BlackBerry | certicom

# BlackBerry V2X CA Certificate Policy

| | |
|---|---|
| **Date** | **August 10, 2020** |
| **Document Revision** | **1.2** |
| **Status** | **Approved** |

TABLE OF CONTENTS



 

 

 

 

 

 

 

 

 

 

# 1 INTRODUCTION

The BlackBerry V2X CA is a Certification Authority (CA) supporting vehicle-to-vehicle and vehicle-to-infrastructure ("V2X") digital certificate lifecycle management roles in a Security Credential Management System (SCMS), a specialized Public Key Infrastructure (PKI) architecture designed by the Crash Avoidance Metrics Partnership LLC. (CAMP) under a remit from the United States Department of Transportation (US-DOT).

This Certificate Policy (CP) establishes the technical, legal and business requirements governing the issuance, distribution, revocation and use of V2X certificates and the administration of the root and subordinate CAs associated with BlackBerry's V2X CA.

The CA derives technical requirements from CAMP's SCMS architecture and IEEE 1609.2 specifications. Operational requirements are drawn from established PKI trust services principles such as WebTrust Principles and Criteria for Certification Authorities v2.1 where applicable.

Although V2X certificates do not use an IETF X.509 certificate format 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

The SCMS, as depicted in Figure 1 below, is a distributed Public Key Infrastructure (PKI) whose purpose is to ensure the authenticity, integrity and privacy of safety critical wireless messages, or so-called V2X messages, sent between vehicles themselves and between roadside infrastructure and vehicles on North American roads and highways.

In this distributed PKI trust model, a trust realm is facilitated by Relying Party use of certificate chain files (CA trust lists) to bridge trust domains. Where trust domains operating under this policy are managed by BlackBerry as the top-level SCMS Manager, BlackBerry shall be considered the trust realm manager. The BlackBerry V2X CA may also participate in other trust realms including US-DOT Connected Vehicle Pilots and future national or transnationally sanctioned V2X Security Credential Management Systems.

## 1.2 DOCUMENT NAME AND IDENTIFICATION

This document is known as the "BlackBerry V2X CA Certificate Policy". X.509 Policy Object Identifiers (OIDs) are not included in IEEE 1609.2 certificates.

**Revision History**

| Date | Changes | Version |
|---|---|---|
| 29 Mar. 2018 | Final draft | - |
| 10 Apr. 2018 | Approved document | 1.0 |
| 28 Nov. 2018 | Policy updates, abridgement and clarifications prior to ECA/PCA launch. | 1.1 |
| 27 Feb. 2020 | Updates for CP and CPS consistency, and device enrolment authentication. | 1.1.1 |
| 10 Aug. 2020 | Adding in subsections as proposed by Deloitte. | 1.2 |

 

## 1.3 PKI PARTICIPANTS

Participants in the SCMS trust model may include CA trust elements, Subscriber organizations, Relying Parties and other participants as described below.

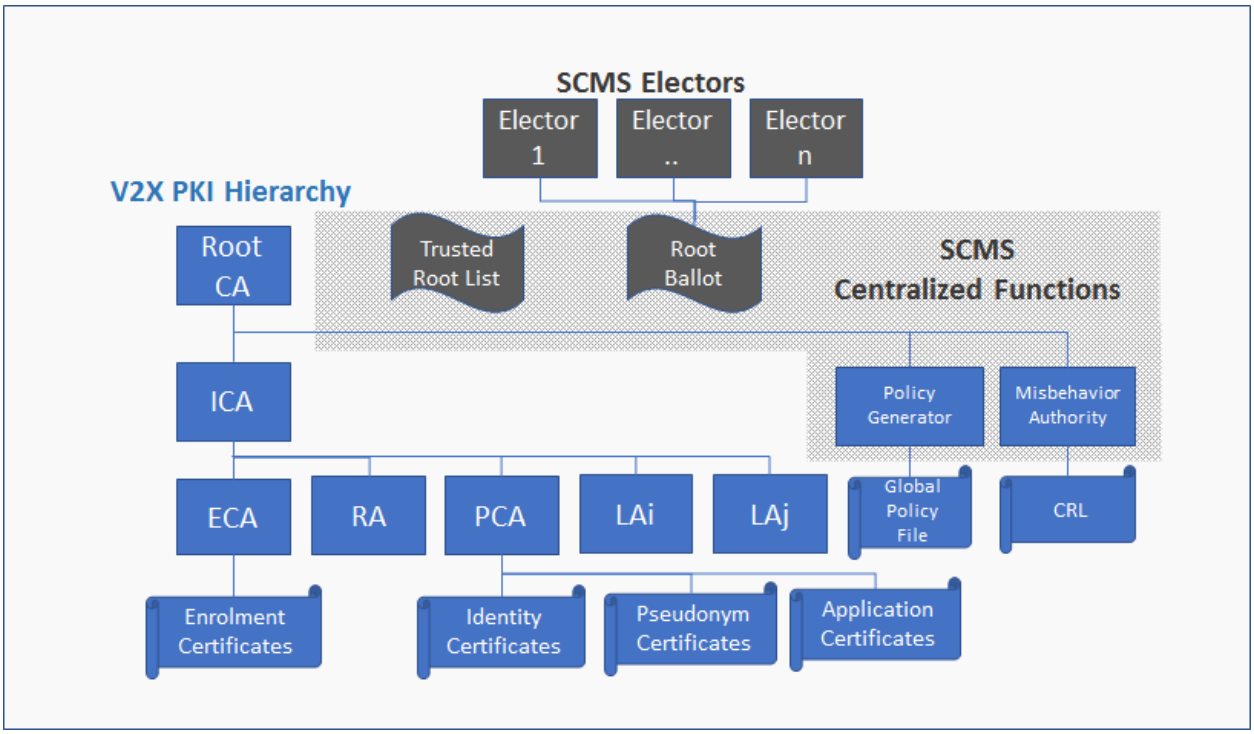


**Figure 1 Security Credential Management System Architecture**

### 1.3.1 CERTIFICATION AUTHORITIES

The CA, through its Policy Authority, is responsible for the management of certificates including registration, identification, authentication and issuance, and ensuring that all aspects of the CA services and CA operations related to certificates issued under the PKI are performed in accordance with its requirements, representations, and warranties.

The CA may issue and manage the following certificate types consistent with CAMP SCMS architecture and IEEE 1609.2 profile specifications:

- Certificates for an off-line self-signed Root CA (RCA)
- Certificates for Intermediate CAs (ICAs) signed by the RCA
- Certificates for a local or global CRL Generator (CRLG), Misbehavior Authority (MA), Policy Generator (PG)
- Enrolment CAs (ECAs), Pseudonym CAs (PCAs), Registration Authorities (RAs), and Linkage Authorities (LAs) subordinate to an ICA.

 

- End-entity Enrolment Certificates, Identity Certificates, Application Certificates and Pseudonym Certificates for certified V2X Onboard Equipment (OBEs) and Roadside Equipment (RSEs) issued by the CA's ECAs and PCAs.

RCA and ICA entities shall be offline trust elements with isolated security perimeters. ECA, PCA and other trust elements should be on-line to enable the CA to offer high-availability PKI services.

ECAs, PCAs and RAs under a BlackBerry V2X CA hierarchy may be operated by BlackBerry or under license by third parties such as an OEM, a certified ITS Station supplier or an IT service provider. In all cases such entities must implement certification policies and practices consistent with this CP.

### 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.

RAs may be operated by authorized entities other than BlackBerry, for instance an OEM customer (a Subscriber) may operate an RA for their own manufacturing line. Such an RA must at a minimum operate in compliance with this CP and commercial license agreements which bind the parties.

RAs must ensure that only properly enrolled end-entities which have not been revoked are issued end-entity certificates. The RA must maintain a blacklist to prevent revoked end-entities from receiving new certificates.

### 1.3.3 SUBSCRIBERS

Subscribers are OEM, Tier 1 automotive manufacturers, governments and road operator organizations who have signed Subscriber Agreements with BlackBerry to receive and use V2X end-entity certificates in their RSEs, OBEs or V2X applications. Subscribers must adhere to CP policies and use certificates and keying material in accordance with the CP to help ensure trust in the security and integrity of the CA.

A Device Configuration Manager (DCM) is a Subscriber's host or service entity in the SCMS architecture which interacts with the Enrolment CA to provision trust anchors, policy files, certificate chain files and enrolment certificates into Subscriber ITS Station modules. The DCM should act as a gatekeeper to enroll only certificate eligible devices with the ECA.

Subject to authorized agreement and conformity to this CP, Subscribers may also license to operate their own Enrolment CA (ECA) or Pseudonym CA (PCA) subordinate CAs, allowing them to manage local certificate issuance, for instance to optimize manufacturing operations.

### 1.3.4 RELYING PARTIES

Relying Parties (RPs) are entities which trust issuing CA certificates and rely upon the validity of CA-issued end-entity certificates to validate the authenticity of V2X messages.

