issuing Certification Authorities, subject to the approval of the QPSPKIPA, may summarily revoke certificates within its domain.

4.9.3 Procedure for Revocation Request

Revocation requests are to be submitted to the CA and shall:

- identify the certificate to be revoked
- explain the reason for revocation
- allow the request to be authenticated (e.g., digitally or manually signed).

The CA will:

- authenticate requests
- add the Revoked Certificates to the CRL
- publish the CRL in accordance with s. 2.2

Revoked certificates shall be included on all new publications of the certificate revocation list until the certificates expire.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this policy.

4.9.5 Time within which CA must Process the Revocation Request

The CA shall process the revocation request on receipt.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties shall exercise due care before undertaking transactions and should use mechanisms and repositories provided by QPS for checking the status of certificates upon which they intend to rely.

4.9.7 CRL Issuance Frequency

Circumstances related to emergency CRL issuance are specified in s. 4.9.12.

A Certification Authority that operates off-line must issue and publish CRLs at least once every 6 months.

A Certification Authority that operates on-line must issue and publish CRLs at least once every 24 hours.

CRL's may be issued and published more frequently than the issuance frequency defined above.

CRL's shall be published not later than the next scheduled update.

All CRL's are published in accordance with ss. 2.2 and 4.9.8.

4.9.8 Maximum Latency for CRLs

CRLs shall be published within four (4) hours of generation or no later than the time specified in the nextUpdate field of the previously issued CRL for same scope which ever will occur first.

4.9.9 On-line Revocation/Status Checking Availability

There is no on-line revocation/status checking mechanism under this CP.

4.9.10 On-line Revocation Checking Requirements

There is no on-line CRL checking mechanism under this CP.

4.9.11 Other Forms of Revocation Advertisements Available

There are no other forms of revocation advertisements available under this CP.

4.9.12 Special Requirements Related To Key Compromise

If a certificate is lost or it is suspected that the private key is compromised, a new CRL containing the revoked certificate must be published within 18 hours of notification. If a CA is compromised, the CA's certificate must be revoked immediately, and the CRL updated immediately.

4.9.13 Circumstances for Suspension

Suspension of certificates is not allowed under this policy.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.10 CERTIFICATE STATUS SERVICES

All CAs shall provide CRLs.

4.10.1 Operational Characteristics

CRLs shall be available using at least one of the QPS standard protocols.

Example protocols include:

- Hypertext Transfer Protocol (HTTP)
- File Transfer Protocol (FTP)
- Lightweight Directory Access Protocol (LDAP).

4.10.2 Service Availability

CRLs will be available from repositories subject to QPS and QGPKIPA service availability requirements for CRL delivery mechanisms.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Refer to s. 4.9. for information about revocation when the certificate reaches end of subscription status.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

CA certificate and Subscriber signature keys are never escrowed by the CAs operating under this CP.

Escrow of Subscriber encryption keys is allowed.

Recovery of escrowed encryption keys requires role separation. Two people (a QPS employee in a Trusted Role and a key recovery agent) must be involved in the recovery operation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Session key recovery is not supported under this CP.

5. Facility Management and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

QPS Issuing Certification Authorities generating Basic and Medium Assurance certificates shall be housed in a secure facility operated to a level at least as secure as PROTECTED as defined in the *Queensland Government Information Security Classification Framework* (QGISCF).

QPS Registration Authorities shall be housed in an intruder resistant location as defined in the QGISCF.

CA cryptographic modules and Hardware Security Modules must be secured to at least the level of PROTECTED as defined in the QGISCF.

5.1.2 Physical access

Refer to s. 5.1.1.

5.1.3 Power and Air Conditioning

At a minimum all critical PKI equipment must be connected to a power supply that allows controlled shutdown in the event of power failure.

All critical PKI equipment must be operated in an environment where the temperature, humidity and air-borne particle concentrations are controlled and maintained within the operating specifications for the equipment.

5.1.4 Water Exposures

The QPS PKI facility shall be protected against water exposure.

5.1.5 Fire Prevention and Protection

The QPS PKI facility shall provide and maintain fire prevention and protection measures.

5.1.6 Media Storage

All PKI media shall be stored in accordance with its QGISCF classification.

5.1.7 Waste Disposal

All PKI waste media shall undergo disposal in accordance with its QGISCF classification.

5.1.8 Off-Site Backup

System backups sufficient to recover from system failure shall be made on a periodic schedule.

One copy of the backup shall be stored at an off-site location with physical and procedural controls commensurate to that of the operational CA.

Requirements for CA private key backup are specified in s. 6.2.4.1.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

Certification Authority Manager (CAM)

The CAM is responsible for overseeing the management and operation of a CA including:

- compliance with the X.509 Certificate Policy for QPS (this document)
- compliance with the CPS for the CA
- participation in regular audits
- compliance with QPS Security Policies and Procedures.

A CAM is required for each QPS CA. The same individual may act as CAM for multiple CAs.

A CAM shall agree in writing to their responsibilities under this CP at the time of appointment.

Certification Authority Administrator (CAA)

The CAA is responsible for the system administration of the CA PKI software including:

- installation, configuration, integration and maintenance of the CA PKI software
- configuring certificate profiles and/or templates
- configuring system audit parameters
- 2nd and 3rd level support.

A CAA cannot generate requests for, or issue certificates to, Subscribers.

PKI Operator (PO)

The PO is responsible for the routine operation of the CA or RA equipment including:

- system backup
- system recovery
- system troubleshooting
- maintaining and archiving audit and event logs.

Registration Authority Manager (RAM)

The RAM is responsible for overseeing the management and operation of a RA including:

- compliance with the X.509 Certificate Policy for QPS (this document)
- compliance with the CPS as it relates to the RA
- participation in regular audits.

A RAM is required for each RA. The same individual may act as a RAM for multiple RAs.

