Information Security Section

Certification Practice Statement

for the

QPS Issuing Certification Authority QPSISC1

Project Name:	Common Access Smart Card
Project ID:	ISC-207
Document Version:	1.0
Status:	Consultation Draft
Author:	Laurie Sherd

1.Table of Contents

1. INTRODUCTION

This Certification Practice Statement (CPS) documents the practices that are employed within the QPS PKI to:

- Request, issue, manage, revoke, and re-key certificates through the QPS Issuing CA (QPSICA1) and the Registration Authorities delegated by the CA for:
  - → Internal authentication to the QPS computer network and ,
  - → Digital signing of emails
- Securely manage the core infrastructure that supports QPSICA1 and its Registration Authorities.

The practices support the implementation of the QPS X509 Certification Policy.

1.1 OVERVIEW

The Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647, Certification Policy and Certification Practices Framework provides a structure for Certification Policy and CPS documents in the form of section headings and recommended content for each section. This document uses that framework.

1.2 DOCUMENT NAME AND IDENTIFICATION

This CPS is called the "Certification Practice Statement for the QPS Issuing Certification Authority QPSICA1"

1.3 PKI PARTICIPANTS

1.3.1 Certification Authorities (CA)

QPSICA1 has been established under the Queensland Police Service Policy Certification Authority QGPCA2 to issue Subscriber certificates for:

- Internal authentication to the QPS computer network,
- Digital signing of emails

1.3.2 Registration authorities (RA)

The ID Issuing Office Registration Authority (IDORA1) has been delegated by QPSICA1 to:

- Verify the identity of Subscribers and
- Request the issuance, revocation and modification of certificates on behalf of the CA for internal authentication to the QPS computer network and email signing.

IDORA1 is located in the QPS Identification Office.

1.3.3 Subscribers

Subscribers of QPSICA1 are:

- QPS Sworn members (police officers)

- QPS Recruits
- QPS Unsworn members (non police officers)
- QPS Contractors
- QPS Approved QG Employees
- QPS Approved QG contractors
- QPS or Queensland Government devices such as firewalls, routers, servers or other hardware or software components used to secure QPS communications.

The Manager, Information Systems Branch has been appointed by the QPS PKI Policy Authority (QPSPKIPA) as the custodian of all QPS infrastructure devices for the purposes of requesting Subscriber certificates from QPSICA1.

1.3.4 Relying parties

Only Queensland Police Service or other Queensland Government entities are Relying Parties for certificates issued by QPSICA1.

There is no separate Relying Party Agreement for certificates issued by QPSICA1.

1.3.5 Other participants

1.3.5.1 Queensland Government PKI Policy Authority

This CPS has been approved by the Queensland Government Public Key Infrastructure Policy Authority (QGPKIPA)

1.3.5.2 Queensland Police Service PKI Policy Authority

This CPS has been approved by the Queensland Police Service Public Key Infrastructure Policy Authority (QPSPKIPA)

1.3.5.3 Other Participants

Refer to the QPS X509 Certification Policy.

1.4 CERTIFICATE USAGE

1.4.1 Appropriate Certificate Uses

The QPS Issuing CA QPSICA1 has been established to issue subscriber certificates for:

- Internal authentication to the QPS computer network,
- Digital signing of emails

All certificates for individual subscribers issued by QPSICA1 for internal authentication to the QPS network and digital signing of emails are issued on smart cards and have a medium assurance level.

Subscriber certificates that are issued by QPSICA1 to devices used to secure QPS communications within the PKI have basic assurance as a minimum.

1.4.2 Prohibited Certificate Uses

QPSICA1 must not issue:

- Certificates to Certification Authorities
- Individual Subscriber certificates with a rudimentary or high assurance level.
- Individual Subscriber certificates with a basic assurance level for internal authentication to the QPS network or digital signing of emails
- Certificates for encryption
- Certificates to entities external to QPS and the Queensland Government.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

The Certificate Authority Manager (CAM) for QPSICA1 is responsible for administering all aspects of this CPS.

1.5.2 Contact Person

Questions regarding this CPS shall be directed to:

The Manager, Information Security Section
Information & Communications Technology Command
Queensland Police Service
BRISBANE QLD 4000

Telephone: (07) 3008 4750
Facsimile: (07) 3221 4060
Email: Manager ISS@police.qld.gov.au

1.5.3 Person Determining CPS Suitability for the Policy

This CPS has been approved by the QGPKIPA and QPSPKIPA.

1.5.4 CPS Approval Procedures

The procedure for amending this CPS is

- A copy of the current approved CPS shall be obtained from the Manager, Information Security Section.
- The copy will be used to provide a draft CPS with amendments in mark-up mode to the QPSPKIPA.
- The draft must be submitted in the same format as the current approved CPS, must use the same Heading and Paragraph Numbering structure and is to contain “Draft” on all pages.
- The version number of the draft CPS will be the previous approved version number incremented by point 1, eg approved version 1.0 would become draft version 1.1
- The draft CPS will be submitted, either by email or in hard copy to the Contact Person nominated in s. 1.5.2 if this CPS for submission to the QPSPKIPA.

- The QPSPKIPA may, subject to the CPS meeting the criteria above and the criteria detailed in the QPS X.509 Certificate Policy for CPSs, approve the CPS for consideration by the QGPKIPA.
- The QGPKIPA may, subject to the CPS meeting all the requirements set by QGPKIPA, approve the draft CPS and will notify the QPSPKIPA of approval.
- The QPSPKIPA will notify the CAM of approval and will arrange for publication of the new CPS on the location identified in Section 2.2 of this CPS.

1.6 DEFINITIONS AND ACRONYMS

See Sections 11 and 12.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

QPSICA1 is the authoritative repository for

- all certificates issued to Subscribers by QPSICA1
- Certificate Revocation Lists relating to Subscriber certificates issued by QPSICA1.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The following certificate information is published for QPSICA1:

- 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

Information on the location of this Certification Practice Statement is published at http://pki.police.qld.gov.au

The X.509 Certificate Policy that relates to this CPS is published at http://pki.police.qld.gov.au by the QPSPKIPA and http://pki.qld.gov.au by the QGPKIPA

2.3 TIME OR FREQUENCY OF PUBLICATION

The frequency with which QPSICA1 publishes CRLs is defined in Section 4.9.7.

2.4 ACCESS CONTROLS ON REPOSITORIES

Information that is published from QPSICA1 to the QPS PKI Website is public information and has read only access.

Information that is published to the QPS Enterprise Directory has read only access and is available to QPS internal staff only.

Access to the QPS PKI Website and the QPS Enterprise Directory to update certificate information (modify, add, delete) for the QPS X509 Certification Policy and this CPS is restricted to the CAM and those QPS employees who have been appointed as Certification Authority Administrators for QPSICA1 as listed in s 5.2.1 of this CPS.

3. IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

All certificates issued by QPSICA1 use the X.500 DN name format for subject and issuer name.

3.1.1 Types of Names

The Name formats used in CA certificate issued to QPSICA1 from the Queensland Government Policy CA QGPCA2 and for Subscriber certificates issued by QPSICA1 are documented in *QPS Certificate Profiles.doc*:

3.1.2 Need for Names to Be Meaningful

QPSICA1 uses the individual Subscriber's Surname and Firstname, appended with the QPS Branch acronym to which the Subscriber is attached within QPS, to ensure that a certificate's Subject Name is meaningful.

3.1.3 Anonymity or Pseudonymity of Subscribers

QPSICA1 does not issue anonymous or pseudonymous certificates.

3.1.4 Rules for Interpreting Various Name Forms

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

3.1.5 Uniqueness of Names

The Manager, Information Security Section maintains a record of QPS Certification Authority names to ensure uniqueness of CA Names within QPS.