 

### 1.3.5 OTHER PARTICIPANTS

In CAMP's SCMS architecture it is envisaged that an SCMS Manager's governance body will nominate independent Electors to ballot trusted CA roots into the SCMS trust realm using Elector signatures. Subject to policies and procedures dictated by the SCMS Manager's Policy Authority, Electors will use a voting scheme to revoke or add new root CAs. Electors may themselves be disenfranchised by a quorum of current Electors through a revocation ballot administered by the SCMS Manager.

A future SCMS Manager operating under the authority of the US-DOT and/or Transport Canada or an international legal convention is anticipated to set future SCMS V2X trust realm certification and governance policies such as CA and Elector eligibility.

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. The BlackBerry V2X CA Policy Authority may amend the CA's policies and certification practices to satisfy any future SCMS Manager requirements.

## 1.4 CERTIFICATE USAGE

### 1.4.1 APPROPRIATE CERTIFICATE USES

Certificates issued under this CP are intended to be used to sign and validate digital signatures for V2X communications and support the life cycle management (issuance, renewal, revocation) of V2X trust element and end-entity certificates in accordance with CAMP and IEEE 1609.2 specifications.

### 1.4.2 PROHIBITED CERTIFICATE USES

Certificates are neither intended nor authorized for use in any application aside from the appropriate certificate uses specified in this CP, nor in any transaction prohibited by law or legal agreement.

## 1.5 POLICY ADMINISTRATION

### 1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT

This CP, related agreements, and security policy documents referenced in this document are administered by the BlackBerry V2X CA Policy Authority, the "PA".

The PA's role includes the approval of the present and future Certificate Policy (CP) versions, authorization management, including defining, deciding and publishing CA approval procedures, approval of the CA's Certificate Practices Statements (CPSs) and its operation to adhere to published trust services principles and the scrutiny of audit reports.

 

### 1.5.2 CONTACT PERSON

All communications regarding these documents should be directed to:

Attn: BlackBerry V2X CA Policy Authority
BlackBerry Limited
4701 Tahoe Boulevard
Mississauga, Ontario
Canada L4W 0B5

Or by email: V2X_PA@BlackBerry.com

### 1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE POLICY

The BlackBerry V2X CA Policy Authority (PA) approves all CPS documents that affect the CA for conformance or suitability to the Policy.

The PA is comprised of senior management responsible for BlackBerry's Certicom business.

### 1.5.4 POLICY UPDATE AND CPS APPROVAL PROCEDURES

The PA shall review CA policies and operational status at least annually or more frequently if required to consider change requests to this CP, other relevant CPs or CPSs. Only the PA may approve amendments to the CP and related CPSs.

Depending on the impact of a proposed change, Subscribers and other stakeholders may be given notice of a proposed change to review and provide feedback. For any major change which impacts Subscriber operations, at least two weeks of review shall be allowed. Once approved, the revised CP shall be implemented and published, driving related changes to corresponding CPSs.

Revisions not denoted "significant" shall be those deemed by the BlackBerry V2X CA Policy Authority to have minimal or no impact on Subscribers and Relying Parties. Such revisions may be made without notice to users of this CP and without changing the version number of this CP and any correspondently changed CPS.

An amended CP shall be binding upon all Subscribers including the Subscribers and parties relying on certificates that have been issued under previous CP versions upon publication.

## 1.6 DEFINITIONS AND ACRONYMS

### 1.6.1 ACRONYMS

| | |
|---|---|
| CA | Certification Authority |
| CAMP | Crash Avoidance Metrics Partnership LLC |
| CP | Certificate Policy |

 

| | |
|---|---|
| CPS | Certification Practices Statement |
| CRL | Certificate Revocation List |
| CRLG | CRL Generator |
| DCM | Device Configuration Manager |
| DN | Distinguished Name |
| EA | Enrolment Authority |
| EC | Enrolment Credential |
| FIPS | Federal Information Processing Standard |
| IETF | Internet Engineering Task Force |
| LA | Linkage Authority |
| MA | Misbehavior Authority |
| NIST | National Institute of Standards and Technology |
| OBE | Onboard Equipment |
| OCSP | Online Certificate Status Protocol |
| OEM | Original Equipment Manufacturer |
| OID | Object Identifier |
| PA | Policy Authority |
| PC | Pseudonym Certificate |
| PCA | Pseudonym CA |
| PG | Policy Generator |
| PKI | Public Key Infrastructure |
| RA | Registration Authority |
| RP | Relying Party |
| RSE | Roadside Equipment |
| SCMS | Security Credential Management System |
| Sub-CA | Subordinate CA |

### 1.6.2 DEFINITIONS

**Applicant:** a legal entity or their authorized representative applying for certificate services from the CA who wishes to become a Subscriber.

**Certificate:** a record that uses a digital signature to bind a public key and an identity.

 

**Certificate Authority:** the entity responsible for all aspects of the issuance and management of its certificates, ensuring that all aspects of the CA services, operations and infrastructure related to certificates are performed in accordance with its stated policies and practices.

**Device Configuration Manager**: an entity which provisions certificate trust anchors and policy files to ITS Station modules.

**ITS Station:** a V2X roadside equipment (RSE) or onboard equipment (OBE) module.

**Key Pair:** a digital Private Key and its corresponding Public Key in an asymmetric cryptosystem.

**Linkage Authority:** an SCMS entity which generates linkage values to help identify anonymous Pseudonym Certificates.

**Private Key:** a secret key known only to the holder of the Key Pair which is used to create digital signatures.

**Public Key:** the key mathematically related to a corresponding Private Key in a Key Pair which is used by Relying Parties to verify digital signatures created by an entity using its Private Key.

**Relying Party:** an entity that relies upon the validity of a certificate to verify information signed by the entity to which the corresponding Private Key belongs.

**Repository:** A Repository defines a location for the storage of certificate authority information. This information may include certificates, certificate revocation list, certificate policies or certificate practice statements.

**Subject:** in X.509 terminology the identity of the entity to which a certificate is issued. In IEEE1609.2 parlance this is the certificate ID.

**Subscriber:** The Subscriber is a legal entity that has been licensed to be issued certificates by the CA.

**Subscriber Agreement:** The Subscriber Agreement is an agreement that must be read and accepted by an Applicant as part of establishing a business agreement for certificate services. The Subscriber Agreement is specific to the digital certificate product type. In some case an End User License Agreement (EULA) or customer license agreement may be used instead.

**Trust Element:** Root CAs, Intermediate CAs, Enrolment CAs, Pseudonym CAs, Registration Authorities, Linkage Authorities, CRL and Policy Generators and Elector systems and related infrastructure relied upon for the secure issuance and management of certificates.

**Trust Realm:** collective of trust domains in a distributed PKI.

 

# 2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

## 2.1 REPOSITORIES

The CA shall publish its currently active Root CA and ICA certificates in a publicly accessible repository and where applicable electronically distribute its CA certificate chains to Subscribers and Relying Parties: https://blackberry.certicom.com/en/legal/certicom-v2x-ca-repository

## 2.2 PUBLICATION OF CERTIFICATION INFORMATION

Repositories shall contain the following information.

- The current CP
- Issued (currently valid) root and ICA certificates
- CRLs for certificates revoked by the CA

CP and CPS documents are published upon their effect, with a change log indicating any updates made since the prior publication.

CA certificates may be published by an SCMS Manager via a Certificate Chain File.

## 2.3 TIME OR FREQUENCY OF PUBLICATION

An amended CP shall be published within 5 business days of the PA's approved effected date.

Re-keyed Root CA and ICA certificates must be published 5 business days before their effective date to allow copies of these certificates to be propagated prior to usage.

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

## 2.4 ACCESS CONTROLS ON REPOSITORIES

Access control to repositories of certification Information must comply at a minimum with the general standards of secure information handling as outlined in ISO/IEC 27001.

 

The CA or repository operator shall implement access controls in relation to all PKI participants and external parties for at least two different levels (e.g. public, restricted to CA level) and prevent unauthorized entities from adding, modifying, or deleting repository entries. These access control mechanisms shall be detailed in the entity's corresponding CPS.

 

# 3 IDENTIFICATION AND AUTHENTICATION

## 3.1 NAMING

### 3.1.1 TYPES OF NAMES

The id field for CA-issued certificates may contain linkage data, host names, or binary identifiers following IEEE 1609.2 specifications.

### 3.1.2 NEED FOR NAMES TO BE MEANINGFUL

CA issued IEEE 1609.2 certificates which contain a name should adhere to CAMP and IEEE 1609.2 naming conventions and use a fully-qualified domain name (FQDN) when securing any externally accessible CA interface.

The name should be pre-fixed by a function identifier (“rca”, ica”, “ma”, “pg”, and “crlg” for certificates issued by a root CA, and “eca”, “ra”, “pca” and “la” for certificates with names issued by an ICA).

### 3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

The CA shall support pseudonymous Subscriber end-entity certificate subjects as specified by IEEE 1609.2.

### 3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

See section 3.1.1.

### 3.1.5 UNIQUENESS OF NAMES

The CA shall ensure that the meaningful names in currently active certificates are unique.