A RAM shall agree in writing to their responsibilities under this CP at the time of appointment

Registration Officer (RO)

The RO is responsible for the routine operation of the RA including:

- ensuring Subscribers comply with the certificate application requirements
- verifying the identity of Subscribers
- enrolling and maintaining Subscribers in the PKI
- requesting and executing the issuance of certificates
- verifying the accuracy of information included in certificates
- requesting and executing the revocation of certificates
- notifying a Subscriber of certificate issuance and revocation.

A RO may request and issue their own certificate provided written approved is obtained from an Authorising Officer before the certificate is issued.

Authorising Officer (AO)

The AO is responsible for maintaining the integrity of certificate issuance including:

- approving the issuance of certificates
- requesting or approving the revocation of certificates.

An AO cannot approve issuance of their own certificate.

Internal Auditor

The Internal Auditor role shall be responsible maintaining the integrity of the QPS PKI including:

- performing or overseeing internal compliance audits to ensure that all Certification Authorities, and associated Registration Authorities are operating in accordance with:
  - the X.509 Certificate Policy for QPS (this document)
  - the associated CPS
  - the QGPKIPA requirements
- reviewing audit and event logs
- the publication of audit reports describing the results of the compliance audits
- making recommendations for change to the QPS PKI policies, operations and practices to ensure compliance is achieved.

An internal auditor must not hold any other trusted role.

Cryptographic Module Administrator Token Holder

The Cryptographic Module Administrator token holder role shall be responsible for:

- Authorize the addition of HSMs to the security world
- Deletion of HSMs from the security world
- Replacement of HSMs in the security world
- Creation of operations tokens
- Replacement of operations tokens
- Replacement the Administrator token set
- Recover HSM operator token holders PINs

Cryptographic Module Operations Token Holder

The Cryptographic Module Operations Token Holder role shall be responsible for:

- Activating offline CA key material
- Activating application keys that use Operations tokens for activation approval

Key Recovery Agent

The Key Recovery Agent is responsible for recovery of escrowed encryption keys.

5.2.2 Number of Persons Required per Task

The QPS PKI requires a maximum of nine Cryptographic Module Administrator Token Holders. All Cryptographic Module Administrator activities identified above require a quorum of two Cryptographic Module Administrator Token Holders to be authenticated prior to starting the tasks.

An Administrator token holder can act as the console operator for an activity, but cannot also act as a token holder to authorise the operation. Two different token holders must authorise the management action. A console operator refers to the person executing the authorised PKI tasks or PKI support tasks.

The Cryptographic Module Administrator Token Holders for the QPS Policy CA can be members of an organisation external to QPS.

Key recovery requires two people (the key recovery agent and one other trusted role) to be involved in the recovery operation.

5.2.3 Identification and Authentication for Each Role

All people assigned to a Trusted Role require QPSPKIPA approval and must have met the identification requirements necessary to meet the medium assurance level, as defined in s. 1.4.1, prior to being appointed to the trusted role/s.

5.2.4 Roles Requiring Separation of Duties

An individual may hold more than one role with the exception of the Auditor role.

An individual holding an auditor role must not be assigned any other role.

Procedural controls shall be in place to ensure separation of duties between the Registration Officers, Authorising Officer and Certification Authority Administrators

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

All people appointed to a Trusted Role:

- are subject to the terms and conditions that apply to their QPS employment or contract arrangement
- should have qualifications and experience commensurate with the functions and responsibilities for the roles defined in this CP.
- should to be appointed in writing by the QPSPKIPA or be party to a contract for PKI services.

5.3.2 Background Check Procedures

No Stipulation.

5.3.3 Training Requirements

The QPSPKIPA is responsible for providing training to people filling QPS PKI related roles and may authorise PKI related training to any party including:

- people appointed to Trusted Roles
- members of the QPSPKIPA
- people from external organisations that support the QPS PKI
- any other member of QPS determined by the QPSPKIPA.

5.3.4 Retraining Frequency and Requirements

The QPSPKIPA may provide re-training to the parties identified in s. 5.3.3.

5.3.5 Job Rotation Frequency and Sequence

The QPSPKIPA may implement job rotation for Trusted Roles subject to the requirements of this CP.

5.3.6 Sanctions for Unauthorised Actions

Any unauthorised actions carried out in relation to the QPS PKI may be subject to administrative or disciplinary action by QPS.

The QPSPKIPA will be responsible for reporting all breaches of this CP, Certification Practice Statements, or other published procedures that may require administrative or disciplinary action to the appropriate QPS Authorities.

5.3.7 Independent Contractor Requirements

Individuals contracted to provide PKI related services for QPS will be subject to the same criteria as QPS employees.

Agencies and organisations contracted to provide PKI related services for QPS will be subject to the terms and conditions of the contract.

5.3.8 Documentation Supplied to Personnel

The QPSPKIPA, or its authorised delegate, will provide personnel with documentation and materials commensurate with their role and/or the training to be provided under this CP.

5.4 AUDIT LOGGING PROCEDURES

The audit logs must be maintained in accordance with:

- s. 95 *Admissibility of statements produced by computers* of the *Evidence Act 1977* (Qld)
- *Queensland Government Information Standard 40: Recordkeeping*
- *Queensland Government Information Standard 41: Managing technology-dependent records.*

5.4.1 Types of Events Recorded

Audit log files shall be generated for all events relating to the security of the QPS PKI.

The following types of PKI auditing should be undertaken:

- security, including:
  - user access
  - file management
  - breaches
  - user account management
  - physical access/site security
- system usage, including:
  - Certificate and CRL management
  - key management;
  - configuration management
  - anomalies and fault management.

For each auditable event, the audit record should include:

- the type of event
- the date and time the event occurred
- a success or failure indicator for attempted CA certificate signature or revocation
- the identity of the entity and/or operator that caused the event
- the message source, destination and contents for messages requesting CA actions.

