Queensland Government
Chief Information Office

Queensland Government
Enterprise Architecture
PKI Framework

Queensland Government Hosted Device Basic Policy Certification Authority T2C35

Certification Practice Statement

Version 1.0

Queensland the Smart State

Queensland Government
Department of Public Works

Approved on behalf of the CAO

Scolari
Signature

CITEC
Organisation

DOUG SCOLARI
Name

DIRECTOR, CLIENT SERVICES.
Title

23/08/2010
Date

Approved on behalf of the QGPKIPA

Signature

CHRISTOPHER GOH
Name

Chair
Title

24/08/2010.
Date

Table of Contents

1 Introduction

1. This Certification Practice Statement (CPS) states the practices under which Queensland Government (QG) operates the hosted QG Device Basic Policy Certification Authority (CA) T2C35.

1.1 Overview

2. This document provides a standard set of provisions to define this Certification Practice Statement within the Queensland Government Public Key Infrastructure (QGPKI).

3. The Certificate Policy (CP) describing the policies followed by the CA in issuing, Renewing, Re-keying, Suspending, or Revoking certificates shall be given in a separate document.

4. This CPS and any subordinate CPSs, where used, shall be approved by the QG Public Key Infrastructure Policy Authority.

1.2 Document Name and Identification

5. Document Name: **Queensland Government Hosted Certification Authority T2C35 Certification Practice Statement**

6. Document Public Location: **http://T2C35.pki.qld.gov.au/T2C35/**

7. Document X.500 OID: **1.2.36.1.3.1.1.1.4.1.1.0.1.0**

Refer to the QGPKI Framework for naming conventions.

1.3 PKI Participants

1.3.1 Certification Authority Owner

8. The Certification Authority Owner (CAO) is the legal entity responsible for the Certification Authority.

9. For the purpose of this CPS, the CAO is Queensland Government (QG).

1.3.2 Policy Authority

10. The Policy Authority (PA) is the entity responsible for the approval of this CPS and the associated CP, Subscriber Agreements, and Relying Party Agreements.

11. For the purpose of this CPS, the PA is the Queensland Government Public Key Infrastructure Policy Authority (QGPKIPA).

12. The PA may appoint a PA Technical Advisory Group to assist it in meeting its obligations and responsibilities.

1.3.3 Certification Authorities

13. A Certification Authority is an entity that signs and issues Certificates. A CA may register Subscribers itself, or may delegate that function to one or more separate Registration Authorities (RAs).

14. The CA is required to perform the Trusted Roles in accordance with Section 5.2.1.

1.3.4 Registration Authorities

15. A Registration Authority may be delegated by a CA to perform identification and registration of Subscribers and associated functions. RAs are not permitted to sign Certificates.

16. The RA is required to perform the Trusted Roles in accordance with Section 5.2.1.

1.3.5 Subscribers

17. Refer to the Certificate Policy.

1.3.6 Relying Parties

18. Refer to the Certificate Policy.

1.3.7 Other Participants

1.3.7.1 Auditors

19. Refer to the Certificate Policy.

1.4 Certificate Usage

20. Refer to the Certificate Policy.

1.4.1 Appropriate Certificate Uses

21. Refer to the Certificate Policy.

1.4.2 Prohibited Certificate Uses

22. Refer to the Certificate Policy.

1.5 Policy Administration

1.5.1 Organisation Administering the Document

23. The registration and maintenance of this CPS is the responsibility of the QGPKIPA.

1.5.2 Contact Person

24. The contact details for the QGPKIPA are

Department of Public Works
Attn: QGPKIPA Chair
c/- QGPKIPA Secretariat
GPO Box 279
Brisbane QLD 4001, Australia

qgpkipa@qld.gov.au

1.5.3 Person Determining CPS Suitability for the Policy

25. Refer to the Certificate Policy.

1.5.4 CPS Approval Procedures

26. Refer to the Certificate Policy.

27. Further details on CPS approval procedures are provided in the QG PKI Operations Manual.

1.6 Definitions and Acronyms

28. Unless the context requires otherwise, terms, expressions, and abbreviations used in this CPS shall have the meaning given in the public document "Queensland Government Public Key Infrastructure Definitions and References" , published under http://pki.qld.gov.au/

2 Publication and Repository Responsibilities

2.1 Repositories

29. A Repository for all PKI-related information issued by this CA shall be located at http://T2C35.pki.qld.gov.au/T2C35/ and made available to all Subscribers and Relying Parties of these Certificates in accordance with the applicable Subscriber Agreements and Relying Party Agreements.