QPSICA1 and IDORA1 use the information from the Subscriber's account in the QPS Enterprise Directory to ensure that the Common Name within the Subject Name field and the UPN or e-mail address in the subjectAltName field are unique to the Subscriber's certificate.

3.1.6 Recognition, Authentication, and Role of Trademarks

No stipulation.

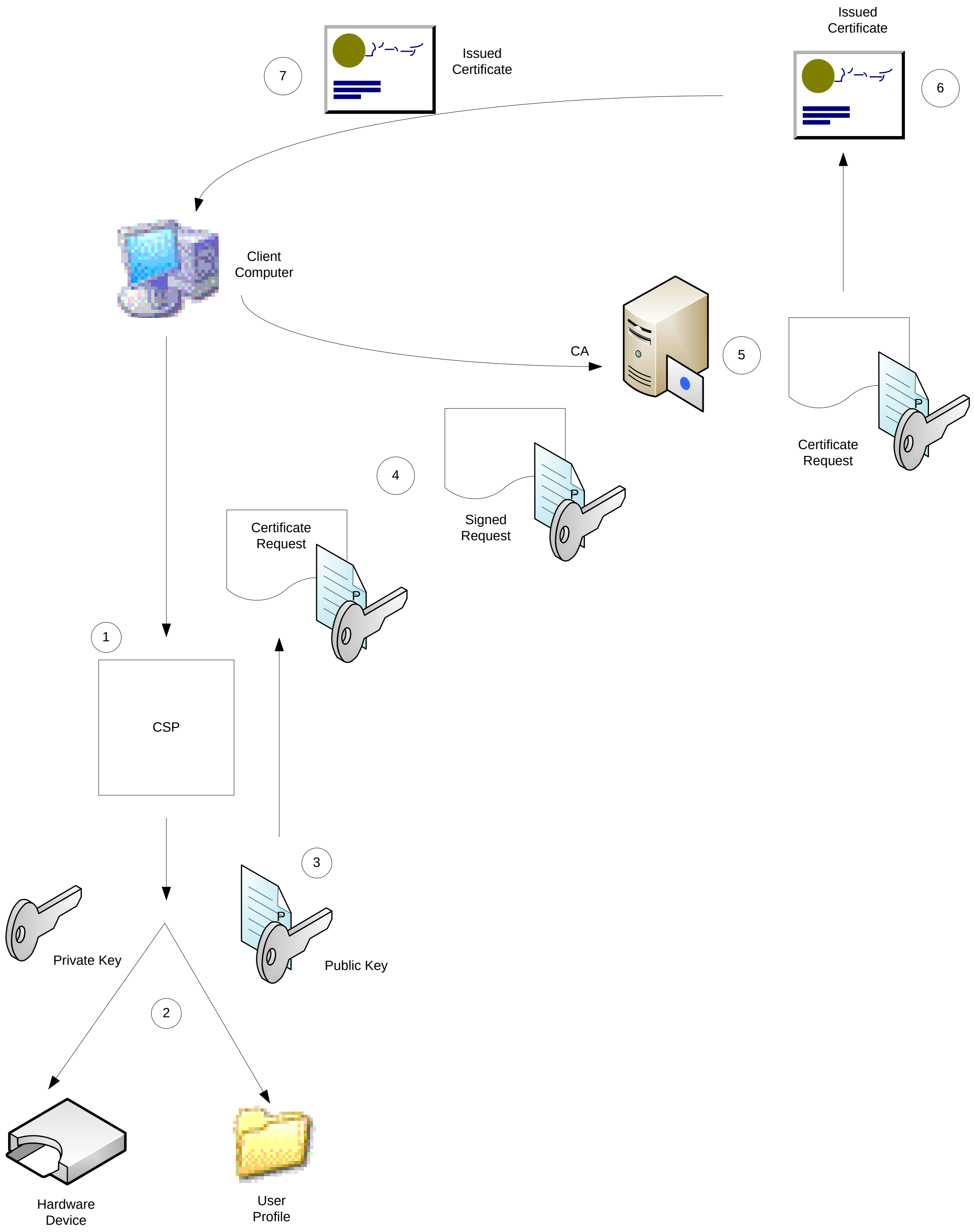
3.2 INITIAL IDENTITY VALIDATION

3.2.1 Method to Prove Possession of Private Key

QPSICA1 and IDORA1 require proof that the subscriber has possession of the private key that corresponds to the public key in the certificate request before a Subscriber certificate is issued or modified.

The process that is used by QPSICA1 and IDORA1 in order to establish this proof is defined in Figure 1 below:

Figure 1: Proof of Identity Process



1. When a new certificate is requested, IDORA1 issues a request to the cryptographic service provider (CSP), designated by the certificate template, to generate a key pair.

2. Key pairs for internal authentication to the QPS computer network are generated on the individual Subscriber’s smart card. The CSP generates a key pair based on the key length designated in the appropriate certificate template.
3. The public key of the key pair is added to the certificate request, along with any other information required by the certificate template.
4. The certificate request is signed by the private key of the Subscriber’s key pair and the private key associated with the RA enrolment certificate and is sent to QPSICA1.
5. QPSICA1 issues the requested certificate or, denies the request, or causes it to be pending until an Authorising Officer for QPSICA1 manually either approves or denies it.
6. The certificate is generated by QPSICA1. It includes the subject information provided in the certificate request that has been built from information in the QPS Enterprise Directory, as well as the public key of the key pair.
7. The certificate is then signed with the CA signing certificate, and the resulting hash is placed in the certificate’s thumbprint extension.
8. The issued certificate is returned electronically to the user and loaded into the individual Subscriber’s smart card. The certificate is now associated with the private key of the key pair and is ready to use.

3.2.2 Authentication of Organisation Identity

QPSICA1 can issue Subscriber certificates for internal authentication to the QPS computer network to members of other Queensland Government Organisations but not to the Organisational entity itself.

Applicants from other Queensland Government Organisations are required to undergo the Identity Validation requirements for certificate issuance as defined in s. 3.2.3 and to have a valid record in the QPS Enterprise Directory prior to the certificate request being processed by QPSICA1 or IDORA1.

3.2.3 Authentication of Individual Identity

QSPICA1 only issues individual Subscriber certificates to individuals who have met the Evidence of Identity (EOI) requirements for persons employed by the Queensland Police Service as defined in the QPS Human Resources manual and who have been issued with a QPS Common Access Smart Card.

The processes that are followed to authenticate an individual’s identity after completion of the EOI process are:

- a record is manually created for the Subscriber in the QPS HR system by HR and electronically transferred to the QPS Enterprise Directory
- if the Subscriber is a contractor, notification of employment is forwarded by HR to the Information Security Section (ISS) using Form QPS0431 and a record manually created in the QPS Enterprise Directory by ISS.

It is the existence of the individual Subscriber’s record in the QPS Enterprise Directory that is used as the authoritative source for authentication of an individual’s identity and issue of a signing certificate by QPSICA1 and its delegated RA’s prior to issuance of an individual Subscriber’s certificate.

3.2.4 Non-verified Subscriber Information

All information that is required by QPSICA1 and IDORA1 to request and issue a certificate is verified prior to certificate issuance, using the processes described in this CPS.

3.2.5 Validation of Authority

All requests to generate key pairs and issue or re-key a CA certificate for QPSICA1, or to generate key pairs and issue / rekey / revoke a RA enrolment certificate issued by QPSICA1, are to be submitted by an authorised person listed in ss 4.1.1, 4.7.2 and 4.9.2 to the Manager, Information Security Section. The Manager, ISS or delegate will validate the authority of the applicant to act on behalf of QPSICA1 by:

- noting on the request the name and, if a QPS employee, the QPS Identification Pass number of the person submitting the request and the date that the request was presented
- checking in the "Schedule of Appointments to Trusted Roles for the QPS PKI" that the person submitting the request was the appointed CAM for QPSICA1 at the date that the request was submitted and
- signing the request to confirm that the person submitting the request was the CAM.

