BlackBerry | certicom

Device CA Certificate Policy

Version 1.9.2

Effective Date: 30 June 2022

BlackBerry Limited

1 INTRODUCTION

The Device CA Certificate Policy (CP) is targeted at applications requiring ECDSA and RSA based X.509 Public Key Certificates (PKCs), ECQV PKCs, or AMS Mini-Cert PKCs used for BlackBerry products. The Device CA operation is geared toward applicatoins with high-volume device manufacturing environments having bulk certificate requirements.

1.1 Overview

This CP is written for PKCs targeted at electronic devices supporting the ZigBee Alliance Smart Energy Profile, the AMS Mini-Cert Profile, and devices supporting X.509 certificate profiles. X.509 certificate profiles are consistent with the Internet Engineering Task Force (IETF) Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile described in RFC 5280.

This CP is consistent with the IETF Public Key Infrastructure X.509 (PKIX) Certificate Policy and Certification Practices Framework as described in RFC 3647.

The Device Certificate Authority (CA) issues the following certificate types:

- X.509 certificate types including CA, subordinate CA (Sub-CA), Administrative, AMS Appliance and Controller Identity, and SSL PKCs,
    - An administrative PKC is an end entity certificate issued to individuals who are administering device PKCs on behalf of an organization.
    - An AMS Appliance and Controller Identity PKC is an end entity certificate issued to appliances and controllers belonging to BlackBerry Certicom's Asset Management System.
    - An SSL PKC is an end entity certificate issued to SSL clients and servers.
- Device certificate types including the AMS Mini-Cert and ZigBee Smart Energy PKCs.
    - An AMS Mini-Cert is a PKC is issued to devices and paired with an AMS Appliance or Controller Identity PKC.
    - A ZigBee Smart Energy PKC is issued to devices conforming to the ZigBee Smart Energy Profile.

It provides a root of trust for the Device CA Public Key Infrastructure (PKI). The PKI uses a hierachical trust model to fulfill Relying Party (RP) requirements for X.509 PKCs.

ZigBee Smart Energy PKCs use an implicit trust model, although the Sub-CA that issues these PKCs is part of the hierarchy of trust created by the CA.

AMS Mini-Certs use an explicit trust model relying upon the Sub-CA that issues them and the AMS Controller or Appliance Identity PKC they are paired with.

This CP is structured so that information on a specific certificate type is delegated to a Device CA Certification Practices Statement (CPS). The following CPSs complement this document.

- Device CA Asset Management System CPS

  This CPS provides additional information on the AMS CA. These CAs issue Device PKCs, called AMS Mini-Cert PKCs, AMS Controller and Appliance Identity PKCs, and AMS SSL Client and Server PKCs.

- Device CA X.509 CPS

  This CPS provides additional information on X.509 certificate types. CAs for these certificate types issue Sub-CA, Device, Administrative, and SSL PKCs.

- Device CA ZigBee Smart Energy Profile CPS

  This CPS provides additional information on ZigBee Smart Energy CA. This CA issues Device PKCs. The administration of these PKCs requires an Administrative PKC. Administrative PKCs fulfill the requirements of the Device CA X.509 CPS.

1.2 Document name and identification

This CP is known as the "Device CA CP." It uses the Object Identifier (OID) { 1.3.132.8.5 } to indicate the PKCs issued under this CP.

1.2.1 Revision History

Date	Changes	Version
3-17-2007	First Version (DRAFT)	0.5
4-24-2007	Changes to Sections 9.6.1 & 9.8 (David Lewis)	1.0
11-07-2008	Made consistent with RFC 3647.	1.1
23-07-2008	Finalized revisions for ZigBee and X.509 CPS.	1.2
19-08-2008	CPS is now Certification Practices Statement everywhere.	1.3
7-Oct-2008	Introduction of multiple administrative certificates for an organization.	1.4
30-Jan-2009	Added AMS PKCs.	1.5
25-Mar-2010	Updated sections 4.12, 6.2 through 6.4 and 6.6 to better reflect the handling and transportation of archive material to data recovery center.	1.6
08-Aug-2014	Updated building address, changes to Section 5.1.2, 5.2 and 5.5.1.	1.7

