BlackBerry | certicom

BlackBerry V2X Root and Intermediate CA Certification Practices Statement

Date	**August 10, 2020**
Author	**Jim Alfred/Randy Tsang**
Document Revision	**1.4**
Status	**Approved**

4701 Tahoe Blvd., 5th Floor, Mississauga, Ontario, Canada, L4W 0B5

main 905-507-4220 • support 1-800-511-8011 • fax 905-507-4230

www.certicom.com

TABLE OF CONTENTS

1 INTRODUCTION

The BlackBerry V2X CA is a Certification Authority (CA) supporting digital certificate lifecycle management roles specified in a Security Credential Management System (SCMS), a trust realm defined by the Crash Avoidance Metrics Partnership (CAMP LLC or CAMP)

This CPS addresses Root CA and ICA requirements from the *BlackBerry V2X CA Certificate Policy*.

This document is largely consistent with Internet Engineering Task Force (IETF) RFC 3647 "Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework".

1.1 OVERVIEW

This Certificate Practices Statement (CPS) scope is to describe the operation of the V2X Root CA(s) (RCAs) and Intermediate CA(s) (ICAs) as defined in the *BlackBerry V2X CA Certificate Policy v1.0* for issuance of certificates which act as trust anchors in a production environment, whether it be in a connected vehicle pilot or for mass production vehicle deployments.

In the BlackBerry V2X CA deployment model these Root and Intermediate CAs are offline and operated from within a high security zone.

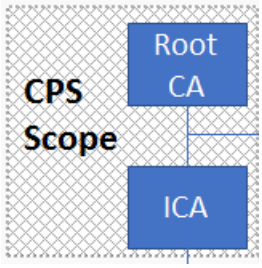

Figure 1 CPS Scope

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is known as the "BlackBerry_V2X_Root_and_Intermediate_CA_Certification_Practices_Statement".

This CPS describes the certification practices of the BlackBerry V2X CA Root and Intermediate CAs under the *BlackBerry V2X CA Certification Policy*.

Revision History

Date	Changes	Version
29 Mar. 2018	Initial Release – pre-approval draft	1.0
13 Apr. 2018	Approved Release	1.0
01 Nov. 2018	Corrected footer document name and consistency. Updated existing Trusted Roles, added CA Observer role and removed CA Operator role. Updated BlackBerry Records Management Directive and	1.1

	BlackBerry Application Development Directive references.	
28 Dec. 2018	Removed CA Observer Trusted Role and reflected changes in the CP.	1.2
25 July 2019	Remove internal hyperlinks for website publication and updated BlackBerry document names.	1.3
27 Feb 2020	Updated for CP and CPS consistency.	1.3.1
10 Aug 2020	Added subsections proposed by Deloitte and addressed deviations.	1.4

1.3 PKI PARTICIPANTS

This CPS describes the certification practices of the BlackBerry V2X CA Root and Intermediate CAs under the *BlackBerry V2X CA Certification Policy*.

1.3.1 CERTIFICATION AUTHORITIES

The CPS addresses only BlackBerry V2X CA Root and ICA entities.

Certification practices associated with subordinate certificate issuing entities in the CA hierarchy including Enrolment CAs and Pseudonym CAs, where applicable, are documented in one or more separate CPSs.

BlackBerry V2X CA Root CA(s) and Intermediate CA(s) are part of the certification path that issues certificates under a BlackBerry V2X CA trust domain. A trust domain may be part of a global SCMS V2X trust realm.

Certification practices adhere to certification policies documented in the *BlackBerry V2X CA Certificate Policy*.

Root CA and Intermediate CA certificate profiles are consistent with Certificate Profiles specified by IEEE 1609.2 and SCMS specifications from CAMP LLC.

The BlackBerry V2X Root CA is:

```
id: rca.prod.v2xca.blackberry.com

issuer: self
```

The BlackBerry V2X Intermediate CA is:

```
id: ica.prod.v2xca.blackberry.com

issuer: hashedId8 of BlackBerry V2X Root CA certificate
```

1.3.2 REGISTRATION AUTHORITIES

BlackBerry V2X CA validates certificate requests for its RCAs and ICAs internally and does not employ an RA function for certificate requests which its RCAs or ICAs issue.

1.3.3 SUBSCRIBERS

BlackBerry V2X ICAs may issue Enrolment CA (ECA), RA or Pseudonym CA (PCA) certificates to itself and to qualified Subscribers.

Subscribers are licensed CA customers who, via signed *Subscriber Agreements*, are obliged to comply to the terms of the CAs certificate policies and build products (OBEs or RSEs) or operate services (e.g. road operators, government transport or specialty service agencies) using products certified to SCMS V2X standards including IEEE 1609.2 and CAMP specifications.

1.3.4 APPLICANT

An Applicant is an entity applying for certificate services from the CA who wishes to become a Subscriber. An employee or representative authorized to act on behalf of the Applicant must review and execute the *Subscriber Agreement*, binding the entity to the terms of the Subscriber Agreement and the certification policies and practices of the CA.

1.3.5 RELYING PARTIES

Qualified RPs shall be required to accept relying party obligations identified in BlackBerry V2X CA participation agreements including but not limited to the requirement to validate trust chains before relying upon any information secured by certificates issued under this CPS.

1.3.6 DEVICE CONFIGURATION MANAGER

A Device Configuration Manager (DCM) should act as a gatekeeper to enroll only legitimate devices with the ECA.

1.3.7 QUALIFIED AUDITOR

A qualified external auditor is responsible for performing audits of root CA, intermediate and subordinate CAs and distribution of audit reports. The audit report includes the recommendations proposed by the accredited auditor and notification to the entity managing the CA on the successful or unsuccessful execution of an audit for any root, intermediate or subordinate CAs and assessing compliance of this CPSs to the CP.

1.3.8 SCMS MANAGER

Once an SCMS Manager is formally established it is envisaged that the BlackBerry V2X CA will operate as a trusted Root CA and Elector under the SCMS Manager's trust realm. The BlackBerry V2X CA Policy Authority may amend the CA's CP and certification practices as required to satisfy SCMS Manager policy requirements.

1.3.9 TRUST REALM ELECTORS

CA Electors, if any, will act in accordance with the CP.

1.4 CERTIFICATE USAGE

1.4.1 APPROPRIATE CERTIFICATE USES

The BlackBerry V2X CA issues certificates intended to secure V2X communications as specified by IEEE 1609.2, including DSRC and/or Cellular V2X communications. Certificates are issued in accordance with the *BlackBerry V2X CA Certificate Policy* based on the SCMS reference architecture and CAMP SCMS and IEEE 1609.2 specifications. Such uses may include in production deployments or in more narrowly defined pilot V2X operating environments. Certificates may be used for no other purpose than those specified by IEEE 1609.2 and SCMS documentation.

1.4.2 PROHIBITED CERTIFICATE USES

Certificates may not be used for any purpose which is prohibited in the *BlackBerry V2X Certificate Policy*. Restrictions are specified in relevant Subscriber or other license agreements.

1.5 POLICY ADMINISTRATION

1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

The BlackBerry V2X CA PA approves this root and ICA CPS and related operational documents and legal agreements.

1.5.2 CONTACT PERSON

Communications regarding CA policies and certification practices should be sent to the PA by registered mail or electronic mail to V2X_PA@BlackBerry.com.

1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE POLICY

Members of the Policy Authority are listed in the internal *BlackBerry V2X CA Organizational Roster* and the V2X_PA email distribution list.

1.5.4 POLICY UPDATE AND APPROVAL PROCEDURES

The PA will review operational status at least annually and more frequently if required to review change requests to this CPS or other relevant CPSs. The update process is managed by the PA in consultation with Subscribers and other stakeholders.

Change requests may be submitted by internal or external stakeholders. External change requests are accepted by the BlackBerry V2X PA via email. Internal change request processes follow the *BlackBerry V2X CA Change Request Process*, with changes ultimately reflected in revised CPSs, processes and documentation.

1.6 DEFINITIONS AND ACRONYMS

See Certificate Policy (CP).

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The CA maintains a repository which is accessible to relevant PKI participants and other stakeholders at: https://blackberry.certicom.com/en/legal/certicom-v2x-ca-repository

2.2 PUBLICATION OF CERTIFICATION INFORMATION

The repository identified in Section 2.1 contains the following information:

- The *BlackBerry V2X CA Certificate Policy*
- The *BlackBerry V2X Root and Intermediate CA Certification Practices Statement*
- The *BlackBerry V2X ECA & PCA Certification Practices Statement*
- Issued (currently valid) Root CA and Intermediate CA certificates
- Access point information of the Root CA and ICAs to obtain CRL information is available within the CA repository

2.3 TIME OR FREQUENCY OF PUBLICATION

Amended Certificate Policies and Certification Practices Statements are published within 5 business days of the PA's approved effected date, with update notices and change logs sent via email to all Subscribers.

