Queensland Health
Public Key Infrastructure

QHPKI Hierarchy

Certificate Policy

and

Certification Practice Statement

V1.1 February 2018

Queensland Government

QHPKI Certificate Policy and Certification Practice Statement

For more information contact:
Cyber Security Group (CSG),
eHealth Queensland, Department of Health, PO Box 117 Fortitude Valley 4006
email mailto:dl-CSG@health.qld.gov.au

An electronic version of this document is available from CSG.

Version Control

Version	Date	Comments
0.1	15/08/2016	Initial draft by ePulse Security.
0.2	19/08/2016	Updates from CSG consultation
0.3	7/09/2016	Updates from Legal advice
1.0	8/09/2016	Release
1.1	28/02/2018	Updates from ISC Meeting Feb 2018

Contents

1. INTRODUCTION

This document follows the framework and structure outlined in the Internet Engineering Task Force's RFC 3647 to describe the authorisation framework for the Queensland Health Public Key Infrastructure (QHPKI) service.

The Public Key Infrastructure is a framework for using digital certificates and their associated keys to verify the identity of users and computers to other users, computers and applications. PKIs are important elements in network and Internet security because many communications, such as business and e-commerce transactions, are dependent on a reliable method to identify the parties to the transaction.

The PKI is not itself an authentication method, but is a system for issuing, managing and revoking the digital certificates and key pairs that are used to authenticate Queensland Health users and computers within the network and across the Internet. The components of the QHPKI include special servers called certification authorities (CAs) together with policies governing how the CAs issue, manage and revoke certificates and store keys, digital certificates and their keys, and applications that can use the PKI.

This document describes the policies for governing the QHPKI hierarchy, which includes a Root CA with a number of subordinate CAs as per the Overview section below.

1.1 Overview

The purpose of a public-key infrastructure is to manage keys and certificates to provide public-key encryption and digital signature services. By managing keys and certificates through a PKI, Queensland Health establishes and maintains a trustworthy networking environment across a wide variety of applications. Users do not have to understand how the PKI manages keys and certificates to take advantage of encryption and digital signature services.

Queensland Health has contracted a managed services provider (Symantec) to host and manage the CAs and the supporting infrastructure on behalf of Queensland Health.

Queensland Health is responsible for the operation and administration of the PKI service in line with this Certificate Policy and Practices document. This includes configuration of the certificate policies and the certificate lifecycles.

1.2 Document Name and Identification

This document is the "Queensland Health Public Key Infrastructure (QHPKI Hierarchy) Certificate Policy and Certification Practice Statement". This document covers all of the CAs within the QHPKI hierarchy.

The following ASN.1 object identifiers relate to this policy.

- "1.2.36.1.3.1.4.1.1.1.13" – QHPKI Hierarchy Policy OID (this document)

1.3 PKI Participants

The following identities participate in the QHPKI framework.

1.3.1 Certification Authorities

The certification authority (CA) is the primary component of a PKI and is simply a server that runs certificate services software. A CA acts as the agent of trust in the PKI by issuing and validating electronic certificates so that applications can use them to authenticate users and devices. CAs create certificates for applications/users by digitally signing a set of data allowing any tampering with the contents of the certificate to be easily detected.

Digital certificates have a specified validity period and the CA securely publishes information regarding the status of each certificate in the system by publishing secure certificate revocation lists (CRLs). Applications consistently and transparently check the appropriate CRL to determine if a certificate is still trustworthy on behalf of users.

The QHPKI Root CA is at the top of the CA hierarchy. This CA only issues certificates to other CAs. Lower level CAs, called subordinate CAs, perform the daily task of issuing certificates to users and computers. The root CA is the most trusted and is kept in a very secure physical location and taken off line when it is not in use. All CAs are securely managed because they store the private keys that are at the heart of the PKI's authentication system.

This policy includes all of the CAs in the QHPKI hierarchy that has the following structure:

- QHPKI Root CA – The top of the trust chain. Signs all of the sub-ordinate CAs.

Subordinate CAs in the QHPKI hierarchy include:

- QHPKI Device Basic Issuing CA – This CA issues certificates to QH devices and servers that allow them to authenticate to services including wireless access; domain controllers; internal QH websites and Microsoft System Center Configuration Manager (SCCM).
- QHPKI User Basic Issuing CA – This CA issues certificates to Queensland Health users to allow them to authenticate to QH services and internal document signing.
- QHPKI Mobile Device Basic Issuing CA – This CA issues certificates to mobile devices that are managed by the QH Enterprise Mobile Management services; currently Blackberry Enterprise Server and MobileIron.

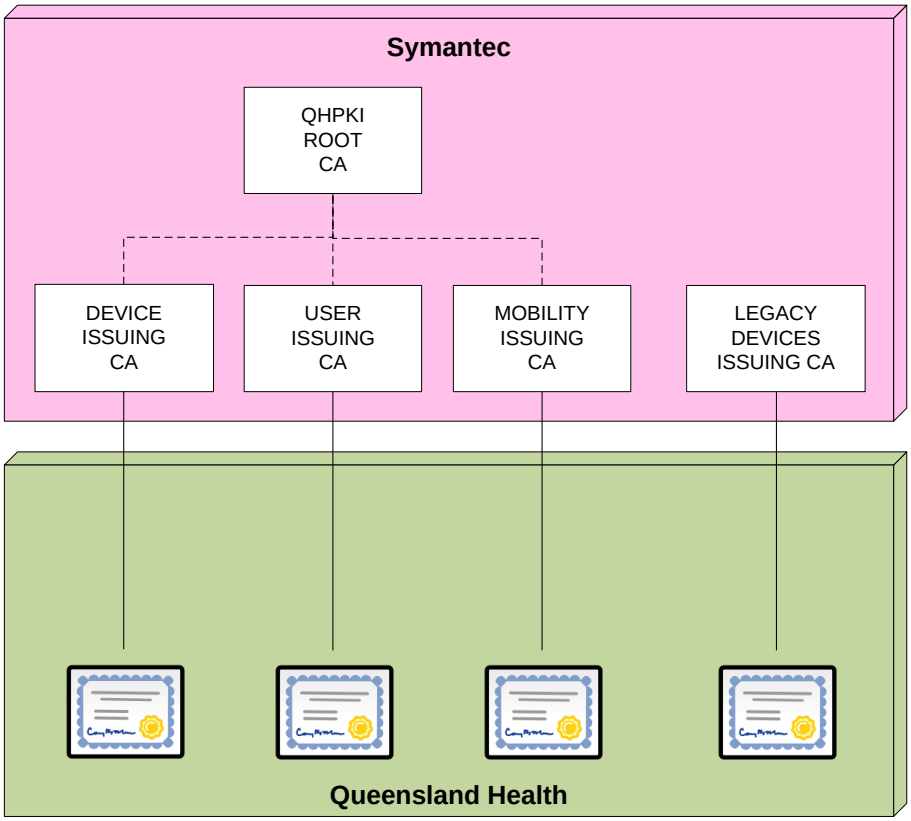

Figure 1 - Queensland Health PKI Hierarchy

Within this document if no CA is specified then the policy or practice applied equally to all CAs within the QHPKI hierarchy. If a policy or practice differs then it will specify the CAs that it is applicable to.

1.3.2 Registration Authorities

A Registration Authority is the PKI component that accepts requests for certificates to be signed on behalf of the operator. The Registration Authority may use workflow to approve the certificate requests or it may just queue all requests waiting for a PKI Administrator approval.

QHPKI Root CA

The QHPKI Root CA Registration Authority is managed by Symantec. The only type of certificate that can be issued from the Root CA is a Sub-CA certificate. This is a manual process. To initiate a new Sub-CA request an authorised QH PKI Administrator must make the request using the Symantec PKI Manager portal.

QHPKI Device Basic Issuing CA

The QHPKI Device Basic Issuing CA has four ways for end-entities to request a certificate. Each of the Registration Authority services utilises the services provided by the Symantec MPKI service.