12-Feb-2018	Removed ecourier CPS. Removed administrator role and added ZPC role. Transferred responsibility of audit log review from Configuration Administrator to CA Operations Manager. Transferred vetting responsibility from Customer Support Personnel to CA Operator. Updated role of Customer Support Personnel and transferred some of this role's responsibilities to ZPC.	1.8
30-Mar-2020	Updated legal entity name, logo, and document names. Modified approver for certificate revocation.	1.9
19-Jan-2021	Updated Zone 3 exit requirement, added vulnerability management to Support Personnel trusted role.	1.9.1
28-Jun-2022	Minor updates for annual review. This CP is public; other CA specific documents are subject to the specific certification practices (CPSs) of each corresponding CA.	1.9.2

1.3 PKI participants

1.3.1 Policy authority

The Policy Authority (PA) is the Device CA Policy Authority.

The Device CA PA approves all agreements (i.e., CP, CPS, RP agreements, and Subscriber agreements) that affect the PKI (see sections 1.3.2 through 1.3.5).

1.3.2 Certification Authorities

The CA is responsible for all aspects of the issuance and management of PKCs including:

- Registration,
- Identification and authentication,
- Issuance, and

- Ensuring that all aspects of the CA services and CA operations and infrastructure related to PKCs issued under the PKI are performed in accordance with the requirements, representations, and warranties of the CP.

The CA supporting the PKI is organized as follows:

- A CA is the entity that creates, signs and issues PKCs to Sub-CAs.
- A Sub-CA is the entity that creates, signs and issues PKCs to Administrators and Devices.

CAs and Sub-CAs are part of the certification path that issues Device and Administrator PKCs. The CA, Sub-CA, and Administrator certificate profiles are consistent with the IETF Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile described in RFC 5280.

CAs do not issue Device PKCs. CAs issue only Sub-CA PKCs. Sub-CAs issue only Device and Administrator PKCs.

Every PKC conforms with a certificate type supported by the PKI. The following certificate types are supported:

- The AMS Mini-Cert certificate type conforms to a proprietary certificate profile developed for the BlackBerry Certicom Asset Management System Mini-Cert Certificate Profile.
- The Smart Energy Certificate type conforms to the ZigBee Alliance Smart Energy Profile.
- The X.509 Certificate type consistent with the IETF Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile described in RFC 5280.

A CPS establishes the practices concerning lifecycle services of each certificate type provided by a Subject CA.

1.3.3 Registration authority

No stipulation.

1.3.4 Subscribers

A subscriber is the entity identified by the subject of a PKC and who asserts that the PKC and the keying material will be used in accordance with this CP. A subscriber is an organization who has been issued an X.509,or Device PKC.

An Administrative PKC identifies a person in an organization as an authorized contact for the administration of that organization’s Device PKCs. Multiple administrative PKCs can be issued to

the same organization.

An X.509 SSL PKC identitifes an client or server connected using the SSL or TLS protocols.

A Device PKC identifies an electronic device.

1.3.5 Relying Parties

Devices and Organizations are RPs of the PKI. In this document, RPs validate PKCs issued to Devices and Adminstrators in conformance with this CP.

The Subject CA CPS for each certificate type describes the services available to an RP for verifying the validity of a PKC.

1.3.6 OCSP Responder

No stipulation.

1.3.7 Other Participants

No stipulation.

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

PKCs issued pursuant to this CP may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage fields within the PKC.

The CPS for each respective Subject CA defines all permitted key usages.

1.4.2 Prohibited certificate uses

PKCs issued under the provisions of this CP may not be used for any application requiring fail-safe performance. Examples of these applications include, but are not limited to, the following:

1. the operation of nuclear power facilities,
2. air traffic control systems,
3. aircraft navigation systems,
4. weapons control systems,
5. any system whose failure could lead to injury, death or environmental damage, and

6. any transactions where applicable law prohibits the use of encryption or digital certificates for such transactions or where otherwise prohibited by law.