If the request is to revoke a CA certificate, the Manager ISS will follow the process defined in s 4.9.3 of this CPS.

Once the applicant's identity and authority has been verified, the Manager, ISS will

- submit the request to the QPSPKIPA for approval and
- if the request was for a CA certificate, submit the request to the QGPKIPA for approval.

3.2.6 Criteria for Interoperation

QPSICA1 does not interoperate with other PKIs.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

Subscriber certificates will not be re-keyed by QPSICA1.

The identity and authority of the applicant submitting a request to re-key a CA Certificate for QPSICA1 will be confirmed using the process defined in s. 3.2.5.

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

4.1.1 Who Can Submit a Certificate Application

An application for a CA certificate for QPSICA1 must be submitted to the QPSPKIPA, through the Manager, Information Security Section using the form "Request for a Certification Authority / Registration Authority Certificate" by the CAM.

An application for a RA enrolment certificate for IDORA1 must be submitted to the QPSPKIPA through the Manager, Information Security Section using the form "Request for a Certification Authority / Registration Authority Certificate" by the CAM.

An application for an individual Subscriber certificate to be issued by QPSICA1 must be submitted to the ID Issuing Office using the form "Application for Logical Access to QPS IT Systems" by one of:

- a Registration Officer for QPSICA1 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 to be issued by QPSICA1 for a device or service must be submitted to the ID Issuing Office using the form "Request for a Device Certificate" by the custodian of the device or service identified in s. 1.3.3 of this CPS.

4.1.2 Enrolment Process and Responsibilities

QPSICA1

The enrolment process and responsibilities for establishing QPSICA1 are:

- appointment of the CAM by the QPSPKIPA, including verification that the CAM had met the IRAL – 3 EOI requirements
- submission of an enrolment request by the CAM to the Manager, ISS and the QPSPKIPA. The request was supported by:
    - → a Risk Assessment for the establishment of the CA
    - → the QPS X509 Certification Policy
    - → the QPSICA1 Certificate Practice Statement
    - → Operational and Security Controls for QPSICA1
    - → Disaster Recovery and Business Continuity Plans for QPSICA1
- Processing of the enrolment request by the QPSPKIPA, including
    - → approval of the enrolment of the CA in the QPS PKI
    - → completion of an Accreditation Audit of the CA as part of the enrolment process
    - → submission of the enrolment request to the QGPKIPA for accreditation of the CA to the QG PKI.
- Submission of the enrolment request to the QGPKIPA for consideration of approval.

IDORA1

The enrolment process and responsibilities for establishing IDORA1 are:

- appointment of the RAM by the QPSPKIPA or CAM, including verification that the RAM has met the IRAL – 3 EOI requirements
- submission of an enrolment request by the CAM using the form "Request for Enrolment of a Certification / Registration Authority in the QPS PKI" to the Manager, ISS and the QPSPKIPA. The request was supported by
    - → a certificate from the CAM that the information on the request was complete and accurate;
    - → documented Operational and Security Controls for the RA
    - → Disaster Recovery and Business Continuity Plans for the RA
- Processing of the enrolment request by the QPSPKIPA, including
    - → Consideration for approval of the enrolment of the RA in the QPS PKI
    - → completion of an Accreditation Audit of the RA as part of the enrolment process,
    - → submission of the enrolment request to the QGPKIPA for accreditation of the RA to the QG PKI.

Subscribers of QPSICA1

Refer to s. 3.2.3 of this CPS. Enrolment of a Subscriber for QPSICA1 occurs when a request for a Subscriber certificate is submitted by IDORA1 through the Registration Authority Web page and the certificate is issued to the Subscriber by QPSICA1 and accepted by the Subscriber.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 Performing Identification and Authentication Functions

The QPSPKIPA, through the Manager, ISS will identify and authenticate the applicant of a request to issue / re-key / revoke a CA or RA enrolment certificate for QPSICA1 using the process defined in s. 3.2.5.

The occupants of the positions appointed as Registration Officers (RO) for IDORA1 are responsible for performing Subscriber identification and authentication functions on behalf of the RA. These functions include:

- checking that all required information has been supplied in the Request form. If there is missing or incorrect information, the RO will notify the applicant of the error/omission and request the submission of a new approved request. This notice for information may be made in writing or via email.
- checking that the Request has been approved by an OIC / Section Head or the device Custodian. Request will need to contain a statement from OIC/Section Head that the info in request is correct and that they are the person's OIC/Section Head.
- matching the Subscriber details on the request with
    - → the current valid record for the Subscriber in the QPS Enterprise Directory, if the request is to issue a certificate, or.

→ the certificate information in QPSICA1 if the request is to revoke a certificate.

- requesting and executing the issuance / revocation of certificates through IDORA1 to QPSICA1 using their own private key and the RA enrolment agent private key to sign the request

4.2.2 Approval or Rejection of Certificate Applications

The QPSPKIPA will reject a request to issue / re-key / revoke a CA or RA enrolment certificate for QPSICA1 if the request

- has not been submitted by the CAM
- is incomplete or contains inaccurate information
- is inconsistent with the QPS X509 certificate policies
- has not been submitted in accordance with the processes defined in this CPS.

The QPSPKIPA will submit all approved requests to issue / re-key / revoke a CA certificate for QPSICA1 to the QGPKIPA for approval.

A request for a Subscriber certificate may be rejected if the request

- is incomplete or contains inaccurate information
- is inconsistent with the QPS X509 certificate policies
- has not been submitted in accordance with the processes defined in this CPS.

In such cases, the rejection of the request will be approved by the RAM for IDORA1. In the RAMs absence the rejection of a request can be authorised by the CAM for QPSICA1.

The applicant who submitted the request will be notified of the reason for rejection by email by the RO.

4.2.3 Time to Process Certificate Applications

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

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

Upon receiving a request for a RA or Subscriber certificate QPSICA1 will:

- confirm that the request has been signed by the subject’s private key and the RA enrolment agent private key
- confirm Subject’s possession of the private key using the process detailed in s. 3.2.1
- generate and issue the certificate
- publish the certificate in accordance with s. 2.2

4.3.2 Notification to Subscriber of Issuance of Certificate

The Registration Officer for IDORA1 will notify the Subscriber or the custodian of a device or service when a certificate has been created and its availability. Notification can be by email, telephone or in-person.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct constituting certificate acceptance

The CAM for QPSICA1 will provide the QPSPKIPA and QGPKIPA with a written or digitally signed receipt notice for the CA certificate.

First use of the private key by QPSICA1 will constitute acceptance of the certificate and notification of Certificate Issuance to other entities.

First use of the private key by IDORA1 will constitute acceptance of the certificate.

First use of a private key by an individual or device Subscriber to QPSICA1 will constitute acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

QPSICA1 will publish information on Subscriber certificates to the locations identified in s. 2.2. The process for publishing the information is defined in the Publication and Repository Design for QPSICA1.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

Refer to s.4.4.1 of this CPS.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

Refer to s. 4.5.1 of the QPS X509 Certification Policy.

4.5.2 Relying Party Public key and Certificate Usage

Refer to s. 4.5.2 of the QPS X509 Certification Policy.

4.6 CERTIFICATE RENEWAL

4.6.1 Circumstance for Certificate Renewal

CA and Subscriber certificates cannot be renewed by QPSICA1.

