BlackBerry | certicom

# BlackBerry V2X CA
# ECA & PCA Certification Practices Statement

| | |
|---|---|
| **Date** | **July 25, 2019** |
| **Author** | **Jim Alfred/Randy Tsang** |
| **Document Revision** | **1.0.3** |
| **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) and certificate specifications based on IEEE 1609.2 standards[i]

This CPS addresses requirements from the BlackBerry V2X CA Certificate Policy for Enrolment CAs (ECAs) and Pseudonym CAs (PCAs).

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 Enrolment CAs and Pseudonym CAs (PCAs) as defined in the BlackBerry V2X CA Certificate Policy v1.0 for issuance of certificates 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 CAs are operated on-line from within a high availability BlackBerry datacenter.

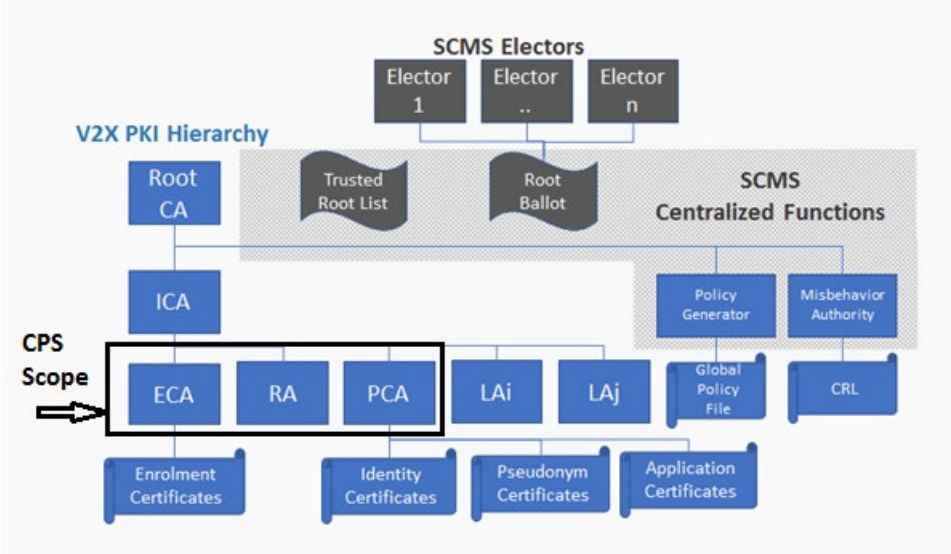


Figure 1 CPS Scope

Although the certificates issued are IEEE 1609.2 rather than X.509 based this CPS is consistent with the Internet Engineering Task Force (IETF) RFC 3647 "Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework".

## 1.2 DOCUMENT NAME AND IDENTIFICATION

This document is known as the “BlackBerry V2X ECA and PCA Certification Practices Statement”.

Revision History

| Date | Changes | Version |
|---|---|---|
| 29 Mar. 2018 | Initial Release – pre-approval draft | 1.0 |
| 18 Oct. 2018 | Amended for test certificate issuance & additional edits | 1.0.1 |
| 28 Dec. 2018 | Removed CA Observer Trusted Role and reflected changes in the CP. | 1.0.2 |
| 25 July 2019 | Remove internal hyperlinks for website publication and updated BlackBerry document names. | 1.0.3 |
| | | |

## 1.3 PKI PARTICIPANTS

### 1.3.1 CERTIFICATION AUTHORITIES

The CPS addresses BlackBerry V2X ECA and PCA entities. Certification practices associated with Root and ICA certificate issuing entities in the CA hierarchy are documented in a separate CPS.

BlackBerry V2X CA ECAs and PCAs 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*.

ECA and PCA certificate profiles and the certificates issued by these entities are consistent with Certificate Profiles specified by IEEE 1609.2 and SCMS specifications from CAMP LLC.