1) **Enterprise Gateway**. This is a QH enterprise active directory domain joined service provided by Symantec that is hosted at Queensland Health. It is used by EAD joined devices to auto-enrol for certificates in line with the EAD Group policies. The Enterprise Gateway service accepts the request, validates that it is complete and meets the certificate profile criteria, signs the request and forwards to the Symantec MPKI service for certificate issuance.

If the certificate profile allows automated issuance then the certificate request will be signed by the Symantec MPKI service and returned to the end-entity.

2) **SCEP enrolment**. Some devices support the ability to perform an automated enrolment using a standard known as “Simple Certificate Enrolment Protocol”. The Symantec MPKI provides a SCEP service which can be used by supported devices to perform these enrolments.

3) **Certificate Signing Request (CSR)**. Some devices are enrolled for certificates manually by an administrator. In this case a CSR is created using a tool which contains the details required to identify that device. The administrator accesses the Symantec portal, completes some details and then copies the CSR request into a field on the page. The request is then validates and assigned to the appropriate queue for a PKI Administrator to approve.

4) **Bulk CSR**. In some cases many CSR requests are generated for a particular system or because many of a same device are being installed. In this case a zip file of all of the CSR’s can be lodged with the Hosting and Directories team with a work order request. The team has a script that enables the quick lodgement of the CSR’s and download of the certificates.

QHPKI Mobility Basic Issuing CA

The QHPKI Mobility Basic Issuing CA only accepts requests from the QH enterprise mobility management platforms, (BES and MobileIron). These platforms use the Symantec provided API’s to make certificate requests and receive the corresponding certificates.

QHPKI User Basic Issuing CA

The QHPKI User Basic Issuing CA has two ways for end-entities to enrol for certificates. Each of these Registration Authority services utilises the services provided by the Symantec MPKI service.

1) **Enterprise Gateway**. This is a QH enterprise active directory domain joined service provided by Symantec that is hosted at Queensland Health. It is used by EAD users to auto-enrol for certificates in line with the EAD Group policies. The Enterprise Gateway service accepts the request, validates that it is complete and meets the certificate profile criteria, signs the request and forwards to the Symantec MPKI service for certificate issuance.

   If the certificate profile allows automated issuance then the certificate request will be signed by the Symantec MPKI service and returned to the end-entity.

2) **Certificate Signing Request (CSR)**. Some applications and/or users require that the certificate is enrolled manually by the user. In this case a CSR is created using a tool which contains the details required to identify the user. The user accesses the Symantec portal, completes some details and then copies the CSR request into a field on the page. The request is then validated and assigned to the appropriate queue for a PKI Administrator to approve.

1.3.3 Subscribers (End Entities)

A Subscriber is the end-entity that is allowed to enrol (subscribe) for a certificate.

QHPKI Root CA

Subscribers of this CA are the subordinate CAs that comprise the QHPKI.

QHPKI Device Basic Issuing CA

Subscribers of this CA are QH devices including network infrastructure, servers, bio-medical devices and telephony systems.

QHPKI Mobility Basic Issuing CA

Subscribers of this CA are the infrastructure that supports the QH enterprise mobility management services (BES and MobileIron) and the mobile devices (smartphones and tablets) that they manage.

QHPKI User Basic Issuing CA

Subscribers of this CA are individuals that have an identity within the QH domain or a QH system.

*Note: This CA **does not** support Subscribers where the entity is a group or shared identity.*

1.3.4 Relying Parties

Relying parties are ***Queensland Health services***, either operated by Queensland Health or on behalf of Queensland Health; and ***Queensland Health users*** that consume certificates of any of the CAs within the QHPKI hierarchy.

1.3.5 Other Participants

The PKI is hosted and managed on behalf of Queensland Health by Symantec.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

QHPKI Root CA

The Root Certificate Authority will issue certificates for Sub CAs for Queensland Health, such as the Device Basic Issuing CA, the Mobile Device Basic Issuing CA, and the User Basic Issuing CA.

Possible future use of the certificates issued by this authority include other Sub CAs at different trust levels for Queensland Health.

The certificate templates that this policy is valid for are:

- Sub-CA

QHPKI Device Basic Issuing CA

The Device Basic Issuing Certificate Authority will issue certificates for end-entities that will use the certificate for authentication and identification to other Queensland Health devices or users; and to initiate an encrypted tunnel between Queensland Health devices or users.

QHPKI Mobility Basic Issuing CA

The Mobility Basic Issuing Certificate Authority will issue certificates for end-entities that are managed by a Queensland Health Enterprise Mobility Management platform as well as the components of those platforms. These certificates are to be used for authentication and identification to other Queensland Health devices or users; and to initiate an encrypted tunnel between Queensland Health devices or users.

QHPKI User Basic Issuing CA

The User Basic Issuing Certificate Authority will issue certificates for end-entities that will use the certificate for authentication and identification to Queensland Health services and servers; encryption; and creating digital signatures.

1.4.2 Prohibited Certificate Uses

QHPKI Root CA

The Root Certificate Authority must not issue certificates to end entities. The Root Certificate Authority must not issue certificates to subordinate CAs that are deemed to be of a higher assurance level that “Medium”.

QHPKI Device Basic Issuing CA

The Device Basic Issuing Certificate Authority must not issue certificates to an end-entity that is not identified as a Queensland Health device or server.

The Device Basic Issuing Certificate Authority must not issue certificates for use with services and systems that are deemed to be of a higher assurance level that “Basic”.

QHPKI Mobility Basic Issuing CA

The Mobility Basic Issuing Certificate Authority must not issue certificates to an end-entity that is not identified as a Queensland Health managed mobile device or a component of the Queensland Health enterprise mobility management platform.

The Mobility Basic Issuing Certificate Authority must not issue certificates for use with services and systems that are deemed to be of a higher assurance level that “Basic”.

QHPKI User Basic Issuing CA

The User Basic Issuing Certificate Authority must not issue certificates to an end-entity that is not identified as a Queensland Health individual user. The User Basic Issuing certification authority must not issue certificate to end-entities that are anonymous, group/team or shared.

The User Basic Issuing Certificate Authority must not issue certificates for use with services and systems that are deemed to be of a higher assurance level that “Basic”.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

This policy is administered on behalf of Queensland Health by the Queensland Health PKI Operational Authority, currently delegated to the eHealth Queensland Cyber Security Sub-Committee:

Post: eHealth Queensland
Attn: QHPKI Operational Authority Chair
c/o Director of Cyber Security Group
PO Box 117
Fortitude Valley, Queensland 4006
Email: SecuritySecretariat@health.qld.gov.au

1.5.2 Contact Person

Security Secretariat Chair
Cyber Security Group

1.5.3 Person Determining CPS Suitability for the Policy

The eHealth Queensland Chief Technology Officer approves the Certificate Policy and Certificate Practice Statement document.

1.5.4 CPS approval procedures

The Cyber Security Working Group makes recommendations for changes to this Certificate Policy and Certificate Practice Statement document. These recommendations are then to be approved by the eHealth Queensland Chief Technology Officer.