2.2 Publication of Certification Information

30. This Certification Practice Statement the associated CP, the associated CA-certificate, and applicable Certificate Status are available from the Repository.

2.3 Time or Frequency of Publication

31. Refer to the Certificate Policy.

2.4 Access Controls on Repositories

32. Further details on access controls on Repositories are provided in the QG PKI Operations Manual.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

33. Refer to the Certificate Policy.

3.1.2 Need for Names to be Meaningful

34. Refer to the Certificate Policy.

3.1.3 Anonymity or Pseudonymity of Subscribers

35. Refer to the Certificate Policy.

3.1.4 Rules for Interpreting Various Name Forms

36. Refer to the Certificate Policy.

3.1.5 Uniqueness of Names

37. Refer to the Certificate Policy.

3.1.6 Recognition, Authentication, and Role of Trademarks

38. Refer to the Certificate Policy.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

39. Where the Subscriber does not generate the Private Key, this is not applicable.

40. Where the Subscriber does generate the Private Key, proof of possession shall be performed by provision of a PKCS#10 Certificate Signing Request (CSR) or equivalent method.

41. If the Subscriber does not generate the Private Key, then the delivery process by which the Private Key is transferred to the Subscriber shall be auditable in accordance with Sections 6.1 and 6.2.

3.2.2 Authentication of Organisation Identity

42. A Registration Officer (RO) shall:

    1. verify the identity of the Subscriber in accordance with Section 3.2.3; and
    2. verify any delegation of authority by the Subscriber.

43. Further details on the RO procedures are provided in Section 4 (RA Procedures) of the QG PKI Operations Manual.

3.2.3 Authentication of Individual Identity

44. A Registration Officer (RO) shall:

    1. verify the identity of the Subscriber.

45. Further details on the RO procedures are provided in Section 4 (RA Procedures) of the QG PKI Operations Manual.

3.2.4 Non-verified Subscriber Information

46. Refer to the Certificate Policy.

3.2.5 Validation of Authority

47. Refer to the Certificate Policy.

3.2.6 Criteria for Interoperation

48. Refer to the Certificate Policy.

3.3 Identification and Authentication for Re-key Requests

49. Refer to the Certificate Policy.

3.3.1 Identification and Authentication for Routine Re-Key

50. Refer to the Certificate Policy.

3.3.2 Identification and Authentication for Re-Key After Revocation

51. Refer to the Certificate Policy.

3.4 Identification and Authentication for Revocation Requests

52. The Registration Officer (RO) shall verify the accuracy of information in the certificate revocation request.

53. Further details on the RO procedures are provided in Section 4 (RA Procedures) of the QG PKI Operations Manual.

54. The Authorising Officer (AO) shall authenticate the request from the RO.

55. Further details on the AO procedures are provided in Section 5 (CA Procedures) of the QG PKI Operations Manual.

4 Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

56. The Registration Officer (RO) shall submit a certificate application to the Authorising Officer (AO).

57. Further details on the RO procedures are provided in Section 4 (RA Procedures) of the QG PKI Operations Manual.

4.1.2 Enrolment Process and Responsibilities

58. The Registration Officer (RO) shall enrol new Subscribers.

59. Further details on the RO procedures are provided in Section 4 (RA Procedures) of the QG PKI Operations Manual.

4.2 Certificate Application Processing

60. The Registration Officer (RO) shall verify the certificate application.

61. Further details on the RO procedures are provided in Section 4 (RA Procedures) of the QG PKI Operations Manual.

4.2.1 Performing Identification and Authentication Functions

62. The Registration Officer (RO) shall verify the identity of Subscribers.

63. Further details on the RO procedures are provided in Section 4 (RA Procedures) of the QG PKI Operations Manual.

4.2.2 Approval or Rejection of Certificate Applications

64. The Registration Officer (RO) shall accept or reject certificate applications from Subscribers.

65. Further details on the RO procedures are provided in Section 4 (RA Procedures) of the QG PKI Operations Manual.

66. The Authorising Officer (AO) shall accept or reject certificate applications from the RO.

67. Further details on the AO procedures are provided in Section 5 (CA Procedures) of the QG PKI Operations Manual.

4.2.3 Time to Process Certificate Applications

68. Refer to the Certificate Policy.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

69. The Certifying Officer (CO) shall authenticate the approved request from the Authorising Officer (AO).

70. The CO shall publish the certificate in accordance with Section 4.4.2.

71. Further details on the CO procedures are provided in Section 5 (CA Procedures) of the QG PKI Operations Manual.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