Relevant CRLs are published within one day of update and prior to the expiry of the current CRL.

2.4 ACCESS CONTROLS ON REPOSITORIES

Repositories are part of an access-controlled BlackBerry portal maintained according to BlackBerry network platform security policies. Logical and physical controls prevent unauthorized write access to repository. Updates may only be performed by authorized BlackBerry portal administrators or programmatically by the CA. Portal administration secured using mutually authenticated HTTPS or SSH connections.

CRL distribution points within the CA hierarchy are readable by PKI participants. Subscribers and other PKI participants can access other areas of repositories using credentials issued by the CA.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 TYPES OF NAMES

The CA conforms to CP naming rules.

3.1.2 NEED FOR NAMES TO BE MEANINGFUL

The names of certificates issued by the Root CA and ICA, where meaningful, will adhere to the CP. The names of the RCA and ICA are listed in section 1.3.1.

3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

End-entity pseudonym certificates as specified by IEEE 1609.2 are anonymized during the issuance process as specified in the CAMP SCMS architecture. End-entities may be de-anonymized by the MA using linkage values provided by the RA when misbehavior is detected.

3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

See section 3.1.1.

3.1.5 UNIQUENESS OF NAMES

The CA checks that the host names of id fields in certificate requests have not been previously used unless the certificate request is a re-key request or a modification request.

3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

The CA registrar validates Subscriber corporate identities and FQDNs used in certificate names during the license application process to ensure that Subscribers are eligible to use any trademark-protected names in applicable certificate subjects.

3.2 INITIAL IDENTITY VALIDATION

3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

RCA and ICA certificate requests are received from and processed by trusted personnel.

RCA/ICA issuance processes verify the signature on the request to determine the requestor has possession of the private key correspond to the public key in the certificate request

An out of band hash fingerprint is used to validate external certificate requests.

3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

Certificates issued to the CA itself are issued through the CA's work flow and change order approval process.

Certificates issued to organizations other than the CA itself, and particularly certificates containing hostname identifiers, are organizationally validated using information disclosed as described in the *BlackBerry V2X CA Subscriber Application Guide*.

Subscriber organizational identities are validated during the application process which:

- Confirms information concerning the organization's legal registration which specifies its name, address and legal status as confirmed through the process below.
- Confirms organization's contact information, including the name, title, and email address of primary, and/or technical contacts acting as authorized administrators.
- Determine that the organization exists by using a third-party identity proofing service, or government database, or organizational documentation issued by a government agency or recognized authority that confirms the of the organization's existence.

3.2.3 AUTHENTICATION OF INDIVIDUAL INFORMATION

An organizational subscriber provides contact information including the name, title, company name and company email address as well as what specialized role, if any, a specific individual subscriber shall have in terms of acting on its behalf.

The CA validates this information by referencing its legal agreement or by written or email authorization from an authorized company representative, confirming the person's authority to act on behalf of the organization according to *BlackBerry V2X CA Subscriber Application Guide*.

3.2.4 NON-VERIFIED CERTIFICATE SUBJECT INFORMATION

Subject identifiers in certificates which are not name-based are not validated prior to issuance.

3.2.5 VALIDATION OF AUTHORITY

Certificates issued by the Root or Intermediate CAs are only be issued with the PA's approval of a certificate request work order.

The CA validates the authority of all certificate issuance or revocation requests from external entities as coming from an authorized representative of the organization using the information provided in sections 3.2.2 and 3.2.3.

3.2.6 CRITERIA FOR INTEROPERATION

BlackBerry participates in private and industry events hosted to demonstrate certificate functionality on commercial V2X devices and interoperability with other SCMS component providers.

3.2.7 AUTHENTICATION OF END-ENTITIES SUBSCRIBER ORGANIZATION

Subscriber organizations, personnel and their authority are validated as described in sections 3.2.2, 3.2.3 and 3.2.5 of the CPS.

3.2.8 AUTHENTICATION OF END-ENTITY DEVICES

End-entity OBE or RSE certificate requests are validating using valid, non-blacklisted Enrolment Certificates (ECs) as described in CAMP SCMS specifications. EC certificate requests are authenticated by using an authenticated DCM or manually by trusting an authorized Subscriber representative.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 IDENTIFICATION AND AUTHENTICATION OF ROUTINE RE-KEY AND RENEWAL REQUESTS

Identification and authentication of re-key or a change in validity period or another certificate attribute is treated as a new certificate application as described in section 3.2.2.

3.3.2 IDENTIFICATION AND AUTHENTICATION OF RE-KEY AND RENEWAL AFTER REVOCATION

Subscribers must submit a new certificate request in the same way as for the initial issuance of a certificate.

If applicable, the circumstances of any suspected compromise and remediation of a certificate's private key which led to a revocation must be taken into consideration during the application process.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

3.4.1 ROOT/ICA/CRLG/PG/MA CERTIFICATES

Revocation requests may be triggered by internal CA processes or by an external entity with legal standing and authority to make such a request. The PA must approve all such work orders.

3.4.2 ECA/RA/PCA CERTIFICATES

Acceptable procedures for authenticating the revocation requests subscriber ECA, RA or PCA certificates are described in 3.2.2.

Validation of Authority of an authorized requestor as documented in 3.2.5 and includes review of a signed, written request which documents the circumstances surrounding the revocation request such that the CA can reasonably judge any future requests for certificate issuance.

3.4.3 ITS STATION ENROLMENT CERTIFICATES

A Subscriber can request such blacklisting for its own ECs in writing or via email correspondence with an authorized Subscriber representative.

3.4.4 PSEUDONYM CERTIFICATES

Pseudonym certificates are revoked by the CRL Generator at the direction of the CA upon request of the Misbehavior Authority and through coordination with Linkage Authorities and other external entities.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

Each such certificate application shall be duly validated, recording the identity of the applicant and the authority under which the application is accepted.

4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

RCAs and ICA certificates may be requested by the CA itself with PA approval or an issuance work order.

PG, CRLG, PG, MA, ECA, RA and PCA certificates may be requested by the CA itself with PA approval.

4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

Any certificates requests to be issued by an RCA or ICA are accompanied with certificate request work orders which detail all attributes of the certificate requested and any special circumstances pertaining to issuance. The PA approves all work orders prior to issuance.

4.2 CERTIFICATE APPLICATION PROCESSING

4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

CA personnel authenticate an ECA, RA or PCA certificate application using documents supplied by the applicant according to section 3 to validate the applicant's identity and authority.

4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

4.2.2.1 Approval or rejection of ICA, ECA and PCA certificates

The CA verifies Sub-CA certificate requests under its trust domain, inspecting relevant Subscriber qualifications and audit reports. If the check of an application is validated, the CA issues the requested certificate, otherwise the request is rejected and no certificate is issued.

4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

The RCA or ICA processes certificate applications within 5 business days after a *Subscriber Agreement* has been signed and all documentation and authorizations concerning the application have been received.

Such authorizations shall include nominations and contact details for at least two duly authorized entity representatives who are authorized to act on behalf of the applicant organization.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

A Root CA issues its own self-signed root, ICA, Sub-CA and ancillary internal certificates as may be required for its own operation following validations described in Section 3.

Request validation is an internal process whereby the PA will approve the certificate application. The CA will generate the request and issue the certificate. Once issued and prior to use the PA will either approve the issued certificate for use or reject the issued certificate. Rejected certificates will be destroyed and re-issue with steps taken to correct the source of disapproval.

4.3.2 NOTIFICATION TO SUBSCRIBER BY THE CA/RA OF ISSUANCE OF CERTIFICATE

The CA will notify a Subscriber of certificate issuance or non-issuance by email and where relevant via its PKI portal.

Email notification includes instructions for downloading certificates or detail problems in the issuing process.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

The certificate is deemed accepted unless the Subscriber reports a problem with the certificate and requests its revocation within 5 business days of receipt.

4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

The CA publishes RCA, ICA, and where relevant CRLG, LA and MA certificates in its repository.

RCA and ICA certificates are distributed in Certificate Chain Files to individual Subscribers or their respective ITS Stations. These Certificate Chain Files may be created by a global SCMS Manager entity.

For certificates which are not published, the CA records and maintains evidence of issued certificates and protects against changes and loss until expiry as part of its data archive.

4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

The CA notifies relevant stakeholders of certificate issuance via email notices where applicable and via certificate chain file updates for automated certificate management processes described in IEEE 1609.2 and SCMS architecture specifications.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

Private keys bound to certificates issued under the CP are used only in accordance with IEEE 1609.2 specifications and protected from exposure or misuse using logical and physical controls as documented in this CPS.

ECA, PCA, RA, CRL, PG and LA certificates are to be used in accordance with IEEE 1609.2 specifications.

4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

The CA admonishes through its CP and therefore assumes that Subscribers and RPs correctly adhere to certificate usage and validation schemes according to IEEE 1609.2 and SCMS specifications.