1.6 Definitions and Acronyms

1.6.1 Definitions

Name	Definition
Automated Registration Authority	An Automated Registration Authority is a system that verifies Subscriber requests using a workflow or pattern for a Digital Certificate and tells the Certificate Authority to issue it. The QHPKI uses the Symantec Enterprise Gateway server for this.
Certificate Authority	Certificate Authority is the entity that issues digital certificates.
Certificate Authority Manager	Certificate Authority Manager is the Service Owner responsible for the day to day operational management of the QHPKI Service. This role has been delegated to the Director of Infrastructure Management.
Certificate Authority Owner	Certificate Authority Owner is the legal entity that is responsible for the QHPKI Service, namely, Queensland within the Department of Health, represented by eHealth, Queensland.
Compliance Auditor	Responsible for appointing auditors to perform regular audits of CA compliance internally.
Managed PKI Service	The product and services provided by the Service Provider that comprise the QHPKI Service.
Operational Authority	The committee responsible for governance of the QHPKI service.
PKI Participants	The parties mentioned in section 1.3 being Certificate Authorities, Registration Authorities, Subscribers, Relying Parties and Symantec.
QHPKI	Queensland Health PKI is defined as the operators of the PKI service; which includes eHealth Queensland and the

Name	Definition
	contracted Service Provider.
Registration Authority	The Registration Authority is the authority in Queensland Health that verifies Subscriber requests for a Digital Certificate and tells the Certificate Authority to issue it.
Registration Authority Administrator	Operational personnel within eHealth Queensland that are responsible for day to day operations of the QHPKI services.
Relying Party	An entity that acts in reliance on the information provided by QHPKI Certificate.
Service Owner	Responsible for the delivery of the service to Queensland Health users and entities. This role is assigned to the Director of Operations.
Service Provider	The contracted managed services provider engaged by eHealth Queensland to provide the Managed PKI Service. Currently this is Symantec.
Service Provider Operators	Operational personnel within the Service Provider that are responsible for day to day operations of the Managed Service.
Subscriber	The end-entity which has enrolled and received a QHPKI certificate.
Trusted Roles	A role within the QHPKI operational team which requires specific additional security checks

1.6.2 Acronyms

Name	Definition
CA	Certificate Authority
CAO	Certification Authority Owner
CP	Certificate Policy
CPS	Certificate Practice Statement
CRL	Certificate Revocation List
EOL	End of Life
HSM	Hardware Security Module
MDM	Mobile Device Management
NIST	National Institute of Standards and Technology (United States Government)
OCSP	Online Certificate Status Protocol
OID	Object Identity (ID)
OA	Operational Authority
PKI	Public Key Infrastructure
QGPKI	Queensland Government Public Key Infrastructure

Name	Definition
QH	Queensland Health
QHPKI	Queensland Health Public Key Infrastructure
SCCM	System Center Configuration Manager – a Microsoft technology to manage a fleet of computers
SLA	Service Level Agreement

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

All of the CAs within the QHPKI hierarchy are operated by Symantec Corporation as the commercial Provider on behalf of Queensland Health.

2.1 Repositories

The Provider is responsible for retaining secure repositories of all issued certificates.

QHPKI User Basic Issuing CA

The certificates issued by the User Basic Issuing Certificate Authority will also be stored within the Queensland Health Enterprise Active Directory as a user attribute.

2.2 Publication of Certification Information

The Managed Service Provider is responsible for publishing the certificate revocation information for the QHPKI Root CA at regular intervals.

Queensland Health will copy the published CRL's from the Managed Service Provider and publish on the Queensland Health PKI Distribution service[1], hosted within the Queensland Health data centre.

2.3 Time or Frequency of Publication

QHPKI Root CA

The Managed Service Provider is responsible for publishing the certificate revocation information for the QHPKI Root CA at least yearly, with a Certificate Revocation List (CRL) overlap period of 1 or more months.

All other QHPKI Issuing CAs

The Managed Service Provider is responsible for publishing the certificate revocation information for the QHPKI Issuing CAs at least every 24 hours.

2.4 Access Controls on Repositories

Information published on the QHPKI Distribution service (such as CRL's and this Certificate Policy and Certificate Practice Statement document) is protected against accidental deletion or alteration by publishing in read-only format.

[1] http://pki.health.qld.gov.au

3. IDENTIFICATION AND AUTHENTICATION

QHPKI Root CA

The Managed Service Provider is responsible for creation of the certificates that are issued by the QHPKI Root CA.

The certificates from this authority are generated by the Managed Services Provider on behalf of Queensland Health only after approval of the QHPKI OA, and all certificate attributes are verified by the QHPKI OA. This is performed by the completion and signing of CA Naming Documents that are required before a CA certificate can be created.

Certificate re-key is handled through issuing a new certificate and revoking the old certificate. Certificate re-key should be used in the following circumstances by a Subscriber:

The hardware security module that holds the sub-CAs key is replaced, lost or stolen

Certificate revocation is not automatically performed when a new certificate is issued to the same entity, because it may be required to have a certificate overlap for Sub-CAs.

All other QHPKI Issuing CAs

The Managed Service Provider is responsible for publishing the certificate revocation information for the QHPKI Issuing CAs at least every 24 hours.

3.1 Naming

3.1.1 Types of Names

QHPKI Root CA

The Root CA issues certificates to the QHPKI sub-ordinate CAs using the following naming convention:

“QHPKI” <<Purpose of CA>> <<Assurance level>> “Issuing CA”

Where the following:

***Purpose of CA**:* *Descriptive name for the CA purpose.*

***Assurance level**:* *Using QGEA assurance levels [Basic|Medium|High]*

CA names must be unique across the QHPKI PKI hierarchy.

All other QHPKI Issuing CAs

All of the sub-ordinate CAs within the QHPKI hierarchy issue certificates to end-entities. The name within the certificate must match at least one of the following criteria:

- The legal entity name for the Subscriber
- The distinguished name that is held in the Queensland Health Enterprise Active Directory for the Subscriber
- The FQDN for the Subscriber

- The hostname of the Subscriber
- The Queensland Health registered email address of the Subscriber

3.1.2 Need for Names to be Meaningful

QHPKI Root CA

Subordinate CA names must indicate the purpose of the sub-CA.

All other QHPKI Issuing CAs

End-entity certificates must clearly identify the end-entity that they are issued to using at least one of the following criteria:

- The legal entity name for the Subscriber
- The distinguished name that is held in the Queensland Health Enterprise Active Directory for the Subscriber
- The FQDN for the Subscriber
- The hostname of the Subscriber
- The Queensland Health registered email address of the Subscriber

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymous and pseudonymous certificates names are not allowed. Either the Subject Name field or the Subject Alternative Name field must be populated.

3.1.4 Rules for Interpreting Various Name Forms

Subject Names shall be X400 names (e.g. CN=My Name,O=Queensland Health,C=AU).

Subject Alternative Names can contain any standardised information necessary in addition to the above names allowable for Subject Names.

3.1.5 Uniqueness of Names

All end-entity subject names must be unique for each issuing CA and must represent a single entity.

QHPKI does not support the issuance of PKI certificates for multiple end-entites (e.g. wild card certificates).

3.1.6 Recognition, Authentication, and Role of Trademarks

Subscriber names must not infringe third party rights, i.e. names must respect trademarks, registered names, and entity names.

3.2 Initial Identity Validation

QHPKI Root CA

Subordinate CA certificates can only be signed/created with approval from the QHPKI Operational Authority (see section 1.5.1).

All other QHPKI Issuing CAs

End-entity certificates must be authorised by a QHPKI Registration Authority Administrator. Acceptable QHPKI Registration Authority Administrators include:

- QHPKI Administrator Users who have been granted the role of "Certificate Approver"
- QHPKI Automated Registration Authority systems can approve the request for certificates from domain joined devices

In some cases a QHPKI Registration Authority Administrator can "pre-approve" the issuance of a certificate by creating a one-time key which can be used during the enrolment to have the certificate issued straight away.

3.2.1 Method to Prove Possession of Private Key

Possession of the private key must be demonstrated during the certificate enrolment by signing the certificate request.

3.2.2 Authentication of Organisation Identity

QHPKI does not issue certificates to organisational identities.

3.2.3 Authentication of Individual Identity

The QHPKI Registration Authority Administrator must authenticate the identity of the Subscriber for the certificate enrolment request against Queensland Health directories and repositories as follows:

QHPKI Device Basic Issuing CA

Devices must have fully qualified names that include a Queensland Health suffix (e.g. health.qld.gov.au).

If the device is a member of the Enterprise Active Directory domain then the subject name must match the name within the directory.

If the device is not a member of the Enterprise Active Directory domain then the certificate request must come from an authorised Queensland Health person or contractor.

Device enrolments must include the email address of the Queensland Health user or team responsible for them.

QHPKI Mobility Basic Issuing CA

Mobile device enrolments can only be accepted from the Queensland Health Enterprise Mobility Management platforms. The EMM platform must ensure that only managed mobile devices are enrolled for a certificate.