1.5 Policy administration

This CP, related agreements, and security policy documents referenced in this document are maintained by the Device CA Policy Authority (PA).

All communications regarding these documents should be directed to:

Attn.: Device CA Policy Authority

c/o Device CA Operations Manager
BlackBerry Certicom
4701 Tahoe Boulevard, Building A
Mississauga, ON
L4W OB5
CANADA

1.6 Definitions and Acronyms

AMS	Asset Management System
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
DN	Distinguished Name
IETF	Internet Engineering Task Force
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PKC	Public Key Certificate
PKI	Public Key Infrastructure
RP	Relying Party
RA	Registration Authority

Applicant: The Applicant is a business with which the CA has an agreement to supply PKCs.

Device: A device is an end-entity owning a PKC.

Certificate Authority: The Certificate Authority is responsible for all aspects of the issuance and management of a PKC including: registration, identification and authentication, issuance, and ensuring that all aspects of the Certificate Authority services and Certificate Authority operations and infrastructure related to PKCs issued under the CP are performed in accordance with the requirements, representations, and warranties of their respective Subject CA CPS.

Certificate Authority Certificate: A self-signed and self-issued certificate in which the Certificate Subject and the Certificate Issuer are the same entity. The *keyCertSign* key usage bit is asserted in these certificates.

Relying Party: The Relying Party is a device or entity that relies upon the information contained within the PKC.

Subscriber: The Subscriber is a business that has been issued an X.509 or Device PKC.

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 as presented during the contract negotiations and is available as part of a valid business agreement between the CA and the Applicant

Subordinate Certificate Authority Certificate: A cross-certificate having a Certificate Issuer different from the Certificate Subject. The *keyCertSign* key usage bit is asserted in these certificates.

Relying Party Agreement: The Relying Party Agreement if applicable is an agreement which must be read and accepted by a business prior to installing certificates into devices and prior to validating, relying on or using a PKC or accessing or using the Repository. It may be available as part of a valid business agreement between the CA and the Applicant.

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

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The CA maintains several information repositories. These repositories contain the following information.

- X.509 PKC revocation information.
- This CP, certificate terms and conditions, relying party agreement, and the subscriber agreement.

2.2 Publication of Certification Information

This CP is published at https://blackberry.certicom.com/en/products/zigbee-certicom-device-authentication-service.

Specific certificate terms and conditions, relying party agreement, the subscriber agreement, and the CA and Sub-CA PKCs are considered private for each CA. The publication of this information and all other X.509 certificate types and Device PKCs and their revocation information is detailed in their respective Subject CA CPS.

2.3 Time or Frequency of Publication

CA and Sub-CA X.509 PKCs are published in accordance with an underlying CPS.

CRLs containing X.509 PKC revocation information where applicable are published every 24 hours and prior to the expiry of the current CRL.

The frequency of publication of Administrative PKCs, Device PKCs and CRL information is detailed in their respective Subject CA CPS.

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 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.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

Within the PKI, the Certificate Subject Name in an X.509 PKC must be an X.501 Distinguished Name (DN) carried in the PKC. The following name forms are supported:

- CA: CN= Certicom <curve identifier or key size> ROOT CA<n>, O=Certicom Corp., C=CA,
- Sub-CA: CN=<defined by Manufacturer>, OU=<defined by Manufacturer>, O=<manufacturer>, C=<country>, L=<defined by Manufacturer>, and
- X.509 PKCs are named as described in their respective Subject CA CPS.
- Device PKCs are named as described in their respective Subject CA CPS.

When the naming element is DirectoryString (i.e., O=, OU=, and L=) either PrintableString or UTF8String is used. The following determines which choice is used:

- PrintableString only if it is limited to the following subset of US ASCII characters (as required by ASN.1):
  A, B, …, Z
  a, b, …, z
  0, 1, …9,
  (space) ‘ ( ) + , - . / : = ?
- UTF8String for all other cases, e.g., subject name attributes with any other characters or for international character sets.