### 3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

The CA should not knowingly issue a certificate with a name which it has determined infringes on the trademark of another and may revoke any certificate which becomes part of a trademark dispute.

 

## 3.2 INITIAL IDENTITY VALIDATION

The CA shall use only legal means to ascertain the identity of a certificate applicant and may, at its own discretion and for any reason, refuse a certificate request.

### 3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

All root CA and ICA certificate applicants shall prove that they rightfully hold the private key corresponding to the public key to be listed in the Certificate using IEEE 1609.2 or other relevant certificate request protocols. The CA shall check this proof.

### 3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

Organization entity validation shall be performed to provide strong assurance of the organization's legal status using 3rd party validation sources, government databases or documentation issued by an applicable government agency or recognized authority.

These procedures shall be documented in the CPS.

### 3.2.3 AUTHENTICATION OF INDIVIDUAL INFORMATION

A person authorized to act on behalf of an organizational Applicant or Subscriber must be validated using the individual's contact information including the name, title, company name, and email address.

This information may be validated using information in a legal agreement such as the Subscriber's license agreement or a registered agent agreement or via written authorization from management within the organization.

This information is treated as confidential as outlined in section 9.4.

### 3.2.4 NON-VERIFIED CERTIFICATE SUBJECT INFORMATION

No stipulation.

### 3.2.5 VALIDATION OF AUTHORITY

Every Subscriber shall define at least one representative person or role responsible for the authorization of requests for new certificates, revocations and renewals, including for any manual registration of ITS Stations at an ECA. The CA shall be notified as soon as possible of any changes to such representatives.

 

### 3.2.6 CRITERIA FOR INTEROPERATION

The CA shall take commercially reasonable steps to support SCMS interoperability for any externally accessible components of the CA or certificates issued thereby which are advertised to support standard SCMS interfaces and IEEE 1609.2 communications mechanisms.

Subscriber organizations likewise may be required to demonstrate compliance to published interoperability requirements prior to being authorized to receive certificates.

### 3.2.7 AUTHENTICATION OF SUBSCRIBER END-ENTITY DEVICE ENROLMENT

Authorized Subscriber representatives or their DCMs shall be used to authenticate end-entities requesting an Enrolment Certificate. Enrolment certificate request formats shall conform to CAMP and IEEE 1609.2 specifications.

End-entity subjects of PCs shall authenticate themselves when requesting certificates by using their unique Enrolment Certificate private key to present to the RA. The RA shall validate the signature, determine the end entity has not been revoked or blacklisted and if valid submit requests to the PCA.

Subscribers should also submit an OmniAir certification indicating all end-entity devices conform to standards. Devices that do not meet OmniAir certification will only be permitted to receive certificates at the discretion of the V2X CA Policy Authority.

## 3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

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

Prior to the expiration of an existing certificate, an entity should request a new certificate to maintain continuity of certificate usage and/or as required, an update of permissions, validity period, CRL, or a new key. The entity should submit the request as a certificate request along with instructions, if any, for the revocation of the old certificate once the new certificate is issued.

The method for identification & authentication for re-keying is the same as for the initial issuance of an initial certificate validation as described in section 3.2.2.

 

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

Re-keying shall be processed as a new request.

## 3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

CA RCA, ICA, RA, LA, ECA, PCA, CRLG, PG and MA certificates may be revoked upon approval of the Policy Authority. Revocation requests shall include circumstances for revocation and a period, if any, for which the to-be-revoked certificate is meant to remain un-revoked (e.g. to support key change over).

A Subscriber request to revoke its ECA, RA or PCA certificate shall be made in writing, signed by an authorized Subscriber representative, and authenticated by the CA using validation of authority procedures documented in 3.2.5.

An authorized Subscriber can request blacklisting for its own ECs via correspondence with the CA.

Pseudonym certificates are revoked by the CRL Generator at the direction of the CA upon request of the Misbehavior Authority and through coordination with Linkage Authorities and other external entities using IEEE 1609.2 and CAMP defined protocols.

 

# 4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

## 4.1 CERTIFICATE APPLICATION

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

The CA does not accept external certificate applications for RCAs or ICAs. Internal applications for ECA, PCA, RA, MA, PG and CRLG certificates are approve by the PA. Other internal certificate (DCM and test certificate) applications may be approved by the CA Operations Manager.

### 4.1.1 WHO CAN SUBMIT A CERTIFICATE APPLICATION

External applications for a certificate must come from an authorized individual or certified entity whose organization has signed and is currently licensed under the appropriate Subscriber Agreement. External stakeholders including government entities may be consulted in this process.

The CA may submit internal certificate applications for its own certificates.

### 4.1.2 ENROLLMENT PROCESS AND RESPONSIBILITIES

#### *4.1.2.1 RA, LA, DCM, ECA, PCA, MA, PG and CRLG Entities*

The CA verifies the authority of the applicant against registered documentation, checks the certificate request and proof of possession of Subscriber's public key. In case of positive checks the CA accepts the request.

#### *4.1.2.2 ITS Stations End-entities*

The initial registration of ITS Station end-entity subjects with the ECA is done by the Subscriber (manufacturer /road operator) through an authorized representative via a secure portal or through an authenticated DCM associated with the Subscriber.

An ITS Station 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. It is the Subscriber's responsibility to maintain the confidentiality of its EC private keys, however they are generated.

 

During the registration of an ITS Station the ECA must verify/ensure that the requested certificate profile including permissions inside the initial request are appropriate for the Subscriber.

Application, Identity and Pseudonym Certificates are issued by the PCA. Applications for these certificates are performed per CAMP specifications. The certificate requests are authenticated using Enrolment Certificates.

## 4.2 CERTIFICATE APPLICATION PROCESSING

### 4.2.1 PERFORMING IDENTIFICATION AND AUTHENTICATION FUNCTIONS

The CA shall verify and authenticate the identity and authority of each applicant as documented in its applicable CPS. This shall include verifying email, phone and address contact details of entity representative with written authorization from a management within the organization permitting the representative to act on behalf of the organization.

### 4.2.2 APPROVAL OR REJECTION OF CERTIFICATE APPLICATIONS

The CA verifies Subscriber certificate applications, inspecting relevant Subscriber qualifications from audit or test reports where relevant as well as the certificate request itself for conformity to IEEE 1609.2 and SCMS requirements.

Properly formatted and validated certificate requests submitted by authorized, validated entities where there is no concern with respect to Subscriber qualifications shall be approved and processed.

Entities submitting rejected applications shall be notified of the cause for rejection.

### 4.2.3 TIME TO PROCESS CERTIFICATE APPLICATIONS

The time to process a certificate application must be acted under a maximum time limit defined in the CPS, but no later than within 10 business days after a Subscriber Agreement has been signed and all documentation and authorizations relevant to the application have been received by the CA.

The CA shall make every reasonable effort to meet its issuance times and to make applicants aware of any factors that may affect issuance times in a timely manner, targeting normal issuance within 2 business days of receiving a fully executed Subscriber agreement and a valid certificate request. Worst case processing time should be no longer than 5 business days from completion of the relevant agreements and receipt of a valid certificate request.

 

## 4.3 CERTIFICATE ISSUANCE

### 4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE

CAs and Sub-CAs or RAs shall verify and authenticate the source of each certificate request and issue certificates in the manner detailed in their respective CPS.

Included in this process, the CA shall evaluate any information fields in the certificate request which require validation and ensure that these fields are correct. If validated the CA shall build and sign the certificate or otherwise shall reject the certificate request and allow the requestor to submit a corrected request.

Issuing CAs shall ensure that the public key is bound to the correct applicant, obtain a proof of possession of the private key where applicable, generate a properly formed certificate, and provide the certificate to the applicant based on flows and protocols specified in CAMP SCMS and IEEE 1609.2 specifications.

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

The CA shall notify Subscriber of issuance by email for any Sub-CAs issued or via automated responses defined by IEEE 1609.2 and CAMP for responses from SCMS ECA or RA interfaces.

## 4.4 CERTIFICATE ACCEPTANCE

### 4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE

The Subscriber or subject's software is responsible for installing the issued certificate on the Subscriber's computer, ITS Station or application according to the Subscriber's system specifications, and the "acceptable use" policy stated as part of the Subscriber Agreement, or other relevant agreements such as EULAs, between the CA and a Subscriber, or as part of this document.

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

The Subscriber should discard all certificates that are not correctly verified, inform the CA and send a new request.

 

### 4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA

Root CA and ICA certificates shall be published in the repository identified in section 2.1.

ECA, RA, PCA and end-entity certificates shall be distributed in Certificate Chain Files to individual Subscribers or their respective ITS Stations.

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

The CA shall direct stakeholders to its repository and notify relevant entities upon certificate issuance if new certificate availability might impact a Certificate Chain File or SCMS Manager function.

## 4.5 KEY PAIR AND CERTIFICATE USAGE

### 4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE

Subscribers must protect their private keys from unauthorized access or use and store their private keys in a secure manner.

Subscribers must use private keys and certificates only in accordance with the usages specified by this CP, IEEE 1609.2 and SCMS documentation.