5.4.2 Frequency of Processing Log

Audit logs shall be reviewed at least annually. The Internal Auditor, in consultation with the QPSPKIPA, shall determine and publish an annual schedule of auditing to be undertaken during the following year.

The audit data must be transferred prior to overwriting or overflow of automated security audit log files.

5.4.3 Retention Period for Audit Log

Audit logs shall be retained in accordance with the Public Records Act 2002 (Qld).

5.4.4 Protection of Audit Log

Audit logs shall be secured to prevent:

- modification
- deletion
- unauthorised access.

Audit logs may be copied for reporting purposes. The copied audit logs must retain the integrity of the information contained in the original.

5.4.5 Audit Log Backup Procedures

Audit logs must be backed up.

5.4.6 Audit Collection System (Internal vs. External)

The Audit Collection System may be:

- wholly external to the QPS PKI
- a component of the QPS PKI
- a combination of external and internal systems identified above.

The audit Collection System shall run independently of the QPS PKI.

If the Audit Collection System is known to have failed, the CA shall cease all operation except for revocation processing until the security audit capability can be restored.

5.4.7 Notification to Event-Causing Subject

The QPSPKIPA may provide notification to a subject that caused an audit event to occur about that audit event.

5.4.8 Vulnerability Assessments

The QPSPKIPA may implement vulnerability assessment and analysis processes and systems to identify potential attempts to breach the security of the QPS PKI.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Events Archived

Archive records shall be detailed enough to establish the validity of a signature and of the proper operation of the PKI. At a minimum, the following documentation and data shall be archived:

- QPSPKIPA and QGPKIPA accreditation documentation for QPS CAs and RAs
- the X.509 Certificate Policy for QPS and updates
- all Certification Practice Statements and updates

- other documentation concerning operations of the PKI as determined by the QPSPKIPA from time to time.
- PKI application / software / repository configuration documentation and updates
- completed application forms relating to certificate requests and revocation requests
- all certificates and CRLs issued and/or published
- audit logs (in accordance with s. 5.4.1)
- identity authentication data as per s. 3.2.3 for:

    - QPSPKIPA members
    - trusted Roles personnel
    - subscribers

- documentation of receipt and acceptance of certificates and/or tokens (if applicable)
- other data or applications to verify archive contents
- all QPS PKI communications involving and between the following parties:

    - QPSPKIPA
    - QGPKIPA
    - personnel holding Trusted Roles
    - Compliance Auditors
    - Subscribers
    - Relying Parties.

5.5.2 Retention Period for Archive

PKI information archives shall be retained in accordance with the *Public Records Act 2002* (Qld).

5.5.3 Protection of Archive

Access to archived information shall be approved by the QPSPKIPA.

Archived information may be copied for reporting purposes. The copied information must retain the integrity of the original data.

The QPSPKIPA may archive any of the following to enable access to archived records:

- PKI operations systems
- PKI hardware
- network infrastructure components
- applications that support the QPS PKI operations
- PKI virtual machines
- PKI applications
- PKI system and equipment configuration.

5.5.4 Archive Backup Procedures

Refer to s. 5.5.2.

5.5.5 Requirements for Time-Stamping of Records

Refer to s. 5.5.2.

5.5.6 Archive Collection System (Internal or External)

The archive collection system may be internal or external to the QPS PKI. The archival collection system must operate independently of the QPS PKI.

5.5.7 Procedures to Obtain and Verify Archive Information

The QPSPKIPA may implement procedures and processes to verify archive information.

5.6 KEY CHANGEOVER

CAs must not issue Subscriber certificates that extend beyond the expiration dates of their own certificates and public keys.

A CA certificate may be re-keyed during the life of the certificate if there is a risk that the CA private key could be compromised. If a re-key occurs, only the new key will be used for certificate signing purposes from that time.

The older, but still valid, certificate must be available to verify old signatures until all of the Subscriber certificates signed under it have also expired or are revoked.

If the old private key is used to sign CRLs that contain certificates signed with that key, then the old key must be retained and protected.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

The QPSPKIPA must be notified if the QPS PKI is compromised or suspected of being compromised.

The QPSPKIPA will investigate and report on the compromise or suspected compromise in accordance with QPS policies.

The QPSPKIPA must notify the QGPKIPA and all relevant QPS PKI stakeholders, if the QPS PKI is compromised.

The following events are examples of compromises or suspected compromises of the QPS PKI that must be reported to the QPSPKIPA:

- unauthorised use of the CA, RA or Subscriber private key is discovered or suspected
- unauthorised use, destruction or modification of a QPS Signing or Encryption Certificate is discovered or suspected
- unauthorised access to any PKI software or hardware is discovered or suspected
- unauthorised access to any PKI information is discovered or suspected
- unauthorised, deliberate or accidental modification, deletion or removal of PKI hardware or software is discovered or suspected
- malicious attacks on the PKI irrespective of the means, infrastructure or resources used.

The QPSPKIPA must be notified of incidents occurring with the QPS PKI.

The following are examples of the types of incidents that must be reported and which require the QPSPKIPA to notify all relevant PKI stakeholders:

- any planned or unplanned outage in the QPS PKI

- disaster recovery procedures are initiated for the QPS PKI or a component of the PKI.

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

The QPSPKIPA must be notified if any computing resources including software, data and hardware are corrupted or suspected of being corrupted.

The QPSPKIPA will implement procedures for the restoration of the QPS PKI if a computing resource, including software, data and hardware, is corrupted.

5.7.3 Private Key Compromise Procedures

Refer to s. 5.7.1.

5.7.4 Business Continuity Capabilities after a Disaster

All CAMs operating under this CP are required to maintain a Business Continuity and Disaster Recovery Plan approved by the QPSPKIPA.