QHPKI User Basic Issuing CA

User certificates must only be approved for issuance to user identities within the Queensland Health Enterprise Active Directory.

User certificates must not be issued to end-entities that are anonymous, group/team or shared.

3.2.4 Non-Verified Subscriber Information

Any other information contained within the certificate other than the subject DN should be treated as unverified

3.2.5 Validation of Authority

QHPKI Root CA

Subordinate CA certificates can only be signed/created with approval from the QHPKI Operational Authority (see section 1.5.1).

All other QHPKI Issuing CAs

End-entity certificates must be authorised by a QHPKI Registration Authority Administrator. Acceptable QHPKI Registration Authority Administrators include:

- QHPKI Administrator Users who have been granted the role of "Certificate Approver"
- QHPKI Automated Registration Authority systems can approve the request for certificates from domain joined devices

In some cases a QHPKI Registration Authority Administrator can "pre-approve" the issuance of a certificate by creating a one-time key which can be used during the enrolment to have the certificate issued straight away.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-Key Requests

Re-key requests are treated in the same way as any other request.

3.3.1 Identification and Authentication for Routine Re-Key

Same as initial identity validation, see section 3.2.

3.3.2 Identification and Authentication for Re-Key after Revocation

Same as initial identity validation, see section 3.2.

3.4 Identification and Authentication for Revocation Request

QHPKI Root CA

Subordinate CA certificates revocation requests must be authorised by the QHPKI Operational Authority (see section 1.5.1).

All other QHPKI Issuing CAs

End-entity certificate requests must be authorised by a QHPKI Registration Authority Administrator.

An end-entity certificate that is linked to an identity within the Queensland Health Enterprise Active Directory domain must be revoked if the identity within the domain is deleted.

An end-entity or an authorised representative of the end-entity may request the certificate to be revoked by creating a service request and assigning it to the QHPKI Administrator resolver group.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can Submit a Certificate Application

QHPKI Root CA

Subordinate CA certificates enrolment requests must be authorised by the QHPKI Operational Authority (see section 1.5.1) and submitted by a QHPKI Administrator.

All other QHPKI Issuing CAs

End-entity certificate requests must be submitted by the named individual or an authorised Queensland Health person on behalf of the individual or device.

If the Subscriber is an Enterprise Active Directory domain joined entity then the enrolment may be submitted on their behalf by an Automated Registration Authority administrator.

4.1.2 Enrolment Process and Responsibilities

QHPKI Root CA

Subordinate CA certificates enrolment requests must be submitted to the Service Provider (Symantec) via the Customer Services team using the appropriate form from the Service Provider.

All other QHPKI Issuing CAs

End-entity certificate requests must be submitted to the services provider via one of the following methods:

- Web-services API
- SCEP interface
- Managed PKI web-portal

4.2 Certificate Application Processing

QHPKI Root CA

The Service Provider shall validate any certificate request for a sub-ordinate CA with the QHPKI team prior to scheduling and issuing the certificate.

All other QHPKI Issuing CAs

If the certificate request is authorised by an Automated Registration Authority administrator then the certificate shall be generated automatically and returned to the Subscriber.

Otherwise, an authorised QHPKI Registration Authority Administrator shall validate the certificate request upon receipt of a service request from the Subscriber after the certificate request has been lodged.

QHPKI Work Instruction, “Approving a QHPKI Subscriber certificate request” outlines more details on how this is to be accomplished.

4.2.1 Performing Identification and Authentication Functions

QHPKI Root CA

The Service Provider shall validate that the certificate request has been authorised by an identified signatory.

All other QHPKI Issuing CAs

Certificate requests are validated by an authorised QHPKI Registration Authority Administrator in accordance with section 3.2.

4.2.2 Approval or Rejection of Certificate Applications

QHPKI Root CA

The Service Provider shall approve or reject any certificate request for a sub-ordinate CA if it is not a valid certificate request format or if the request has not been authorised by a recognised signatory.

All other QHPKI Issuing CAs

The QHPKI Registration Authority Administrator shall accept or reject the certificate request from Subscribers in line with the provisions within the QHPKI Work Instruction “Approving a QHPKI Subscriber certificate request”.

4.2.3 Time to Process Certificate Applications

QHPKI Root CA

Processing timeframes are defined in the SLA with the managed Service Provider.

All other QHPKI Issuing CAs

There is no stipulation as to the total time elapsed from certificate enrolment to approval or rejection of the certificate enrolment.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

Copies of issued certificates are retained by the CA for archiving and revocation purposes.

The Subscriber certificate shall be published in accordance with section 4.4.2.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Where a certificate is not automatically issued the Subscriber shall be notified by email of the issuance of the certificate.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following actions performed by the Subscriber shall act as acceptance of the Certificate and associated Keys:

- First use of a User Credential allowing access to the Private Key; or
- First use of the Private Key following the issuing of the Certificate

The following actions performed by the Subscriber shall act as an acknowledgement and acceptance of the Subscriber Agreement:

- First use of a User Credential allowing access to the Private Key; or
- First use of the Private Key following the issuing of the Certificate.

The following actions performed by the Relying Party shall act as an acknowledgement and acceptance of the Relying Party Agreement:

- First use of a Certificate; or
- First download of the CA-certificate.

Certificates are deemed to be accepted by the Subscriber unless the CA is notified otherwise.

4.4.2 Publication of the Certificate by the CA

Certificates shall be published to the applicable repositories upon issuance.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.4.4 Distributors of CA-certificates and PKI-aware Applications

A Relying Party that:

- Distributes the CA-certificate as part of a PKI-aware application or through any other means; or
- Distributes a PKI-aware application that accepts a Relying Party Agreement on the behalf of an end user of that application, or bypasses the requirement for such acceptance via some other mechanism,

shall notify all third parties to whom the PKI-aware application, or the CA-certificate, is distributed of the terms of the Relying Party Agreement and that by use of a Certificate issued by the CA, through running the PKI-aware application or through other means, the third party will be deemed to have accepted the Relying Party Agreement.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

The Subscriber shall use a Private Key and Certificate only for Permitted Uses in accordance with Section 1.4.1 and in the Subscriber Agreement, and in a manner consistent with applicable Certificate content (e.g. keyUsage extension).

Use of a Private Key and Certificate is subject to the terms of the Subscriber Agreement.

The Subscriber should not use an Authentication/Signature Private Key after the associated Certificate has been Revoked or has expired.

A Private Key shall not be used beyond the maximum lifetime permitted under this CP for that Key in accordance with Section 6.3.2, except when used to decrypt previously encrypted information.

4.5.2 Relying Party Public Key and Certificate Usage

A Relying Party shall use a Public Key and Certificate only for Permitted Uses in accordance with Section 1.4.1 and in the Relying Party Agreement, and in a manner consistent with applicable Certificate content (e.g. keyUsage extension).

Use of a Public Key and Certificate is subject to the terms of the Relying Party Agreement.

A Relying Party should not use a Public Key after the associated Certificate has been revoked or has expired.

A Public Key should not be used beyond the maximum lifetime permitted under this CP for that Key in accordance with Section 6.3.2.

It is the sole responsibility of a Relying Party to determine the suitability of a Certificate for a given application.

4.6 Certificate Renewal

Certificate Renewal is the practice of issuing a new certificate without changing the Subscriber or other participant's public key or any other information in the certificate.

4.6.1 Circumstance for Certificate Renewal

QHPKI Root CA

Certificate renewal is not permitted for sub-ordinate CAs.

All other QHPKI Issuing CAs

No stipulation.

4.6.2 Who May Request Renewal

The Subscriber or agent acting on behalf of the Subscriber must initiate the certificate renewal request.

4.6.3 Processing Certificate Renewal Requests

Certificate renewal requests, where allowed, are processed in the same way as a certificate enrolment.

4.6.4 Notification of New Certificate Issuance to Subscriber

Certificate renewal requests, where allowed, are notified in the same way as a certificate enrolment.

4.6.5 Conduct constituting acceptance of a renewal certificate

As per section 4.4.