### 4.5.2 RELYING PARTY PUBLIC KEY AND CERTIFICATE USAGE

Relying Parties (RPs) are informed of the correct usage and validation of digital signatures by means of the IEEE 1609.2 standard and SCMS documentation to which their application software or devices shall be expected to comply.

Before relying upon any signatures Relying Parties shall verify the validity of certificates by checking downloaded certificate revocation lists, certificate chains and repositories and verify the validity period and application permissions under which the certificate was issued.

Relying on an unverifiable or invalid digital signature may result in risks that the RP assumes in whole and which the CA does not assume in any way. Warranties, to the extent they are explicitly offered, are valid only if the steps detailed above have been carried out.

If the circumstances of reliance exceed the assurances delivered under the provisions of this CP or any license agreement no additional assurances are offered.

 

## 4.6 CERTIFICATE RENEWAL

The CA shall not support certificate renewals. Expiring certificate renewals shall be processed as initial certificate requests using a re-key process per Section 4.7.

## 4.7 CERTIFICATE RE-KEY

Certificates shall be re-keyed when a Subscriber requests a new certificate with different validity period be issued to a subject host or FQDN, identifying it as a re-key request. A re-key request shall be treated as original certificate request; however, it is not permitted to re-use the previously certified key pair and the requestor must inform the CA when the previously issued certificate, if not expired, may be revoked. In addition to the new validity period, new permissions or other information updates may be represented in the new certificate.

### 4.7.1 CIRCUMSTANCES FOR CERTIFICATE RE-KEY

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

### 4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY

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

### 4.7.3 PROCESSING CERTIFICATE RE-KEY REQUESTS

Certificate processing shall be treated as original certificate requests per Section 4.2.

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

### 4.7.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO CERTIFICATE SUBJECT

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

### 4.7.5 CONDUCT CONSTITUTING ACCEPTANCE OF RE-KEYED CERTIFICATE

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

 

### 4.7.6 PUBLICATION OF THE RE-KEYED CERTIFICATE BY THE CA

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

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

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

## 4.8 CERTIFICATE MODIFICATION

Certificates are modified when the CA or an authorized Subscriber requests a new certificate is to be issued for an existing host with a slightly modified FQDN and the same validity period but application permissions and/or other certificate information to be changed. A certificate modification request shall be treated as original certificate request; the requestor must inform the CA of the reason for the modification and when the previously issued certificate, if not expired, may be revoked.

### 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 used or widely deployed.

### 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 shall be 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 shall 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 shall be treated as original certificate requests per Section 4.3.

### 4.8.5 CONDUCT CONSTITUTING ACCEPTANCE OF MODIFIED CERTIFICATE

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

### 4.8.6 PUBLICATION OF THE MODIFIED CERTIFICATE BY THE CA

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

## 4.9 CERTIFICATE REVOCATION AND SUSPENSION

The CA may revoke its own certificates or those of a Subscriber because of a re-key or certificate modification, to protect the integrity of the CA due to suspicion of a compromised or misused key pair or due to premature termination of a Subscriber license agreement.

Revocation requests may also be accepted from CA stakeholders with contractual authority or legal jurisdiction such as Transport Canada, the US Department of Transportation or a designated Misbehavior Authority with cause to justify a revocation. A Subscriber's authorized representative may also request revocation of its own certificates.

The CA shall use a CRL to revoke an unexpired certificate, and where applicable providing notice by publishing the updated CRL in its repository to inform stakeholders that the certificate should no longer be relied upon.

Revocation of a CRL generator certificate shall mean ceasing the use of the CRL generator certificate private key to sign CRLs. The Root CA may issue a new CRL generator certificate which can then be used to add the revoked CRL generator certificate to the CRL.

### 4.9.1 CIRCUMSTANCES FOR REVOCATION

Certificate revocation may be performed for the following circumstances:

 

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

### 4.9.2 WHO CAN REQUEST REVOCATION

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

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

The CA may revoke and blacklist EC and PC end-entity certificates on consultation with a Misbehavior Authority or any reason the PA believes such said certificate usage is non-compliant with this CP or is a threat to road safety or the effectiveness and integrity of the SCMS.

### 4.9.3 PROCEDURE FOR REVOCATION REQUEST

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

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

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

 

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

Misbehavior Authority driven revocation of certificates issued by a PCA or ECA, when available, would be an automated process.

### 4.9.4 REVOCATION REQUEST GRACE PERIOD

The CA or Subscriber must make a revocation request without delay once a security concern or risk associated with a certificate has been identified and any risks associated with revocation have been fully considered.

A grace period of up to 30 business days may be afforded to a Subscriber in the event such grace period could not undermine the integrity or security of the CA.

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

CAs must process a revocation request within three business days of its approval.

### 4.9.6 REVOCATION CHECKING REQUIREMENT FOR RELYING PARTIES

Relying Parties must check the relevant CRL prior to relying upon a CA or Subscriber certificate, using software which properly processes trust path certification schemes as specified in IEEE 1609.2.

### 4.9.7 CRL ISSUANCE FREQUENCY (IF APPLICABLE)

See section 2.3.

### 4.9.8 MAXIMUM LATENCY FOR CRLS

The CA shall publish as soon as possible following revocation processing and within one business day or less of any revocation.

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

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

 

### 4.9.10 ON-LINE REVOCATION CHECKING REQUIREMENTS

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

### 4.9.11 OTHER FORMS OF REVOCATION ADVERTISEMENTS AVAILABLE

No stipulation.

### 4.9.12 SPECIAL REQUIREMENTS REGARDING KEY COMPROMISE

In the event the CA identifies a critical component such as a RCA, ICA, ECA, PCA or end-entity certificate such as an RA certificate has been compromised it shall temporarily halt operation of that component and perform an analysis to determine the source of the breach and act to mitigate damage to the PKI, including notification of Subscribers, RPs and other stakeholders about the compromise and its mitigation.

Where key compromise is not disputed the CA shall revoke issuing CA or Subscriber end-entity certificates and publish a revised CRL within 24 hours.

New certificates shall not be issued until the root cause of the compromise has been identified and if possible mitigated.

### 4.9.13 CIRCUMSTANCES FOR SUSPENSION

The CA does not support temporary suspension of certificate validity.

### 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

CA certificate status services may support a local trust domain or act in support of the SCMS Manager. When offered by the CA, CRL services shall support high availability access to Relying Parties.

### 4.10.1 OPERATIONAL CHARACTERISTICS

CRL repositories, where relevant, may be hosted by the CA or by a third-party service provider providing secure, reliable, high-availability access which can distribute CRLs to relying parties using SCMS CRL Generator methods described in CAMP and IEEE 1609.2 specifications.

### 4.10.2 SERVICE AVAILABILITY

Published CRLs shall be available 24x7 from a redundant, high availability service.

### 4.10.3 OPTIONAL FEATURES

No stipulation.

## 4.11 END OF SUBSCRIPTION

At the end of a Subscriber subscription, the CA will cease issuing certificates on a Subscriber's behalf. Other end of subscription conditions, if any, shall be subject to Subscriber license agreements.

## 4.12 KEY ESCROW AND RECOVERY

The CA does not escrow private keys.

### 4.12.1 KEY ESCROW AND RECOVERY POLICY PRACTICES

Not available.

### 4.12.2 SESSION KEY ENCAPSULATION AND RECOVERY POLICY AND PRACTICES

Not available.

 

# 5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The system shall be designed and operated in a manner such that adequate capacity and processing power and storage is available to meet CA capacity demands and reviewed periodically to address projected capacity and business continuity demands.

## 5.1 PHYSICAL CONTROLS

All trust model operations shall be conducted within a physically protected environment that deters and detects unauthorized use of, access to, or disclosure of sensitive information and to systems. Trust model elements shall use physical security controls in compliance with ISO 27001.

The CA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not activated. CA cryptographic tokens shall be protected against theft, loss, and unauthorized use. CA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated.

### 5.1.1 SITE LOCATION AND CONSTRUCTION

The locations and construction of the facilities housing the CA, equipment and data (HSM, activation data, backup of key pair …) shall be consistent with facilities used to house high value and sensitive information.

CA systems shall be operated in an environment separated into multiple progressively secure physical perimeters, with policies and procedures implemented to ensure that the physical environments are isolated from networks outside the trust model.

The Root CA shall be normally offline to further isolate it from other trust elements.

ECA, PCA and other trust elements may be operated online within a secure cloud computing environment so long as logical security controls are in place to isolate trust elements from other applications.

The security techniques employed should be designed to resist a large number and combination of different forms of attack. The mechanisms used include at minimum:

- Facility and room access controls
- Perimeter alarms, security cameras, reinforced walls and vibration or motion detectors.

 

### 5.1.2 PHYSICAL ACCESS

Equipment and data (HSM, activation data, backup of key pair, computer, log, key ceremony script, certificate request …) shall be protected from unauthorized access. The physical security mechanisms for equipment at a minimum shall be in place to:

- Provide at least four layers of increasing security to access sensitive root CA systems.
- Monitor, either manually or electronically, for unauthorized intrusion.
- Ensure no unauthorized access to the hardware and activation data is permitted.
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure, tamper-evident containers.
- Ensure only authorized personnel have physical access to HSMs
- Require two trusted roles to access HSM and activation data.
- At all times accompany and monitor any individual temporarily authorized to enter CA secured areas.
- Ensure an access log is maintained and inspected periodically.