5.8 CA OR RA TERMINATION

The CAM or RAM must notify the QPSPKIPA and all relevant stakeholders if a QPS CA or RA is to be terminated, including notification of procedures for the continuance or otherwise of PKI services.

The QPSPKIPA must notify the QGPKIPA if a QPS CA is terminated.

When a CA or RA is terminated, the CAM or RAM must:

- surrender the CA/RA keys
- implement the archival processes defined in s. 5.5.

6. TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

QPS Policy CA QGPCA2

Generation of key pairs for the QGPCA2 will be requested by the QPSPKIPA from the QGPKIPA and will be subject to the policies of this CP and the QG Root CP.

QPS Issuing Certification Authorities

Key pairs for QPS issuing CAs shall be generated in FIPS 140-2 level 3 or higher cryptographic modules.

The QPSPKIPA will approve all requests to generate key pairs for QPS Issuing CAs. Requests must be made to the QPSPKIPA by the Issuing CA CAM.

Registration Authorities

Key pairs for QPS RAs shall be generated in FIPS 140-2 level 2 or higher cryptographic modules.

Generation of key pairs for QPS RAs will be requested by the CAM for the RA.

Subscribers

Subscriber key pairs for Medium Assurance certificates shall be generated in a FIPS 140-2 level 2 or higher cryptographic module that must reside on the Subscriber security device, for example, smart card or token.

Subscriber key pairs for Basic Assurance certificates can be generated in FIPS 140-1/2 level 2 software cryptographic modules (usually web browser certificate cache or other comparable certificate store).

Subscriber key pairs can be generated by:

- the Subscriber
- a QPS RA
- a QPS Issuing CA.

6.1.2 Private Key Delivery to Subscriber

For Medium Assurance signing certificates, the Subscriber private key must be generated on the device used to store the key.

If a Subscriber's private key is generated by a CA or RA, the key must be delivered to the Subscriber identified in the Subject Name of the certificate using a secure delivery method. The Subscriber shall acknowledge receipt of the private signature key.

6.1.3 Public Key Delivery to Certificate Issuer

A QPS Issuing CA must securely deliver its public key to the QGPCA2 Policy CA using an approved request signed by the QPS Issuing CA.

A QPS RA must securely deliver the Subscriber's public key to the QPS Issuing CA using an approved request signed by the RA.

6.1.4 CA Public Key Delivery to Relying Parties

The Public Keys for the QG Root CA, the QPS Policy CA QGPCA2, and QPS Issuing CAs are made available at the locations specified in ss. 2.1 and 2.2 of this CP.

6.1.5 Key Sizes

This CP requires use of RSA PKCS #1 or RSASSA-PSS signatures. Additional restrictions on key sizes and hash algorithms are detailed below. Certificates issued under this policy shall contain RSA public keys. The following key sizes and algorithms must be enforced for the QPS PKI:

- QPS Basic Assurance certificates shall contain subject public keys of at least 1024 bits for RSA and be signed with the corresponding private key.
- QPS Medium Assurance certificates shall contain subject public keys of at least 2048 bits for RSA and be signed with the corresponding private key.
- Policy CAs that generate certificates for issuing CAs under this CP shall use signature keys of at least 4096 bits for RSA algorithms.

- Issuing CAs that generate certificates for entities and CRLs under this CP shall use signature keys of at least 2048 bits for RSA algorithms.
- CAs that generate certificates and CRLs under this policy shall use the SHA-1 hash algorithm when generating digital signatures.

6.1.6 Public Key Parameters Generation and Quality Checking

Not Stipulated.

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

The use of a specific key is constrained by the key usage extension in the X.509 certificate. All certificates shall include a critical key usage extension.

Subscriber user certificates shall be used only for digital signing or encrypting, but not both. In particular:

- Certificates used for authentication set the digitalsignature bit
- Certificates used for key encryption set the keyEncipherment bit
- Certificates used for data encryption set the dataEncipherment bit
- Certificates used for digital signatures set the digitalsignature bit
- CA certificates set cRLSign and keyCertSign bits
- Certificates used for key agreement set the keyAgreement bit.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is FIPS 140-2 *Security Requirements for Cryptographic Modules.*

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

A single person shall not be permitted to activate or access any cryptographic module that contains the complete CA private key for a policy CA operating under this CP.

All off-line CA management operations will require that the actions of the CA operator be authorised by two separate individuals. The two individuals (K) can be comprised of any of the Cryptographic Module operator token holders (M) (see s. 5.2.2).

Issuing CA private keys will be protected using module protection. Module protection ensures that a CA's private key is only accessible within the confines of a FIPS 140-2 level 3 Cryptographic Module device.

6.2.3 Private Key Escrow

CA and Subscriber private signature keys are never escrowed or exported.

Subscriber private encryption keys may be escrowed.

6.2.4 Private Key Backup

Private keys for the QPS Policy CA (QGPCA2) must be backed up securely.

Private keys for QPS Issuing CAs and RAs must be backed up using the cryptographic module's backup capability.

No more than two backup copies of the CA private signature keys may be made.

All copies of the CA and RA private signature key shall be accounted for and protected in the same manner as the original.

At least one copy of the CA or RA private signature key shall be stored off-site.

6.2.5 Private Key Archival

CA and Subscriber private signatures keys shall not be archived.

Subscriber encryption private keys shall be archived securely and shall require role separation in the key recovery procedures (see s. 5.2.2). The encryption private key in archive must not be stored in plaintext.

6.2.6 Private Key Transfer into or from a Cryptographic Module

A private key not stored in a cryptographic module must never exist in plaintext form outside the cryptographic module boundary.

Private key transfer must only be performed by personnel holding trusted roles.

6.2.7 Private Key Storage on Cryptographic Module

Refer to s. 6.2.1.

6.2.8 Method of Activating Private Key

For certificates issued under this policy, the Subscriber must be authenticated to the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to passwords, PINs or biometrics.

Entry of activation data shall be protected from disclosure, that is, the data should not be displayed while it is entered.