The BlackBerry V2X ECA is:

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

issuer: hashedID8 of ica.prod.v2xca.blackberry.com
```

The BlackBerry V2X PCA is:

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

issuer: hashedID8 of ica.prod.v2xca.blackberry.com
```

### 1.3.2 REGISTRATION AUTHORITIES

RAs are responsible for accepting inbound end-entity Pseudonym Certificate (PC), Identity and Application Certificate requests from Subscribers, authenticating requests using Enrolment Certificates (ECs) issued by a

trusted Enrolment CA (ECA). An RA marshals certificate request bundles to a Pseudonym CA (PCA) for end-entity certificate issuance.

The RA associated with the BlackBerry Certicom V2X Pseudonym CA is:

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

issuer: hashedId8 of ica.prod.v2xca.blackberry.com
```

### 1.3.3 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.

Subscriber technical qualifications and the types of certificates to which they are entitled (enrolment certificates, pseudonym certificates, identity and application certificates, or Registration Authority certificates) are detailed in license agreements which bind the Subscriber to the BlackBerry V2X CA CP and this and other relevant CPSs.

### 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 are device manufacturers which have installed BlackBerry V2X CA trust anchors in their devices. They shall be implied to have accepted relying party obligations identified in *BlackBerry V2X CA Certificate Policy* or relevant 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) is a host or service entity used by a device manufacturer in order to facilitate interaction between the Enrolment CA and ITS Station modules in order to automate the ITS Station enrolment process and provision trust anchors and policy files in the SCMC V2X architecture. It should act as a gatekeeper to enroll only legitimate devices with the ECA.

DCM interfaces have not been standardized by CAMP or IEEE and management practices are outside the scope of this CPS.

### 1.3.7 QUALIFIED AUDITOR

A qualified external auditor is responsible for performing audits of root CA, intermediate and where applicable, 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 CPSs to the *BlackBerry V2X CA CP*.

### 1.3.8 SCMS MANAGER

A future SCMS Manager or Managers is anticipated to set high-level certification policies for the SCMS V2X trust realm.

Once such 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.

### 1.3.9 TRUST REALM ELECTORS

In CAMP's proposed SCMS Manager deployment architecture it is envisaged that the SCMS Manager will nominate Electors to ballot trusted CA roots into the SCMS V2X trust realm.

## 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, including appropriately authorized test certificates such as those required issued by the ECA or PCA components in order to validate internal operations, e.g. disaster recovery validation. Issuance of any internal test certificates must be pre-approved and resulting certificates must be destroyed after use.

### 1.4.2 PROHIBITED CERTIFICATE USES

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

## 1.5 POLICY ADMINISTRATION

### 1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

This CPS, related agreements, and security policy documents referenced in this document are administered by the BlackBerry V2X CA Policy Authority (BBV2X PA) or more simply, “the PA”.

The BlackBerry V2X CA PA approves this 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 CPS 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 *BlackBerry V2X CA 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

The CPS is available to Subscribers and qualified relying parties.

## 2.2 PUBLICATION OF CERTIFICATION INFORMATION

The repository identified in Section 2.1 publishes the following information:

- A reference to the relevant Certificate Policy and Certification Practices Statements
- Where acting as a qualified CRL distribution system, subscriber access to a CRL containing revoked but unexpired ECA, RA and PCA certificates

For clarity we note that CRL distribution responsibilities ultimately lie with the SCMS Manager. For certain environments such as a connected vehicle pilot this responsibility may fall to the BlackBerry V2X CA.

## 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, where applicable, 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. 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

Types of names follow IEEE 1609.2 specifications for V2X certificates.

### 3.1.2 NEED FOR NAMES TO BE MEANINGFUL

The names of ECAs, PCAs and the corresponding RAs and LAs follow the naming requirements specified in the BlackBerry V2X CA CP. ECA and PCA names are listed in section 1.3.2.

### 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 dis-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

No stipulation.

### 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

CAMP specified certificate request protocols are used to make enrolment, identity, application and pseudonym certificate requests. Request validation proves possession of the private key.

### 3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

Certificate requests are accepted from authorized points of contact within the organization or programmatically via an authenticated remote service interface (e.g. DCM interfaces) based on a previously issued authentication credential.

Certificates issued to organizations other than the CA itself are organizationally validated using information disclosed as part of a Subscriber Agreement, EULA, or other relevant legal agreements. Verification is done at time of registration by appropriate means and in accordance with the present Certificate Policy.