Keys on removable cryptographic modules shall be deactivated prior to storage. When not in use, removable cryptographic modules and the activation data used to access or enable cryptographic modules shall be placed in a safe. Activation data shall either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module in a way that allows only one person having access to private key.

A security check of the facility housing equipment shall occur if the offline CA facility is to be left unattended. A trusted role person or group shall be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

### 5.1.3 POWER AND AIR CONDITIONING

Secure facilities of trust model elements including any certificate repositories which require 24X7 operation shall be equipped with reliable access to electric power to ensure operation with no major or minor failures. Primary and back-up power are required in case of external power failure to enable power sufficient for a minimum of 6 hours operation and a graceful shutdown

 

of the on-line trust model equipment in case of lack of power. Facilities shall be equipped with heating/ventilation/air conditioning systems to maintain the temperature and relative humidity of the trust model equipment within operational range.

### 5.1.4 WATER EXPOSURES

Secure facilities of trust model elements should be protected in a way that minimizes impact from water exposure.

### 5.1.5 FIRE PREVENTION AND PROTECTION

To prevent damaging exposure by flame or smoke, trust model element facilities shall be constructed, equipped and operated to address fire related threats. Media should be protected by fire resistant containers.

### 5.1.6 MEDIA STORAGE

Media used within the trust model elements should be securely handled to protect media from damage, theft and unauthorized access.

An inventory must be maintained for all information assets, with the definition of the protection requirements to those assets consistent with the risk analysis.

### 5.1.7 WASTE DISPOSAL

Trust model elements should implement procedures for the secure and irreversible disposal of waste (paper, media, or any other waste) to prevent the unauthorized use of, access to, or disclosure of waste containing Confidential/Private Information. All removable media used for the storage of sensitive information such as keys, activation data or files must be destroyed before being released for disposal.

### 5.1.8 OFF-SITE BACKUP

Back-ups of CA components, sufficient to recover from system failure, must be made after a CA deployment and after each new CA key pair generation.

Back-up copies of essential business information and software must be taken periodically. Adequate back-up facilities must be provided to ensure that all essential business information and software can be recovered following a disaster or media failure.

Back-up arrangements for individual systems should be periodically tested to ensure that they meet the requirements of the business continuity plan. At least one full backup copy must be

 

stored at an offsite location (disaster recovery). The back-up copy must be stored at a site with physical and procedural controls commensurate to that of the operational PKI system.

Access to backup data is subject to the same access requirements as the operational data. In case of complete loss of data, the required information for putting the CA back in operation shall be completely recovered from the backup data. Private CA key material shall not be backed up using standard back up mechanism, but rather using the process of the HSM for backing up sensitive keying material.

## 5.2 PROCEDURAL CONTROLS

### 5.2.1 TRUSTED ROLES

Employees, contractors, and consultants that are designated to fulfill trusted roles shall be considered “Trusted Persons”. Persons seeking to become Trusted Persons by obtaining a Trusted Position shall meet the screening requirements of this CP.

Trusted roles have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in certificate applications;
- the acceptance, rejection, or other processing of certificate applications, revocation requests, or renewal requests;
- the issuance, or revocation of certificates, including personnel having access to restricted portions of its repository or the handling of Subscriber information or requests.

Trusted roles include, but are not limited to:

- system administration,
- designated engineering, and
- executives that are designated to manage infrastructure trustworthiness.

The CA shall make a clear definition of all trusted roles in its CPS.

### 5.2.2 NUMBER OF PERSONS REQUIRED PER TASK

Trust model elements shall establish, maintain, and enforce rigorous control procedures to ensure the separation of duties based on trusted roles and to ensure that more than a single Trusted Person is required to perform sensitive tasks.

 

Policy and control procedures must be in place to ensure separation of duties based on job responsibilities. The most sensitive tasks, such as the access and the management of CA cryptographic hardware (HSM) and its associated key material must require the authorization of more than one Trusted Person.

### 5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE

All persons assigned a role as described in this CP should be identified and authenticated to ensure that said role enables them to perform their PKI duties.

Trust model elements shall verify and confirm the identity and authorization of all personnel seeking to become Trusted before such personnel are:

- issued with their access devices and granted access to the required facilities,
- given credentials to access and perform specific functions on CA systems.

### 5.2.4 ROLES REQUIRING SEPARATION OF DUTIES

Roles requiring separation of duties include but are not limited to:

- Access to sensitive CA areas
- the acceptance, rejection, revocation requests or other processing of CA certificate applications
- the generation, issuing or destruction of a CA certificate or keying material.

Segregation of duties may be enforced using PKI equipment, procedures or both.

## 5.3 PERSONNEL CONTROLS

### 5.3.1 QUALIFICATIONS, EXPERIENCE, AND CLEARANCE REQUIREMENTS

Trust Model elements shall employ enough personnel who possess knowledge, experience and appropriate qualifications necessary for the job functions and services offered. PKI personnel fulfill the requirements of "knowledge, experience and qualifications" through formal training and credentials, actual experience, or a combination of the two.

New CA personnel shall be subject to employment screening practices to provide assurance they have no criminal record or background which suggests untrustworthiness or unreliability.

 

### 5.3.2 BACKGROUND CHECK PROCEDURES

Trust model elements shall conduct background checks for personnel seeking to become Trusted Persons. Issues revealed in a background check may be grounds for rejecting candidates.

Reports containing such information shall be evaluated by human resources and concerns reported to the PA, taking actions that are reasonable considering the type, magnitude, and frequency of the behavior uncovered by the background check.

### 5.3.3 TRAINING REQUIREMENTS

Trust model elements shall provide their personnel with the requisite training needed to perform their job responsibilities relating to CA operations competently and satisfactorily. Training programs shall be periodically reviewed to ensure it address elements relevant to functions performed by their personnel. Training programs shall address the elements relevant to the role, including:

- security principles and mechanisms of the trust model elements,
- hardware and software versions in use,
- all duties the person is expected to perform and internal and external reporting processes and sequences,
- PKI business processes and workflows,
- incident and compromise reporting and handling, and
- disaster recovery and business continuity procedures, as well as
- sufficient IT knowledge.

### 5.3.4 RETRAINING FREQUENCY AND REQUIREMENTS

Trust model elements shall provide refresher training and updates to their staff to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

Individuals in trusted roles shall be made aware of changes in the PKI operations, with accompanying training where applicable.

 

### 5.3.5 JOB ROTATION FREQUENCY AND SEQUENCE

Job rotation frequency and sequence are not stipulated provided the technical skills, experience and proper access rights of roles are supported. The administrators of trust model elements shall ensure that any change in staff will not affect the security of the system.

### 5.3.6 SANCTIONS FOR UNAUTHORIZED ACTIONS

Each trust model element shall define a formal disciplinary process to ensure that unauthorized actions are appropriately sanctioned. In severe cases role assignments and corresponding privileges must be withdrawn.

### 5.3.7 INDEPENDENT CONTRACTOR REQUIREMENTS

Trust model elements may permit independent contractors or consultants to become Trusted Persons only under the condition that the contractors or consultants are trusted by the entity to the same extent as if they were employees and they fulfill the same requirements applicable to employees.

Otherwise, independent contractors and consultants shall have access to dedicated PKI equipment only to the extent they are escorted and directly supervised by Trusted Persons.

### 5.3.8 DOCUMENTATION SUPPLIED TO PERSONNEL

Trust model elements shall provide their personnel with requisite training and access to documentation needed to perform their job responsibilities competently and satisfactorily.

## 5.4 AUDIT LOGGING PROCEDURES

Audit log files shall be generated for all events relating to the security of the CA. Where possible, the security audit logs should be automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism should be used.

All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits. The security audit logs for each auditable event defined in this section shall be maintained in accordance with sections 5.4.3 and 5.5.2.

### 5.4.1 TYPES OF EVENTS RECORDED

Trust model elements, where applicable, should record the following types of audit events:

- Physical facility access

 

- Trusted roles management
- Logical access
- Data from the authentication process for Subscribers and trust model elements
- Acceptance and rejection of certificate applications
- ITS Station registration
- HSM management
- IT and network management
- Patching / change management

The audit logs shall not permit access to privacy related data according to General Data Protection Regulations concerning private vehicles.

### 5.4.2 FREQUENCY OF PROCESSING LOG

Event logs shall be reviewed in response to alerts based on irregularities and incidents within their CA systems and in addition periodically every year.

Audit log processing shall consist of a review of the event logs and documenting the reason for all significant events in an audit log summary. Audit log reviews shall include a verification that the log has not been tampered with, an inspection of all log entries, and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews shall be documented.

### 5.4.3 RETENTION PERIOD FOR AUDIT LOG

Log records shall be maintained for annual audit reviews. Summary records related to CA certificate life cycles should be kept at least one year after the corresponding certificate expires.