4.6.6 Publication of the renewal certificate by the CA

As per section 4.4.

4.6.7 Notification of certificate issuance by the CA to other entities

As per section 4.4.

4.7 Certificate Re-Key

Certificate re-key is when a Subscriber or end-entity generates a new key pair and applies for the issuance of a new certificate to replace an existing certificate using the new key pair.

4.7.1 Circumstance for Certificate Re-Key

Certificate re-key is required if:

- The certificate has been revoked; or
- The private key of a certificate has (or suspected of having) been compromised.

Certificate re-key is permitted if:

- The Certificate has not expired; and
- The Certificate information is still correct

4.7.2 Who May Request Certification of a New Public Key

The Subscriber may request a certificate re-key.

4.7.3 Processing Certificate Re-Keying Requests

The process for re-key is the same as the process for issuance of a certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

As per section 4.4.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

As per section 4.4.

4.7.6 Publication of the Re-Keyed Certificate by the CA

As per section 4.4.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As per section 4.4.

4.8 Certificate Modification

Certificate modification is where a Subscriber changes elements within a certificate, except the public key, and requests that the certificate is re-issued.

4.8.1 Circumstance for Certificate Modification

Certificate modification is not permitted under QHPKI.

Certificate modification is handled as a combination of revocation of the original certificate and issuance of a new certificate for the same entity.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A Certificate issued under this CP shall be revoked where:

- The Subscriber's Private Key has been compromised
- The Subscriber's Keys or Certificate are no longer required

- The Subscriber wishes to change any of the details within the certificate
- The CA or any delegated RA Private Keys have been compromised
- The Subscriber submits a request to Revoke
- The RO requests revocation, for whatever reason

A Certificate may also be Revoked at the direction of the QHPKI Operational Authority.

4.9.2 Who can Request Revocation

QHPKI Root CA

The QHPKI Operational Authority will issue a revocation request directly to the Service Provider for sub-ordinate CAs or the QHPKI Root CA.

All other QHPKI Issuing CAs

The Subscriber or end-entity may raise a service request for revocation of their own certificate, which will be acted upon by an authorised QHPKI Registration Authority Administrator.

An Automated Registration Authority administrator may initiate a revocation request on behalf of a Subscriber where this is authorised.

The QHPKI Operational Authority may issue a revocation request, which will be acted upon by an authorised QHPKI Registration Authority Administrator.

4.9.3 Procedure for Revocation Request

QHPKI Root CA

The QHPKI Operational Authority will issue a revocation request in writing directly to the Service Provider.

The Service Provider shall execute the revocation request including;

- Mark the certificate as revoked within the certificate database
- Add the certificate to the appropriate CRL
- Publish an updated CRL
- Stop the CA from using the certificate to sign any further certificate requests

All other QHPKI Issuing CAs

The certificate revocation request shall be verified and processed by an authorised QHPKI Registration Authority Administrator in line with the provisions within the QHPKI Work Instruction “Revoking a QHPKI Subscriber certificate”.

4.9.4 Revocation Request Grace Period

The Revocation Request Grace Period is one (1) Business Day from when the compromise is first identified.

4.9.5 Time Within which CA Must Process the Revocation Request

QHPKI Root CA

The Service Provider will process the revocation request within 1 business day of the written notification unless mutually agreed with the QHPKI Operational Authority.

Updated CRLs are to be published within 1 hour from issuance.

All other QHPKI Issuing CAs

The certificate revocation request shall be processed by an authorised QHPKI Registration Authority Administrator within two business days of the revocation request being lodged as a service request.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying parties must check current CRL or OCSP information before accepting a certificate.

CRLs may be cached, but the Relying Party accepts all risks from cached CRLs.

4.9.7 CRL Issuance Frequency (if applicable)

QHPKI Root CA

CRLs are published yearly with a CRL overlap period of 30 days.

The QHPKI Operational Authority may request that the CA publish a CRL out of schedule to make sure that relying parties receive revocation information in a timely fashion.

All other QHPKI Issuing CAs

CRLs are published at least every 24 hours, with a validity of 24 hours.

4.9.8 Maximum Latency for CRLs (if applicable)

No stipulation.

4.9.9 On-Line Revocation/Status Checking Availability

All QHPKI Certificate Status Services include online CRLs, and the location of the CRL shall be encoded in the appropriate Certificate extension.

If the Certificate Status Services include OCSP, the location of the OCSP responder shall be encoded in the appropriate Certificate extension.

4.9.10 On-Line Revocation Checking Requirements

It is the sole responsibility of a Relying Party to determine which if any on-line Certificate Status Services are used.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Re-Key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

Certificate suspension is not supported.

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 QHPKI Certificate Status Services include online CRLs, and the location of the CRL shall be encoded in the appropriate Certificate extension.

If the Certificate Status Services include OCSP, the location of the OCSP responder shall be encoded in the appropriate Certificate extension.

4.10.1 Operational Characteristics

QHPKI CAs shall require that Certificate Status be available via an HTTP URL which shall be encoded in the appropriate Certificate extension.

If OCSP is supported the location of the OCSP responder shall also be encoded in the appropriate Certificate extension.

4.10.2 Service Availability

The current Certificate Status shall be available with the frequency and latency as given in Sections 4.9.7 and 4.9.8.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Subscription ends by either the certificate expiry or revocation, whichever event occurs first.

4.12 Key Escrow and Recovery

QHPKI Root CA

Key escrow is not supported for certificates issued by the Root CA.

All other QHPKI Issuing CAs

Escrow of Authentication/Signature Private Keys shall not be performed.

4.12.1 Key Escrow and Recovery Policy and Practices

Backup and recovery of Private Keys shall be the responsibility of the Subscriber.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

QHPKI is operated on behalf of Queensland Health by the Service Provider. The majority of the components and systems are hosted within the Service Providers facilities and operated by the Service Provider under contract to Queensland Health.

However, there are some components that are hosted within Queensland Health facilities and operated by Queensland Health.

5.1 Physical Controls

All CAs and RAs operating under QHPKI shall operate with physical and environmental security controls appropriate to the Certificate Assurance Levels of the Certificates issued.

5.1.1 Site Location and Construction

All components operating under QHPKI shall be housed in secure facilities.

5.1.2 Physical Access

Equipment used to host QHPKI components shall be protected from unauthorised access.

The QHPKI Operational Authority shall specify physical access controls that are required to be implemented.

5.1.3 Power and Air Conditioning

All critical components shall be equipped with primary and backup power systems to ensure continuous, uninterrupted access to electric power. Also, these secure facilities shall be equipped with primary and backup heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

The secure facilities of the QHPKI shall be protected against water exposure.

5.1.5 Fire Prevention and Protection

The secure facilities hosting QHPKI shall provide standard fire prevention and protection measures, in line with local applicable safety regulations.

5.1.6 Media Storage

All media containing sensitive PKI information, including security audit, archive, or backup information, shall be stored in a location separate from the secure facilities housing the QHPKI equipment, with at least equivalent security to the facilities housing the QHPKI equipment.

5.1.7 Waste Disposal

Sensitive information shall not be compromised through the waste disposal procedures.

5.1.8 Off-Site Backup

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

5.2 Procedural Controls

5.2.1 Trusted Roles

The following roles are required to maintain the security of the QHPKI.

Role	Responsibility
Certificate Authority Manager	Responsible for the secure and compliant operation of the CA. This role is assigned to the eHealth Queensland Chief Technology Officer.
Certification Authority Owner	The Certification Authority Owner (CAO) is the legal entity responsible for the CA. This role is assigned to eHealth Queensland.
Compliance Auditor	Responsible for appointing auditors to perform regular audits of CA compliance internally. This role is assigned to the Senior Director, Cyber Security Group.
QHPKI Operational Authority	Responsible for the approval of and compliance with CA policies and practices. This role is assigned to the eHealth Queensland Cyber Security Working Group, see section 1.5.1.
QHPKI Service Owner	Responsible for the delivery of the service to Queensland Health users and entities. This role is assigned to the Director of Infrastructure Operations.
Registration Authority	The Registration Authority is the authority within Queensland Health that verifies Subscriber requests for a Digital Certificate and tells the Certificate Authority to issue it. This role has been delegated to members of the Hosting and Directories team.
Registration Authority Administrator	Operational personnel within eHealth Queensland that form the Registration Authority and are responsible for day to day operations of the QHPKI services.
Service Provider	The contracted managed services provider engaged by eHealth Queensland to provide the Managed PKI Service. Currently this is Symantec.
Service Provider Operators	Operational personnel within the Service Provider that are responsible for day to day operations of the Managed Service.