### 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 a previously authorized company representative or in the event such representative is not available a senior manager within the organization, 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

No stipulation.

### 3.2.5 VALIDATION OF AUTHORITY

The information provided in sections 3.2.2 and 3.2.3, license agreements and company purchase orders are used to validate authority for certificate requests.

### 3.2.6 CRITERIA FOR INTEROPERATION

BlackBerry participates in private and industry events hosted to demonstrate certificate functionality on test and commercial V2X devices and interoperability with other SCMS component providers. The OmniAir Consortium ® (www.omniair.org) and its PlugFest(s) are one such forum.

### 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.

Eligibility of end entity devices for certification is confirmed with an authorized test lab prior to licensing subscribers. License agreements bind subscribers to enroll for and use PCs only in eligible end entity devices.

### 3.2.8 AUTHENTICATION OF END-ENTITITY 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

Pseudonym certificates are short-lived which are routinely reissued with new ECVQ based keys.

Unless the certificate request is simply an update to an existing valid pseudonym certificate 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 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.

### 3.4.2 ITS STATION ENROLMENT CERTIFICATES

A Subscriber can request blacklisting for its own ECs in writing or via email correspondence with an authorized Subscriber representative. Blacklisting will also occur if a corresponding ITS Station or application certificate is revoked to ensure that no further certificates are issued for the device.

### 3.4.3 PSEUDONYM, APPLICATION AND IDENTITY CERTIFICATES

Pseudonym, application and identity 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 certificate application is 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

Subscribers register ITS Station at an ECA using Enrollment Credential certificate requests. These may be registered manually by an authorized representative or programmatically through an authenticated DCM. External databases and stakeholders including government entities and certification laboratories may be consulted in this process.

Once enrolled, an ITS Station may send Pseudonym Certificate, Identity Certificate or Application Certificate requests without any Subscriber interaction by using its valid EC to authenticate with an RA, and the RA from this point acting as the intermediary between the ITS Station and the PCA.

Test certificate requests may be approved by a CA Operations Manager.

### 4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

Authorized Subscribers manage the enrolment of a device with an ECA and PCA.

#### *4.1.2.1 RA, ECA and PCA entities*

During the enrolment process an external ECA/PCA will send relevant documents (e.g. its CPS and audit report where applicable, Subscriber Agreement and authorized representative documents) to the CA for approval.

The CA verifies the request and the received documents and application form (containing authorized representative signatures) and, where applicable, a certificate request fingerprint. In case of positive checks of the documents the CA accepts said request and check against the application and request fingerprint.

#### *4.1.2.2 ITS Stations*

The initial registration of ITS Station (ITS-S) end-entities subjects with the ECA is done by the responsible Subscriber (manufacturer /operator) through either an authorized representative or through an authenticated DCM associated with the Subscriber.

An ITS-S or its DCM may generate an EC key pair (refer to section 6.1) and create a signed EC request according to IEEE 1609.2 and CAMP specifications.

During the registration of an ITS-S the ECA verifies that the requested certificate profile is from an authorized subscriber with permission to request said certificate type and any special attributes requested.

Regular vehicles may have only one ITS Station registered at an ECA. Special purpose vehicles (such as police cars and other special purpose vehicles with specific rights) may be registered at an additional ECA or have one additional ITS Station for authorizations that are in scope of the special purpose.

Service ID permissions for roadside equipment ITS Stations and special vehicles may require authorization by the responsible government entity.

Once enrolled with an EC certificate, an ITS Station may send a PC certificate request to its RA, using its EC for authentication. The RA will automate issuance for subsequent PC top-ups.

## 4.2 CERTIFICATE APPLICATION PROCESSING

### 4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

End-entity certificate request authentication is automated using an Enrolment CA to enroll ITS Stations into the PKI or via a manual process where requests are submitted from an authorized subscriber via a PKI portal.

#### *4.2.1.1 Identification and authentication of ITS Stations*

One it has become a licensed Subscriber, a manufacturer or ITS Station operator is provided credentials to enroll its ITS Stations with an ECA typically utilizing an automated the enrolment scheme (Device Configuration Manager as described by CAMP) to interface with module manufacturing systems and the ECA. The ECA will authenticate the Subscriber's credential, check that the information in the ITS Station's EC certificate request and if valid proceeds to issuance.

#### *4.2.1.2 Pseudonym, Application and Identity Certificates*

An RA authenticates an ITS Station EC and determine it has not been blacklisted prior to passing valid requests to a CA for issuance.