72. Refer to the Certificate Policy.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

73. Refer to the Certificate Policy.

4.4.2 Publication of the Certificate by the CA

74. Refer to the Certificate Policy.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

75. Refer to the Certificate Policy.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

76. Refer to the Certificate Policy.

4.5.2 Relying Party Public Key and Certificate Usage

77. Refer to the Certificate Policy.

4.6 Certificate Renewal

78. Refer to the Certificate Policy.

4.6.1 Circumstance for Certificate Renewal

79. Refer to the Certificate Policy.

4.6.2 Who May Request Renewal

80. Refer to the Certificate Policy.

4.6.3 Processing Certificate Renewal Requests

81. Refer to the Certificate Policy.

4.6.4 Notification of New Certificate Issuance to Subscriber

82. Refer to the Certificate Policy.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

83. Refer to the Certificate Policy.

4.6.6 Publication of the Renewal Certificate by the CA

84. Refer to the Certificate Policy.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

85. Refer to the Certificate Policy.

4.7 Certificate Re-key

86. Refer to the Certificate Policy.

4.7.1 Circumstance for Certificate Re-key

87. Refer to the Certificate Policy.

4.7.2 Who May Request Certification of a New Public Key

88. Refer to the Certificate Policy.

4.7.3 Processing Certificate Re-keying Requests

89. Refer to the Certificate Policy.

4.7.4 Notification of New Certificate Issuance to Subscriber

90. Refer to the Certificate Policy.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

91. Refer to the Certificate Policy.

4.7.6 Publication of the Re-keyed Certificate by the CA

92. Refer to the Certificate Policy.

4.7.7 Notification of Certificate Issuance by the CA to other Entities

93. Refer to the Certificate Policy.

4.8 Certificate Modification

4.8.1 Circumstance for Certificate Modification

94. Refer to the Certificate Policy.

4.8.2 Who May Request Certificate Modification

95. Refer to the Certificate Policy.

4.8.3 Processing Certificate Modification Requests

96. Refer to the Certificate Policy.

4.8.4 Notification of New Certificate Issuance to Subscriber

97. Refer to the Certificate Policy.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

98. Refer to the Certificate Policy.

4.8.6 Publication of the Modified Certificate by the CA

99. Refer to the Certificate Policy.

4.8.7 Notification of Certificate Issuance by the CA to other Entities

100. Refer to the Certificate Policy.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

101. Refer to the Certificate Policy.

4.9.2 Who Can Request Revocation

102. Certificate Revocation can be requested by the Subscriber or the Registration Officer (RO).

103. The RO shall submit a certificate revocation request to the Authorising Officer (AO).

104. Further details on the RO procedures are provided in Section 4 (RA Procedures) of the QG PKI Operations Manual.

4.9.3 Procedure for Revocation Requests

105. The Registration Officer (RO) shall accept or reject certificate revocation requests from Subscribers.

106. Further details on the RO procedures are provided in Section 4 (RA Procedures) of the QG PKI Operations Manual.

107. The Authorising Officer (AO) shall authenticate the certificate revocation request from the RO.

108. The AO shall accept or reject certificate revocation requests from the RO.

109. Further details on the AO procedures are provided in Section 5 (CA Procedures) of the QG PKI Operations Manual.

110. The Certifying Officer (CO) shall authenticate the approved certificate revocation request from the AO.

111. The CO shall:

    1. Revoke the certificate; and
    2. Update the Certificate Status Services with details of the revoked certificate.

112. Further details on the CO procedures are provided in Section 5 (CA Procedures) of the QG PKI Operations Manual.

4.9.4 Revocation Request Grace Period

113. Refer to the Certificate Policy.

4.9.5 Time within which CA must Process the Revocation Request

114. Refer to the Certificate Policy.

4.9.6 Revocation Checking Requirement for Relying Parties

115. Refer to the Certificate Policy.

4.9.7 CRL Issuance Frequency

116. Refer to the Certificate Policy.

4.9.8 Maximum Latency for CRLs

117. Refer to the Certificate Policy.

4.9.9 On-Line Revocation/Status Checking Availability

118. Refer to the Certificate Policy.

4.9.10 On-Line Revocation Checking Requirements

119. Refer to the Certificate Policy.

4.9.11 Other Forms of Revocation Advertisements Available

120. Refer to the Certificate Policy.

4.9.12 Special Requirements Related to Key Compromise

121. The Subscriber shall notify the Registration Officer (RO) in the case of a Private Key compromise in accordance with the Subscriber Agreement. The RO shall maintain an auditable record of any such notification in accordance with the QG PKI Framework.