All certificates should be validated and checked against application messaging permissions and the relevant trusted certification path, taking due care to process validity periods, CRLs and other relevant revocation publication methods prior to use.

4.6 CERTIFICATE RENEWAL

Expiring certificate renewals are processed as initial certificate requests using a re-key process per Section 4.7.

4.6.1 CIRCUMSTANCES FOR CERTIFICATE RENEWAL

Certificates requests for certificates pending expiry are processed as initial certificate requests.

4.6.2 WHO MAY REQUEST RENEWAL

Authorization is treated as original certificate requests per Section 4.1.

4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

Certificate processing is treated as original certificate requests per Section 4.2.

4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

Certificate issuance notification is treated as original certificate requests per Section 4.3.

4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF RENEWAL CERTIFICATE

Certificate acceptance shall be treated as original certificate requests per Section 4.4.

4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA

Certificate publication is treated as with original certificate requests per Section 4.4.

4.6.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Certificate notification is treated as with original certificate requests per Section 4.4.

4.7 CERTIFICATE RE-KEY

The CA monitors its RCA, ICA, PG, CRL, MA and its own ECA, RA and PCA certificate lifetimes and ensures that they are re-keyed prior to expiry, or if a certificate modification is required. The process of re-issuance includes the generation of new certificate key pairs.

4.7.1 CIRCUMSTANCES FOR CERTIFICATE RE-KEY

Entities seeking a new certificate for an existing certificate submit the request using a new key pair and identify the request as a re-key.

4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

Certificate request authorization is treated as original certificate requests per Section 4.1.

4.7.3 PROCESSING CERTIFICATE RE-KEY REQUESTS

Certificate processing is treated as original certificate requests per Section 4.2.

After re-keying a Subscriber certificate, the CA will revoke the old certificate after a period specified by the customer to transition to the re-keyed certificate.

4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO CERTIFICATE SUBJECT

Certificate issuance notification is treated as original certificate requests per Section 4.3.

4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF RE-KEYED CERTIFICATE

Certificate acceptance is treated as original certificate requests per Section 4.4.

4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

Certificate publication is treated as original certificate requests per Section 4.4.

4.7.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Certificate notification is treated as original certificate requests per Section 4.4.

4.8 CERTIFICATE MODIFICATION

The CA may modify its RCA, ICA, PG, CRL, MA and its own ECA, RA and PCA certificates using previously certified keys only to correct a minor discrepancy, change a host name or other certificate attributes and only if the issued certificate has not been widely distributed. The PA must approve a work order for such a modification.

4.8.1 CIRCUMSTANCES FOR CERTIFICATE MODIFICATION

Permitted circumstances include a minor name change to the subject hostname or FQDN, a change of application permissions or a minor error in the certificate profile or other information embedded within the certificate provided the certificate has not been widely deployed and used.

4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION

Entities seeking a modified certificate for an existing subject with a minor modification to the subject name or certificate permissions may submit the request using the previously certified key pair and identify the request as a modification request and the reason for it. Certificate request authorization is treated as original certificate requests per Section 4.1.

The CA may, at its own discretion, also modify a certificate if an error has been discovered.

4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS

Certificate processing is treated as original certificate requests per Section 4.2.

After issuing a new certificate, if the old certificate has already been distributed to Relying Parties the CA will revoke the old certificate after a period to transition to the re-keyed certificate. If the old certificate has not yet been distributed to Relying Parties the CA and Subscriber may destroy the old certificate rather than revoking it.

4.8.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO CERTIFICATE SUBJECT

Certificate issuance notification is treated as original certificate requests per Section 4.3.

4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

Certificate acceptance conduct is treated as original certificate requests per Section 4.4.

4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

Certificate publication is treated as with original certificate requests per Section 4.4.

4.8.7 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Certificate notification is treated as with original certificate requests per Section 4.4.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

RCA / ICA CPS:

The CA's certificate revocation practices are described below:

4.9.1 CIRCUMSTANCES FOR REVOCATION

Certificate revocation may be performed for the following circumstances:

- If the CA has reason to believe that the private key associated with a certificate has been compromised (revealed, lost, stolen)
- If the IEEE 1609.2 equivalent subject or identifier in the certificate is no longer associated with the Subscriber
- If there is incorrect information included in the certificate which may cause it to be used or relied upon inappropriately
- If the Subscriber agreement has been terminated
- If the Subscriber has violated its license or certificate usage agreements
- If the entity subject to suspension or revocation has materially failed and is unable to mitigate security or processing integrity concerns of a relevant audit
- If ordered by a court or entity with contractual or legal jurisdiction

4.9.2 WHO CAN REQUEST REVOCATION

The CA or an authorized Subscriber representative can request the revocation of its own certificates by submitting an authorized Certificate Revocation work order request detailing the reason for revocation.

Subscriber-dedicated ECA and PCA certificates being revoked for a reason other than certificate modification or re-keying must also be approved in writing by an executive within the Subscriber organization responsible for ITS Station certification.

4.9.3 PROCEDURE FOR REVOCATION REQUEST

The PA will review and approve the revocation request of any certificate issued by the Root or ICA or any revocation request made by an authorized entity. The *Certificate Revocation Request Work Order* will provide an effective revocation date, the reason for the revocation and any special instructions regarding notification of Subscribers or other stakeholders.

An approval or rejection decision will be made within five (5) business days. The effective revocation date may be amended by the PA at its sole discretion.

Once approved and on the target revocation date the certificate will be revoked and added to a CRL to be published to Subscribers and Relying Parties.

PA approval is not required to process a revocation request from a Subscriber for its own certificates however written approval of such requests is required from management within the organization responsible for such matters.

4.9.4 REVOCATION REQUEST GRACE PERIOD

The CA will consider any revocation requests which impact the security or integrity of the PKI within 1 business day. Other requests will be considered within 5 business days.

4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

The CA will process a revocation request on or before its effective revocation date, which shall be no more than 1 business day for revocations which have a high potential to negatively impact the security or integrity of the PKI.

4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES

RP devices and application software must check relevant CRLs and certification paths prior to relying upon a certificate.

4.9.7 CRL ISSUANCE FREQUENCY

The CRL is published regularly with a schedule established by the PA per section 2.3.

4.9.8 MAXIMUM LATENCY FOR CRLS

Maximum CRL latency is one business day.

4.9.9 ON-LINE REVOCATION / STATUS CHECKING AVAILABILITY

The CA does not support any on-line revocation / certificate status checking such as Certificate Status Protocol (OCSP).

4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

The CA does not support on-line certificate status protocol.

4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

No stipulation.

4.9.12 SPECIAL REQUIREMENTS REGARDING KEY COMPROMISE

The CA will use commercially reasonable efforts to notify potential RPs if it discovers or suspects that one of the CA's private keys has been compromised, publishing a CRL and communicating a mitigation plan which will be developed based on the identified root cause of the compromise and the severity of the issue.

Analysis will be performed for revocations to determine the cause of the compromise and whether there is reason to consider any mitigation actions.

4.9.13 CIRCUMSTANCES FOR SUSPENSION

Not applicable.

4.9.14 WHO CAN REQUEST SUSPENSION

Not applicable.

4.9.15 PROCEDURE FOR SUSPENSION REQUEST

Not applicable.

4.9.16 LIMITS ON SUSPENSION PERIOD

Not applicable.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 OPERATIONAL CHARACTERISTICS

Local CRLs are hosted by in a high availability BlackBerry data center provisioned for disaster recovery support. Global SCMS CRLs are hosted by an entity designated by the SCMS Manager.

4.10.2 SERVICE AVAILABILITY

CRLs are hosted by in a high availability BlackBerry data center provisioned for disaster recovery support.

4.10.3 OPTIONAL FEATURES

No stipulation.

4.11 END OF SUBSCRIPTION

Any end-of-subscription conditions on certificates are declared in relevant subscriber agreements.

4.12 KEY ESCROW AND RECOVERY

4.12.1 PRIVATE KEY ESCROW AND RECOVERY POLICIES AND PRACTICES

Not applicable.

4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The system has been designed to operate in a manner which addresses CA capacity demands and performance requirements. The architecture is designed for scalability which can be addressed simply by adding more compute, HSM and storage capacity. Performance is monitored and requirements are reviewed periodically to address projected capacity and business continuity demands.

5.1 PHYSICAL CONTROLS

5.1.1 SITE LOCATION AND CONSTRUCTION

The Root CA and ICA are installed in a secure facility in BlackBerry's Mississauga, Ontario facility on Tahoe Boulevard and operated in an off-line fashion. The secure facility is used for conducting Root and ICA keying ceremonies, and for Root and ICA issuance of certificates for online components of the PKI such as ECA, PCA, RA, LA, PG, CRLG and MA.

The construction of the facility housing the CA equipment is consistent with facilities used to house high-value, sensitive information. Facility construction includes re-enforced doors, walls, ceilings, and floors.