### 5.4.4 PROTECTION OF AUDIT LOG

Integrity and confidentiality of the audit log shall be guaranteed by a role-based access control mechanism. Internal audit logs may only be accessed by authorized personnel.

Users must not be able to modify their own log files.

Each electronic log entry shall be integrity protected where applicable.

 

Events must be logged in such a way that they cannot be easily deleted (except after transfer to long term media) within the period that they are required to be held.

Event logs must be protected to remain readable for the duration of their storage period.

### 5.4.5 AUDIT LOG BACKUP PROCEDURES

Audit logs and audit summaries must be backed up via enterprise backup mechanisms, under the control of authorized trusted roles, separated from their component source generation. Electronic audit log backups must be protected with the same level of access controls as defined for the original logs.

### 5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)

Trust model element equipment shall activate electronic audit processes at system startup and deactivate them only at system shutdown.

At the end of each operating period and at the operational life of CA private keys the collective status of equipment should be logged and reported to the Operations Management of the respective PKI element for a confirmation of deployed system assets.

### 5.4.7 NOTIFICATION TO EVENT-CAUSING SUBJECT

When an event is logged by the audit collection system, where applicable it must link the event to a trusted role.

### 5.4.8 VULNERABILITY ASSESSMENTS

The PKI auditor and PKI operations manager responsible for trust model elements must review and explain all significant events in an audit log summary. Such reviews involve verifying that event logs have not been tampered with, there is no discontinuity or other loss of audit data, and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. Actions taken as a result of these reviews must be documented.

Assessments shall include:

- Document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities.
- Implement detection and prevention organizational and/or technical controls under the control of the trust model elements to protect PKI systems against viruses and malicious software.

 

- Undergo or perform a vulnerability scan after any system or network changes that the trust model elements determine are significant for PKI component, and at least quarterly on public and private IP addresses identified by the CA as on-line PKI components and at least annually on off-line PKI components.
- Undergo a penetration test on the PKI's online systems on at least an annual basis; and
- Track and remediate vulnerabilities according to enterprise cybersecurity policies and risk mitigation methodology.

## 5.5 RECORDS ARCHIVAL

### 5.5.1 TYPES OF RECORDS ARCHIVED

Trust model elements shall archive records detailed enough to establish the validity of CA signatures and of the proper operation of the PKI. These shall include events records related to physical and logical access, CA operations, key generation and certificate issuance.

The trust model elements shall retain all documentation relating to certificate requests and the verification thereof, and all root CAs and CA Certificates and revocation thereof.

### 5.5.2 RETENTION PERIOD FOR ARCHIVE

All records shall be maintained by the corresponding CA at least three (3) years after the corresponding certificates have expired.

### 5.5.3 PROTECTION OF ARCHIVE

Trust model elements shall store the archive of records in a secure storage facility or secure, distributed network archive.

The archive shall be protected against unauthorized viewing, modification, deletion, or other tampering by storage within a trustworthy system.

### 5.5.4 ARCHIVE BACKUP PROCEDURES

Trust model elements may be backed up in any manner which allows a Disaster Recovery operation to be successfully performed with records available in sufficient detail to address audit logging requirements.

 

### 5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS

Trust model elements managing archive records must be securely synchronized with an accepted time source.

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

### 5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL OR EXTERNAL)

No stipulation.

### 5.5.7 PROCEDURES TO OBTAIN AND VERIFY ARCHIVE INFORMATION

Trust model elements shall allow only authorized Trusted Personnel to obtain access to the archive.

## 5.6 KEY CHANGEOVER

The CA shall generate a new CA key pair and a corresponding new certificate before expiry of current certificates.

The validity period of the new CA certificate shall start prior to the planned deactivation of the current private key. The CA shall take care that the new certificate is distributed to relevant Subscribers and Relying Parties before the start of its validity period.

The old CA private key shall be deactivated and not be used to issue certificates once the new CA certificate becomes valid.

## 5.7 COMPROMISE AND DISASTER RECOVERY

The CA shall have recovery procedures in place to reconstitute the CA in accordance with service level agreements in the event of a catastrophic failure, as described in the following subsections.

### 5.7.1 INCIDENT AND COMPROMISE HANDLING PROCEDURES

Trust model elements shall monitor equipment and detect potential hacking attempts or other forms of compromise. If compromise is detected the trust model element shall perform an investigation to determine the nature and the degree of damage and a mitigation plan.

 

Where relevant, CA entities must alert Subscriber and applicable stakeholders which are under agreement with CA to allow them to activate their own incident management plans.

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

If a disaster is discovered that prevents the proper operation of a trust model element, the trust model element shall suspend its operation and investigate whether also the private key has been compromised.

The corruption of computing resources, software, and/or data shall be reported to CA management within 24 hours for the highest levels of risk. All other events need to be included in the periodic CA management reports.

### 5.7.3 ENTITY PRIVATE KEY COMPROMISE PROCEDURES

If the private key of a CA is compromised, lost, destroyed or suspected of being compromised, the CA shall:

- suspend its operation,
- start the disaster recovery and migration plan,
- investigate the issue which generated the compromised situation and notify the superior CA or Policy Authority, which may order certificate revocation,
- alert all Subscribers with which an agreement exists.

### 5.7.4 BUSINESS CONTINUITY CAPABILITIES AFTER A DISASTER

The entities operating secure facilities for CA operations shall develop, implement and maintain a disaster recovery plan designed to mitigate the effects of any kind of natural or man-made disaster. Disaster recovery plans address the restoration of information systems services and key business functions.

## 5.8 CA AND RA TERMINATION

The CA shall provide at least 90 days' notice to Subscriber of its intent to assign its CA operations and Subscriber Agreement, or at least 180 days' notice of its intent to terminate CA service without assignment. Where applicable, it shall assign Subscriber licenses and transfer relevant PKI data and archives to an authorized assignee.

 

In the case of a severe compromise of the CA with no ability to recover, the CA shall suspend certificate issuance immediately.

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

- Provide Subscribers and relevant stakeholders and regulatory authorities notice of termination.
- Stop issuing certificates with validity periods beyond the proposed termination or suspension date.
- 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.

In the event of the termination of the CA services, the CA shall be responsible for keeping all relevant records regarding the needs of CA and PKI components.

 

# 6 TECHNICAL SECURITY CONTROLS

## 6.1 KEY PAIR GENERATION AND INSTALLATION

### 6.1.1 KEY PAIR GENERATION

The CA key pair generation process shall fulfill the following requirements:

- Each CA participant shall generate its own key pairs according to section 6.1.5 and 6.1.6 following specifications detailed in the National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS PUB) 186-4 Digital Signature Standard.
- Private keys for CA and Sub-CA and CRL signing entities shall be generated within and protected by a Hardware Security Module (HSM) which has been NIST validated to FIPS 140-2 Level 3 standards.
- The CA shall ensure that the integrity and authenticity of its public keys and any associated parameters are maintained during distribution to Sub-CA participants.

Root CA key pair generation must be witnessed by an independent 3rd party auditor to create a verifiable audit trail that proves the security requirements for procedures were followed. The audit trail must identify and document any failures or anomalies in the key generation process, and any corrective actions taken. The documentation of the procedure must be detailed enough to show that appropriate role separation was used.

### 6.1.2 PRIVATE KEY DELIVERY TO SUBSCRIBER

No explicit private keys are delivered to Subscribers.

### 6.1.3 PUBLIC KEY DELIVERY TO CERTIFICATE ISSUER

A public key must be delivered to the CA in a manner which allows the CA to determine the requestor's proof of the possession of the private key.

### 6.1.4 CA PUBLIC KEY DELIVERY TO RELYING PARTIES

CA and Sub-CA certificates shall be published as described in section 2.2.

 

### 6.1.5 KEY SIZES

The CA shall support at least one signature algorithm required in IEEE 1609.2-2016 as specified by FIPS 186-4.

### 6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

Public key parameters must be generated and checked in accordance with NIST FIPS 186-4.

### 6.1.7 KEY USAGE PURPOSES

CA Key usages must adhere to key usages specified for corresponding entities in CAMP SCMS and IEEE 1609.2 specifications.

## 6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

### 6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

Cryptographic modules shall ensure that CA private keys are not accessible in clear text outside the cryptographic module. Cryptographic modules shall include an access control mechanism to prevent unauthorized use of private keys.

The relevant standard for cryptographic modules is FIPS 140-2 “Security Requirements for Cryptographic Modules”. The module shall be validated to FIPS 140-2 Level 3.

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

For the Root CA or ICA, a single person shall not be permitted to invoke the complete CA signature process or access any cryptographic module containing the CA private signing key.

Manual activation of keys in a cryptographic module shall require two-factor authentication involving at least two authorized trusted personnel.

For on-line Sub-CAs (i.e. ECAs and PCAs), at least two token holders must be required to activate a private key. Once activated a Sub-CA may perform signature processes automatically.

### 6.2.3 PRIVATE KEY ESCROW

There is no stipulation on private key escrow.