### 4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

#### 4.2.2.1 Approval or rejection of EC

If a valid and correct enrolment certificate request is received from an ITS Station or its corresponding DCM on behalf of an authorized Subscriber, the ECA generates the requested certificate. The Subscriber is bound to ensure that only its eligible ITS Stations make such requests.

Validation includes ensuring that the enrolment profile matches a profile and certificate permissions to which the Subscriber is entitled. If the certificate request is invalid or exceeds the Subscriber's permissions, then ECA shall refuse the certificate request and send a response containing the reason of the certificate issuance refusal.

#### 4.2.2.2 Approval or rejection of Pseudonym, Application and Identity Certificates

The ITS Station establish communications with the RA, possibly via a Device Configuration Manager (DCM), to make an initial request. The RA confirms the continued enrolment and non-blacklisted status of the ITS Station using its EC and blacklist to validate an authorized certificate request. If the request can be validated the RA will submit the request to the PCA for fulfilment. The RA may continue to automatically make requests on the ITS Station's behalf according to the active profile.

Rejected certificate requests are logged and reported to the relevant Subscriber.

### 4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

Under ideal conditions the ECA and PCA process valid certificate applications in less than 10 minutes. Under heavy load a full 3-year top-up request may require up to 1 business day to process.

## 4.3 CERTIFICATE ISSUANCE

### 4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

#### 4.3.1.1 Enrolment Certificate issuance

The ECA authenticates and verify that the information in an Enrolment Certificate (EC) certificate request is valid and has been submitted on authority of a Subscriber authorized to receive certificates with the requested application identifier (SSID) and credential holder permission (SSP) attributes per CAMP certificate profile specifications and any applicable government policies.

In case of positive validation, the ECA shall issue an EC certificate and send it to the ITS Station.

#### 4.3.1.2 *Pseudonym, Application and Identity Certificates issuance*

The RA validates Pseudonym, Application and Identity Certificate requests against the ITS Station Enrolment Certificate and forwards valid, non-black-listed requests to a CA for issuance and responses from the CA and provide them to the ITS Station.

Certificate requests and responses are encrypted to ensure confidentiality and signed to assure authentication, integrity and privacy.

Mal-formed or unauthorized requests are rejected.

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

ECA / RA will notify a Subscriber of certificate availability or rejection via a programmatic response defined by CAMP and IEEE 1609.2, or where applicable via a PKI portal or email response (e.g. for manually certificate request submissions).

Depending on how certificates are requested, responses are sent to the requestor in one of the following ways:

- If requested via a CAMP specified SCMS https interface, the requestor can retrieve the issued certificate using that interface within 1 business day of making the request.
- If requested via the PKI portal, the requestor can download the certificate via the portal or receive an error notification within 1 business day of making the request.
- If requested via email, notification of certificate issuance will be sent by email within 3 business days to the requestor's email address with instructions for downloading.

## 4.4 CERTIFICATE ACCEPTANCE

### 4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

#### 4.4.1.1 *End-entity (ITS Station)*

As soon as possible, the ITS-S should verify the response received from ECA/RA against its original request, including the signature and the certificate chain. The ITS-S should discard all EC/RA responses that are not correctly verified and send a new request, logging such errors if possible so they may be reported to the Subscriber and the CA.

### 4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

The CA does not publish ECA, PCA or RA certificates or end-entity certificates issued by ECA or PCA entities in its repository.

### 4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES

Not applicable to this CPS.

## 4.5 KEY PAIR AND CERTIFICATE USAGE

### 4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

Subscribers are obliged to use private keys bound to certificates issued under the CP and this CPS only in accordance with the usages specified for the certificates via IEEE 1609.2 attributes and their respective Subscriber Agreements and to protect these keys from disclosure or unauthorized use.

Subscribers should not register for nor deploy end-entity certificates into ITS stations with permissions for which its ITS Stations are not authorized.

### 4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

The CA, through the CP, informs RPs that 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.

The CA assumes RPs correctly adhere to certificate usage and validation schemes according to IEEE 1609.2 and SCMS specifications.

## 4.6 CERTIFICATE RENEWAL

### 4.6.1 CIRCUMSTANCES FOR CERTIFICATE RENEWAL

Not applicable.

### 4.6.2 WHO MAY REQUEST RENEWAL

Authorization are treated as original certificate requests per Section 4.1.

### 4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS

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

### 4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER

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

## 4.7 CERTIFICATE RE-KEY

Subscriber Enrolment, Pseudonym, Identity and Application certificate rekeying practices are described below:

### 4.7.1 CIRCUMSTANCES FOR CERTIFICATE RE-KEY

Enrolment Certificates, Identity Certificates and Application Certificates are not re-keyed.