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

RA enrolment certificates and Subscriber certificates will not be re-keyed by QPSICA1.

The CA certificate issued to QPSICA1 by QGPCA2 can be re-keyed subject to:

- the Identification and Authentication processes defined in s. 3.3 of this CPS are completed prior to the re-key and:
- the certificates that are to be issued by QPSICA1 will have an expiry date later than the expiry date of the CA certificate for QPSICA1

4.7.2 Who May Request Certification of a New Public Key

The CAM for QPSICA1 may submit a request to re-key the CA certificate.

4.7.3 Processing Certificate Re-keying Requests

All requests to re-key a CA certificate for QPSICA1 will be approved by the QPSPKIPA and QGPKIPA prior to the re-key using the procedures defined in ss. 3.2.5 and 3.3.

Once approval has been received from the QPSPKIPA and QGPKIPA, a new key pair will be generated for QPSICA1 using the processes identified in the document “Appendix I – PKI Management Tasks”.

The CAM for QPSICA1 will then generate a request for a new CA certificate using the new signing key.

The CAM will submit the new certificate request by email to QGPCA2.

The CAM is responsible for the accuracy of the information in the re-key request.

The new CA certificate will be returned from QGPCA2 to the CAM by email.

4.7.4 Notification of New Certificate Issuance to Subscriber

Subscriber certificates will not be re-keyed by QPSICA1.

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. 2.2

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

Refer to s. 4.4.1

4.8 CERTIFICATE MODIFICATION

4.8.1 Circumstance for Certificate Modification

CA and Subscriber certificates will not be modified by QPSICA1.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No Stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No Stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No Stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No Stipulation

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

Subscriber certificates will not be suspended by QPSICA1.

A CA certificate issued to QPSICA1 or a Subscriber certificate issued by QPSICA1 can 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 circumstance that may require a certificate to be revoked are:

- 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.

4.9.2 Who Can Request Revocation

A request to revoke a CA Certificate issued to QPSICA1 can be made by:

- the CAM
- a member of the QPSPKIPA
- the QGPKIPA.

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

A request to revoke a RA enrolment certificate issued by QPSICA1 can be made by:

- the RAM
- the CAM
- the QPSPKIPA.

All requests to revoke a RA enrolment certificate issued by QPSICA1 will be approved by the CAM prior to the revocation occurring. The CAM must inform the QPSPKIPA when revocation occurs.

A request to revoke a Subscriber certificate issued by QPSICA1 can 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 Manager, Information Security Section
- the custodian of a device or service

- a Registration Officer or RAM delegated by QPSICA1
- the CAM of the CA that issued the certificate
- a member of the QPSPKIPA.

All requests to revoke an individual Subscriber certificate issued by QPSICA1 will 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.

QPSICA1, subject to the approval of the QPSPKIPA, can summarily revoke certificates within its domain.

4.9.3 Procedure for Revocation Request

A request to revoke a CA or RA enrolment certificate issued to or by QPSICA1 is to be submitted in writing to the QPSPKIPA through the Manager, Information Security Section using the form “Request to Revoke a Certification Authority, Registration Authority or Subscriber Certificate”.

The request will:

- identify the certificate to be revoked
- explain the reason for revocation
- be signed by the applicant

The Manager, ISS or delegate will:

- verify the identity and authority of the applicant to request revocation of a CA/RA enrolment certificate for QPSICA1 by
  - → following the process defined in s. 3.2.5 if the applicant is the CAM
  - → confirming with the Chair of the QPSPKIPA and noting on the request that the applicant has acted with the full knowledge of the QPSPKIPA if the applicant is a member of the QPSPKIPA.
  - → confirming with the Chair of the QGPKIPA by email that the applicant is a current member of the QGPKIPA and has acted with the full knowledge of the QGPKIPA if the applicant is a member of the QGPKIPA. The confiming email will be attached to the application.
- submit the request and any attachment to the QPSPKIPA for approval.
- If the request is for revocation of a CA certificate, submit the request to the QGPKIPA for approval and revocation of the CA certificate by QGPCA2.

A request to revoke a Subscriber certificate that has been issued by QPSICA1 can be made by the applicant:

- completing and sending a request that has been approved by one of the persons identified in s.4.9.2 to the Registration Officer, IDO using the form “Request to Revoke a Certification Authority, Registration Authority or Subscriber Certificate” or
  - sending a request by email to the Registration Officer, IDO that:
    - → identifies the certificate to be revoked
    - → explains the reason for revocation
    - → contains the approval of one of the persons identified in s.4.9.2

The Registration Officer will authenticate the request using the processes defined in s. 4.2.1.

On receipt of the request, QPSICA1 will

- revoke the certificate
- add the revoked certificate to the CRL
- publish the CRL in accordance with s. 2.2

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this CPS.

4.9.5 Time within which CA must Process the Revocation Request

QPSICA1 will process the revocation request on receipt.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties should exercise due care before undertaking transactions and should use the information provided by QPS at the locations identified in s. 2.2 for checking the status of certificates issued by QPSICA1.

4.9.7 CRL Issuance Frequency

QPSICA1 issues and publishes CRLs at least once every 24 hours to the locations identified in s. 2.2.

4.9.8 Maximum Latency for CRLs

CRLs issued by QPSICA1 are 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

No stipulation.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation

4.9.12 Special Requirements Related To Key Compromise

If a smart card that contains a Subscriber certificate is suspected of being lost, or it is suspected that the private key is compromised, the Subscriber's account will be disabled in the QPS Enterprise Directory, in turn disabling the Subscriber's access to QPS IT resources. When the loss of the smart card or key compromise is confirmed, the Subscriber certificate will be revoked and a new CRL containing the revoked certificate will be published within 18 hours of notification of loss or compromise to the Registration Officer, IDO.

The procedures to notify the Registration Officer, IDO that a Subscriber certificate has been lost or compromised and should be revoked are the same as those identified in s. 4.9.3

If QPSICA1 is compromised, the QPSPKIPA and QGPKIPA are to be notified and the CA certificate issued to QPSICA1 will be revoked immediately by QGPCA2 and the CRL updated.

4.9.13 Circumstances for Suspension

QPSICA1 does not suspend certificates.

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

4.10.1 Operational Characteristics

CRLs issued by QPSICA1 are available through the following protocols:

- Hypertext Transfer Protocol (HTTP)
- 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

QPSICA1 does not issue certificates for encryption

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Session key recovery is not supported by this CPS.

5. Facility Management and Operational Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

QPSICA1 is housed in the Herston Datacentre. The site controls are described in the following table.

Control Measure	Secure Areas	Provided at Herston Y/N	Description of Control
Tamper-evident barriers, highly resistant to covert entry[1]	Yes	Yes	All entry to the Data Centre is sealed unless you have approved swipe card access. There are three separate access points that must be passed through to gain entry to the data centre and even then the cabinets housing the PKI infrastructure are locked C Class cabinets
An effective means of providing access control during both operational and non-operational hours	Yes	Yes	Herston have an Operations Centre that is contactable from 6am – 10pm and after hours contact staff for 10pm – 6am callouts
All persons to wear passes	Yes	Yes	
All visitors escorted at all times	Yes	Yes	Visitors cannot get access to the floor without being escorted
Appropriately secured points of	Yes	Yes	See Number 1

entry and other openings			
during non-operational hours a monitored security alarm system, providing coverage for all areas where security classified information is stored	Yes	Yes	
An approved means of limiting entry to authorised persons	Yes	Yes	Even authorised people external to Health cannot gain entry to the Data Centre without being escorted by Health staff.

In addition to the above, additional controls are provided for internal access within the datacentre. To get to the floor that the data centre resides on there is cameras and swipe card access. To get into the data centre there are camera's and swipe card access.