5.2.2 Number of Persons Required per Task

Multi-person control shall be in accordance with Section 6.2.2.

5.2.3 Identification and Authentication for Each Role

No stipulation.

5.2.4 Roles Requiring Separation of Duties

Procedural controls shall be in place to ensure separation of duties between the various Trusted Roles supporting components of the QGPKI, including:

- Split-knowledge systems or key-splitting techniques may be used
- An Auditor shall not hold any other role within QHPKI
- A QHPKI Registration Authority Administrator shall not approve the issuance of a certificate for which they are the Subscriber
- A QHPKI Registration Authority Administrator shall not approve the revocation of a certificate for which they are the requestor

Service Provider roles that require separation of duties include (but are not limited to)

- The validation of information in CA Certificate Applications
- The acceptance, rejection, or other processing of CA certificate applications, revocation requests, key recovery requests or renewal requests, or enrolment information
- The issuance or revocation of CA Certificates
- The handling of Subscriber information or requests
- The generation, issuing or destruction of a CA certificate
- The loading of a CA to a Production environment

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Personnel appointed to Trusted Roles shall be appropriately qualified, competent and trustworthy.

5.3.2 Background Check Procedures

All personnel appointed to Trusted Roles that access QHPKI components shall undergo background checks as per the Queensland Health HR Policy.

The Service Provider is responsible for conducting appropriate background checks on personnel that access the Managed Service components that support the QHPKI service commensurate with the level of trust required by that role and in accordance with local laws and regulations.

5.3.3 Training Requirements

Personnel appointed to Trusted Roles shall be trained to a level commensurate with the level of trust required by that role.

Training shall include:

- PKI principles and mechanisms

- Operation of the CA or RA system as applicable to their role
- Responsibilities of the Trusted Role

5.3.4 Retraining Frequency and Requirements

No stipulation.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

No stipulation.

5.3.7 Independent Contractor Requirements

The CAO shall ensure that any independent contractors or subcontractors involved in the provision or operation of the Certification Authority are bound to the obligations specified in this document.

5.3.8 Documentation Supplied to Personnel

The Service Provider shall ensure that personnel appointed to Trusted Roles have access to documentation and materials sufficient to enable them to meet the obligations and responsibilities of their Trusted Roles.

5.4 Audit Logging Procedures

Audit logs are retained for CA components by the Provider of the CA infrastructure and shall be retained in accordance with the sections below.

5.4.1 Types of Events Recorded

All PKI related activity logging functions of the systems supporting PKI operations shall be enabled.

For each auditable event, the audit record shall include, as applicable:

- The type of event
- The date and time the event occurred
- The identity of the trusted role who performed the action
- The success or failure status of the action
- Any associated activity log records for the systems supporting PKI operations.

Where possible, the security audit data shall be automatically collected; when this is not possible a logbook, paper form, or other physical mechanism shall be used.

5.4.2 Frequency of Processing Log

A periodic review shall be performed at least once every 12 months, or upon request from the Compliance Auditor.

5.4.3 Retention Period for Audit Log

All audit logs shall be retained in accordance with a Queensland State Archives approved retention and disposal schedule.

5.4.4 Protection of Audit Log

All audit logs shall be protected such that only the Compliance Auditor is authorised to permit archive or deletion of audit logs.

5.4.5 Audit Log Backup Procedures

Security audit data shall be backed up in accordance with Section 5.1.8.

5.4.6 Audit Collection System (Internal vs. External)

The security audit process shall run independently and shall not be under the control of any personnel directly related to certificate processing.

Security audit processes shall be invoked at system startup, and cease only at system shutdown.

Records shall be maintained of instances where security audit processes do not operate.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

The Compliance Auditor shall request that additional vulnerability assessments are carried out when required.

5.5 Records Archival

The Service Provider is responsible for records management where the records exist within the Managed Service.

5.5.1 Types of Records Archived

The following records shall be archived

- All audit logs in accordance with Section 5.4.1 shall be archived
- Certificate application information
- Documentation supporting certificate applications
- Certificate lifecycle information e.g., revocation, rekey and renewal application information.

5.5.2 Retention Period for Archive

For records archived by the Service Provider, the archive retention shall be in accordance with the Managed Services contract.

For records archived by Queensland Health, the archive retention shall be in accordance with a Queensland State Archives approved retention and disposal schedule.

5.5.3 Protection of Archive

For records archived by the Service Provider, the archive protection shall be in accordance with the Managed Services contract.

For records archived by Queensland Health, the archive protection shall be in accordance with a Queensland State Archives approved retention and disposal schedule.

5.5.4 Archive Backup Procedures

For records archived by the Service Provider, the archive backup shall be in accordance with the Managed Services contract.

For records archived by Queensland Health, the archive backup shall be in accordance with a Queensland State Archives approved retention and disposal schedule.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic-based.

5.5.6 Archive Collection System (Internal or External)

The Service Provider's archive collection systems are internal, except for Automated Registration Authority servers. Symantec assists the Automated Registration Authority servers in preserving an audit trail. Such an archive collection system therefore is external to Queensland Health.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key Changeover

5.6.1 Procedures for Key Changeover

Prior to the expiration of a CA Certificate for a QHPKI CA within the hierarchy, key changeover procedures are enacted to facilitate a smooth transition for entities within the QHPKI hierarchy. The CA key changeover process requires that:

- An old CA ceases to issue new Certificates no later than 60 days before the point in time ("Stop Issuance Date") where the remaining lifetime of the old CA key pair equals the approved Certificate Validity Period for the specific type(s) of Certificates issued by CAs in the QHPKI hierarchy.

- Upon successful validation of Subordinate CA (or end-user Subscriber) Certificate requests received after the “Stop Issuance Date,” Certificates will be signed with a new CA key pair.

The old CA continues to issue CRLs signed with the original old CA private key until the expiration date of the last Certificate issued using the original key pair has been reached

5.6.2 Procedures Notifying Relying Parties of Key Changeover

CA certificates and their corresponding public keys for all CAs within the QHPKI hierarchy shall be available for download from the QHPKI website (http://pki.health.qld.gov.au).

CA certificates shall be published by the Enterprise Active Directory as trusted and therefore distributed by the Active Directory to domain joined devices.

QHPKI Operational Authority shall ensure that a notice is sent to all relying parties advising that they need to ensure that they download and install new CA certificates when they are release.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Compromise and disaster recovery of the Managed PKI Service is the responsibility of the Service Provider.

- The Service Provider shall follow the documented incident procedures that are identified within the contract for the provision of the service.
- The Service Provider shall notify Queensland Health in writing of any incident or compromise that affects the provision of the underpinning Managed PKI Service that supports QHPKI.

The Automated Registration Authority server is hosted within Queensland Health. It is the responsibility of eHealth Queensland to monitor these servers for incidents or compromise.

- Any identified security incident or compromise of the Automated Registration Authority server shall be notified to the QHPKI Operational Authority within 24 hours.
- The Operational Authority shall ensure that incident management procedures are in place including sufficient backup of data and logs.

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

Compromise and disaster recovery of the Managed PKI Service is the responsibility of the Service Provider.

- The Service Provider shall follow the documented incident procedures that are identified within the contract for the provision of the service.

- The Service Provider shall notify Queensland Health in writing of any incident or compromise that affects the provision of the underpinning Managed PKI Service that supports QHPKI.

The Automated Registration Authority server is hosted within Queensland Health. It is the responsibility of eHealth Queensland to monitor these servers for incidents or compromise.