122. Further details on the RO procedures are provided in Section 4 (RA Procedures) of the QG PKI Operations Manual.

4.9.13 Circumstances for Suspension

123. Refer to the Certificate Policy.

4.9.14 Who Can Request Suspension

124. Refer to the Certificate Policy.

4.9.15 Procedure for Suspension Request

125. Refer to the Certificate Policy.

4.9.16 Limits on Suspension Period

126. Refer to the Certificate Policy.

4.10 Certificate Status Services

127. Refer to the Certificate Policy.

4.11 End of Subscription

128. Refer to the Certificate Policy.

4.12 Key Escrow and Recovery

4.12.1 Key Escrow and Recovery Policy and Practices

129. The Escrow Officer (EO) shall validate all recovery requests for Confidentiality Private Keys.

130. Further details on the EO procedures are provided in Section 2 (PKI Roles) of the QG PKI Operations Manual.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

131. Refer to the Certificate Policy.

5 Facility, Management, and Operational Controls

5.1 Physical Controls

132. Details of the physical and environmental security control procedures are provided in Section 8 (Controls) of the QG PKI Operations Manual.

5.1.1 Site Location and Construction

133. Details of the site location and construction are provided in Section 8 (Controls) of the QG PKI Operations Manual.

5.1.2 Physical Access

134. Details of the physical access procedures are provided in Section 7 (Procedures) of the QG PKI Operations Manual.

5.1.3 Power and Air Conditioning

135. Details of the power and air conditioning are provided in Section 8 (Controls) of the QG PKI Operations Manual.

5.1.4 Water Exposures

136. Details of the water exposure prevention procedures are provided in Section 8 (Controls) of the QG PKI Operations Manual.

5.1.5 Fire Prevention and Protection

137. Details of the fire prevention and protection procedures are provided in Section 8 (Controls) of the QG PKI Operations Manual.

5.1.6 Media Storage

138. Details of the media storage procedures are provided in Section 8 (Controls) of the QG PKI Operations Manual.

5.1.7 Waste Disposal

139. Details of the waste disposal procedures are provided in Section 8 (Controls) of the QG PKI Operations Manual.

5.1.8 Off-Site Backup

140. Details of the off-site backup procedures are provided in Section 8 (Controls) of the QG PKI Operations Manual.

5.2 Procedural Controls

5.2.1 Trusted Roles

5.2.1.1 Certification Authority Owner

141. The CAO has responsibility for:

1. establishing the PA;
2. ensuring that the appointment of all personnel to Trusted Roles is performed in accordance with Section 5.3;
3. notifying all participants of an intention to terminate the CA; and
4. complying with Privacy requirements in accordance with Section 9.4.

142. Further details are provided in Section 3 (Approval Procedures) of the QG PKI Operations Manual.

5.2.1.2 Policy Authority

143. The PA has responsibility for:

1. ensuring compliance with requirements set out by the QGPKIPA; and
2. ensuring compliance with QGPKIPA policy directions.

144. The PA has responsibility for approval of:

1. the establishment of the CA;
2. the appointment of the CAM;
3. this CPS;
4. the associated CP;
5. Subscriber Agreements;
6. Relying Party Agreements;
7. the Records Management Policy (record protection, retention and disposal); and
8. the Disaster Recovery Plan.

145. Further details are provided in Section 3 (Approval Procedures) of the QG PKI Operations Manual.

5.2.1.3 Certification Authority Manager

146. The CAM has responsibility for ensuring that their respective CA:

1. complies with the requirements set out by the QGPKIPA;
2. complies with the requirements of the Subscriber Agreement with the CA that issued the CA-certificate; and
3. complies with the conditions and obligations set out in the CP and this CPS.