IDORA1 is housed in the ID Issuing Office. The site controls are described in the following table.

Control Measure	Intruder Resistant Area	Provided at ID Issuing Office Y/N	Description of Control
Tamper-evident barriers, highly resistant to covert entry[1]	Yes	Yes	All entry to the ID Issuing Office is sealed 24 x 7 unless you have approved swipe card access. After hours access to the building is controlled by swipe card.
An effective means of providing access control during both operational and non-operational hours	Yes	Yes	After hours access is controlled for the building housing the ID Issuing Office. Access to the ID Issuing Office is controlled 24 x 7 by swipe card.
all persons to wear passes	Yes	Yes	All QPS employees are required to display official QPS Identification.
all visitors escorted at all times	Yes	Yes	Visitors are escorted at all times.
appropriately secured points of entry and other openings	No	Yes	See Number 1
during non-operational hours a monitored security alarm system, providing coverage for all areas where security classified information is stored	No	No	
an approved means of limiting entry to authorised persons	No	Yes	Visitors are escorted at all times and must present to the Visitor's access point before access is granted.

All Hardware Security Modules used by the QPS PKI are stored in the Herston datacentre in C-class cabinets as defined in the QGISCF.

5.1.2 Physical access

Refer to s. 5.1.1.

5.1.3 Power and Air Conditioning

The Herston datacentre provides 30 mins of power in the UPS to shutdown critical services.

Herston uses a Semens system for temperature and humidity control. HEPA filters are present in the A/C for particle control and APC dust trackers are installed in the Data Centre. In addition APC Netbotz monitors the air inside and outside of the datacentre.

5.1.4 Water Exposures

No liquid is present in the floors above the datacentre at Herston. In addition flood detectors are present under the raised floor of the datacentre to detect any water exposure.

5.1.5 Fire Prevention and Protection

The Herston datacentre has a Vesda fire suppression system as well as a FM 200 system.

5.1.6 Media Storage

All PKI media at Herston is stored in C-class cabinets

5.1.7 Waste Disposal

Herston has on-site facilities to dispose of paper such as shredders.

All electronic media & equipment is returned to QPS Headquarters for destruction or sanitisation.

5.1.8 Off-Site Backup

System backups are undertaken daily and they are stored at both Herston and Police HQ. The mechanism to perform this backup is an EMC device called Avamar. An Avamar device resides at both Herston and Police HQ and they are replica's of each other.

Requirements for CA private key backup are specified in s. 6.2.4.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

All positions that have been appointed to Trusted Roles in the QPS PKI are listed in the "Schedule of Appointments to Trusted Roles for the QPS PKI".

Certification Authority Manager (CAM)

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

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

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.

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.

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.

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.

Cryptographic Module Administrator Token Holder

The Cryptographic Module Administrator token holder role is responsible for the following HSM management activities:

- 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

5.2.2 Number of Persons Required per Task

QPSICA1 has nine Cryptographic Module Administrator token holders. The Cryptographic Module Administrator activities identified in s. 5.2.1 require a quorum of two Cryptographic Module Administrator token holders (not including the Console operator) for QPSICA1 to be authenticated prior to starting the tasks.

A Cryptographic Module 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 and Operations token holders for the QPS Policy CA QGPCA2 can be members of an organisation external to QPS.

All Cryptographic Module Administrator and Operator tokens for QPSICA1 are stored in a B-class safe by the Manager, Information Security Section. Whenever a token is required to perform an action for QPSICA1, the token holder must sign for the token in the Token Register maintained by the Manager Information Security Section.

All tokens must be returned and signed in to the Token Register by the token holder to the Manager, Information Security Section when the activity has been completed.

5.2.3 Identification and Authentication for Each Role

All people assigned to a Trusted Role for QPSICA1 and IDORA1 have been appointed by the QPSPKIPA and have met the evidence of identity requirements:

- for an employee or contractor of the QPS, as defined in s. 3.2.3 .
- for medium assurance as defined in the QPS X509 Certificate Policy.

5.2.4 Roles Requiring Separation of Duties

The QPSPKIPA ensures separation of duties for Trusted Roles appointed to manage and operate QPSICA1 and IDORA1 by:

- maintaining a Schedule of Appointments to Trusted Roles for the QPS PKI.
- not appointing the same person to more than one of the following roles
    - → Registration Officers
    - → Authorising Officer
    - → Certification Authority Administrators
- not appointing an Auditor to any other Trusted Role.
- undertaking regular audits of the QPS PKI.
- applying the polices and processes for access control and separation of duty defined in.
    - → this CPS
    - → the QPS X509 Certificate Policy and
    - → the QPS Information Management Manual

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

All people appointed to a Trusted Role for QPSICA1 or IDORA1 are subject to the terms and conditions that apply to their QPS employment or contract arrangement and have been appointed to the role on the basis of their qualifications and experience.

5.3.2 Background Check Procedures

No Stipulation.

5.3.3 Training Requirements

Refer to the QPS X509 Certification Policy.

5.3.4 Retraining Frequency and Requirements

Refer to s. 5.3.4 of the QPS X509 Certification Policy.

5.3.5 Job Rotation Frequency and Sequence

Refer to s. 5.3.5 of the QPS X509 Certification Policy.

5.3.6 Sanctions for Unauthorised Actions

Refer to s. 5.3.6 of the QPS X509 Certification Policy.

5.3.7 Independent Contractor Requirements

Refer to s. 5.3.7 of the QPS X509 Certification Policy.

5.3.8 Documentation Supplied to Personnel

Refer to s. 5.3.8 of the QPS X509 Certification Policy

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

The following types of application, security and system events are logged for QPSICA1

- security events
    - → Backup and restore of the CA database
    - → Changes to the CA configuration
    - → Changes to the CA security settings
    - → Issue and management of certificate requests
    - → Revocation of certificates and publishing of CRL’s
    - → Storing and retrieval of archived keys
    - → Starting and stopping Certificate Services.

For each auditable event, the audit record includes:

- the type of event and event ID (see table below)
- 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.

Event ID	Event Description
772	The certificate manager denied a pending certificate request.
772	Certificate Services received a resubmitted certificate request. This means that a certificate manager issued a certificate that was pending.

774	Certificate Services revoked a certificate
775	Certificate Services received a request to publish the CRL.
776	Certificate Services published the CRL.
777	A certificate request extension changed.
778	One or more certificate request attributes changed.
779	Certificate Services received a request to shut down.
780	Certificate Services backup started.
781	Certificate Services backup completed.
782	Certificate Services restore started.
783	Certificate Services restore completed.
784	Certificate Services started.
785	Certificate Services stopped.
786	Security permissions for Certificate Services changed.
787	Certificate Services retrieved an archived key.
788	Certificate Services imported a certificate into its database.
789	The audit filter for Certificate Services changed.
790	Certificate Services received a certificate request.
791	Certificate Services approved a certificate request and issued a certificate.
792	Certificate Services denied a certificate request.
793	Certificate Services set the status of a certificate request to pending.
794	The certificate manager settings for Certificate Services changed.
795	A configuration entry changed in Certificate Services.
796	A property of Certificate Services changed
797	Certificate Services archived a key.
798	Certificate Services imported and archived a key
799	Certificate Services published the CA certificate to the QPS Enterprise Directory.
800	One or more rows have been deleted from the certificate database.
801	Role separation enforcement is enabled. If role separation enforcement is enabled, the event log entry will state Yes. If it is disabled, the event log entry will state No

Source: “Microsoft Windows Server 2003 PKI and Certificate Security”, Brian Komar with the Microsoft PKI Team

The following types of PKI user events are logged for QPSICA1 and IDORA1

- login/logout in the Windows system event log
- user account management via the QPS Enterprise Directory

- system usage, including known or suspected breaches, anomalies and fault management through the Incident and Compromise Handling Procedures identified in s. 5.7.1 of this CPS

5.4.2 Frequency of Processing Log

A scheduled task “OnlineCABackupEventLogs” has been created to copy the Application, Security and System audit event logs for QPSICA1 to the QPSICA1 E drive on a daily basis. These logs are then included in the daily backup schedule for QPS and stored in the locations identified in s. 5.1.8 .