The site location and construction, when combined with other physical security protection mechanisms such as intrusion sensors, electronic access controls and video surveillance of the facility provides robust protection against unauthorized access to the CA equipment and records.

5.1.2 PHYSICAL ACCESS

Physical access to the CA secure facility in Mississauga is restricted to employees on the *Permanent Authorized Access List*, the *Special Authorized Access List* and escorted visitors. The addition and removal of employees on each list, along with the activities permitted when visitors are present are defined in the *BlackBerry V2X CA Physical Security Policy*.

Physical access controls on the facility include the following.

- Facility access requires pass key and pass code to pass through electronic door locks. Door locks include remote monitoring, alarm, and dispatch of security personnel to address alarm events.
- Facility access requires dual person access to pass through physical door locks.
- Facility contains a safe requiring two combinations to open.
- Facility access points are under video surveillance.
- Facility is under video surveillance.
- Logs are kept of all access, including names and roles of escorted visitors.

The use of physical access controls is defined in the *BlackBerry V2X CA Physical Security Policy*. The process for managing security incidents is described in the *BlackBerry V2X CA Security Incident Management* document.

5.1.3 POWER AND AIR CONDITIONING

The CA security bunker facility in Mississauga has sufficient power and air conditioning to ensure the reliable operation of all equipment related to the correct operation of the Root CA/ICA.

5.1.4 WATER EXPOSURES

CA equipment and media is installed so that it is not in danger of water exposure.

5.1.5 FIRE PREVENTION AND PROTECTION

The facilities that house the CA are constructed and equipped, and procedures implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures meet all local applicable safety regulations.

5.1.6 MEDIA STORAGE

Media related to the operation of the CA is stored in two locations.

- A copy of root and ICA keying material and activation data is securely stored within a safe within the facility and cryptographically secured. Activation tokens are stored in key safes and inactive removeable HSMs are stored in a safe in tamper evident containers.
- A copy of all CA data, including electronic copies of paper records, is retained in off-site BlackBerry backup facilities. All CA keying material or sensitive data stored off-site is cryptographically secured and integrity protected.

5.1.7 WASTE DISPOSAL

Electronic media that have reached the end of their lifecycle are destroyed as described in the *BlackBerry V2X CA Data Classification and Management Policy*.

All outdated paper documents are destroyed as described in the *BlackBerry V2X CA Data Classification and Management Policy*.

5.1.8 OFF-SITE BACKUP

A full backup of CA software and data including a backup of keying material is created for local recovery or DR operation.

The database and HSM of the Root CA / ICA is backed up after every successful key ceremony and root or ICA signing operation. This backup is then transferred to the backup storage facility in Cambridge, ON and logged into a *Disaster Recovery Backup Log*.

5.2 PROCEDURAL CONTROLS

5.2.1 TRUSTED ROLES

The reliable and correct operation of the CA requires personnel to fulfill the following trusted roles (see *BlackBerry V2X CA Trusted Roles and Responsibilities*) which are overseen by the BlackBerry V2X CA Policy Authority.

5.2.1.1 Policy Authority

The Policy Authority is responsible for establishing, maintaining and enforcing policies and procedures governing the CA.

5.2.1.2 CA Operations Manager

The CA Operations Manager provides administrative and management oversight of all CA operations.

5.2.1.3 CA Technical Operations Manager

The CA Technical Operations Manager provides management oversight of all CA technical operations. This role ensures maintenance of critical systems and may involve assisting the CA IT Configuration Administrator.

5.2.1.4 CA Internal Auditor

The CA Internal Auditor is responsible for reviewing the audit logs and performing or overseeing internal compliance audits to ensure that the CA and associated administrative applications are operating in accordance with the BlackBerry V2X CP and this CPS.

5.2.1.5 CA IT Configuration Administrator

The CA IT Configuration Administrator is responsible for installing and configuring system hardware and software, and for updating the CA software and performing system maintenance.

5.2.1.6 HSM Token Holder

Access to keys inside an HSM is controlled using smart cards. Each token is activated with a password. Smart cards are assigned to trusted personnel who must present his smart card and enter a password when creating or activating the use of a key inside an HSM. Token holders may also be CA Operators but will include other trusted personnel to support the CA's Disaster Recovery requirements.

Subject to customer agreement, customer specific CA keys may be protected by a separate set of smart cards. Only authorized personnel of the operational environment shall have access to the secure area of the root CAs/ICAs or Sub-CAs smart cards. The smart cards may be assigned to representatives from the customer organization.

5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

Internal control procedures are designed to ensure that at a minimum, two trusted persons are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons, with a minimum of at least two HSM smart card holders required to create or activate a key. Once a module is activated with operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device

5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

Personnel fulfilling trusted roles are screened by BlackBerry hiring practices and criminal background checks.

Trusted role personnel are given requisite system logons, access to secure facilities and smart cards for HSM access as befits their roles and responsibilities in the CA.

All personnel fulfilling a trusted role are identified on the *Permanent and Special Authorized Access Lists*. These lists are posted in the CA facility.

5.2.4 ROLES REQUIRING SEPARATION OF DUTIES

Roles requiring separation of duties include roles requiring access to sensitive areas, the activation of cryptographic modules, the generation of CA keying materials and the processing of CA certificate applications as documented in *BlackBerry V2X CA Access Control Policy* and CA keying ceremonies documentation.

A person can fulfill multiple roles as described in section **Error! Reference source not found.**, except in cases when two persons of the same role are required for a procedure, an individual can only act as one person of that role. For example, if a procedure calls for two HSM smart card holders, a single person cannot act as both.

5.3 PERSONNEL CONTROLS

5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

Trusted roles and responsibilities, as specified in the CPS, are documented in job descriptions and clearly identified. PKI personnel have job descriptions defined to ensure separation of duties and least privilege, and position sensitivity is determined based on the duties and access levels, background screening and employee training and awareness

All CA personnel are subject to BlackBerry HR policies and terms of employment.

Personnel undergo annual security training as documented in the *BlackBerry V2X CA Personnel Training Procedure*.

5.3.2 BACKGROUND CHECK PROCEDURES

Background investigation and the hiring process follow BlackBerry standard procedures for employee screening, as described in the document Background Screening Guidelines, which is maintained by BlackBerry's Human Resources (HR) group and by the CA's *Personnel Hiring and Disciplinary Procedure* documents.

Checks completed for all external hires include the following:

- Validation of previous five year of employment history, if applicable.
- Validation of highest level of education attended and/or required for the position.
- Validation of professional certification.
- Criminal history review.

5.3.3 TRAINING REQUIREMENTS

The training requirements for CA personnel are described in the *BlackBerry V2X CA Personnel Training Procedure*.

5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

All CA personnel are trained to correctly operate all CA software and hardware relevant to their roles. CA personnel shall be re-trained whenever the Policy Authority or the CA Operations Manager determines that a significant change has been made to the software, hardware, or the BlackBerry V2X CA policies and procedures.

5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

Any change in roles in the administration or operation of trust model elements is accompanied by a change of account access and smart card privileges where relevant, authorized and documented by an approved work order and publication of a revised list of trusted role personnel.

5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

Disciplinary action is taken whenever it is determined that a CA employee has violated the CA procedures, or has acted in a manner detrimental to the CA objectives, such that actual or apparent compromise of security and integrity is possible.

Actions do not have to be intentional to result in disciplinary action.

The employee's immediate supervisor normally assesses the need for disciplinary action. HR may assist in the implementation of any disciplinary actions.

Employees are given formal documentation of the violation.

If dismissed from a role, the employee's CA access credentials are removed.

See the *BlackBerry V2X CA Personnel Disciplinary Procedure*.

5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

Independent contractors fulfilling permanent trusted roles shall be treated in role qualification and assignment as ordinary employees. Other contractors or personnel acting in a non-trusted role or temporary capacity (e.g. maintenance technician, auditor) shall be escorted and supervised when accessing dedicated PKI equipment with their presence authorized in approved work PKI orders and logged in authorized visitor logs.

5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

CA personnel are provided copies of this CP/CPS, all CA Operations policies and procedures relevant to their trusted role, and all CA Operating Manuals. Specialist administrators and technicians may have access to design documentation or software to facilitate a deeper understanding of underlying PKI system behavior.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 TYPES OF EVENTS RECORDED

Security audit logs are automatically collected for access to PKI facilities. In addition to electronic logs, a visitor logbook is used to record the entrance and exit of personnel.

Electronic video and signed paper copies of keying ceremonies are archived and kept of keying ceremonies and other physical interactions with the CA. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

Each event related to certificate life cycle is logged in such a way that it can be attributed to the person that performed it. All data related to a personal identity are protected against non-authorized access.

A periodic internal audit log summarizes the last period's CA activities, including items which are not captured directly by the CA system.

The list of recorded events and the duration of their archival is contained in the *BlackBerry V2X CA Log Management* document.