3.1.2 Meaningfulness

The Common Name (CN=) and Organization (O=) attributes in the Certificate Issuer field of PKCs issued by the CA unambigously identify “Certicom Corp” as the issuer, unless this is a hosted CA PKC.

The Organization (O=) and Organizational Unit (OU=) attributes in the Certificate Subject of Sub-CA and hosted CA PKCs unambigously and accurately identify the legal entity that is the subject of the certificate.

The meaningfulness of the Certificate Subject field of X.509 and Device PKCs is described in their respective Subject CA CPS.

3.1.3 Anonymity or Pseudonymity of Subscribers

The CA does not issue PKCs containing anonymous or pseudonym names.

3.1.4 Rules for Interpreting Various Name Forms

See section 3.1.1.

3.1.5 Uniqueness of Names

The Common Name (CN=) of the Certificate Subject field of all CA and Sub-CA PKCs is unique.

The uniqueness of the Common Name (CN=) of the Certificate Subject field of all X.509 and Device PKCs is detailed in their respective Subject CA CPS.

3.1.6 Recognition, Authentication, and Role of Trademarks

CAs do not knowingly issue a PKC with a name that a court of competent jurisdiction has determined infringes on the trademark of another.

CAs issuing PKCs to Sub-CAs that include trademark-protected names must verify that applicant is authorized to request on behalf of the trademark owner. If the Sub-CA includes an organizational unit name that is trademarked, then the trademark must be owned by the applicant.

The recognition, authentication, and role of trademark-protected names in all X.509 and Device PKCs are detailed in their respective Subject CA CPS.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

All X.509 certificate requests are submitted using a PKCS #10 certification request.

A Device PKC certificate request may be submitted using a PKCS #10 certification request. If a Device PKC is requested without submitting a PKCS #10 certification request then the generation and protection of the keying material for that device is detailed in the Subject CA CPS.

3.2.2 Authentication of Organization Identity

The information used to authenticate an organization for purposes of certificate issuance are disclosed as part of the Subscriber Agreement. It is treated as confidential for the purposes of the privacy and protection of data as outlined in Section 9.4 of this CP.

The following information is required to authenticate an organization.

1. A valid and current License Agreement for the organization.

2. Organization contact information, including the name, title, company name, department, address, email address, telephone numbers of primary, technical, and billing contacts.

3. DUNS Number, a nine-digit number assigned to an organization by Dun & Bradstreet, (www.dnb.com).

Additional authentication requirements are described in the Subject CA CPS.

3.2.3 Authentication of Individual Information

The following information is required to authenticate an individual subscriber or a person acting on behalf of an organizational subscriber.

1. Individual contact information including the name, title, company name, department, address, email address, telephone and fax numbers.

The identification and authentication requirements for an individual subscriber or person acting on behalf of an organizational subscriber are described in the Subject CA's CPS.

This information is treated as confidential as outlined in Section 9.4 of this CP.

3.2.4 Non-Verified Certificate Subject Information

Only a verified Organization ID and vetted MAC address information is included in PKCs. Subscriber "ownership" of MAC addresses is not verified. Optional attributes in PKC requests are not verified.

3.2.5 Validation of Authority

The primary contact shall be contacted via email or telephone using the email or telephone numbers provided in section 3.2.2 to provide the identity validation.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-Key Requests

3.3.1 Identification and Authentication of Routine Re-Key and Renewal Requests

Prior to X.509 PKC expiration, or at the time of contract renewal, a Subscriber shall request or be prompted to re-key. Re-keying is allowed in accordance with Section 4.7.

The CA does not re-key Device PKCs except under special agreement with licensee.

3.3.2 Identification and Authentication of Re-Key and Renewal After Revocation

The CA does not re-key or renew after revocation. Subscribers must re-submit a certificate request, as described in Section 3.2.