Audit logs for QPSICA1 are reviewed annually for accreditation purposes by an external auditor and at least annually by an internal auditor to ensure the integrity of the PKI is being maintained.

5.4.3 Retention Period for Audit Log

Audit logs for QPSICA1 and IDORA 1 are retained for the period defined in s. 1.4 of the General Retention and Disposal Schedule for Administrative Records issued by the Queensland State Archives.

5.4.4 Protection of Audit Log

Access to audit logs for QPSICA1 is restricted by Group Policy in the QPS Enterprise Directory.

Those members listed in the QPS-P-PKI-CAAudit group have access to audit logs for auditing purposes.

Those members listed in the QPS-P-PKI-Backup group have access to audit logs for backup and archival purposes.

Audit logs for QPSICA1 can be copied for reporting purposes. Any request to copy audit logs is to be made in writing to the QPSPKIPA with details of:

→ The start and end dates of the audit logs required.

→ The purpose of the request

→ Who will be given copies of the audit logs or information extracted from the logs and the number of copies to be made

→ Who will extract the data and how will it be undertaken.

→ How the requestor will maintain the integrity of the information contained in the original audit log.

5.4.5 Audit Log Backup Procedures

The following configuration settings have been applied to QPSICA1 for the security event log:

- Maximum size of the Security event log: 128Mb
- Retention method for security log: Do not overwrite events (clear log manually)
- Audit: Shutdown system immediately if unable to log security audits: Enabled

The cumulative effect of these settings is that if the Security event log fills up, the CA server will shutdown. To mitigate the risk of audit data being overwritten, and CA shutdown, the Application, Security and System audit logs for QPSICA1 are copied to the QPSICA1 E drive on a daily basis. These logs are then included in the daily ISB backup schedule for QPS.

One copy of the logs is stored at QPS Headquarters and a second copy is to be stored at the Herston datacentre as detailed in s 5.1.8.

Further details on the configuration of Audit logs for QPSICA1 can be found in the document "CA and NetHSM Installation for QPS"

5.4.6 Audit Collection System (Internal vs. External)

The Audit Collection System for QPSICA1 is a component of the Windows 2003 system processes and Certificate Services. Access to audit data is restricted to those QPS members listed in the QPS-P-PKI-CAAudit group.

5.4.7 Notification to Event-Causing Subject

The QPSPKIPA has made no determination for QPSICA1 or IDORA1 regarding notification to event causing subject.

5.4.8 Vulnerability Assessments

The QPSPKIPA has made no determination for QPSICA1 or IDORA1 regarding the implementation of vulnerability assessment and analysis processes.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Events Archived

Documents, applications and data that will be archived for QPSICA1 and IDORA1 is:

- QGPKIPA and QPSPKIPA accreditation documentation
- the X.509 Certificate Policy for QPS and updates
- the Certification Practice Statement for the QPS Issuing Certification Authority QPSISC1
- other documentation concerning operations of the CA as determined by the QPSPKIPA from time to time.
- the CA and NetHSM Installation documentation for QPS
- completed application forms relating to certificate requests and revocation requests
- all certificates and CRLs issued and/or published
- audit logs (identified in 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 CA certificates

- 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, including device owners

  → Relying Parties.

The CAM of QPSICA1 is responsible for archiving all available records identified in this section.

The CAM will notify the QPSPKIPA:

- of all records to be archived for QPSICA1 or IDORA1
- of all locations of all archived records
- how the archived records have been protected
- the procedure for retrieving archived records
- when archival action has been completed

Procedures for archiving documentation, applications and data for QPSICA1 and IDORA1 are defined in the Records Retention and Disposal Handbook published by the QPS Administration Branch.

5.5.2 Retention Period for Archive

Archive data for QPSICA1 and IDORA 1 are retained for the period defined in s. 1.4 of the General Retention and Disposal Schedule for Administrative Records issued by the Queensland State Archives.

5.5.3 Protection of Archive

All archived records for QPSICA1 and IDORA1 are protected and stored in accordance with the Records Location, Storage and Disaster Management Handbook published by the QPS Administration Branch.

All requests to:

- access archived documents, applications and data from QPSICA1 or IDORA1 or
- to copy archived documents, applications and data from QPSICA1 or IDORA1 for reporting purposes

are to be submitted in writing to the QPSPKIPA for approval, through the Manager, Information Security Section, with details of:

- the archived documents, applications and data required, including the start and end dates for archived audit logs
- The reason for access or for copying the archived documents, applications and data

- Who will be given copies of the archived documents, applications and data and the number of copies to be made
- How the requestor will maintain the integrity of the information contained in the original archived documents, applications and data.

5.5.4 Archive Backup Procedures

Archived application, security and system data is not backed up for QPSICA1 or IDORA1, other than where the data or application is retained as part of the standard ISB backup process as defined in s5.1.8.

Documentation that is archived is not backed up.

5.5.5 Requirements for Time-Stamping of Records

No stipulation

5.5.6 Archive Collection System (Internal or External)

The Archive Collection System for QPSICA1 and IDORA1 is external to the QPS PKI and is managed by the QPSPKIPA in accordance with the Records Retention and Disposal Handbook and the Records Location, Storage and Disaster Management Handbook published by the QPS Administration Branch.

5.5.7 Procedures to Obtain and Verify Archive Information

No processes have been implemented by the QPSPKIPA to verify archive information for QPSICA1 and IDORA1.

5.6 KEY CHANGEOVER

All Subscriber certificates issued by QPSICA1 are revoked or expire at end of life and are never re-keyed.

The CA certificate for QPSICA1 may be re-keyed during the life of the certificate if there is a risk that the CA private key associated with the existing certificate could be compromised. If a re-key of the CA certificate is required for QPSICA1, the process defined in s. 4.7 must be followed and only the new key will be used for certificate signing purposes from that time.

The old private key must be available to verify 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 using the procedures defined in s. 6.2

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

The procedures to be followed if:

- QPSICA1 or IDORA1 are compromised, or are suspected of being compromised
- an Incident occurs which impacts the security of QPSICA1 or IDORA1 or the QPS PKI,

are:

- the person identifying the Incident or suspected compromise is to notify the Manager, Information Security Section or delegate, who will conduct an investigation in accordance with s 4.6 “Security Incidents” of the Information Management Manual and the procedures defined in the Information Security Incident Management procedures.
- the Manager, Information Security Section or delegate will notify the Chair of the QPSPKIPA of the Incident when it is first reported and provide a regular update to the Chair during any investigation of the incident.
- at the completion of the investigation the Manager, Information Security Section will provide a report to the QPSPKIPA on the outcome of the investigation which identifies
    - → the circumstances that led to the incident,
    - → the impacts of the incident on the PKI and other QPS systems or resources
    - → any interim actions taken during the investigation
    - → a plan detailing the actions required to resolve the impacts and to prevent similar incidents from occurring.
- The QPSPKIPA will notify the QGPKIPA and all relevant QPS PKI stakeholders by email, if any component of the QPS PKI is compromised.

Any actions required to ensure that the integrity of QPSICA1, IDORA1, or the QPS PKI is maintained are to be undertaken as soon as practicable following the notification of the incident.