147. In particular, the CAM shall have responsibility for:

1. ensuring that the generating, issuing, and Revocation of Certificates occurs in accordance with the CP and this CPS including:
   a) Certificate profile requirements in accordance with Section 7.1;
   b) CRL profile requirements in accordance with Section 7.2; and
   c) OCSP profile requirements in accordance with Section 7.3;
2. ensuring that, at the time Certificates are signed and returned to the Subscriber or RA:
   a) the Certificates accurately reflect the information provided to the CA by the Subscriber or RA; and
   b) the Certificates contain all of the elements required by the Certificate profile;
3. ensuring that appropriate access controls are maintained on the Repository in accordance with Section 2.4;
4. ensuring that the CA receives Revocation requests for Certificates and takes appropriate action;
5. ensuring that physical access controls are implemented in accordance with Section 5.1;
6. authorising audits;
7. ensuring that the CA conducts and participates in regular audits;
8. ensuring that procedures are implemented for handling security audit data in accordance with Section 5.4;
9. appointment of all Trusted Roles in accordance with Section 5.3;
10. acting as the custodian of CA and RA archived data and ensuring that data archived is in accordance with Section 5.5;
11. ensuring that procedures are implemented for handling compromise and disaster recovery in accordance with Section 5.7;
12. ensuring the no Certificate requests are signed by the CA once the CA has been terminated; and
13. ensuring that the Subscriber Agreement contains:
    a) Private Key requirements in accordance with Sections 3.2.1, 6.1.1, and 6.2.1;
    b) acknowledgement of Certificate acceptance in accordance with Section 4.4.1;
    c) Private Key backup, recovery, and escrow requirements in accordance with Sections 4.5.1, 4.12.1, and 6.2.4;
    d) agreement to use Private Key for Permitted Uses in accordance with Section 1.4.1;
    e) Private Key compromise reporting timeframes commensurate with the appropriate Certificate Assurance Level in accordance with Sections 4.9.4 and 4.9.12;
    f) the process to indicate end of Subscription to the CA in accordance with Section 4.11;
    g) acceptance of transferred liability in accordance with Section 9.6, 9.7, and 9.8;
    h) consent to the use of Personal Information in accordance with Section 9.4.5;
    i) acknowledgement of intellectual property rights in accordance with Section 9.5; and
    j) an indemnity in favour of the CAO in accordance with Section 9.9.

148. Further details are provided in Section 5 (CA Procedures) of the QG PKI Operations Manual.

5.2.1.4 Registration Authority Manager

149. The RAM has responsibility for ensuring that their respective RA:

1. complies with the requirements set out by the QGPKIPA; and
2. complies with the conditions and obligations set out in the CP and this CPS.

150. In particular, the RAM shall have responsibility for:

1. ensuring enrolment and registration procedures are completed in accordance with the requirements of the CP and this CPS;
2. ensuring the identity of Subscribers is verified and validated as part of the authentication requirements as governed by the CP and this CPS;
3. ensuring that the issuance, use, revocation, and re-issuance of credentials meets the requirements of the CP and this CPS; and
4. conducting and participating in regular audits.

151. Further details are provided in Section 4 (RA Procedures) of the QG PKI Operations Manual.

5.2.1.5 Registration Officer

152. The RO role shall be responsible for registering Subscribers, that is:

1. enrolling new Subscribers;
2. accepting or rejecting Certificate applications from Subscribers;
3. verifying the identity of Subscribers, in accordance with Section 3.2;
4. verifying the accuracy of information used to initiate requests;
5. verifying proof of possession of Private Key if required;
6. requesting the issuance of Certificates;
7. requesting the Revocation of Certificates;
8. requesting the Suspension of Certificates; and
9. requesting the removal of the Suspension of a Certificate.

153. Further details are provided in Section 4 (RA Procedures) of the QG PKI Operations Manual.

5.2.1.6 Authorising Officer

154. The AO role shall be responsible for approving requests from the RO, that includes:

1. approving the issuance of Certificates;
2. approving the Revocation of Certificates;
3. approving the Suspension of Certificates; and
4. approving the reversal of Certificate Suspension.

155. Further details are provided in Section 5 (CA Procedures) of the QG PKI Operations Manual.

5.2.1.7 Certifying Officer

156. The CO role shall be responsible for executing approved requests from the AO, that is:

1. executing the issuance of Certificates;
2. executing the Revocation of Certificates;
3. executing the Suspension of Certificates;
4. executing the reversal of Certificate Suspension; and
5. publication of the result of any of the above actions to the Certificate Status Services in accordance with Section 4.4.2;

157. Further details are provided in Section 5 (CA Procedures) of the QG PKI Operations Manual.

5.2.1.8 Auditor

5.2.1.8.1 Security Auditor

158. The Security Auditor role shall be responsible for:

1. reviewing, maintaining, and archiving audit logs; and
2. performing vulnerability assessments in accordance with Section 5.4.8.