- Any identified security incident or compromise of the Automated Registration Authority server shall be notified to the QHPKI Operational Authority within 24 hours.

The Operational Authority shall ensure that incident management procedures are in place including sufficient backup of data and logs.

5.7.3 Entity Private Key Compromise Procedures

Upon the suspected or known compromise of a QHPKI CA or the Managed PKI Service infrastructure, the Service Provider shall enact appropriate procedures to safeguard the operations and trustworthiness of the QHPKI hierarchy.

Upon the suspected or known compromise of a QHPKI Automated Registration Authority server the following procedures shall be completed:

- Revoke and re-issue (with new keys) all Automated RA certificates that are suspect or known to have been compromised.
- Change Service Account passwords.
- Review all logs to determine breach.
- Review every end-entity certificate issued by Automated RA and revoke any that are suspicious.
- Notify relying parties and system owners of period of suspected compromise.

5.7.4 Business Continuity Capabilities after a Disaster

The QHPKI Operational Authority shall ensure that sufficient procedures are in place to ensure the continued operation of the QHPKI service, including but not limited to:

- Contracts with the Service Provider
- Data backups
- Monitoring of the SLA's

5.8 CA or RA Termination

Prior to the termination of the CA, the QHPKI Operational Authority shall ensure that data is archived in accordance with Section 5.5.

Notification of CA or RA termination to all PKI Participants shall be provided in accordance with Section 9.11.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

CA key pair generation is the responsibility of the Service Provider.

6.1.1 Key Pair Generation

All CA key pairs shall be generated using cryptographic hardware modules.

All Automated Registration Authority administrator key pairs (used in the Production environment) shall be generated and stored within a cryptographic hardware security module.

End-entity key pairs shall be generated exclusively for use with the QHPKI certificate enrolment.

6.1.2 Private Key Delivery to Subscriber

Where possible the Private Key shall be generated by the end-entity Subscriber on their device.

If the Private Key is to be delivered to the end-entity Subscriber it shall be sent via a secure channel and receipt shall be confirmed by the Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

Public Keys shall be submitted in such a way that proves possession of the corresponding Private Key.

6.1.4 CA Public Key Delivery to Relying Parties

No stipulation.

6.1.5 Key Sizes

QHPKI CA Keys must be a minimum size of 4096 bit RSA modulus.

End-entity Subscriber keys must be a minimum size of 2048 bit RSA modulus.

6.1.6 Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7 Key Usage Purposes (as per X.509 v3 key usage field)

No stipulation.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

Private key protection and cryptographic module engineering controls for CA keys are the responsibility of the Service Provider.

6.2.1 Cryptographic Module Standards and Controls

No stipulation.

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

No stipulation.

6.2.3 Private Key Escrow

No stipulation.

6.2.4 Private Key Backup

No stipulation.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA keys shall not be transferred from a cryptographic module.

Automated Registration Authority keys shall not be transferred from a cryptographic module.

End-entity Subscriber keys shall have no stipulation.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation.

6.2.8 Method of Activating Private Key

CA keys shall have protection including procedures to ensure that they can only be activated by an authorised person(s).

All other keys shall have no stipulation.

6.2.9 Method of Deactivating Private Key

No stipulation.

6.2.10 Method of Destroying Private Key

No stipulation.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The public key is archived by the CA as described in the Service Provider's CPS.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

QHPKI Root CA key pairs shall have maximum lifespan of 35 years.

QHPKI Issuing CA key pairs shall have a maximum lifespan of 15 years.

Subscriber key pairs shall have a maximum lifespan of 10 years.

6.4 Activation Data

Activation data management for CA keys is the responsibility of the Service Provider.

6.4.1 Activation Data Generation and Installation

No stipulation.

6.4.2 Activation Data Protection

No stipulation.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

Computer security controls for the Managed PKI Service are the responsibility of the Service Provider.

6.5.1 Specific Computer Security Technical Requirements

No stipulation.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

Lifecycle technical controls for the Managed PKI Service are the responsibility of the Service Provider.

6.6.1 System Development Controls

No stipulation.

6.6.2 Security Management Controls

The QHPKI Operational Authority shall ensure that sufficient documented security management controls exist.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

Network security controls within the Managed PKI Service are the responsibility of the Service Provider and shall be documented by the Service Provider.

The QHPKI Operational Authority shall ensure that appropriate Network Security controls are documented and implemented to ensure the security of the QHPKI.

6.8 Time-Stamping

No stipulation.

7. CERTIFICATE, CRL, AND OCSP PROFILES

CA Certificate profiles are documented by QHPKI in the Service Provider's CA Naming forms.

CRL and OCSP profiles are the responsibility of the Service Provider.

CRL's are copied to QHPKI repositories that are held within Queensland Health environments.

7.1 Certificate Profile

Certificates shall conform to the IETF PKIX, RFC 5280

7.1.1 Version Number(s)

The version shall be 3 (value is 2).

7.1.2 Certificate Extensions

The issuerUniqueId extension shall not be used.

The subjectUniqueId extension shall not be used.

The authorityKeyIdentifier extension is not required in the QHPKI Root CA-certificate.

The authorityKeyIdentifier extension shall be included in all other Certificates issued under this CP.

The subjectKeyIdentifier extension shall be included in all CA-certificates issued under this CP.

The subjectKeyIdentifier extension should be included in all other Certificates issued under this CP.

7.1.3 Algorithm Object Identifiers

All certificates shall identify the algorithm as 1.2.840.113549.1.1.11 (SHA-256WithRSAEncryption) or better.

7.1.4 Name Forms

CA-certificates shall not have an empty Subject name.

DNs may contain the domainComponent attribute, as defined in RFC 4519.

DNs shall comply with RFC 5280 and RDNs shall be sequenced, in accordance with X.501.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

This document shall be indicated by an object identifier (OID) asserted as the first policy information term in the Certificate Policies extension of the Certificate.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

In the certificate the OID asserted in accordance with Section 7.1.6 shall have a Pointer qualifier containing a URI referring to the QHPKI Repository.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

CRLs shall conform to the IETF PKIX, RFC 5280.

7.2.1 Version Number(s)

The version shall be 2 (value is 1).

7.2.2 CRL and CRL Entry Extensions

The authorityKeyIdentifier extension shall be included in all CRLs.

The cRLNumber extension shall be included in all CRLs.

7.3 OCSP Profile

The OCSP service is provided by the Service Provider.

7.3.1 Version Number(s)

OCSP version 1 shall be used.

7.3.2 OCSP Extensions

Appropriate extensions from RFC 2560 may be used in OCSP requests and responses.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or Circumstances of Assessment

Compliance audits must occur at least annually.

8.2 Identity/Qualifications of Assessor

Compliance is assessed by a specialist in Information Security Solutions and shall be appointed by the eHealth Queensland Cyber Security Group.

8.3 Assessor's Relationship to Assessed Entity

The assessor is either an external assessor or a staff member of eHealth Queensland and is independent from the Service Provider.

8.4 Topics Covered by Assessment

The compliance audit shall include topics as directed by eHealth Queensland which may include (but not limited to):

- Review audit trail
- Compare to Operational Authority documentation and requests
- Review audit report submitted by Service Provider.

8.5 Actions Taken as a Result of Deficiency

The handling of audit deficiencies shall be in accordance with the directions of the Director of Cyber Security Group and the QHPKI Operational Authority.

8.6 Communication of Results

The communication of the results from an assessment shall be directed by the chair of the QHPKI Operational Authority.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Fees are payable to the Service Provider and are defined in the contract with the Service Provider. The following sections identify fees payable by end-entity Subscribers to QHPKI and **NOT** the fees payable to the Service Provider.

9.1.1 Certificate Issuance or Renewal Fees

Fees may be payable by Subscribers for the issue or Renewal of Certificates. Where fees are payable, an up to date fee schedule shall be provided to Subscribers by way of a Notice in accordance with Section 9.11.