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 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 procedures defined in s. 5.7.1 are to be followed if any computing resources including software, data and hardware are corrupted or suspected of being corrupted for QPSICA1 or IDORA1.

Procedures for the restoration of QPSICA1 or IDORA1 if a computing resource, including software, data and hardware, is corrupted are detailed in the Disaster Recovery and Business Continuity Plan for the CA.

5.7.3 Private Key Compromise Procedures

If a private key generated by or for QPSICA1 or IDORA1 is compromised, or suspected of being compromised the following procedures are to apply:

- the person identifying the compromise or suspected compromise will notify the Manager, Information Security Section or delegate who will investigate and report on the compromise using the procedures detailed in s. 5.7.1 above.
- If the compromise relates to a Subscriber’s private key that has been generated by QPSICA1, the QPSPKIPA will notify the QGPKIPA of the compromise and arrange for:
    - → all certificates that have been issued to the Subscriber using the private key to be revoked.
    - → the certificates to be published on a CRL,
    - → any outstanding certificate requests signed by the Subscriber’s private key to be rejected,
    - → the smart card that contains the private key to be recovered from the Subscriber, if available,
    - → the key pair for the Subscriber to be destroyed as per the procedures detailed in s. 6.2 below.
- If the compromise relates to a private key generated for IDORA1 by QPSICA1 the QPSPKIPA will notify the the QGPKIPA of the compromise and arrange for:
    - → all enrolment certificates that have been issued to IDORA1 to be revoked.
    - → all revoked certificates to be published to the CRL
    - → any outstanding certificate requests signed by the private key of IDORA1 to be rejected,
    - → the key pair for IDORA1 to be destroyed as per the procedures detailed in s. 6.2 below
    - → IDORA1 to be removed as a Registration Authority in the QPS PKI
- If the compromise relates to the CA private key that has been generated for QPSICA1 the QPSPKIPA will notify the QGPKIPA of the compromise and arrange for:
    - → all certificates that have been issued by QPSICA1 using the private key to be revoked, including requesting revocation of the CA certificate from the QGPKIPA
    - → all revoked certificates to be published to the CRL
    - → any outstanding certificate requests held by QPSICA1 to be rejected,
    - → the key pair for QPSICA1 to be destroyed as per the procedures detailed in s. 6.2 below.
    - → QPSICA1 to be removed as a Certification Authority in the QPS PKI.

5.7.4 Business Continuity Capabilities after a Disaster

Refer to the Business Continuity and Disaster Recovery Plan for QPSICA1 and IDORA1.

5.8 CA OR RA TERMINATION

The CAM for QPSICA1 and IDORA1 will notify the QPSPKIPA and all Subscribers and Relying Parties if the services provided by QPSICA1 or IDORA1 are to be terminated, including notification of the procedure defined in the Business Continuity and Disaster Recovery Plan for the continuance or otherwise of PKI services.

The QPSPKIPA will notify the QGPKIPA if QPSICA1 or IDORA1 are to be terminated.

If QPSICA1 or IDORA1 are terminated, the CAM must:

- surrender the CA/RA keys to the QPSPKIPA
- 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

QPSICA1

Key pairs for QPSICA1 are generated in a Common Criterial Evaluation Assurance Level (EAL) 4+ rated HSM using the procedures detailed in the document “CA and NetHSM Installation for QPS”. The private key is stored on the HSM key store and the public key in the local store of the CA.

Approval to generate a key pair must be obtained by the CAM for QPSICA1 from the QPSPKIPA and QGPKIPA before a key pair can be generated. The process for requesting generation of a key pair is defined in s. 4.1.1 for enrolment of QPSICA1 and s. 3.2.5 for validation of authority.

Registration Authorities

Key pairs for IDORA1 are generated in a Common Criterial Evaluation Assurance Level (EAL) 4+ rated HSM. The private key is protected by the HSM and the public key stored in the local certificate store of the RA.

Approval to generate a key pair must be obtained by the CAM for QPSICA1 from the QPSPKIPA and QGPKIPA before a key pair can be generated. The process for requesting generation of a key pair is defined in s. 4.1.1 for enrolment of IDORA1 and s. 3.2.5 for validation of authority.

Subscribers

Subscriber key pairs for certificates issued by QPSICA1 for authentication to the QPS network and email signing are generated on smart cards. The keys are generated using the process described in s. 3.2.1:

Subscriber key pairs for Basic Assurance certificates issued to devices by QPSICA1 are generated in the local certificate store on the device.

6.1.2 Private Key Delivery to Subscriber

Subscriber key pairs for certificates issued by QPSICA1 for authentication to the QPS network and email signing are generated on smart cards by the ID Issuing Office using the procedure detailed in s.3.2.1. The smart card with the private key is delivered to the Subscriber through:

- a face-to-face process between the Subscriber and a Registration Officer for IDORA1
- mailing the smart card to the Subscriber's OIC / Section Head for issuance to the Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

QPSICA1 delivers its public key to the Qld Govt Policy CA QGPCA2 through the request made by QPSICA1 for a CA certificate. The request is delivered to the Certificate Issuer in a text file via email. IDORA1 delivers the Subscriber's public key to QPSICA1 during Certificate request using the process defined in s. 3.2.1.

6.1.4 CA Public Key Delivery to Relying Parties

Public Keys for IDORA1 are made available to Relying Parties at the locations specified in s. 2.2.

6.1.5 Key Sizes

The QPS PKI uses the PKCS standard for signature algorithms.

The following key sizes and algorithms are used by 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 as a minimum 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 key usage purposes that apply to Subscriber certificates issued by QPSICA1 are detailed in the document "QPS Certificate Profile".

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

QPSICA1 private keys are protected by a Common Criterial Evaluation Assurance Level (EAL) 4+ rated HSM using module protection as detailed in the document “Installation of the QPS PKI”. Module protection ensures that QPSICA1’s private key is only accessible within the confines of the netHSM Cryptographic Module device.

QPSICA1 has nine Cryptographic Module Administrator token holders. The Cryptographic Module Administrator activities require a quorum of two Cryptographic Module Administrator token holders (not including the Console operator) to be authenticated prior to activating or accessing .

6.2.3 Private Key Escrow

QPSICA1 does not issue encryption certificates at this time.

6.2.4 Private Key Backup

The procedures for backing up QPSICA1 and the CA private keys are detailed in the documents “Installation of the QPs PKI” and “Appendix H – CA Disaster Recovery with nCipher” and involve:

- executing the CA backup script held on QPSICA1 to backup critical CA and nCipher configuration, security world, module and key files to the E drive on the CA and
- including the E drive in the daily network backup set. QPS uses HP Data Protector as its primary backup software on the network.
- storing a copy of the backup off-site as detailed in s.5.1.8

6.2.5 Private Key Archival

Private keys for QPSICA1 and Subscriber signature certificates are not archived.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Backup of private keys for QPSICA1 is performed by QPS employees appointed to the Trusted Role of PKI Operator. A list of appointments is contained in the “Schedule of Appointments to Trusted Roles for the QPS PKI”.

Private keys for QPSICA1 are protected and stored on a Common Criterial Evaluation Assurance Level (EAL) 4+ rated HSM using module protection as detailed in the document “Installation of the QPS PKI”.

Subscriber private signing keys are generated on the Subscriber’s smart card and never leave the smart card.

6.2.7 Private Key Storage on Cryptographic Module

Refer to s. 6.2.6

6.2.8 Method of Activating Private Key

Activation of the private key for QPSICA1 requires that a HSM Operator token be available on the HSM to validate the participation of the HSM in a FIPS 140-2 level 3 security world. In addition, any administrative activities on the HSM require a quorum of 2 Cryptographic Module Administrator Token Holders to be present to authorise the activity.