159. Further details are provided in the applicable sections of the QG PKI Operations Manual.

5.2.1.8.2 Compliance Auditor

160. Refer to the Certificate Policy.

5.2.1.9 Off-Line HSM Custodian

161. The Off-Line HSM Custodian shall be responsible for the physical security of a HSM when not in legitimate use.

162. Further details are provided in Section 6 (HSM Procedures) of the QG PKI Operations Manual.

5.2.1.10 HSM Security Officer

163. The HSM Security Officer role shall be responsible for:

1. initialisation, configuration, and activation of a HSM for use; and
2. establishing and maintaining HSM Operators and HSM Users.

164. Further details are provided in Section 6 (HSM Procedures) of the QG PKI Operations Manual.

5.2.1.11 HSM Operator

165. The HSM Operator shall be responsible for:

1. establishing and maintaining HSM operational environment; and
2. managing HSM backups and recovery.

166. Further details are provided in Section 6 (HSM Procedures) of the QG PKI Operations Manual.

5.2.1.12 HSM User

167. The HSM User role shall be responsible for:

1. generating Keys in the HSM; and
2. using Keys in the HSM.

168. Further details are provided in Section 6 (HSM Procedures) of the QG PKI Operations Manual.

5.2.1.13 Operator

169. The Operator role shall be responsible for the routine operation of the CA or RA equipment and operations such as system backups and recovery.

170. Further details are provided in Sections 4 (*RA Procedures*) and 5 (*CA Procedures*) of the QG PKI Operations Manual.

5.2.1.14 System Administrator

171. The System Administrator role shall be responsible for:

1. installation, configuration, and maintenance of the CA or RA;
2. establishing and maintaining system accounts;
3. configuring Certificate profiles or templates; and
4. configuring system audit parameters.

172. Further details are provided in Sections 4 (RA Procedures) and 5 (CA Procedures) of the QG PKI Operations Manual.

5.2.1.15 Escrow Officer

173. The Escrow Officer shall be responsible for:

1. secure escrow of Confidentiality Private Keys;
2. recovery of Escrowed Keys; and
3. validation of recovery requests.

174. Further details are provided in Section 2 (PKI Roles) of the QG PKI Operations Manual.

5.2.2 Number of Persons Required for Task

175. Refer to the Certificate Policy.

5.2.3 Identification and Authentication for Each Role

176. Refer to the Certificate Policy.

5.2.4 Roles Requiring Separation of Duties

177. Refer to the Certificate Policy

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

178. Refer to the hosting provider’s documentation.

5.3.2 Background Check Procedures

179. Refer to the role establishment sections within Sections 4 (RA Procedures), Section 5 (CA Procedures) and Section 6 (HSM Procedures) of the QG PKI Operations Manual.

5.3.3 Training Requirements

180. Refer to the role establishment sections within Sections 4 (RA Procedures), Section 5 (CA Procedures) and Section 6 (HSM Procedures) of the QG PKI Operations Manual.

5.3.4 Retraining Frequency and Requirements

181. Refer to the role establishment sections within Sections 4 (RA Procedures), Section 5 (CA Procedures) and Section 6 (HSM Procedures) of the QG PKI Operations Manual.

5.3.5 Job Rotation Frequency and Sequence

182. Refer to the hosting provider’s documentation.

5.3.6 Sanctions for Unauthorised Actions

183. Refer to the hosting provider’s documentation.

5.3.7 Independent Contractor Requirements

184. Refer to the role establishment sections within Sections 4 (RA Procedures), Section 5 (CA Procedures) and Section 6 (HSM Procedures) of the QG PKI Operations Manual.

5.3.8 Documentation Supplied to Personnel

185. All Trusted Roles identified in Section 5.2.1 shall be provided with:

1. the CP;
2. the CPS;
3. the QG PKI Operations Manual;
4. the QGPKI Framework; and
5. any relevant QG standards, policies, or other documentation referenced by any of the documents identified above.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

186. Refer to the Certificate Policy.

5.4.2 Frequency of Processing Log

187. Refer to the Certificate Policy.

5.4.3 Retention Period of Audit Log

188. Refer to the Certificate Policy.

5.4.4 Protection of Audit Log

189. Details of the audit log protection procedures are provided in the applicable sections of the QG PKI Operations Manual.

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (Internal vs. External)

191. Refer to the Certificate Policy.

5.4.7 Notification to Event-Causing Subject

192. Refer to the Certificate Policy.

5.4.8 Vulnerability Assessments

193. Details of the vulnerability assessment procedures are provided in Section 8 (Controls) of the QG PKI Operations Manual.