For the QPS Policy CA (QGPCA2), a minimum of two of the authorised Cryptographic Module Operations Token Holders must authorise activation of the private key.

For issuing CAs under this CP, the private key material must be protected so that only authorized modules can activate the CA's private key. Activation will require that a HSM Operations token be available to validate the existence of a FIPS 140-2 level 3 security context.

6.2.9 Method of Deactivating Private Key

After use, the cryptographic module for off-line CAs shall be deactivated, for example, via a manual logout procedure, removal of the Cryptographic Module Operations tokens, or automatically after a period of inactivity as defined in the applicable CPS.

6.2.10 Method of Destroying Private Key

The CAM shall ensure that CA and RA private signature keys are destroyed when they are no longer needed.

Cryptographic Module Operator Token Holders shall surrender their Cryptographic Module tokens to CA/RA personnel or trusted agents for destruction when they are no longer

needed. Physical destruction of the Hardware Security Module (HSM) is not required. The HSM tokens may be destroyed.

Subscriber digital signature private keys shall be destroyed by the CAM, RAM or Registration Officer.

6.2.11 Cryptographic Module Rating

See s. 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

All certificates and associated public keys issued by the QPS Policy CA and QPS Issuing Certification Authorities under this CP must be archived.

6.3.2 Certificate Operational Periods and Key Usage Periods

The usage period for the QPS Policy CA (QGPCA2) key pair is a maximum of 34 years (based on a 4096 bit key length).

The QPS Policy CA (QGPCA2) private key may be used to sign certificates with a maximum life time of 10 years.

For all QPS Issuing Certification Authorities operating under this policy the usage period for the QPS Issuing CA key pair is a maximum of 10 years (based on a key length of 2048 bits).

The QPS Issuing CA private key may be used to sign certificates with a maximum life time of five years, but may be used to sign CRLs for the entire usage period.

All certificates signed by a CA key pair operating under this CP must expire before the end of the CA's key pair's validity period.

All Subscriber certificates issued to QPS permanent employees under this policy must have a maximum validity period of five years.

All Subscriber certificates issued to QPS contractors under this policy must have a maximum validity period of one year.

All Subscriber signature private keys must have the same validity period as their corresponding public key.

The usage period for Subscriber key management private keys and Subscriber encryption private keys is not restricted.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

CA activation data (eg, password, PINs) may be user-selected by each of the multiple parties holding that activation data. If the activation data must be transmitted, it shall be via a securely protected channel.

RA and Subscriber activation data may be user-selected.

Transmission of activation data must be via one or more securely protected channels. The cryptographic module must not be used for transmission of activation data. The transmission process must not be part of the key pair generation process.

The Subscriber activation process may involve the use of authorised third parties.

All activation data must be securely destroyed once it is no longer required.

6.4.2 Activation data protection

Activation Data for CAs shall be protected by a FIPS-140 certified device and its activation will require a quorum of designated operators

Information used to unlock Subscriber private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms.

6.4.3 Other Aspects of Activation Data

QPS may implement data activation processes for Subscribers that allow a person other than the Subscriber to hold part, but not all parts, of the activation data.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

QPS CA equipment shall use operating systems that:

- require authenticated logins
- provide discretionary access control
- provide a security audit capability
- meet the terms and conditions of the X.509 Certificate Policy for QPS (this document).

6.5.2 Computer Security Rating

No Stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

QPS PKI related system development and implementation must use controls that do not breach the terms and conditions of the X.509 Certificate Policy for QPS (this document).

6.6.2 Security Management Controls

The configuration, including modifications and upgrades of QPS PKI components shall be documented.

There shall be a mechanism for detecting unauthorised modification to the software or configuration of QPS PKI components.

The QPS Issuing Certification Authorities must only have applications or component software or hardware installed that are directly related to the operation of the QPS PKI.

6.6.3 Life Cycle Security Controls

Equipment (hardware and software), including modifications and upgrades, procured for the QPS PKI shall be:

- purchased through a mechanism that will to reduce the likelihood that any particular component was tampered with.
- shipped or delivered via controlled methods that provide a continuous chain of accountability from its origin to its destination and handover to QPS
- deployed using QPS authorised personnel.

6.7 NETWORK SECURITY CONTROLS

The QPS Policy CA (QGPCA2) will normally be off-line, except on an as needed basis. The QPS Policy CA (QGPCA2) must never be connected to the QPS network.

QPS Issuing CAs must be connected to the QPS network.

Network security controls must include:

- protection of QPS PKI equipment against known network attacks
- boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment

6.8 TIME-STAMPING

A source of trusted time should be used to support time stamping of data.

7. CERTIFICATE, CRL AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

Certificates generated under this QPS PKI CP shall conform to the IETF PKIX, RFC 5280.

Certificates generated under this QPS PKI CP shall use only a signatureAlgorithm identified in RFC 3279, RFC 4055, or RFC 4491.

QG PKI High Assurance certificates generated under this QPS PKI CP shall not use any signatureAlgorithm involving the MD2, MD4 or MD5 message digest algorithms. Such algorithms shall be accepted for any other certificates which may be recognised by the QPS PKI.

All certificates shall have a fixed notAfter date. A notAfter date of 99991231235959Z shall not be used.

7.1.1 Version Numbers

All QPS PKI certificates shall be X.509 version 3 certificates where the version field contains the integer ‘2’.

Formats of the various certificates issued under this CP are described in *QPS Certificate Profile.doc*.

7.1.2 Certificate Extensions

Standard certificate extensions used in certificates issued under this CP must be defined in the Certificate Profile in the CPS for the CA and shall comply with RFC 5280.

QPS PKI certificates shall not include critical private extensions.

7.1.3 Algorithm Object Identifiers

Certificates issued by the CAs under this CP shall identify the signature algorithm using the OID: sha-1WithRSAEncryption { iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5 }.