3.4 Identification and Authentication for Revocation Request

See Section 4.9.3 (Procedure for Revocation Request).

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can Submit a Certificate Application

All applications for a PKC must come from an authenticated individual or organization.

4.1.2 Enrollment Process and Responsibilities

A recognized individual or administrator must provide their credentials to CAs to demonstrate their identity, to demonstrate their authority, and to provide contact information.

CAs receive and approve requests for Sub-CA PKCs from the Device CA PA.

Sub-CAs receive and approve requests for Device and X.509 PKCs from an administrator whose identity and authorization has been established.

A request for an X.509 PKC, other than a CA or Sub-CA PKC, requires an out of band communication that the individual requesting the PKC is authorized to request it. This out of band communication requires confirmation with the organization's primary contact that the individual requesting the PKC is authorized to do so.

CA and Sub-CA PKCs are authorized by the Device CA PA and the certification requests for these PKCs are generated and fulfilled during the CA and Sub-CA key ceremonies.

Additional enrollment requirements may be specified in the Subject CA CPS.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

CAs and Sub-CAs verify and authenticate the identity of each applicant, as described in Section 3.2.

X.509 and Device PKC identification and authentication functions are performed as described in their respective Subject CA CPS.

4.2.2 Approval or Rejection of Certificate Applications

The CA approves or rejects a certification request. Approval is granted if the applicant's identity has been authenticated as described in Section 3.2, and payment, if required, has been received.

Rejection is based on inability to successfully authenticate the applicant, not receiving

required information from the applicant, or not paying for the PKC (if required).

4.2.3 Time to process certificate applications

The CA makes reasonable efforts to confirm certificate application information and issue a PKC within a reasonable time frame. The time frame is specified in the individual Business agreement with a worst case service time of 5 business days.

From time to time, events outside of the control of the CA may delay the issuance process. However, 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.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

CAs and Sub-CAs verify and authenticate the source of each PKC certificate request.

If a PKCS #10 certification request is provided, CAs and Sub-CAs ensure that the public key is bound to the correct applicant, obtain a proof of possession of the private key, generate a properly formed PKC, and provide the PKC to the applicant.

If a PKCS #10 certification request is not provided, CAs and Sub-CAs ensure that key pairs are generated, generate a properly formed PKC, encrypt the private key, and provide the encrypted private key and PKC to the applicant.

Device PKCs are issued in the manner detailed in their respective Subject CA CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The CA notifies the subscriber of PKC issuance via download or shipping notfications.

Notifications of certificate issuance are sent to the subscriber’s electronic mail address. It includes instructions for downloading certificates and private key. FTP access is provided to the subscriber for a limited time period.

The subscriber’s electronic email address is provided to the CA through an enrollment form obtained as part of the initial entity validation (see section 3.2).

Additional information is detailed in the Subject CA CPS.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The subscriber is responsible for installing the issued certificate on the subscriber's computer, token, device, or application according to the subscriber's system specifications, and the "acceptable use" policy stated as part of the Subscriber Agreement between the CA and a Subscriber or as part of the this document and the Subject CA CPS.

Acceptance of a PKC is described in the respective Subject CA CPS.

4.4.2 Publication of the Certificate by the CA

CA, and Sub-CA PKCs are published in the repository identified in section 2.2.

The publication of X.509 PKCs, other than CA and Sub-CA PKCs is detailed in their respective Subject CA CPS.

The CA records and maintains evidence of issued PKCs and their uniqueness in such a way that they are protected against changes and loss (see the Device CA Internal Audit Policy document).

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

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 and store their private keys in a secure manner.

Only the Certificate Subject may have access to the Subject's private key.

Subscribers must use private keys only in accordance with the usages specified in their respective Subject CA CPS. See Sections 1.4.1, 6.1.7, and 7.1.

4.5.2 Relying Party Public Key and Certificate Usage

An RP must adhere to the policies under which the PKC is issued (including the key usage extension field in the PKC).