Activation of the private key for IDORA1 requires an authorised person to authenticate to the QPS network using either a smart card and PIN, or a userid and password.

All certificates issued to a Subscriber's smart card by QPSICA1 for authentication to the network and email signing require the Subscriber to authenticate to the smart card before the associated private key(s) is activated. Authentication requires the Subscriber to enter a personal identification number (PIN) on the workstation or laptop which is then verified against the encrypted PIN on the smart card before information can be accessed on the card

Entry of the PIN is not displayed while it is entered.

6.2.9 Method of Deactivating Private Key

The private key of QPSICA1 can be de-activated by stopping Certificate Services on the CA. The private key is also de-activated automatically when the key reaches the end of its usage period.

In the event of a suspected compromise of the private key, it may be necessary for the CAM of QPSICA1 to switch off the CA until the compromise has been fully investigated. If this occurs, QPSICA1 must be restored within 24 hours before the next CRL update period.

The private key for IDORA1 will only be de-activated when the key is suspected of being compromised. In the event of a suspected compromise of the private key, IDORA1 will be switched off by the CAM until the compromise has been fully investigated.

Private keys stored on a smart card can be de-activated through re-initialisation of the smart card by a Registration Officer in the ID Issuing Office. Generally, the smart card is surrendered to the ID Issuing Office for physical destruction of the card rather than re-initialisation.

6.2.10 Method of Destroying Private Key

Private keys for QPSICA1 can be destroyed by reinitialising the HSM as per the procedure defined in the document “Installation of the QPS PKI”. Destruction of private keys for QPSICA1 must be approved by the QPSPKIPA.

When an Administrator or Operator Token for QPSICA1 is lost, damaged, no longer required, or needs to be re-assigned to a new holder, the token will be returned to the Manager, Information Security Section, who will:

- if the token is lost, investigate the circumstances of the loss using the procedures identified in s. 5.7.1 and update the Token Register
- if the token is damaged, arrange for the token to be destroyed and note its destruction in the Token Register.

- if the token is no longer required as part of the key set, either arrange for the token to be destroyed or retain the token in the B-class safe used to store the tokens and update the Token Register accordingly.

The private key for IDORA1 will be destroyed only if the key is compromised or when the key usage period expires. If the private key is compromised, the previous certificate will be revoked with a revocation reason of "Key Compromised" and a new certificate issued by QPSICA1. Destruction of the private key for IDORA1 must be approved by the QPSPKIPA. If the key usage period expires, the key becomes inoperative and no destruction of the key is required.

Subscriber digital signature private keys shall be destroyed by the CAM, RAM or Registration Officer by destruction of the smart card on which the key is stored.

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 QPSICA1 are archived in accordance with the processes defined in s. 5.5.

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.

The usage period for the QPSICA1 key pair is a maximum of 10 years (based on a key length of 2048 bits).

The QPCICA1 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 the key pair for QPSICA1 must expire before the end of the CA’s key pair’s validity period.

All Subscriber certificates issued to QPS permanent employees by QPSICA1 must have a maximum validity period of five years.

All Subscriber certificates issued to QPS contractors by QPSICA1 must have a maximum validity period of one year.

All Subscriber signature private keys generated by QPSICA1 must have the same validity period as their corresponding public key.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Activation data (eg, password, PINs) for QPSICA1, IDORA1 and Subscribers is user-selected by the persons holding that activation data.

6.4.2 Activation data protection

Activation Data for QPSICA1 is protected a Common Criteria Evaluation Assurance Level (EAL) 4+ rated HSM and its activation will require a quorum of designated operators

6.4.3 Other Aspects of Activation Data

No stipulation

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

Refer to the document “Installation of the QPS PKI” for the build and configuration technical requirements for QPSICA1 and IDORA1.

Both QPSICA1 and IDORA1 use operating systems that:

- require 2 factor authenticated logins
- provide discretionary access control through the QPS Enterprise Directory and role separation of duties.
- provide a security audit capability as defined in s. 5.4

6.5.2 Computer Security Rating

No Stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

All system development controls and processes are documented in “Installation of the QPS PKI” in the QPS PKI document set comprising:

- Installation of the QPS PKI.doc
- Appendix F – NetHSM Management.doc
- Appendix G – NetHSM Replacement.doc
- Appendix H – CA Disaster Recovery with nCipher.doc
- Appendix I – PKI Mangement Tasks
- The QPS CPS for QPSICA1.doc

These controls and the processes used to build and configure QPSICA1 and IDORA1 have been approved by the QPSPKIPA, the Queensland Government PKI accreditation process and the internal QPS Change Advisory process for implementation of Information Systems in the QPS production environment.

6.6.2 Security Management Controls

Security management controls for QPSICA1 are consistent with QPS Security Policies and include:

- Detailed documentation of the build and configuration for QPSICA1 in "Installation of the QPS PKI".
- Auditing of application, security and system changes as defined in s. 5.4 and regular monitoring of audit logs to detect unauthorised modification to the software or configuration of QPSICA1.
- only applications or component software on the CA that are directly related to the operation of the QPS PKI.

6.6.3 Life Cycle Security Controls

The Lifecycle Security Controls used in the development and configuration of QPSICA1 are:

- all equipment (hardware and software), including modifications and upgrades, procured for the QPS PKI has been purchased under the QPS and Queensland Government Purchasing arrangements from recognised PKI vendors.
- All cryptographic hardware and software components employed in the QPS PKI have been certified to the equivalent FIPS 140-2 standard as the Common Criteria level specified for such equipment by the Queensland Government in the QG Root Certification Policy.
- All equipment has been configured on-site in secured QPS premises by authorised QPs personnel.
- Any development and configuration will be undertaken with regard to the policies and procedures defined in the:
  - → QPS X.509 Certificate Policy
  - → QPS CPS for QPSICA1
  - → ISB Policies and procedures

6.7 .NETWORK SECURITY CONTROLS

QPSICA1 is connected to the QPS network.

Network security controls include:

- protection of QPSICA1 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

6.8 TIME-STAMPING

A source of trusted time is used to support time stamping of data.

7. Certificate, CRL and OCSP Profiles

7.1 CERTIFICATE PROFILE

The certificate profile for the QPSICA1 CA certificate and Subscriber certificates issued by QPSICA1 is detailed in the document “QPS Certificate Profiles”.

7.2 CRL PROFILE

The CRL profile for QPSICA1 is detailed in the document “QPS Certificate Profiles”.

7.3 OCSP PROFILE

Not applicable.

8. Compliance Audit and Other Assessments

Refer to the QPS X509 Certification Policy and the Queensland Government PKI Framework.

9. Other Business and Legal Matters

Refer to the QPS X509 Certificatio Policy and the Queensland Government PKI Framework.

10. Bibliography

Refer to the QPS X509 Certificatio Policy

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

Acronym / abbreviation	Word / phrase
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
IDO	Identification Issuing Office
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
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

Acronym / abbreviation	Word / phrase
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.

Term	Definition
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 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.

Term	Definition
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]
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

Term	Definition
	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]
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]

Term	Definition
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
01/03/09	0.01	Draft	Initial draft for internal team review	Laurie Sherd	Ian Taylor Peter Wibberley
30/03/09	0.02	Draft	Updated after consultation	Laurie Sherd	Ian Taylor Peter Wibberley Brian Komar (S6)
31/03/2009	1.0	Final	Released for Consultation	Laurie Sherd	ISB, ISS

4. Authorisation

Date	Version	Status	Approved by	Position	Signature
2009	1.00	Final	Tony Fisher	Manager, Security Section, QPS	

END OF DOCUMENT