Each audit record includes the following (either recorded automatically or manually for each auditable event):

- Type of event
- Date and time the event occurred.
- Result of the event: success or failure where appropriate.

- Identity of the entity and/or operator that caused the event if applicable.
- Identity of the entity for which the event is addressed

5.4.2 FREQUENCY OF PROCESSING LOG

Event logs are reviewed as part of periodic internal audits. Refer to the *BlackBerry V2X CA Log Management* document.

5.4.3 RETENTION PERIOD FOR AUDIT LOG

BlackBerry V2X CA Operations maintains its written *summaries* of audit log reviews for a period not less than 7 years, or as necessary to comply with applicable laws. Audit logs are also kept until the completion of the next full accreditation audit or as specified in the *BlackBerry V2X CA Log Management* document.

5.4.4 PROTECTION OF AUDIT LOG

Audit logging information generated by the CA is integrity protected by the CA software. It is maintained in secure CA facilities until it is copied by the CA IT Configuration Administrator. Audit logs are electronically archived and retained in a secure BlackBerry repository as part of the CA records archive.

5.4.5 AUDIT LOG BACKUP PROCEDURES

Electronic audit logs follow the backup described in section 5.1.8.

Audit summaries are backed up at least quarterly.

5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

The audit log collection system is internal to the CA software and hardware. Automated audit processes are invoked at system and application startup, and cease during system shutdown.

Audit summary collection is external to the CA software and hardware and includes a periodic assessment of deployed hardware and software assets.

5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

Audit log events record, where applicable, the associated trusted role or trusted person(s) as one of the event details.

5.4.8 VULNERABILITY ASSESSMENTS

The BlackBerry V2X CA Operations Team will perform routine self-assessment of security controls as described in the *Risk Assessment and Mitigation Strategy* document.

5.5 RECORDS ARCHIVAL

5.5.1 TYPES OF RECORDS ARCHIVED

CA records shall be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate (including revoked or expired certificates) issued by the CA. At a minimum, the following data shall be backed up:

- PKI Operations and Event Logs
- *Certificate Policy* document
- *Certification Practices Statement* documents
- Contractual obligations, if any
- Other agreements concerning operations of the CA
- BlackBerry V2X CA baseline configuration (see the *BlackBerry V2X CA Configuration Management Policy*)
- Modifications and updates to the BlackBerry V2X CA baseline configuration (see the *BlackBerry V2X CA Configuration Management Policy*)
- All certificates issued and/or published
- Audit log data (as described in section 5.4.1)
- Subscriber identity authentication data
- Subscriber agreements or EULAs, if applicable
- Enrollment forms & verification evidence
- All CRLs issued and/or published
- Other data or applications to verify archive contents
- Documentation required by compliance auditors

5.5.2 RETENTION PERIOD FOR ARCHIVE

The BlackBerry V2X CA retains records of certificates and the associated documentation (see section 5.5.1) for a period of three (3) years after corresponding certificate expiry, unless otherwise stipulated as part of a valid business agreement.

The retention term begins on the date of certificate expiration or revocation.

5.5.3 PROTECTION OF ARCHIVE

Archive records are stored in a secure BlackBerry network archive maintained according to the *BlackBerry Records Management Directive* in a manner that prevents unauthorized modification or destruction.

The contents of the archive shall not be deleted except with approval of the PA or as required by law.

5.5.4 ARCHIVE BACKUP PROCEDURES

Offline trust model elements are incrementally backed up after keying ceremonies with full backups at least annually.

On-line trust model elements incrementally back up system archives daily and perform full backups monthly. Copies of paper-based records are scanned periodically and maintained in a remote electronic archive.

5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

Trust element system clocks are synchronized with an accepted time standard and CA archive records are time-stamped as they are created.

The system time on an offline trust element must be verified and manually adjusted if necessary prior to operating the CA using the time source referencing a reliable carrier network.

5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

The archive collection system is internal to the CA software.

5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

The procedures detailing how to obtain, verify, package, transmit, and store the CA archive information are published in the *BlackBerry Media Sanitization and Disposal Standard*.

5.6 KEY CHANGEOVER

Changeover of CA and Sub-CA keys will be scheduled at least two months prior to a CA or Sub-CA certificate's expiry. Prior to doing any changeover, the CA ensures that system time and software integrity are up to date and valid using procedures documented in the *BlackBerry V2X CA Internal Audit Plan*. New certificates will be issued with a validity period beginning approximately 2 weeks from the date of issuance and distributed to relevant subscribers and relying parties. Once valid, only new CA and Sub-CAs will be used to issue certificates and old CA keys will be deactivated and backups destroyed.

5.7 COMPROMISE AND DISASTER RECOVERY

The following describes the general principles applied to all CAs:

- The CA and supporting trust elements are deployed in accordance with BlackBerry operational requirements for high availability requirements for critical customer facing services.
- The CA implements processes and procedures described in the *BlackBerry V2X CA Disaster Recovery and Business Continuity Plan (DRBCP)*.

5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

If personnel responsible for the management of the RCA/ICA detect or receive a report of a potential hacking attempt or other form of compromise, they will perform an investigation to determine the nature and the degree of damage. The scope of potential damage is assessed by the personnel responsible for the management of the CA entity to determine if the PKI component needs to be rebuilt, if only some certificates need to be revoked, and/or if the PKI component has been compromised.

In addition, the CA entity determines which services are to be maintained and how, in accordance with the CA's *Disaster Recovery and Business Continuity Plan*.

As part of the *BlackBerry Security Incident Management Directive*, if a security incident is suspected BlackBerry security specialists are called in to determine root cause and possible damage. BlackBerry security incident response procedures are followed to mitigate issues. In the case of a compromised PKI component and particularly the compromise of a private key, the CA will alert its stakeholders to allow them to also mitigate risks.

The *Disaster Recovery and Business Continuity Plan* (DRBCP) is executed if required.

Supporting procedures are reviewed periodically (at least on an annual basis) and are revised and updated as needed.

5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED

CA personnel perform system back-ups on a regular basis. Back-up copies are made of CA Private Keys and are stored off-site in a secure location (see the *BlackBerry V2X CA Data Classification and Management Policy*).

In the event of corruption or a disaster whereby the primary and disaster recovery CA operations become inoperative at the primary facility and the Disaster Recovery / Mirror Site, the CA will re-initiate its operations on replacement hardware using backup copies of its software, data and CA private keys at a comparable, secured facility.

The system is designed for high availability (HA) to mitigate the risk of any single point of failure. Where a critical system component has suffered damage to impact HA capability, spare equipment may be employed while new equipment orders are expedited. Reporting of corrupt resources must be within 24 hours for the highest level of risk once identified.

5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

In case of a CA key compromise, the PA shall be notified within 24 hours of the discovery or suspicion of a key compromise event. Subsequently, the CA installation shall be reestablished. If the CA distributes a trusted certificate for use as a trust anchor, the new self-signed certificate must be distributed via the standard secure out-of-band mechanisms.

Subscribers shall be notified but subscriber certificates will not be renewed automatically by the CA under the new key pair. The CA will require subscribers to repeat the initial certificate application process.

RPs may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of CA operation with new certificates.

5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

BlackBerry maintains data center and disaster recovery facilities in Cambridge and Brampton, Ontario. After a disaster BlackBerry will execute its *Disaster Recovery and Business Continuity Plan* (DRBCP) to resume operations from this location until a primary operations site can be restored.

CA personnel will be able to securely activate CA private keys using m-of-n (2 of 5) split key shares in DR facilities to recover core CA operations.

5.8 CA AND RA TERMINATION

As soon as possible prior to termination, the CA will advise all other organizations to which it has issued certificates of its termination plans and, where applicable, assign subscriber licenses and transfer relevant PKI data and archives to an authorized assignee.

In the event of the termination of the CA service without assignment, the CA shall:

- Provide subscribers/licensees, legal and applicable regulatory authorities in the US and Canada notice of termination.
- Stop issuing certificates with validity periods beyond the proposed termination or suspension date.
- On termination date, in the case of a terminated Sub-CA, the superior CA shall revoke the Sub-CA and issue a new CRL with the list of revoked sub-CAs. In the case of a root CA the corresponding CA shall revoke itself by issuing a CRL containing itself.
- Communicate last revocation status information (CRL signed by root CA) to the relying party indicating clearly that it is the latest revocation information.
- Destroy the CA private key.
- Archive all audit logs and other records prior to termination and if applicable transfer to an appropriate authority.

Archived records are transferred to an entity designated by the PA. In the event of the termination of the CA services, BlackBerry will be responsible for keeping all relevant records regarding the needs of CA and PKI components.

The requirements of this article may be varied by license agreement to the extent that such modifications affect only the contracting or licensed parties.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 KEY PAIR GENERATION

Cryptographic keying material used by CAs to sign certificates, CRLs or status information is generated in HSMs which have been NIST validated to FIPS 140-2 Level 3. The protection of cryptographic keying material is described in the *BlackBerry V2X CA Access Control Policy*.