The re-keying concept does not apply to Pseudonym Certificates.

### 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.

### 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

Subscriber ECA, RA and PCA and ITS Station certificate modification practices are described below:

### 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

Subscribers 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 Subscribers and 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

The CA's certificate revocation practices are described below:

### 4.9.1 CIRCUMSTANCES FOR REVOCATION

ITS Station Enrolment Certificates (ECs) issued by the ECA may be revoked by the CA if the ECA has been revoked or compromised or if there is reason to believe an ITS Station itself has had its EC compromised. EC certificate CRLs are not published. Revocation of an EC shall lead to it being placed on an RA's blacklist such that no further Pseudonym Certificates, Identity Certificates or Application Certificates may be issued by relying upon it.

An ITS Station's Pseudonym, Identity or Application certificates may be revoked for loss or suspected compromise of the ITS Station or application or its private key.

### 4.9.2 WHO CAN REQUEST REVOCATION

The Misbehavior Authority may request the revocation of an ITS Station's Pseudonym, Identity or Application implicit certificates by recovering PC certificate linkage values and publishing in a CRL according to CAMP specifications. Corresponding enrolment certificates will be blacklisted.

A Subscriber may request revocation of its own ITS Station's enrolment or implicit certificates.

### 4.9.3 PROCEDURE FOR REVOCATION REQUEST

An Enrolment Certificate is revoked by blacklisting the certificate with its corresponding RA.

An ITS Station implicit certificate is revoked by the CRL generator adding revoked linkage IDs corresponding to the ITS Station certificates onto the global CRL.

### 4.9.4 REVOCATION REQUEST GRACE PERIOD

A Subscriber must notify the CA immediately of any compromise to its private keys which could negatively impact the safety of Relying Parties. A Subscriber may make non-security critical revocation requests at their convenience. Grace periods are not supported at the ECA / PCA issuance level.

### 4.9.5 TIME WITHIN WHICH CA MUST PROCESS THE REVOCATION REQUEST

ECAs must remove revoked subscriber devices within 1 business day of revocation.

RAs must remove revoked subscriber devices within 1 business day of revocation so that PCAs do not receive valid PC requests from revoked subscriber devices.

### 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 (IF APPLICABLE)

The CRL is published, when applicable, with a schedule established by the PA per section 2.3.

### 4.9.8 MAXIMUM LATENCY FOR CRLS

Maximum CRL latency, where applicable, is one business day.

### 4.9.9 ON-LINE REVOCATION / STATUS CHECKING AVAILABILITY

Not applicable.

### 4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

Not applicable.

### 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 ECA or PCA private keys has been compromised, publishing a CRL where appropriate 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

The ECA and PCA entities do not publish their own CRLs. These functions are handled by an SCMS Manager via a centralized CRL Generator.

#### 4.10.2 SERVICE AVAILABILITY

ECA and PCA entities do not publish their own CRLs.

#### 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

## 5.1 PHYSICAL CONTROLS

### 5.1.1 SITE LOCATION AND CONSTRUCTION

CA equipment is installed in secure data centers in Cambridge, Ontario and Brampton, Ontario and may be hosted in other secure data centers which also host BlackBerry services.

The construction of the facility housing the equipment is consistent with facilities used to house high-value, sensitive information. Requirements for constructing the facility included re-enforced doors, walls, ceilings, and floors, and video surveillance of the facility.

Site location and construction, when combined with other physical security protection mechanisms such as intrusion sensors, provides robust protection against unauthorized access to the CA equipment and records.

### 5.1.2 PHYSICAL ACCESS

Physical access to the CA data centers is managed by the BlackBerry Global Technology Services (GTS) department, with specific access to PKI components authorized by the CA operations team. The use of physical access controls is defined in *BlackBerry Physical Security Policy* (CS-POL-0119.13). The process for managing security incidents is described in the *BlackBerry Security Incident Management Directive* (CS-DIR-0108).

### 5.1.3 POWER AND AIR CONDITIONING

The data center which houses online CA equipment is designed and operated by the BlackBerry Infrastructure Platforms team under supervision of the Chief Information Security Officer (CISO). It has been designed to provide uninterrupted services essential to BlackBerry and its customers.

### 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 trust elements 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.

- 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.
- 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

The ECAs and PCAs use two or more HSMs to provide load balancing as well as high availability. The HSM contents are also copied to an HSM in the Disaster Recovery (DR) site. The databases of the Sub-CA systems are replicated to a database available to the DR site through a secure internal network on an ongoing basis.

Access to backup media stored off-site is limited to authorized personnel. Authorized personnel are identified using BlackBerry V2X CA Organizational Chart maintained by the CA Operations Manager.