Reliance is accepted as reasonable under the provisions made for the RP under this CP, the Subject CA CPS, and within the Relying Party Agreement, if applicable. If the circumstances of reliance exceed the assurances delivered by the PKI under the provisions of this CP then the RP must obtain additional assurances.

All X.509 PKCs must be validated and checked against the relevant CRL prior to use. PKCs are issued to a Subscriber for a specific purpose and the private key associated with the PKC may only be used in accordance with the usages specified in this CP.

Relying on an unverifiable digital signature may result in risks that the RP assumes in whole and which the CA does not assume in any way.

RPs are informed of the corrected usage and validation of digital signatures and authentication, by means of this CP, any applicable CPS, and other documentation published in its public repository and available from the Device CA Policy Authority (see Sections 2.2 and 9.11 of this CP).

Warranties are valid only if the steps detailed above have been carried out.

RP use of the public key in a Device PKC is described in their Subject CA CPS.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

CA and Sub-CA PKC renewal is described in their Subject CA CPS.

All other X.509 PKC and Device PKC renewal is described in their Subject CA CPS.

4.6.2 Who May Request a Certificate Renewal

Who may request an X.509 or Device PKC renewal is described in their Subject CA CPS.

4.6.3 Processing Certificate Renewal Requests

The processing of X.509 and Device PKC renewals is described in their Subject CA CPS.

4.6.4 Notification of New Certificate Issuance to Certificate Subject

Notification of X.509 and Device PKC renewal is described in their Subject CA CPS.

4.6.5 Conduct Constituting Acceptance of Renewal Certificate

Acceptance of renewed X.509 and Device PKC is described in their Subject CA CPS.

4.6.6 Publication of the Renewal Certificate by the CA

Publication of renewed X.509 and Device PKC by the CA is described in their Subject CA CPS.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

X.509 PKCs may be re-keyed as described in their Subject CA CPS.

4.7.2 Who May Request Certification of a New Public Key

Who may request an X.509 or Device PKC re-key is described in their Subject CA CPS.

4.7.3 Processing Certificate Re-Key Requests

The processing of X.509 and Device PKC re-key is described in their Subject CA CPS.

4.7.4 Notification of New Certificate Issuance to Certificate Subject

Notification of X.509 and Device PKC re-key is described in their Subject CA CPS.

4.7.5 Conduct Constituting Acceptance of Re-Keyed Certificate

Acceptance of re-keyed X.509 and Device PKC is described in their Subject CA CPS.

4.7.6 Publication of the Re-Keyed Certificate by the CA

Publication of re-key X.509 and Device PKC by the CA is described in their Subject CA CPS.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate modification

4.8.1 Circumstances for Certificate Modification

PKCs are not modified under any circumstances.

4.8.2 Who May Request Certificate Modification

No stipulations.

4.8.3 Processing Certificate Modification Requests

No stipulations.

4.8.4 Notification of New Certificate Issuance to Certificate Subject

No stipulations.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulations.

4.8.6 Publication of the Modified Certificate by the CA

No stipulations.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulations.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

The circumstances under which an X.509 and a Device PKC may be revoked are detailed in their respective Subject CA CPS.

4.9.2 Who can Request Revocation

The Device CA PA can revoke a PKC for any reason.

Who can request a revocation of an X.509 PKC is described in their respective Subject CA CPS.

4.9.3 Procedure for Revocation Request

Prior to the revocation of a PKC, the revocation request is verified. Verification requires that the revocation request is:

- Made by an entity with legal jurisdiction and authority to request revocation.

Additional procedures employed to verify revocation requests are defined in the Subject CA CPS.

4.9.4 Revocation Request Grace Period

There is no revocation grace period.

4.9.5 Time Within Which CA Must Process the Revocation Request

Authenticated revocation requests are fulfilled within 24 hours.

4.9.6 Revocation Checking Requirement for Relying Parties

No stipulation.

4.9.7 CRL Issuance Frequency

See section 2.3.