5.5 Records Archival

5.5.1 Types of Records Archived

194. Refer to the Certificate Policy.

5.5.2 Retention Period of Archive

195. Refer to the Certificate Policy.

5.5.3 Protection of Archive

196. Details of the archive protection procedures are provided in Section 8 (Controls) of the QG PKI Operations Manual.

5.5.4 Archive Backup Procedures

197. Details of the archive backup procedures are provided in Section 8 (Controls) of the QG PKI Operations Manual.

5.5.5 Requirements for Time-Stamping of Records

198. Details of the archive time-stamping procedures are provided in the applicable sections of the QG PKI Operations Manual.

5.5.6 Archive Collection System (Internal vs. External)

199. Refer to the Certificate Policy.

5.5.7 Procedures to Obtain and Verify Archive Information

200. Refer to the Certificate Policy.

5.6 Key Changeover

201. Refer to the Certificate Policy.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

202. Details of the incident and compromise handling procedures are provided in the applicable sections of the QG PKI Operations Manual.

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

203. Details of resources, software and/or data corruption procedures are provided in the applicable sections of the QG PKI Operations Manual.

5.7.3 Entity Private Key Compromise Procedures

204. Details of the incident and compromise handling procedures are provided in the applicable sections of the QG PKI Operations Manual.

5.7.4 Business Continuity Capabilities After a Disaster

205. Details of business continuity procedures are provided in the applicable sections of the QG PKI Operations Manual.

5.8 CA or RA Termination

206. Refer to the Certificate Policy.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

207. Details of the Key Pair generation procedures are provided in Section 5 (CA Procedures) of the QG PKI Operations Manual.

6.1.2 Private Key Delivery to Subscriber

208. Details of the Private Key delivery procedures are provided in Section 4 (RA Procedures) of the QG PKI Operations Manual.

6.1.3 Public Key Delivery to Certificate Issuer

209. Refer to the Certificate Policy.

6.1.4 CA Public Key Delivery to Relying Parties

210. Refer to the Certificate Policy.

6.1.5 Key Sizes

211. Refer to the Certificate Policy.

6.1.6 Public Key Parameters Generation and Quality Checking

212. Refer to the Certificate Policy.

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

213. Refer to the Certificate Policy.

6.2 Private Key protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

214. Refer to the Certificate Policy.

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

215. Details of the multi-person control procedures are provided in Section 8 (Controls) of the QG PKI Operations Manual.

6.2.3 Private Key Escrow

216. Refer to the Certificate Policy.

6.2.4 Private Key Backup

217. Refer to the Certificate Policy.

6.2.5 Private Key Archival

218. Refer to the Certificate Policy.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

219. Details of the Private Key transfer procedures are provided in Section 6 (HSM Procedures) of the QG PKI Operations Manual.

6.2.7 Private Key Storage on Cryptographic Module

6.2.7.1 CA Private Keys

220. Details of the CA Private Key storage procedures are provided in Section 6 (HSM Procedures) of the QG PKI Operations Manual.

6.2.7.2 Subscriber Private Keys

221. Refer to the Certificate Policy.

6.2.8 Method of Activating Private Key

222. Details of the Private Key activation procedures are provided in Section 6 (HSM Procedures) of the QG PKI Operations Manual.

6.2.9 Method of Deactivating Private Key

223. Details of the Private Key deactivation procedures are provided in Section 6 (HSM Procedures) of the QG PKI Operations Manual.

6.2.10 Method of Destroying Private Key

224. Details of the Private Key destruction procedures are provided in Section 6 (HSM Procedures) of the QG PKI Operations Manual.

6.2.11 Cryptographic Module Rating

225. Refer to the Certificate Policy.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

226. Details of the Key archival procedures are provided in Section 6 (HSM Procedures) of the QG PKI Operations Manual.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

227. Refer to the Certificate Policy.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

228. Refer to the Certificate Policy.

6.4.2 Activation Data Protection

229. Details of the activation data protection procedures are provided in applicable sections of the QG PKI Operations Manual.

6.4.3 Other Aspects of Activation Data

230. Refer to the Certificate Policy.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

231. Details of the operating systems security procedures are provided in Section 8 (Controls) of the QG PKI Operations Manual.

6.5.2 Computer Security Rating

232. Refer to the Certificate Policy.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

233. Details of the system development control procedures are provided in Section 8 (Controls) of the QG PKI Operations Manual.

6.6.2 Security Management Controls

234. Details of the security management control procedures are provided in Section 8 (Controls) of the QG PKI Operations Manual.

6.6.3 Life Cycle Security Controls

235. Details of the life cycle security control procedures are provided in Section 8 (Controls) of the QG PKI Operations Manual.