## 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 PKI Services Trusted Roles and Responsibilities Policy*).

#### *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. This role may involve assisting the CA IT Configuration Administrator in the performance of their duties; however, this is discouraged.

#### *5.2.1.3 CA Technical Operations Manager*

The CA Technical Operations Manager provides technical oversight of all CA 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 this CP/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.

Activation of an HSM to use the ECA or PCA private key is controlled using smart cards. Each smart card is unlocked with a password. Smart cards are assigned to trusted personnel who must present his smart card and enter a password when activating the use of a new HSM.

Subject to customer agreement, customer specific CA keys may be protected by HSMs that are activate with a separate set of smart cards. Only authorized personnel of the operational environment shall have access to the secure area of the ECAs and PCAs 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 activate a new HSM. 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 Offsite 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 BlackBerry V2X CA keying ceremonies documentation.

A person can fulfill multiple roles as described in section 5.2.1, 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 *BlackBerry V2X CA 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 *BlackBerry PKI Services Personnel Disciplinary Procedure*.

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 Plan*.

### 5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

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 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 PKI Services 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 operations documents. 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 apart from automatically issued certificates 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 Audit 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.
- Serial or sequence number of entry (for automatic journal entries).
- 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 Audit Log Management* document.

### 5.4.3 RETENTION PERIOD FOR AUDIT LOG

CA Internal Auditor 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 Audit 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 per its risk assessment procedure which includes vulnerability scans/patches and annual review checklists.

## 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 one (1) year after corresponding certificate expiry and no less than seven (7) years, 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 *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

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

### 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. 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 ECA/PCA 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 *BlackBerry V2X CA Disaster Recovery and Business Continuity Plan (DRBCP)*.

As part of *BlackBerry V2X CA Security Incident Management Policy*, 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 *BlackBerry V2X CA 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.

### 5.7.3 ENTITIY 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 *BlackBerry V2X CA 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 (3 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 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.

## 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 activate 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 ECA and PCA 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 automatically without further human interaction. Access to an activated Sub-CA private key is controlled using a passphrase.

CA entity 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 BlackBerry V2X CA Organizational Chart. 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.

### 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 smart cards according to techniques specified by the module manufacturer. To activate a key, at least two trusted persons must present their smart cards together with the associated passwords.

For ECA and PCAs 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

A CA key stored in the HSM can be deactivated by performing a factory reset on the HSM. After a factory reset, all keys previously associated with the HSM are not usable.

#### 6.2.10 METHOD OF DESTROYING PRIVATE KEY

ECA and PCA private signing keys stored in HSMs are destroyed using the method offered by the cryptographic module.

#### 6.2.11 CRYPTOGRAPHIC MODULE RATING

See section 6.2.1.

### 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.

#### 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 be 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 *BlackBerry V2X CA Access Control Policy* and *BlackBerry PKI Services Password Management Procedure*.

### 6.4.2 ACTIVATION DATA PROTECTION

Data used to unlock private keys in cryptographic modules is 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

### 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*).

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 *BlackBerry V2X CA Software Installation and Maintenance Procedure*.

### 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 is performed continuously, with emergency security patching expedited and non-emergency patching planned on a quarterly release cycle.

## 6.7 NETWORK SECURITY CONTROLS

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 is extended to include hostnames for BlackBerry CA entities where applicable.

### 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 is not applicable to this CPS.

### 7.1.4 ENROLLMENT CA (ECA) CERTIFICATE PROFILE

The ECA certificate profile is listed below.