Certificates under this CP will use the following OID for identifying the algorithm for which the subject key was generated: rSAEncryption {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.1.4 Name Forms

The subject and issuer fields of the certificate are populated with a unique Distinguished Name in accordance with s. 3.1. The attribute type is further constrained by RFC 5280 and RFC 2247.

7.1.5 Name Constraints

Refer to s. 7.1.4.

7.1.6 Certificate Policy Object Identifier

Certificates issued under this policy shall assert the OID appropriate to the level of assurance with which it was issued, as defined in s. 1.2.

7.1.7 Usage of Policy Constraints Extension

Certificates issued under this CP will not use the policy constraints extension.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this policy shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The certificatePolicies extension must not be marked critical.

The certificatePolicies extension may not be present in the certificate. If not present then the assurance level for the certificate is Basic. The Relying Party should process the certificate in a manner commensurate with the Basic level of assurance.

If present the certificate must contain one of the OIDs identified in s. 1.2. The Relying Party should process the certificate in a manner commensurate with the level of assurance asserted.

7.2 CRL PROFILE

CRLs generated under this CP must conform to the IETF PKIX, RFC 5280.

7.2.1 Version Numbers

CAs operating under this CP will issue X,509 version two (v2) CRLs with the version field populated with the integer ‘1’.

7.2.2 CRL and CRL Entry extensions

The CRLs issued by CAs operating under this CP must not use proprietary extensions. All extensions defined by the X.509 standard are marked non-critical.

Format of the CRL profile is described in *QPS Certificate Profile.doc*.

7.3 OCSP PROFILE

Not applicable.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The QPSPKIPA must ensure that the QPS PKI is:

- accredited by the QGPKIPA prior to using the QPS PKI for operational purposes
- audited annually by an external auditor to maintain accreditation to the QG PKI.

The QPSPKIPA may engage the services of the QPS Internal Auditor, or any other qualified auditor, to undertake audits of the QPS PKI, in addition to the annual Accreditation Audit.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

External auditors engaged by the QPSPKIPA to assess the QPS PKI will be selected from the Queensland Government PKI Audit Panel.

The QPS Internal Auditor may be used to conduct QPS PKI assessments.

The QGPKIPA will be responsible for auditing the QG Root CA and QG Policy CAs.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The internal or external auditors must not hold any other Trusted Role in the QPS PKI.

8.4 TOPICS COVERED BY ASSESSMENT

The topics to be covered by the annual Accreditation Audit of the QPS PKI are:

- compliance of the QPS PKI with the QG requirements for an annual audit
- CP changes
- CPS changes
- compliance of the QPS Issuing Certification Authorities with the QPS Certificate Policy for QPS (this document)
- compliance of the QPS Registration Authorities with the QPS Certificate Policy for QPS (this document)
- compliance of the QPS Issuing Certification Authorities with its Certification Practice Statement
- security breaches and compromises and mitigation.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

The QPSPKIPA must consider all recommendations arising from an audit assessment.

The CAM for an Issuing CA is responsible for addressing any serious deficiencies in a timely manner.

The QPSPKIPA must take timely and appropriate action to ensure the QPS PKI does not compromise the QG PKI.

8.6 COMMUNICATION OF RESULTS

The Accreditation Audit report shall be provided to the QPSPKIPA by the external Auditor. The QPSPKIPA will provide a copy of the Accreditation Audit report to:

- QPS Executive
- QGPKIPA.

Internal assessment reports shall be provided to the QPSPKIPA. The QPSPKIPA may provide a copy of the annual assessment report to other parties

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

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

QPS maintains its own insurance in line with QG policy.

9.2.2 Other Assets

QPS is not liable for damages caused by the implementation of this policy or related Certification Practice Statements.

9.2.3 Insurance or Warranty Coverage for End-Entities

QPS maintains its own insurance in line with QG policy.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

Information relating to this CP shall be protected in accordance with:

- this CP
- *Queensland Government Information Standard 18: Information Security*
- *Queensland Government Information Security Classification Framework* (QGISCF).

9.3.1 Scope of confidential information

All non-public QPS information is classified in accordance with QGISCF and is confidential.

9.3.2 Information not within the scope of confidential information

All information classified as public in accordance with QGISCF is not confidential.

9.3.3 Responsibility to protect confidential information

All QPS PKI participants must protect QPS information in accordance with the QGISCF.

9.4 PRIVACY OF PERSONAL INFORMATION

Private information collected under this CP will be protected in accordance with this CP and the *Queensland Government Information Standard 42: Information Privacy*.

9.4.1 Privacy plan

No Stipulation.

9.4.2 Information treated as private

The following QPS PKI information is classified as private:

- CA, RA or Subscriber private key
- audit logs
- user PIN or password.

9.4.3 Information not deemed private

No Stipulation.

9.4.4 Responsibility to protect private information

All PKI participants who obtain access to Private QPS PKI information that does not occur as part of their normal duties must manage that information in accordance with:

- this CP
- *Queensland Government Information Standard 18: Information Security*
- *Queensland Government Information Standard 42: Information Privacy*.

It is the responsibility of the PKI participant to immediately notify the QPSPKIPA about any information security incident.

The QPSPKIPA will manage the incident in accordance with:

- the terms and conditions contained in this CP
- *Queensland Government Information Standard 18: Information Security*
- *Queensland Government Information Standard 42: Information Privacy*.

9.4.5 Notice and consent to use private information

A Subscriber may be required to sign a release from privacy for the private key used for encryption.

9.4.6 Disclosure pursuant to judicial or administrative process

Not stipulated.

9.4.7 Other information disclosure circumstances

Not stipulated.

9.5 Intellectual Property Rights

All intellectual property contained within and/or related to the QPS PKI is owned by QPS.