 

### 6.2.4 PRIVATE KEY BACKUP

Generating, storing and use of backups of private keys shall fulfill the requirements of at least the same security level as required for the original keys. A CA private key shall never leave an HSM in plaintext form.

### 6.2.5 PRIVATE KEY ARCHIVAL

CA and Sub-CA private keys shall not be archived except in encrypted form.

### 6.2.6 PRIVATE KEY TRANSFER INTO OR FROM A CRYPTOGRAPHIC MODULE

Transfer of private keys into or from a cryptographic module shall fulfill the requirements of at least the same security level as required for the original keys.

### 6.2.7 PRIVATE KEY STORAGE ON CRYPTOGRAPHIC MODULE

Storing of private keys shall fulfill the requirements of at least the same security level as required for the original keys.

### 6.2.8 METHOD OF ACTIVATING PRIVATE KEY

CA private keys stored in cryptographic modules must be activated using a minimum of two authorized persons with activation tokens.

### 6.2.9 METHOD OF DEACTIVATING PRIVATE KEY

The private keys stored on the HSM shall be deactivated as recommended by the manufacturer.

### 6.2.10 METHOD OF DESTROYING PRIVATE KEY

The destruction of the private key shall be done using the mechanism described by the cryptographic module manufacturer.

### 6.2.11 CRYPTOGRAPHIC MODULE RATING

See section 6.2.1**Error! Reference source not found.**.

 

## 6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

### 6.3.1 PUBLIC KEY ARCHIVAL

The CA shall retain copies of all CA public keys for archival in accordance with section 5.5 for at least three (3) years after any certificate based on these public keys ceases to be valid.

### 6.3.2 CERTIFICATE OPERATIONAL PERIODS AND KEY PAIR USAGE PERIODS

All certificates and corresponding keying materials shall have maximum validity and operational periods not exceeding those in SCMS and IEEE 1609.2 specification. It is assumed that certificates exceeding NIST recommended key lifetimes may be re-keyed in future.

Overlap of certificate lifetimes shall allow sufficient time for the introduction of re-keyed certificates and certificate chains prior to the expiry of old certificates. CA private keys should be retired from signing subordinate certificates in ample time to accommodate the key changeover process.

## 6.4 ACTIVATION DATA

Activation data or authentication factors required to operate cryptographic modules and access protected keys should be either biometric in nature or memorized. If written down, activation data shall be physically secured or encrypted under a FIPS approved cryptographic algorithm and not be stored with the cryptographic module.

### 6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION

No stipulation.

### 6.4.2 ACTIVATION DATA PROTECTION

The CA uses a combination of cryptographic and physical access control mechanisms to protected activation data. The CA uses smart cards to control the use or activation of a private key.

### 6.4.3 OTHER ASPECTS OF ACTIVATION DATA

No stipulation.

 

## 6.5 COMPUTER SECURITY CONTROLS

The controls of the CA shall be designed according to an ISO/IEC 17799 code of practice for information security management controls with control objectives to address risks related to the confidentiality, integrity and availability of CA assets.

### 6.5.1 SPECIFIC COMPUTER SECURITY TECHNICAL REQUIREMENTS

The Issuing CA PKI components must include the following functions:

- Require authenticated logins for trusted role;
- Provide discretionary access control with least privilege;
- Provide security audit capability;
- Require use of strong password policy;
- Require use of cryptography for session communication;
- Require trusted path for identification and authentication;
- Provide means for malicious code protection;
- Provide means to maintain software integrity;
- Provide domain isolation and partitioning different systems and processes. For accounts capable of directly causing certificate issuance, Issuing CA shall enforce multifactor authentication.

### 6.5.2 COMPUTER SECURITY RATING

No stipulation.

## 6.6 LIFE CYCLE TECHNICAL CONTROL

The CA’s technical controls shall be designed to encompass the whole life cycle of the CA, including concerns for crypto agility, how equipment is procured, installed, maintained, and updated.

### 6.6.1 SYSTEM DEVELOPMENT CONTROLS

The CA's system development controls are as follows:

 

- Use software that has been designed and developed under a formal, documented development methodology;
- Hardware and software procured are purchased in a fashion to reduce the likelihood that any particular component was tampered with;
- Hardware and software are developed in a controlled environment;
- All hardware must be shipped or delivered via controlled methods;
- The hardware and software are dedicated to performing CA activities. There are no other applications, hardware devices, network connections, or component software installed which are not part of the CA operation;
- Proper care is taken to prevent malicious software from being loaded onto the equipment; and
- Hardware and software updates are purchased or developed in the same manner as original equipment; and are installed by trusted and trained personnel in a defined manner

### 6.6.2 SECURITY MANAGEMENT CONTROLS

The CA follows a change management process for all modifications and upgrades required, such changes are documented and controlled by CA team as a means to detect unauthorized modifications to the systems. All software to be loaded is checked to ensure software is modifications free and intended software version.

### 6.6.3 LIFECYCLE SECURITY CONTROLS

The CA's technical controls are designed to encompass the whole life cycle of the CA, including concerns for crypto agility, how equipment is procured, installed, maintained, and updated.

## 6.7 NETWORK SECURITY CONTROLS

The Root CA and ICA shall be operated in an isolated, normally off-line security facility. External certificate requests shall be scanned for malware prior to processing.

ECA, PCA and other on-line CA trust elements shall be protected by firewalls and an intrusion prevention system in dedicated secure datacenters which offer resilient, dedicated external network links.

## 6.8 TIME STAMPING

See section 5.5.5.

 

# 7 CERTIFICATE, CRL, AND OCSP PROFILES

## 7.1 CERTIFICATE PROFILES

The CA shall issue digital certificates conforming to IEEE 1609.2 and CAMP SCMS specifications. Name spaces, where applicable, shall be extended to include BlackBerry or Subscriber hostnames.

All certificates shall indicate permissions for the types of certificates, messages or data which they may sign.

At the beginning of the overlapping time of successive CAs, enrolment credential and pseudonym certificates shall be issued by the new entity for distribution to Subscribers and Relying Parties. During the overlapping time expiring CA certificates shall only be used for verification.

The BlackBerry name spaces for the certificates are:

| Trust Element | Name |
|---|---|
| RCA | `rca.prod.v2xca.blackberry.com` |
| ICA | `ica.prod.v2xca.blackberry.com` |
| ECA | `eca.prod.v2xca.blackberry.com` |
| PCA | `pca.prod.v2xca.blackberry.com` |
| RA | `ra.prod.v2xca.blackberry.com` |
| LA1 and LA2 | `la1.prod.v2xca.blackberry.com` and `la2.prod.v2xca.blackberry.com` |
| MA | `ma.prod.v2xca.blackberry.com` |
| PG | `pg.prod.v2xca.blackberry.com` |
| CRLG | `crlg.prod.v2xca.blackberry.com` |

## 7.2 CRL PROFILE

CRLs issued by a CA under this policy shall conform to IEEE 1609.2 and SCMS specifications. CRLs may be aggregated to a central CRL Generator.

 

### 7.2.1 VERSION NUMBERS

The CA shall issue CRLs in compliance with IEEE 1609.2 standards.

### 7.2.2 CRL AND CRL ENTRY EXTENSION

No stipulation.

## 7.3 OCSP PROFILE

No stipulation.

### 7.3.1 VERSION NUMBERS

No stipulation.

### 7.3.2 OCSP EXTENSION

No stipulation.

# 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The CA shall select an independent, certified auditor to verify that the CA operates in accordance with the applicable CP and CPS according to AICPA/CICA WebTrust for Certification Authorities principles and criteria.

The audit shall include all requirements of this Certificate Policy to be fulfilled by the CA to be audited. The scope of the audit shall cover all processes mentioned in its CP and CPS, the premises and responsible persons.

## 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 assessor shall have the following qualifications:

- Qualifications and experience: Auditing must be the individual's or group's primary business function. The individual or at least one member of the audit group must be qualified as a Certified Information Systems Auditor (CISA), an AICPA Certified Information Technology Professional (CPA.CITP), a Certified Internal Auditor (CIA), or have another recognized information security auditing credential.
- Expertise: The individual or group must be trained and skilled in the auditing of secure information systems and be familiar with public key infrastructures, certification systems, and the like, as well as Internet security issues (such as management of a security perimeter), operations of secure data centers, personnel controls, and operational risk management.
- Rules and standards: The individual or group must conform to applicable standards, rules, and best practices promulgated by the Canadian Institute of Chartered Accountants, the American Institute of Certified Public Accountants (AICPA), the Institute of Chartered Accountants of England & Wales (ICAEW), the International Accounting Standards adopted by the European Commission (IAS), Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), or another qualified auditing standards body.
- Reputation: The firm must have a reputation for conducting its auditing business competently and correctly.
- Disinterest: The firm must have no financial interest, business relationship, or course of dealing that could foreseeable create a significant bias for or against the CA.

## 8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

In addition to the foregoing prohibition on conflicts of interest, the assessor shall have a contractual relationship with the CA for the performance of the audit, but otherwise, shall be independent.