```
Enrolment CA
Name: eca.prod.v2xca.blackberry.com
Hash: b1024f6bddd4d14e8562589ece27f010d37ec7bc5fb937f4694543befd05dba4
Start: October 4, 2018
Duration: 40 years
Certificate: eca.prod.v2xca.blackberry.com_certificate.b64
Details:
Sequence (ExplicitCertificate) {
  Integer (3)
  Enumerated (CertificateExplicit(0))
  Choice (IssuerIdentifier) :
    [0] OctetString (
      dc 17 99 6c 9e 02 ea bd
    )
  Sequence (ToBeSignedCertificate) {
    Choice (CertificateId) :
      [1] UTF8 "eca.prod.v2xca.blackberry.com"
    OctetString (
      8d 7b bf
    )
    Integer (2)
    Sequence (ValidityPeriod) {
      Integer (465762046)
      Choice (Duration) :
```

```
            [6] Integer (40)
         }
         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 (
                     84 00 01
                  )
            }
         }
         Sequence (SequenceOfPsidGroupPermissions) {
            Sequence (PsidGroupPermissions) {
               Choice (SubjectPermissions) :
                  [1] Null
               Integer (1)
               Integer (0)
               BitString (
                  40
               )
            }
         }
         Sequence (PublicEncryptionKey) {
            Enumerated (AES_128_CCM(0))
            Choice (BasePublicEncryptionKey) :
               [0] Choice (EccP256CurvePoint) :
                  [3] OctetString (
                     95 77 0f 72 2f 7a ce 40    a0 33 0e 86 9a ce 9b 27
                     a2 4d 0c 95 d4 00 56 f1    19 cf b0 fe 54 a9 7d 21
                  )
         }
         Choice (VerificationKeyIndicator) :
            [0] Choice (PublicVerificationKey) :
               [0] Choice (EccP256CurvePoint) :
                  [2] OctetString (
                     a5 d6 94 88 db df 63 4b    52 a5 21 54 f5 11 b3 09
                     b1 ee aa 60 e0 1d 3d f0    1e c8 eb 4e b3 c2 97 e5
                  )
      }
      Choice (Signature) :
```