CA keys are generated in auditable keying ceremonies as document by CA key ceremony procedures. Public keys are published for relying parties according to Section 2.2.

The CA does not generate Subscriber key pairs.

6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

The CA delivers no explicit private key material to Subscribers.

Implicit certificate private key contribution material is always encrypted in transit and in final form encrypted for the certificate Subject according to IEEE 1609.2 specifications.

6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

Public keys generated by Subscribers are sent to CA entities using CAMP and IEEE 1609.2 specified protocols which enable the CA to validate possession of the private key.

Certificate requests are transmitted over secure, authenticated links or validated using out-of-band fingerprint techniques when requests are transmitted via email.

6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

The CA and Sub-CA certificates, where applicable, are published as described in section 2.2.

6.1.5 KEY SIZES

The CA supports ECDSA with NIST P-256/SHA-256 and ECDSA with NIST P384/SHA256 signature algorithms for IEEE 1609.2 as specified in FIPS 186-4.

6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

The CA supports ECDSA and RSA as defined in FIPS 186-4 using FIPS certified cryptographic modules for CA key generation.

Certificate public keys are validated prior to certificate issuance following FIPS 186-4 specifications.

6.1.7 KEY USAGE PURPOSES

Certificate key usage fields are set to adhere to specifications for CA entities as described in IEEE 1609.2 and CAMP SCMS documentation and as described in the Certificate Profiles of this CPS.

Root CA and ICA certificate signing key usages are asserted as critical.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

CA entities use cryptographic modules validated to FIPS 140-2 level 3 for generating, utilizing and securing CA private keys.

6.2.2 PRIVATE KEY (N OUT OF M) MULTI-PERSON CONTROL

At least two authorized persons are required to invoke the complete CA signature process or access any cryptographic module containing the CA private signing key. Manual access to the cryptographic module requires a two-factor authentication for the administrator. (See the *BlackBerry V2X CA Access Control Policy*).

For Sub-CAs, at least two token holders are required to activate the private key. Once activated, the Sub-CA private key can be used to sign certificate requests without further human interaction. Access to an activate Sub-CA private key is controlled using a passphrase.

CA signing keys are backed up under two-person control. Access to CA signing keys backed up for disaster recovery is under at least two-person control. CA Personnel required for two-person control are identified on the *Permanent Authorized Access List*. This list is available for inspection during compliance audits.

6.2.3 PRIVATE KEY ESCROW

CA private keys are not escrowed.

6.2.4 PRIVATE KEY BACKUP

CA Private Keys are generated inside a FIPS 140-2 Level 3 validated HSM. When deactivated these keys are encrypted and protected by multiple cryptographic tokens that enforce two-person control described in section 6.2.2.

Backups of the private keys are created using techniques specified by the module manufacturer. A private key is always encrypted when it leaves the protection boundary of an HSM.

CA and Sub-CA private key back up is described in the *BlackBerry V2X CA Data Classification and Management Policy*.

6.2.5 PRIVATE KEY ARCHIVAL

CA and Sub-CA private keys are not archived.

6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

A private key is transferred into or from an HSM using techniques specified by the module manufacturer using at least two-person control to reactivate the key as described in Thales HSM Management document.

6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

See section 6.2.4.

6.2.8 METHOD OF ACTIVATING PRIVATE KEY

Private keys stored in an HSM are activated using USB tokens according to techniques specified by the module manufacturer. To activate a key, at least two trusted persons must present their USB tokens together with the associated passwords.

For the Root CA and ICA which are normally offline, activation is required every time the entity is activated for a private key is generation or signing operation.

For ECAs, PCAs, RAs, CRLGs PGs or LAs, a private key is activated for automatic signing. Once activated, signing can be performed by presenting the appropriate passphrase.

The CA maintains no involvement in the protection or distribution of Subscriber private keys.

6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

For the Root CA, the HSM is never left in an unlocked, unattended state or otherwise left open to unauthorized access. After use, the cryptographic module is deactivated as recommend by the manufacturer and documented in the Thales HSM User Guide.

Cryptographic tokens are removed and securely stored when not in use.

6.2.10 METHOD OF DESTROYING PRIVATE KEY

Root CA and ICA private signing keys stored in HSMs are destroyed using the method offered by the cryptographic module.

All backups of the private keys are likewise destroyed so that the destroyed private key cannot be re-activated as is documented in the *BlackBerry V2X CA Security World Archive Management Procedure*.

6.2.11 CRYPTOGRAPHIC MODULE RATING

See section **Error! Reference source not found.**.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 PUBLIC KEY ARCHIVAL

The CA retains copies of all CA entity public keys for archival in accordance with section 5.5 for at least three (3) years after any certificate based thereon ceases to be valid as described in the *BlackBerry V2X CA Security World Archive Management Procedure*.

6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

All certificates and corresponding keying materials have maximum validity periods not exceeding those recommended by SCMS and IEEE 1609.2 specifications.

CA private keys may begin being used at any point after their corresponding certificate validity period begins and will be retired and prevented from signing new certificates at least 30 days prior to expiry to accommodate certificate re-keying and distribution.

The validity periods of certificates subject to this CPS is described in section 7.

6.4 ACTIVATION DATA

Certification practices associated with activation data are described in the following sub-sections.

6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

All CA personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords according to the *BlackBerry V2X CA Access Control Policy* and *BlackBerry PKI Services Password Management Procedure* document.

6.4.2 ACTIVATION DATA PROTECTION

Data used to unlock private keys in cryptographic modules is be protected from disclosure by a combination of cryptographic and physical access control mechanisms with dual factor access tokens assigned to individual operations team members according to *BlackBerry V2X CA Access Control Policy*.

6.4.3 OTHER ASPECTS OF ACTIVATION DATA

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

CA security controls are described in the following sub-sections.

6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

Technical security controls on the BlackBerry V2X CA server are described in the *BlackBerry V2X CA Access Control Policy*.

Computer security controls ensure that CA and administration operations are performed as specified using computer security functions provided by the operating system, or through a combination of operating system, software, and physical safeguards:

- Require authenticated logins
- Provide a security audit capability
- Restrict access control to CA services and PKI roles
- Enforce separation of duties for PKI roles
- Require identification and authentication of PKI roles and associated identities
- Require use of cryptography for database security and external session communication
- Archive CA history and audit data
- Require self-test security-related CA services

The system (hardware, operating system, application software) and ancillary environment is operated only in controlled configurations using approved hardware and software.

Trust elements exposed to external networks are monitored for malware and intrusion and security patches are applied on a regular basis.

6.5.2 COMPUTER SECURITY RATING

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROL

The CA's life cycle technical controls are described in the following sub-sections.

6.6.1 SYSTEM DEVELOPMENT CONTROLS

The System Development Controls for the CA and RA are as follows:

- Software developed specifically for the CA is developed in a controlled environment, using development processes as documented by *BlackBerry Information Systems Development Directive*.
- Hardware and software procured to operate the CA are purchased in a fashion to reduce the likelihood that any component was tampered with. Cryptographic modules are re-initialized before installation. Operating systems are installed from scratch using trusted system images.
- The authenticity of third-party components, updates and relevant security patches is cryptographically validated before adding to CA code repository.

6.6.2 SECURITY MANAGEMENT CONTROLS

The configuration of the CA system, in addition to any modifications and upgrades, is documented and controlled (see the *BlackBerry V2X CA Configuration Management Policy* document).

The CA software, when first loaded, is verified as being that supplied from the vendor, with no modifications, and the version intended for use.

The CA hardware and software, consisting of the HSMs and the servers (physical or virtual) running the CA application are dedicated to the CA. Where CA operation supports multiple CAs, the hardware platform can support multiple CAs.

Proper care is taken to prevent malicious software from being loaded onto the CA equipment to ensure that only authorized, validated applications required to perform the operation or monitoring

are used in the CA operating environment as documented in the V2X PKI software installation and maintenance procedures via Work Order approval processes.

6.6.3 LIFE CYCLE SECURITY CONTROLS

CA software, and particularly any trust elements exposed to external networks, is evaluated against potential vulnerabilities and patched with security updates as required. Vulnerability assessments for offline CA components is performed at least annually.

Scanning and recommendations to patch on-line CA trust elements are performed continuously, with emergency security patching expedited and non-emergency patching planned on a quarterly release cycle.

6.7 NETWORK SECURITY CONTROLS

The Root CA and ICA are operated in an isolated, normally off-line security facility. External certificate requests are scanned for malware in a secure staging area prior to processing.

Sub-CA and on-line CA trust elements are protected by firewalls and an intrusion prevention system in dedicated secure datacenters which offer resilient, dedicated external network links.

Secure temporary links between offline CA trust elements and on-line ancillary online CA (e.g. CRLG) and Sub-CA entities are established to process internal Sub-CA or supporting trust element enrolment.