9.6 Representations and Warranties

The QPS makes no representations or warranties in regard to any part of the QPS PKI, or any Key or Certificate, other than as specifically provided in this CP.

This CP is not a contract and cannot be used for warranty purposes.

No Certification Practice Statements under this CP may be entered into as legally binding contracts. Certification Practice Statements under this CP may not be used for warranty purposes.

9.7 Disclaimers of Warranties

QPS disclaims all warranties, express or implied in respect of this CP and any related CPS.

9.8 Limitations of Liability

The QPS shall not be liable to any party in respect to this CP.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This CP, in its entirety, and all Certification Practice Statements, shall remain in force for the life of the QPS PKI unless superseded.

This CP becomes effective when approved by the QPSPKIPA.

9.10.2 Termination

Termination of this CP is at the discretion of the QPSPKIPA in consultation with QGPKIPA.

9.10.3 Effect of Termination and Survival

The requirements of this CP remain in effect through to the end of the archive period for the last certificate issued.

9.11 Individual Notices and Communications with Participants

The QPSPKIPA shall establish appropriate procedures for communications with parties operating under this policy, as applicable.

9.12 Amendments

9.12.1 Procedure for Amendment

The QPSPKIPA shall review this CP at least annually. Corrections, updates, or changes to this CP shall be publicly available.

Proposals for change to this CP shall be provided to the in s. 1.5.2. The proposals must include:

- detailed description of the change
- change justification
- contact information for the person requesting the change.

The QPSPKIPA may consider any proposals for change.

The QPSPKIPA must approve all proposed changes to this CP before they are included in this CP.

The QPSPKIPA must forward all modifications to this CP and all Certification Practice Statements to the QGPKIPA for consideration and approval before any change is made to the QPS PKI.

9.12.2 Notification Mechanism and Period

Amendments to this CP may be posted to the CP URL identified in s. 1.2.

The amendments, or the modified CP, may be distributed electronically to QPSPKIPA participants.

9.12.3 Circumstances under which OID must be Changed

A new OID is required if this policy introduces a new assurance level.

9.13 Dispute Resolution Provisions

The QPSPKIPA shall facilitate the resolution between entities when conflicts arise as a result of the use of certificates issued under this policy.

9.14 GOVERNING LAW

This CP and any CPS that certificates are issued under, are 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 Queensland.

9.15 COMPLIANCE WITH APPLICABLE LAW

All Parties agree to abide by the provisions of all relevant legislation, and the requirements of any Commonwealth, State, Territory or local body when conducting activities under this CP.

9.16 MISCELLANEOUS PROVISIONS

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated. The process for updating this CP is described in s. 9.12.

Clauses that relate to Intellectual Property Rights, safety, integrity, accuracy of information, confidentiality, privacy, liability and indemnity will survive the expiration or termination (for whatever reason) of this CP and the CPS of the Certificate that is issued.

9.17 OTHER PROVISIONS

No stipulation.

10. BIBLIOGRAPHY

Chokhani, Ford, Sabett, Merrill and Wu, 'Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework', *Network Working Group RFC 3647*, November 2003.

Federal Information Processing Standards (FIPS) Publications,140-2 *Security Requirements for Cryptographic Modules,* 25 May 2001.

Federal Public Key Infrastructure Policy Authority, *X.509 Certificate Policy for the US Federal PKI Common Policy Framework*, version 3647 - 1.4, 13 August 13, 2008.

Internet Engineering Task Force (IETF), *Public Key Infrastructure X.509 (IETF PKIX), RFC 3647, Certificate Policy and Certification Practice Statement frameworks*

Queensland Government Chief Information Office, *Queensland Government Authentication Framework (QGAF)*, version 1.0.1, October 2006.

Queensland Government Chief Information Office, *Queensland Government Information Security Classification Framework (QGISCF)*, version 1.0, 1 April 2008.

Queensland Government Chief Information Office, *Root Certificate Policy*, version 0.1.0, Consultation Draft.

Standards Australia, *Australian Standard 4539 - Public Key Authentication Framework (PKAF)*, May 2002.

11. ACRONYMS AND ABBREVIATIONS

Acronym / abbreviation	Word / phrase
AIA	Authority Information Access
CA	Certification Authority
CAA	Certification Authority Administrator
CAM	Certification Authority Manager
CN	Common Name
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
EO	Enrolment Officer
FIPS	Federal Information Processing Standards Publications (US)
FTP	File Transfer Protocol
GEA	Government Enterprise Architecture
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ID	Identification
IETF	Internet Engineering Task Force
IRAL	Identity Registration Assurance Level
ISB	Information Systems Branch
ISO	International Organization for Standardization
ISS	Information Security Section
LDAP	Lightweight Directory Access Protocol
MD	Message Digest
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organisational Unit

Acronym / abbreviation	Word / phrase
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure X.509
PO	PKI Operator
QG	Queensland Government
QGAF	Queensland Government Authentication Framework
QGISCF	Queensland Government Information Security Classification Framework
QGPCA	Queensland Government Policy Certification Authority
QGPCA2	Queensland Government Policy Certification Authority hosting the QPS Certification Policy
QGPKIPA	Queensland Government Public Key Infrastructure Policy Authority
QGRCA	Queensland Government Root Certification Authority
QPS	Queensland Police Service
QPSPKIPA	Queensland Police Service Public Key Infrastructure Policy Authority
RA	Registration Authority
RAM	Registration Authority Manager
RFC	Request For Comments
RO	Registration Officer
RSA	Rivest-Shamir-Adleman (encryption algorithm)
RSASSA-PSS	RSA Signature Scheme with Appendix - Probabilistic Signature Scheme
SHA	Secure Hash Algorithm
UPN	User Principle Name
URL	Uniform Resource Locator
WWW	World Wide Web