```
        [0] Sequence (EcdsaP256Signature) {
            Choice (EccP256CurvePoint) :
                [0] OctetString (
                    cc 03 9d dc 45 c5 04 cb    aa c9 d4 d8 c4 e3 53 8c
                    98 6d ed e6 98 91 17 21    6b 5a 1f 20 95 ec c0 62
                )
            OctetString (
                69 d4 4b 01 5a 8b 1e 50    01 08 f2 25 29 44 a2 f3
                c5 05 76 d9 26 dc 61 9d    08 ba cd 94 03 c7 b7 9f
            )
        }
}
```

### 7.1.5 PSEUDONYM CA (PCA) CERTIFICATE PROFILE

The PCA certificate profile is listed below.

```
Pseudonym CA
Name: pca.prod.v2xca.blackberry.com
Hash: 60d01c31b65ef1f1e765de4d6cf341713c06c957fb131fe284657773f307ea42
Start: October 4, 2018
Duration: 4 years
Certificate: pca.prod.v2xca.blackberry.com_certificate.b64
Details:
Sequence (ExplicitCertificate) {
    Integer (3)
    Enumerated (CertificateExplicit(0))
    Choice (IssuerIdentifier) :
        [0] OctetString (
            dc 17 99 6c 9e 02 ea bd
        )
    Sequence (ToBeSignedCertificate) {
        Choice (CertificateId) :
            [1] UTF8 "pca.prod.v2xca.blackberry.com"
        OctetString (
            8d 7b bf
        )
        Integer (2)
        Sequence (ValidityPeriod) {
            Integer (465762114)
            Choice (Duration) :
                [6] Integer (4)
        }
        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 (
                  85 00 01
               )
         }
      }
      Sequence (SequenceOfPsidGroupPermissions) {
         Sequence (PsidGroupPermissions) {
            Choice (SubjectPermissions) :
               [1] Null
            Integer (1)
            Integer (0)
            BitString (
               80
            )
         }
      }
      Sequence (PublicEncryptionKey) {
         Enumerated (AES_128_CCM(0))
         Choice (BasePublicEncryptionKey) :
            [0] Choice (EccP256CurvePoint) :
               [2] OctetString (
                  d0 8c 0e cd f7 81 44 2c    47 ae d0 8c ea 14 83 ce
                  50 16 42 f3 ce 90 26 e1    56 bd d4 07 6b ff 2a b4
               )
      }
      Choice (VerificationKeyIndicator) :
         [0] Choice (PublicVerificationKey) :
            [0] Choice (EccP256CurvePoint) :
               [3] OctetString (
                  40 7e b0 a7 98 10 b1 61    5b 90 52 aa c4 49 65 c4
                  f9 ae 5c 60 ae 4b 03 76    cf 26 4d 19 29 c7 5a 9e
               )
   }
   Choice (Signature) :
      [0] Sequence (EcdsaP256Signature) {
         Choice (EccP256CurvePoint) :
            [0] OctetString (
               1a f2 27 7a 47 57 a0 5e    fd 77 11 8a 3e 47 b8 0c
               fd 47 d1 fe 28 fe 53 4a    e5 c6 3f fc 1f aa c1 03
            )
         OctetString (
            92 3c c1 7e 9b 9c 44 c4    82 a6 ef 48 dd 9f ba 32
```

```
            72 40 66 a1 b6 84 7c 9a    81 09 cd 55 36 6d d8 16
        )
    }
}
```

### 7.1.6 ENROLMENT CERTIFICATE (EC) PROFILE

The EC profile is defined by CAMP.

### 7.1.7 RSE IDENTITY CERTIFICATE PROFILE

The RSE Identity certificate profile is defined by CAMP.

### 7.1.8 OBE IDENTITY CERTIFICATE PROFILE

The OBE identity certificate profile is defined by CAMP.

## 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")
```

CRLs generation is not relevant to this CPS.

# 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. Assessment requirements will be reviewed annually to determine which if any formal 3rd party assessments are relevant.

## 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

No stipulation.

## 8.4 TOPICS COVERED BY ASSESSMENT

Audits cover the topics indicated in the CP.

## 8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

In case of an ECA/PCA audit, depending on the audit result the PA may select from a number of options to resolve any deficiencies, including: modifying the governing CP, allowing a grace period for the ECA/PCA to undertake corrective actions to its certification practices, ordering a suspension of operations while the entity addresses audit issues, or revoking the entity and any related certificates and allowing the entity to resume operations only after re-submitting an acceptable audit report to the PA.

## 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 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

### 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.

### 9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION

An auditor's summary letter confirming the effectiveness of the controls set forth may not be 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.

### 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

No stipulation.

### 9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

Each Subscriber shall represent and warrant that it understands and shall comply in all material aspects with relevant portions of the BlackBerry V2X CA Certificate Policy and its Subscriber Agreement.

### 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

Term and termination policies are governed by the CP and relevant legal 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 V2X CA 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

No stipulation.

## 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

Other provisions are subject to applicable business agreements.

## 9.17 OTHER PROVISIONS

Other provisions are subject to applicable business agreement.

---

[i] References:

IEEE Std 1609.2™-xxx (Amendments of IEEE Std 1609.2-2016)

CAMP LLC documentation: https://stash.campllc.org/projects/SCMS/