6.8 TIME STAMPING

See section 5.5.5.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILES

Certificates are issued to conform to IEEE 1609.2 and SCMS specifications. Certificate profile templates are available from CAMP LLC at:

https://stash.campllc.org/projects/SCMS/repos/scms-asn/raw/cert-profile.asn?at=refs%2Fheads%2Frelease%2F1.2.2

This template has been extended to include hostnames for BlackBerry CA entities.

7.1.1 ROOT CA CERTIFICATE PROFILE

The V2XCA Root CA Certificate Profile is detailed below:

```
Name: rca.prod.v2xca.blackberry.com
Hash: 1346ddf49a7fe552e64c70c475c12a687128b6738a0ebd66f99af5239d8d7bbf
Start: 27 Feb 2018
Duration: 70 years
Certificate: rca.prod.v2xca.blackberry.com_certificate.b64
Details:
Sequence (ExplicitCertificate) {
   Integer (3)
   Enumerated (CertificateExplicit(0))
   Choice (IssuerIdentifier) :
      [1] Enumerated (SHA256(0))
   Sequence (ToBeSignedCertificate) {
      Choice (CertificateId) :
         [1] UTF8 "rca.prod.v2xca.blackberry.com"
      OctetString (
         00 00 00
      )
      Integer (0)
      Sequence (ValidityPeriod) {
         Integer (446837241)
         Choice (Duration) :
            [6] Integer (70)
      }
      Sequence (SequenceOfPsidSsp) {
         Sequence (PsidSsp) {
```

```
      Integer (35)
      Choice (ServiceSpecificPermissions) :
         [0] OctetString (
            81 00 01
         )
   }
   Sequence (PsidSsp) {
      Integer (256)
      Choice (ServiceSpecificPermissions) :
         [0] OctetString (
            00 01 00 01 01 01 00
         )
   }
}
Sequence (SequenceOfPsidGroupPermissions) {
   Sequence (PsidGroupPermissions) {
      Choice (SubjectPermissions) :
         [1] Null
      Integer (3)
      Integer (-1)
      BitString (
         c0
      )
   }
   Sequence (PsidGroupPermissions) {
      Choice (SubjectPermissions) :
         [0] Sequence (SequenceOfPsidSspRange) {
            Sequence (PsidSspRange) {
               Integer (35)
            }
         }
      Integer (1)
      Integer (-1)
      BitString (
         c0
      )
   }
   Sequence (PsidGroupPermissions) {
      Choice (SubjectPermissions) :
         [0] Sequence (SequenceOfPsidSspRange) {
            Sequence (PsidSspRange) {
               Integer (38)
```

```
                }
              }
            Integer (1)
            Integer (-1)
            BitString (
              c0
            )
          }
          Sequence (PsidGroupPermissions) {
            Choice (SubjectPermissions) :
              [0] Sequence (SequenceOfPsidSspRange) {
                Sequence (PsidSspRange) {
                  Integer (256)
                }
              }
            Integer (1)
            Integer (-1)
            BitString (
              c0
            )
          }
        }
        Choice (VerificationKeyIndicator) :
          [0] Choice (PublicVerificationKey) :
            [0] Choice (EccP256CurvePoint) :
              [2] OctetString (
                74 21 6d 1e 8b 12 8e 38    9c 83 e5 6b d9 4f 88 98
                d0 c2 c9 19 bd 79 41 e8    3d d4 a9 28 a9 15 65 f0
              )
      }
      Choice (Signature) :
        [0] Sequence (EcdsaP256Signature) {
          Choice (EccP256CurvePoint) :
            [0] OctetString (
              54 fe 55 3b 5c 5d d8 0a b6 14 18 0c 6b 40 07 ce
              98 0a 21 45 27 7b 1b 51 c3 77 66 2c 6f 68 b0 27
            )
          OctetString (
            b6 19 95 92 ee 73 79 6d 79 a1 3e 06 21 89 de 31
            eb 1a 94 e8 96 ab 6b 47 76 be 33 28 b0 76 11 d8
          )
        }
    }
```

7.1.2 INTERMEDIATE CA CERTIFICATE PROFILE

The ICA certificate profile is listed below.

Intermediate CA
Name: ica.prod.v2xca.blackberry.com
Hash: 60bbf7a7a4923404587f6cc3efe57f4687be4030cc2ff44fdc17996c9e02eabd
Start: 27 Feb 2018
Duration: 50 years
Certificate:ica.prod.v2xca.blackberry.com_certificate.b64
Details:

```
Sequence (ExplicitCertificate) {
   Integer (3)
   Enumerated (CertificateExplicit(0))
   Choice (IssuerIdentifier) :
      [0] OctetString (
         f9 9a f5 23 9d 8d 7b bf
      )
   Sequence (ToBeSignedCertificate) {
      Choice (CertificateId) :
         [1] UTF8 "ica.prod.v2xca.blackberry.com"
      OctetString (
         8d 7b bf
      )
      Integer (2)
      Sequence (ValidityPeriod) {
         Integer (446851539)
         Choice (Duration) :
            [6] Integer (50)
      }
      Choice (GeographicRegion) :
         [3] Sequence (SequenceOfIdentifiedRegion) {
            Choice (IdentifiedRegion) :
               [0] Integer (124)
            Choice (IdentifiedRegion) :
               [0] Integer (484)
            Choice (IdentifiedRegion) :
               [0] Integer (840)
         }
      Sequence (SequenceOfPsidSsp) {
         Sequence (PsidSsp) {
            Integer (35)
            Choice (ServiceSpecificPermissions) :
               [0] OctetString (
```

```
                83 00 01
            )
        }
    }
    Sequence (SequenceOfPsidGroupPermissions) {
        Sequence (PsidGroupPermissions) {
            Choice (SubjectPermissions) :
                [1] Null
            Integer (2)
            Integer (0)
            BitString (
                c0
            )
        }
        Sequence (PsidGroupPermissions) {
            Choice (SubjectPermissions) :
                [0] Sequence (SequenceOfPsidSspRange) {
                    Sequence (PsidSspRange) {
                        Integer (35)
                        Choice (SspRange) :
                            [1] Null
                    }
                    Sequence (PsidSspRange) {
                        Integer (256)
                        Choice (SspRange) :
                            [1] Null
                    }
                }
            Integer (1)
            Integer (-1)
            BitString (
                c0
            )
        }
    }
    Choice (VerificationKeyIndicator) :
        [0] Choice (PublicVerificationKey) :
            [0] Choice (EccP256CurvePoint) :
                [3] OctetString (
                    a5 8f 20 eb 8f d4 20 7e 60 97 49 74 eb 82 cc 4e
                    0f 7a 92 59 c1 56 7e 1b 42 30 18 51 06 e5 ff 30
                )
}
```

```
Choice (Signature) :
   [0] Sequence (EcdsaP256Signature) {
      Choice (EccP256CurvePoint) :
         [0] OctetString (
            a6 07 60 bd 6d 98 8e 90 b5 2c e9 83 43 fa d8 dd
            23 2f e9 0d 8c 0a d7 23 cc 84 6c 66 a6 b3 c7 0e
         )
      OctetString (

         12 23 f2 7b 09 bd 45 8e    a1 0e 7c 4b 8b 51 d6 67

         ad 55 15 8e 5c ba 96 61    70 3f 1b ac 78 51 ba 33

      )

   }

}
```

7.1.3 MA CERTIFICATE PROFILE

No MA certificate has been issued.

7.1.4 ENROLMENT CA (ECA) CERTIFICATE PROFILE

Not applicable for this CPS.

7.1.5 PSEUDONYM CA (PCA) CERTIFICATE PROFILE

Not applicable for this CPS.

7.1.6 ENROLMENT CA (ECA) CERTIFICATE PROFILE

Not applicable for this CPS.

7.1.7 RSE IDENTITY CERTIFICATE PROFILE

Not applicable for this CPS.

7.1.8 OBE IDENTITY CERTIFICATE PROFILE

Not applicable for this CPS.

7.1.9 ENROLMENT CERTIFICATE (EC) CERTIFICATE PROFILE

The EC certificate profile is listed below.

7.2 CRL PROFILE

The CRL Generator name space is extended to include a BlackBerry hostname:

```
name ( ... | "crlg.cvp.v2xscms.com" | "crlg.prod.v2xca.blackberry.com")
```

The CRL Generator certificate profile is listed below.

7.2.1 VERSION NUMBER(S)

CRL conform to IEEE 1609.2.x standards.

7.2.2 CRL AND CRL ENTRY EXTENSIONS

CRL conform to IEEE 1609.2.x standards.

7.3 OCSP PROFILE

No stipulation.

7.3.1 VERSION NUMBER(S)

No stipulation.

7.3.2 OCSP EXTENSIONS

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

ECA and PCA PKI elements of the SCMS trust model have no formal external audit or compliance stipulation at this time. Internal assessments are done on an annual basis where no formal external assessments are required.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

The CA shall order an assessment for the RCA and ICA in the following cases:

- Annually after commencing operation
- As directed by the PA after a significant suspension of operations due to a severe security breach or a significant audit concern.