12. GLOSSARY

Term	Definition
Access Control	Process of granting access to information system resources only to authorised users, programs, processes, or other systems.
Activation data	Private data, other than keys, that are required to access cryptographic modules (i.e. unlock private keys for signing or decryption events).
Applicant	The Subscriber is sometimes also called an 'applicant' after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed.
Arc	An arc is an individual sub tree of an Object Identifier (OID) tree.
Archive	Long-term, physically separate storage.
Assurance level	A specific level on a hierarchical scale representing successively increased confidence that a target of evaluation adequately fulfils particular requirements [QGAF]
Audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.
Audit data / Audit log	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event.
Authentication	Authentication is a process that tests a claimant's assertion of their Identity against an earlier registration process, generally by checking the validity of previously issued authentication credentials. [QGAF]
Backup	Copy of files and programs made to facilitate recovery if necessary.
Binding	Process of associating two related elements of information.
Biometric	A physical or behavioural characteristic of a human being.
Certificate, digital certificate	A digital representation of information which at least: • identifies the certification authority issuing it • names or identifies its Subscriber • contains the Subscriber's public key • identifies its operational period, and • is digitally signed by the certification authority issuing it. As used in this CP, the term 'certificate' refers to X.509 certificates that expressly reference the OID of this CP in the certificatePolicies extension.
Certification Authority (CA)	An entity that issues Digital Certificates (especially X.509 certificates), vouches for their contents, is trusted by Relying Parties to do so, and may provide warranties to

Term	Definition
	that effect, and even some level of indemnity [QGAF].
Certificate Policy (CP)	A certificate policy is a specialised form of administrative policy tuned to electronic transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise, recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
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 (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates that it has issued, that are revoked prior to their stated expiration date.
Confidentiality	Assurance that information is not disclosed to unauthorised entities or processes.
Cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS 140-2]
Digital signature	A string of characters appended to a digital object that demonstrates that the originating device had access to a particular private key. An important use is to enable Authentication of the Identity that generated, sent, or takes responsibility for that digital object. This assumes that a considerable number of conditions hold. See Public Key Infrastructure. See also the Authentication Concepts document for more information. [QGAF]
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.
Evidence of Identity	Evidence (eg in the form of documents) used to substantiate the identity of the presenting party, usually produced at the time of registration (ie when authentication credentials are issued). [QGAF]
Issuing CA	A CA that issues certificates to QPS RAs and Subscribers.
Key	A key is a string of characters used with a cryptographic algorithm to encrypt and decrypt. [QGAF]

Term	Definition
Key escrow	A deposit of the private key of a Subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the Subscriber, the terms of which require one or more agents to hold the Subscriber's private key for the benefit of the Subscriber, an employer, or other party, upon provisions set forth in the agreement.
Key pair	Two mathematically related keys having the properties that: • one (public) key can be used to encrypt a message that can only be decrypted using the other (private) key, and • even knowing the public key, it is computationally infeasible to discover the private key
Modification (of a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorisations granted to the subject, are changed by issuing a new certificate.
Non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. Technical non-repudiation refers to the assurance a relying party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key.
Object Identifier (OID)	A specialised formatted number that is registered with an internationally recognised standards organisation, the unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the Federal PKI, OIDs are used to uniquely identify certificate policies and cryptographic algorithms.
Policy CA	The Certification Authority that hosts the QPS X.509 Certificate Policy.
Private key	The secret component of a pair of cryptographic keys used to digitally sign messages on behalf of an entity. [AGAF]
Public key	The publicly disclosable component of a pair of Cryptographic Keys used to digitally sign messages on behalf of an entity. [AGAF]
Public Key Infrastructure (PKI)	A secure method of exchanging information. PKI uses the ‘public/private key’ method, for encrypting IDs and documents/messages. It starts with the Certification Authority which issues digital certificates that authenticate the identity of people and organisations over a public system. [QGAF]
QPSPKIPA	The QPSPKIPA is the Queensland Police Service Authority responsible for setting, implementing and administering policy decisions regarding the QPS PKI Architecture.
Registration authority (RA)	An entity that conducts a registration process on behalf of a service provider.[QGAF]

Term	Definition
Re-key (a certificate)	To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate that contains the new public key.
Relying Party	A person or entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Renew (a certificate)	The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate.
Repository	A database containing information and data relating to certificates as specified in this CP; may also be referred to as a directory.
Revoke a certificate	To prematurely end the operational period of a certificate effective at a specific date and time.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Signature Certificate / Digital Signing Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Smart card	A hardware token, usually taking the form of a credit-card sized plastic card with an embedded chip. May be used to carry information for authentication including a digital certificate.[QGAF]
Subscriber	A Subscriber is an entity that: • is the subject named or identified in a certificate issued to that entity • holds a private key that corresponds to the public key listed in the certificate, and • does not itself issue certificates to another party. This includes, but is not limited to an individual or device or service.
Subscriber certificate	A certificate in which the subject is not a CA or RA.
X.509	An international standard for public key certificate formats and a certification path validation algorithm.

13. CONTROL SHEET

1. Document information

Project name:	Common Access Smart Card
Project ID:	ISC-207
Authors:	Laurie Sherd Peter Wibberley

2. Document Revision History

Date	Version	Status	Description	Author/s	Reviewed by
	0.01	Draft	Updated after consultation	Laurie Sherd Peter Wibberley	
	0.02	Draft	Updated after consultation	Laurie Sherd Peter Wibberley	Greg Ensbey Jenny Somers
26 Feb 2009	0.03	Draft			

3. Document reviewer approval

Date	Version	Status	Reviewed by	Position	Signature
Feb 2009		Draft	Gyl Stacey	Manager, ISB	
Feb 2009		Draft	Tony Fisher	Manager, ISS	

4. Authorisation

Date	Version	Status	Reviewed by	Position	Signature
2009	1.00	Final	Paul Stewart	Assistant Commissioner, Information & Communications Technology, QPS	

END OF DOCUMENT