## 8.4 TOPICS COVERED BY ASSESSMENT

Topics covered by the annual CA audit shall include but are not limited to CA business practices disclosure (i.e., this CP), the service integrity of CA operations and the environmental controls that are implemented to ensure a trustworthy system.

Customers operating their own ECAs, or PCAs under CA license referencing this CP must undergo their own annual audits and report any exceptions or irregularities and the steps taken to remedy them to the PA.

 

## 8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports any material noncompliance with applicable law, this CP and any associated certification practices or contractual obligations related to the CA services described herein, the CA shall develop a plan to cure such noncompliance, subject to the approval of the PA and any third party to whom the CA is legally obligated to satisfy.

In the event the CA fails to take appropriate action in response to the report, the PA may instruct the Operations Manager to revoke the certificates affected by such non-compliance and/or suspend the CA until such corrective measures are taken or a mitigating Certificate Policy or Certification Practices Statement is approved.

## 8.6 COMMUNICATION OF RESULTS

The results of all audits under this CP shall be reported to the PA and any appropriate entities, as may be required by law, regulation or legal agreement. At its option, the CA may provide interested parties with the letter containing the attestation of management and its auditor's letter concerning the effectiveness of controls. Otherwise, all audit information will be considered confidential business information in accordance with section 0.

 

# 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

The CA is entitled to charge fees to its registered PKI participants. Any fees charged by BlackBerry Certicom V2X PKI certificate services are subject to business agreements.

### 9.1.1 CERTIFICATE ISSUANCE OR RENEWAL FEES

No stipulation.

### 9.1.2 CERTIFICATE ACCESS FEES

No stipulation.

### 9.1.3 REVOCATION OR STATUS INFORMATION ACCESS FEES

No stipulation.

### 9.1.4 FEES FOR OTHER SERVICES

No stipulation.

### 9.1.5 REFUND POLICY

No stipulation.

## 9.2 FINANCIAL RESPONSIBILITY

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

### 9.2.1 INSURANCE COVERAGE

The CA shall maintain adequate insurance for its business and activities with terms, limits and conditions including Cyber Security (Network Liability and Privacy Liability) and Technology Professional Liability (Errors & Omissions Liability) consistent with those reasonably expected to

 

be obtained by similarly situated prudent and responsible organizations in its industry and those insurance as applicable law may call for.

#### 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

The BlackBerry V2X CA keeps business information such as legal agreements, operations plans, disaster recovery plans and production information and procedures confidential. It uses reasonable security controls corresponding to the sensitivity of the information to prevent the exposure of such records to the public or unauthorized personnel. Customer names may be publicly disclosed by agreement or disclosed to certain 3rd parties as required by applicable regulations.

#### 9.3.1 SCOPE OF CONFIDENTIAL INFORMATION

The CA shall specify and define information to be held confidential within CPS.

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

Any information not categorized as confidential within the CPS may be deemed public information.

#### 9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION

The CA shall contractually obligate employees and contractors to protect confidential information. The CA shall provide training to employees on how to handle confidential information

### 9.4 PRIVACY OF PERSONAL INFORMATION

The BlackBerry V2X CA keeps personal information such as customer contacts and information about specific vehicles confidential and uses reasonable security controls to prevent the exposure of such records to the public or unauthorized personnel.

 

The application of the BlackBerry's privacy policy is subject to applicable laws including legislation, regulations and the orders of courts or other lawful authorities, lawful requests for information or legal processes.

### 9.4.1 PRIVACY PLAN

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

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

### 9.4.2 INFORMATION TREATED AS PRIVATE

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

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

### 9.4.3 INFORMATION NOT DEEMED PRIVATE

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

### 9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION

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

### 9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION

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

### 9.4.6 DISCLOSURE PURSUANT TO JUDICIAL OR ADMINISTRATIVE PROCESS

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

 

- The party to whom BlackBerry owes a duty to keep information confidential.
- The party requesting such information.
- A valid & enforceable, uncontested court order, if any.

### 9.4.7 OTHER INFORMATION DISCLOSURE CIRCUMSTANCES

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

## 9.5 INTELLECTUAL PROPERTY RIGHTS

The CA shall operate in a manner with protects BlackBerry's rights and respect the rights of its Subscribers and business associates.

"BlackBerry" and "Certicom" are registered trademarks of BlackBerry. BlackBerry may have other trade and service marks that have not been registered, but that nonetheless are and shall remain the property of BlackBerry.

"WebTrust" is a trademark of the Canadian Institute of Chartered Accountants.

## 9.6 REPRESENTATIONS AND WARRANTIES

### 9.6.1 CA REPRESENTATIONS AND WARRANTIES

BlackBerry represents that the BlackBerry V2X CA shall comply in all material aspects with this CP, its related certification practices and their corresponding internal policies and procedures and all applicable regulations regarding the CA's operation. Except as stated in this CP and relevant business agreements, BlackBerry makes no other representations or warranties regarding its BlackBerry V2X CA service, expressed or implied.

BlackBerry reserves its right to modify such representations at its discretion or as required by law.

### 9.6.2 RA REPRESENTATIONS AND WARRANTIES

No stipulation.

### 9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES

Each Subscriber shall represent and warrant that it will:

- Materially comply with the terms and conditions of its Subscriber agreement and relevant aspects of this Certificate Policy.

 

- Provide correct and accurate information in communications with the CA and when requesting any certificate and confirm the accuracy of certificate data prior to its use.
- Minimize risk of private key compromise by ensuring that they and their agents or representatives have adequate knowledge, training, processes and procedures, and use appropriately secure hardware for generating and using private keys.
- Use certificates for legal and authorized purposes in accordance with the terms and conditions expressed in the Certificate Policy and Subscriber Agreement.
- Cease using the certificate if any information in it becomes obsolete or invalid or its private key is suspected of compromise.
- Request the revocation of a certificate in case of any occurrence where compromise of said certificate is suspected or information in the certificate might materially affect the integrity of the PKI.

Without limiting other Subscriber obligations stated herein, a Subscriber alone is solely responsible for any representations or warranties it makes to third parties.

Upon accepting a certificate, the Subscriber represents to BlackBerry and to Relying Parties that at the time of acceptance and until further notice:

- All representations made by the Subscriber to BlackBerry regarding the information contained in a valid certificate are accurate and true to the best of the Subscriber's knowledge.
- Transactions effectuated using the private key corresponding to the public key included in the certificate are the acts of the Subscriber and that the certificate has been accepted and is properly operational at that time and until further notice to BlackBerry.

### 9.6.4 RELYING PARTY REPRESENTATIONS AND WARRANTIES

By accepting V2X CA roots in its trust list, a Relying Party accepts that to reasonably rely on a BlackBerry V2X CA certificate, the Relying Party must:

- Use software compliant with IEEE 1609.2 as profiled by CAMP and approved by US-DOT and published CAMP specifications.
- Verify the certificate by referring to the relevant CRL to determine its status and the status of all CA certificates in its trust chain.
- Trust a certificate only if it and all CA certificates in the certificate trust chain are valid and unexpired.
- Take any other reasonable steps to minimize the risk of relying on a digital signature created by an invalid, revoked or expired certificate.

 

### 9.6.5 REPRESENTATIONS AND WARRANTIES OF OTHER PARTICIPANTS

Not applicable.

## 9.7 DISCLAIMERS OF WARRANTIES

Except as represented and warranted in this Certificate Policy or as explicitly stated in applicable business agreements, BlackBerry disclaims all warranties express or implied.

## 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

This Certificate Policy and any amendments hereto shall become effective upon publication in the Repository and shall remain in effect until replaced with a newer version or terminated. The process of updating this CP and effect of any change to it or its corresponding CPS which may impact Subscribers shall be communicated to Subscribers as described in Section 1.5.4.

## 9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Notices or enquires to the BlackBerry V2X Policy Authority should be directed to:

Attn: BlackBerry V2X CA Policy Authority
BlackBerry Technology Solutions - Certicom 4701 Tahoe Boulevard
Mississauga, Ontario
Canada L4W 0B5

By email: V2X_PA@BlackBerry.com
By telephone: +1-905-507-9473

## 9.12 AMENDMENTS

Section 1.5.4 describes the procedure for amending the BlackBerry V2X CA Certificate Policy and corresponding certification practices.

 

## 9.13 DISPUTE RESOLUTION PROVISIONS

Provisions governing BlackBerry V2X CA services and potential dispute resolution mechanisms are specified in applicable business agreements.

## 9.14 GOVERNING LAW

Unless otherwise agreed explicitly in a business agreement, BlackBerry V2X CA services are governed by, and construed in accordance with, the laws of the Province of Ontario, Canada. This choice of law is made to ensure uniform interpretation of this CP, regardless of the place of residence or place of use of BlackBerry V2X CA digital certificates or other services.

## 9.15 COMPLIANCE WITH APPLICABLE LAW

The BlackBerry V2X CA shall aim to comply with all applicable laws and regulations.

## 9.16 MISCELLANEOUS PROVISIONS

Other provisions would be subject to applicable business agreements.

## 9.17 OTHER PROVISIONS

Other provisions may be found in applicable business agreement.

 