8.2 IDENTITY & QUALIFICATIONS OF ASSESSOR

The BlackBerry V2X CA retains an auditor which meets *Certificate Policy* qualification requirements.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The BlackBerry V2X CA retains an auditor which meets *Certificate Policy* qualification requirements.

8.4 TOPICS COVERED BY ASSESSMENT

Root CA / ICA audits cover the topics indicated in the CP.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

In case of a CA audit, depending on the audit result the PA may decide to modify its CP and CPS in to resolve the non-conformance, allow a grace period for a non-conforming entity to undertake corrective actions in its certification practices, or to suspend the entity's operation, and if necessary, re-order an audit report to be provided to the PA prior to approval to resume operations. In extreme instances the PA may require that the CA revoke certificates which are a security concern with respect to the audit discrepancy.

8.6 COMMUNICATION OF RESULTS

The CA will provide the audit report for the CA itself to the PA with any corrective action plans required to address an audit exception or irregularity for approval or suspension notification. It may post a certificate of conformity in its repository or provide such certificate to its Applicants and Subscribers.

9 OTHER BUSINESS AND LEGAL MATTERS

This section describes the legal representations, warranties and limitations associated with BlackBerry's V2X CA services.

9.1 FEES

Any fees charged by BlackBerry Certicom V2X PKI certificate services are subject to business agreements.

9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES

No stipulation.

9.1.2 CERTIFICATE ACCESS FEES

No stipulation.

9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

No stipulation.

9.1.4 FEES FOR OTHER SERVICES

No stipulation.

9.1.5 REFUND POLICY

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

The financial responsibilities of BlackBerry and its Subscribers are subject to business agreements.

9.2.1 INSURANCE COVERAGE

No stipulation.

9.2.2 OTHER ASSETS

No stipulation.

9.2.3 INSURANCE OR WARRANTY COVERAGE FOR END-ENTITIES

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

The BlackBerry V2X CA keeps business information and internal security-sensitive information confidential and maintains reasonable controls and secure information handling process as outlined in ISO/IEC 27001 to prevent the exposure of such records to non-trusted personnel. Depending upon circumstances, some information may be shared under NDA.

- Any business continuity incident response, contingency, and disaster recovery plans
- Any other security practices, measures, mechanisms, plans, or procedures used to protect the confidentiality, integrity or availability of information
- Any information held by BlackBerry as private information in accordance with section 9.4
- Any transactional, audit log and archive record identified in section 5.4 or 5.5 including certificate application records and documentation submitted in support of certificate applications whether successful or rejected.
- Transaction records, financial audit records, external or internal audit trail records and any detailed audit reports.

9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

An external auditor’s summary letter confirming the effectiveness of the controls set forth is not considered confidential.

9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

The CA observes applicable rules on the protection of personal data deemed by law or the BlackBerry's privacy policy (see section 9.4) to be confidential and is bound by the terms of its CP and applicable legal agreements.

Subscribers are likewise bound by license agreement to confidentiality obligations.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 PRIVACY PLAN

The BlackBerry V2X CA and associated BlackBerry platform services entities follow the BlackBerry corporate privacy policy https://ca.blackberry.com/legal/privacy-policy for any information related to processing of personal information which includes the collection, use, processing, transfer, storage or disclosure of personal information.

The application of the BlackBerry Privacy Policy is subject to applicable laws including legislation, regulations and the orders of courts or other lawful authorities, other lawful requests or legal processes.

9.4.2 INFORMATION TREATED AS PRIVATE

Personal customer contact details, business terms, customer certificate volumes, and linkages corresponding to Subscriber end entity PCs are deemed private.

Production pseudonym certificate linkage values which can be used to identify pseudonym certificates are only disclosed to authorized Misbehavior Authorities.

9.4.3 INFORMATION NOT DEEMED PRIVATE

Certificates, CRLs, and any personal or corporate information appearing in them, are not deemed private however their disclosure may be limited to PKI stakeholders.

9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

Each party should protect the confidentiality of private information that is in its possession, custody or control with the same degree of care that it exercises with respect to its own information of like import, but in no event less than reasonable care, and use appropriate safeguards and otherwise exercise reasonable precautions to prevent the unauthorized disclosure of private information.

9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

A party may use private information with the subject's express written consent or as required by applicable law or court order except that pseudonym certificate linkage values may be shared with a requesting Misbehavior Authority when authorized by the PA to receive such information.

9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

BlackBerry V2X CA will not release any confidential information, unless as otherwise required by law, without an authenticated, reasonably specific request by an authorized party specifying:

- The party to whom BlackBerry owes a duty to keep information confidential.

- The party requesting such information.
- A valid & enforceable, uncontested court order, if any.

9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

All personnel in trusted positions handle all information in strict confidence including those requirements of Canadian and US laws concerning the protection of personal data.

9.5 INTELLECTUAL PROPERTY RIGHTS

BlackBerry will protect its trademarks and respect those of others, seeking permission from owners before promoting any other company's trademark on its website or in conjunction with its service.

Certificates issued by the CA are the exclusive property of BlackBerry. BlackBerry gives permission to reproduce and distribute certificates according to business agreement provided they are reproduced and distributed in full. BlackBerry reserves the right to revoke the certificate at any time and at its sole discretion.

Subscriber private and public keys are the property of the Subscribers.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA REPRESENTATIONS AND WARRANTIES

CA representations and warranties are stated in the BlackBerry V2X CA CP and related business agreements.

9.6.2 RA REPRESENTATIONS AND WARRANTIES

Not applicable.

9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

Subscriber representations and warranties are stated in the BlackBerry V2X CA CP and related business agreements.

9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES

Relying parties must accept the limitations on the usage of and trust in digital certificates and take actions as described in the CP to minimize the risk of relying upon an invalid, revoked or expired certificate.

9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

Not applicable.

9.7 DISCLAIMERS OF WARRANTIES

Disclaimers of warranties is subject to applicable business agreements.

9.8 LIMITATIONS OF LIABILITY

Limitations of liability are subject to business agreement.

9.9 INDEMNITIES

Indemnities are subject to business agreement.

9.10 TERM AND TERMINATION

9.10.1 TERM

The *BlackBerry V2X CA Certificate Policy* and any amendments hereto become effective on a date approved by the PA and the Certificate Policy has been published in the CA repository.

9.10.2 TERMINATION

The *BlackBerry V2X CA Certificate Policy* as amended from time to time will remain in force until it is replaced by a new version or is otherwise terminated in accordance with this section 9.10.

9.10.3 EFFECT OF TERMINATION AND SURVIVAL

The conditions and effect resulting from termination or amendment of the *BlackBerry V2X CA Certificate Policy* will be communicated in accordance with the Certificate Policy itself and stipulations in valid business agreements.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Notices to and correspondence with the CA may be made by contacting the PA in writing, or by email or telephone as noted in the CP.

Notices to participants are be made via electronic or registered mail or via the repository, depending upon the type of notice or communication being transmitted. Individual notices regarding certification policies

and practices or technical matters are sent to the Subscriber's primary authorized representative(s) or technical contacts. Legal or financial notices may be sent directly to Subscriber legal or billing contacts.

Communication with Subscribers will also include notifications regarding and scheduled maintenance outages or holiday schedules for the front office staff and technical support teams. Such communications will be sent by email on a quarterly basis or more frequently in required to notify Subscribers of an isolated event.

These communications are part of the *BlackBerry PKI Services Communications Plan*.

9.12 AMENDMENTS

9.12.1 PROCEDURE FOR AMENDMENT

Section 1.5.4 describes the procedures and approval process for amending the CP and its corresponding certification practices.

9.12.2 NOTIFICATION MECHANISM AND PERIOD

Section 1.5.4 describes the procedures and approval process for amending a CP or corresponding certification practices.

9.12.3 CIRCUMSTANCES UNDER WHICH OID MUST BE CHANGED

Certificate Policy OIDs are not applicable to IEEE 1609.2 certificates.

9.13 DISPUTE RESOLUTION PROVISIONS

Dispute resolution provisions, if applicable, are specified in relevant business agreements.

9.14 GOVERNING LAW

Laws governing BlackBerry V2X CA services are specified in applicable business agreements.

9.15 COMPLIANCE WITH APPLICABLE LAW

BlackBerry V2X CA certification practices will endeavor to comply with applicable national, provincial, local and foreign laws, rules, regulations, ordinances, decrees and orders including but not limited to restrictions on exporting software, hardware or technical information. Such representations are subject to business agreements.

9.16 MISCELLANEOUS PROVISIONS

Miscellaneous provisions such as agreement scope and completeness, assignment, severability, enforcement and force majeure are subject to applicable business agreements.

9.17 OTHER PROVISIONS

Other provisions are subject to applicable business agreement.