6.7 Network Security Controls

236. Details of the network security control procedures are provided in Section 8 (Controls) of the QG PKI Operations Manual.

6.8 Time Stamping

237. Refer to the Certificate Policy.

7 Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

238. Refer to the Certificate Policy.

7.2 CRL Profiles

239. Refer to the Certificate Policy.

7.3 OCSP Profiles

240. Refer to the Certificate Policy.

8 Compliance Audit and Other Assessments

241. The CA complies with the Compliance Audit and Other Assessments requirements in accordance with the Certificate Policy.

8.1 Frequency or Circumstances of Assessment

242. Refer to the Certificate Policy.

8.2 Identity/Qualifications of Assessor

243. Refer to the Certificate Policy.

8.3 Assessor’s Relationship to Assessed Entity

244. Refer to the Certificate Policy.

8.4 Topics Covered by Assessment

245. Refer to the Certificate Policy.

8.5 Actions Taken as a Result of Deficiency

246. Refer to the Certificate Policy.

8.6 Communications of Results

247. Refer to the Certificate Policy.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

248. Refer to the Certificate Policy.

9.1.2 Certificate Access Fees

249. Refer to the Certificate Policy.

9.1.3 Revocation or Status Information Access Fees

250. Refer to the Certificate Policy.

9.1.4 Fees for Other Services

251. Refer to the Certificate Policy.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

252. Refer to the Certificate Policy.

9.2.2 Other Assets

253. Refer to the Certificate Policy.

9.2.3 Insurance or Warranty Coverage for End- Entities

254. Refer to the Certificate Policy.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

255. Refer to the Certificate Policy.

9.3.2 Information Not Within the Scope of Confidential Information

256. Refer to the Certificate Policy.

9.3.3 Responsibility to Protect Confidential Information

257. Refer to the Certificate Policy.

9.4 Privacy of Personal Information

258. Refer to the Certificate Policy.

9.4.1 Privacy Plan

259. The privacy plan is reviewed by the Certification Authority Owner (CAO) as part of the Compliance Audit.

9.4.2 Information Treated as Personal

260. Refer to the Certificate Policy.

9.4.3 Information Not Deemed Personal

261. Refer to the Certificate Policy.

9.4.4 Responsibility to Protect Personal Information

262. Personal information is protected in accordance with Sections 5 and 6.

9.4.5 Notice and Consent to Use Personal Information

263. Notice and consent to the use of personal information is encompassed by the Subscriber Agreements and Relying Party Agreements.

9.4.6 Disclosure Required by Law

264. Refer to the Certificate Policy.

9.4.7 Other Information Disclosure Circumstances

265. Refer to the Certificate Policy.

9.5 Intellectual Property Rights

266. Intellectual Property rights are encompassed by the Subscriber Agreements and Relying Party Agreements.

9.6 Representations and Warranties

9.6.1 Certification Authority Owner Representations and Warranties

267. Refer to the Certificate Policy.

9.7 Disclaimer of Warranties

268. Disclaimers of Warranties are encompassed by the Subscriber Agreements and Relying Party Agreements.

9.8 Limitation of Liability

9.8.1 Certification Authority Owner Liability

269. Certification Authority Owner liability is encompassed by the Subscriber Agreements and Relying Party Agreements.

9.9 Indemnities

270. Indemnities are encompassed by the Subscriber Agreements and Relying Party Agreements.

9.10 Term and Termination

9.10.1 Term

271. Refer to the Certificate Policy.

9.10.2 Termination

272. Refer to the Certificate Policy.

9.10.3 Effect of Termination and Survival

273. Refer to the Certificate Policy.

274. Termination procedures are described in Section 5 (CA Procedures) of the QG PKI Operations Manual.

9.11 Individual Notices and Communications with Participants

275. Refer to the Certificate Policy.

9.12 Amendments

276. Amendment procedures are described in Section 3 (Approval Procedures) of the QG PKI Operations Manual.

9.12.1 Procedure for Amendment

9.12.2 Notification Mechanisms and Period

277. Refer to the Certificate Policy.

9.12.3 Circumstances under Which OID Must Be Changed

278. Refer to the Certificate Policy.

9.13 Dispute Resolution Procedures

279. Refer to the Certificate Policy.

9.14 Governing Law

280. Refer to the Certificate Policy.

9.15 Compliance with Applicable Law

281. Refer to the Certificate Policy.

9.16 Miscellaneous Provisions

282. Refer to the Certificate Policy.