9.1.2 Certificate Access Fees

Fees may be payable for Certificate access. Where fees are payable, an up to date fee schedule shall be provided by way of a Notice in accordance with Section 9.11.

9.1.3 Revocation or Status Information Access Fees

Fees may be payable for Revocation or Status information access fees. Where fees are payable, an up to date fee schedule shall be provided by way of a Notice in accordance with Section 9.11.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

A refund policy may apply to any fees levied in accordance with Section 9.1. Where a refund policy applies it shall be documented in the fee schedule.

9.2 Financial Responsibility

eHealth Queensland is financially responsible for the operation of the CA on behalf of Department of Health.

9.2.1 Insurance Coverage

QHPKI does not provide any insurance coverage or warranty for the benefit of PKI Participants in relation to any loss or damage that they may suffer as a result of participating in the Certificate application process, or using a Certificate or associated Keys issued under this CP.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

Each PKI Participant acknowledges that QHPKI does not provide any insurance coverage or warranty for the benefit of PKI Participants in relation to any loss or damage that they may suffer as a result of participating in the Certificate application process or using a Certificate or associated Keys issued under this CP.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

QHPKI may receive Confidential Information from PKI Participants in the course of fulfilling its functions.

Subject to Section 9.3.2, Confidential Information means, in relation to a PKI Participant, information that:

- is information from which a person who is receiving or has received a public sector health service could be identified; or
- is by its nature confidential; or
- is communicated by the PKI Participant to the CAO as being confidential; or
- QHPKI knows or ought to know is confidential.

9.3.2 Information Not Within the Scope of Confidential Information

Notwithstanding Section 9.3.1, Confidential Information does not include information which:

- Is already lawfully disclosed by the CAO prior to the CAO being required to treat the information as confidential
- Is lawfully received from a third party who is not bound by a duty of confidentiality
- Has become public knowledge, other than through a breach of an obligation of confidence by QHPKI
- Was independently developed or released by QHPKI without reference to the Confidential Information
- Is information that the PKI Participant provides for inclusion within a Certificate
- Is information indicating that a Certificate has been Revoked or Suspended, though not including the reason behind this Certificate Status
- Includes any information relating to the PKI Participant's use of the Repository

9.3.3 Responsibility to Protect Confidential Information

All Queensland Health Information that is stored by the Service Provider must be managed and protected in accordance with legislative and policy requirements, including in relation to non-disclosure of security classified information (for example, 'confidential information' in Part 7 of the *Hospital and Health Boards Act 2011*) and those whom the Service Provider engages unless permitted by legislation.

Appropriate controls for Queensland Health Information must be applied in accordance with the Queensland Government Information Security Classification Framework (QGISCF).

Nothing within Section 9.3.3 shall be construed to prevent QHPKI from disclosing any information provided by a PKI Participant in the following circumstances:

- To any Minister or to Parliament in connection with the carrying out of any functions, duties, powers and discretions conferred on the CAO
- To such legal advisors, financial advisers, auditors or insurers of the CAO as may be necessary for any proceedings or investigation involving the CAO, or for the purposes of facilitating the CAO's performance of its functions under this CP
- To the extent required by law.

9.4 Privacy of Personal Information

In this Section 9.4, "Personal Information" has the same meaning as in Section 12 of the *Information Privacy Act 2009* (QLD) (Privacy Act).

Each PKI Participant acknowledges that in performing its functions QHPKI may receive Personal Information from PKI Participants.

9.4.1 Privacy Plan

No stipulation.

9.4.2 Information Treated as Private

No stipulation.

9.4.3 Information not Deemed Private

Notwithstanding any other provisions within Section 9.4, the following information will not be treated as Personal Information by QHPKI:

- Any information contained within a Certificate
- Any information relating to PKI Participant's use of the Repository

9.4.4 Responsibility to Protect Private Information

QHPKI shall protect any Personal Information received from PKI Participants in accordance with its obligations under the Privacy Act, any relevant contractual undertakings and any other applicable law.

9.4.5 Notice and Consent to use Private Information

Each PKI Participant consents to the collection, use, storage, transfer, and disposal of Personal Information by QHPKI for the purposes of fulfilling its functions.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Nothing within Section 9.4shall be construed to prevent QHPKI from disclosing any Personal Information of a PKI Participant to the extent required by law.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

No stipulation.

9.6 Representations and Warranties

Each PKI Participant acknowledges that QHPKI does not provide any specific representations or warranties as to the accuracy of the information contained in any Certificate issued by a QHPKI CA.

9.6.1 CA Representations and Warranties

No stipulation.

9.6.2 RA Representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

No stipulation.

9.6.4 Relying Party Representations and Warranties

No stipulation.

9.6.5 Representations and Warranties of other Participants

No stipulation.

9.7 Disclaimers of Warranties

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

9.8 Limitations of Liability

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

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

If any term or condition implied by law is unable to be excluded by QHPKI, then the liability of QHPKI and any of its officers, employees, agents, and contractors (including sub-contractors), for any breach of the implied term or condition is limited to:

- Re-performing the services to which the term or condition applies
- Paying the cost of re-performing those services

9.9 Indemnities

To the maximum extent permitted by applicable law, Subscribers are required to indemnify Queensland Health for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party
- The Subscriber's failure to protect the Subscriber's private key, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

Relying parties indemnify Queensland Health to the extent permitted by applicable law for:

- The Relying Party's failure to perform the obligations of a Relying Party
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

9.10 Term and Termination

9.10.1 Term

The document becomes effective upon publication by eHealth Queensland. Amendments to this document become effective upon publication by eHealth Queensland.

9.10.2 Termination

The document as amended from time to time shall remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

Upon termination of this document, Subscribers are nevertheless bound by its terms and conditions for all certificates issued for the remainder of the validity of such certificates.

9.11 Individual Notices and Communications with Participants

A Repository for all QHPKI related information shall be located at http://pki.qld.gov.au/QHPKI/

For the purpose of this Section 9.11, a Notice includes a consent, information, Certificate application, request, or any other communication provided under or in connection with QHPKI.

A Notice to a party under this document is only given or made if it is in writing and distributed in one of the following ways:

- Delivered or posted to that party at its postal address as advised to the other party
- Published on the Repository, in accordance with Section 2.1
- Published via a Certificate Status Service.

A Notice shall be provided on the Repository when any of the following events occur:

- A new or updated CP, CPS, Subscriber Agreement, or Relying Party Agreement is approved
- There is a change to any fee or refund payable in connection with this CP
- For any other event which the QHPKI Operational Authority deems appropriate.

Each PKI Participant acknowledges that they are responsible for keeping themselves informed of any Notices issued in accordance with this Section 9.11.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendments to this CP shall be approved by the QHPKI Operational Authority.

Updates supersede any previous or conflicting versions of this document.

Comments regarding the suitability of this document may be advised at any time and should be directed to QHPKI Operational Authority for consideration.

9.12.2 Notification Mechanism and Period

Amendments of this policy come into effect as soon as a new version is published by the QHPKI Operational Authority and PKI Participants will be notified in accordance with section 9.11.

9.12.3 Circumstances Under Which OID Must be Changed

The QHPKI Operational Authority shall determine if changes to this document require a change of certificate policy object identifiers (OID) of the certificate policies corresponding to this class of certificate.

9.13 Dispute Resolution Provisions

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

- The Parties shall use their best endeavours to resolve any problem that arises by negotiating with each other.

9.14 Governing Law

This document, Subscriber Agreements, and Relying Party Agreements, 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 the State of Queensland, except as identified in existing contracts.

9.15 Compliance with Applicable Law

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

9.16 Miscellaneous Provisions

In the event that a clause or provision of this CP is held to be unenforceable by a court of law or other tribunal having authority, the remainder of the CP shall remain valid.

9.16.1 Survival of Terms

Sections of this document, Subscriber Agreements, and Relying Party Agreements, that relate to Intellectual Property Rights, safety, integrity, accuracy of information, confidentiality, right to information, privacy, insurance, warranty, liability, and indemnity will survive the expiration or termination (for whatever reason) of the relevant policy, statement, or agreement.