4.9.8 Maximum Latency for CRLs

No stipulation.

4.9.9 On-Line Revocation/Status Checking Availability

No stipulation.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements for CA Key Compromise

The CA will use commercially reasonable efforts to notify potential RPs if it discovers or suspects that a CA's Private Key has been compromised.

4.9.13 Circumstances for Suspension

No stipulation.

4.9.14 Who can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

No stipulation.

4.12 Key Escrow and Recovery

4.12.1 Private Key Escrow and Recovery Policies and Practices

Escrow and recovery of subscriber private keys is not performed.

Escrow and recovery of CA and Sub-CA private keys is defined in the "Device CA Escrow and Recovery Policies".

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

Security requirements imposed on a conforming CA are indicated in the Subject CA CPS. In every case, this policy states that CA must be run on a dedicated workstation. The workstation must be physically secured.

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

5.1.1 Site Location and Construction

The site is located at BlackBerry Limited in Mississauga, Ontario, Canada.

The site includes the grounds surrounding the building, the elevator lobbies, the reception area, and the area limited to BlackBerry personnel and escorted visitors. The site covers Zone 1 and Zone 2 (see BlackBerry PKI Services Physical Security Policy).

The construction of the facility housing the CA equipment is consistent with facilities used to house high-value, sensitive information. Requirements for constructing the facility included reinforced doors, walls, ceilings, and floors, video surveillance of facility, as well as shock and motion sensors.

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

5.1.2 Physical Access

Physical access to the site is restricted to employees and escorted visitors. Physical access controls on the site include the following.

- Site access requires a pass key to pass through electronic door locks. Door locks include remote monitoring, alarm, and dispatch of security personnel to address alarm events.
- Site access points are under video surveillance.

Physical access to the facility (the high security zone, or Zone 3) is restricted to employees on the Permanent Authorized Access List, the Special Authorized Access List and escorted visitors. The addition and removal of employees on each list, along with the activities permitted when visitors are present are defined in the BlackBerry PKI Services Physical Security Policy.

Physical access controls on the facility include the following.

- Facility access requires pass key and pass code to pass through electronic door locks. Door locks include remote monitoring, alarm, and dispatch of security personnel to address alarm events.
- Facility access requires a key to pass through one physical door bolt.
- Facility access requires dual person badge access to enter and exit Zone 3.
- Facility contains a safe requiring two combinations to open.
- Facility access points are under video surveillance.
- Facility is under video surveillance.
- Logs are kept of all access, including names and roles of escorted visitors.

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

5.1.3 Power and Air Conditioning

The Facility has sufficient power and air conditioning to ensure the reliable operation of all equipment related to the correct operation of the CA.

In the event of a failure of the primary power source the CA has the capability to lock out input, finish any pending actions, and record the state of the equipment prior to an automatic shutdown.

The directories (containing CA-issued certificates and CRLs) shall be provided with uninterrupted power sufficient for a minimum of 6 hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

The facilities that house the CA are constructed and equipped, and procedures implemented, to prevent and extinguish fires or other damaging exposure to flame or smoke. These measures meet all local applicable safety regulations. A description of the CMA's approach for recovery from a fire disaster are included in the Disaster Recovery Plan as specified in Section 5.7.4.

5.1.6 Media Storage

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

1. A copy of all CA data is retained at an off-site backup facility. All CA stored off-site is cryptographically secured.

2. A copy of CA keying material and activation data is securely stored within a safe within the facility. All CA keying material is cryptographically secured. All CA keying material and activation data is encrypted and stored in tamper evident containers.

5.1.7 Waste Disposal

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

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

5.1.8 Off-Site Backup

System backups follow a plan that include scheduled off-site storage of backup media. This plan includes provisions for completely restoring the system from backups.

The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA.

Access to backup media stored off-site is limited to authorized personnel. Authorized personnel are identified using an Authorization List approved by the Policy Authority.

5.2 Procedural Controls

5.2.1 Trusted Roles

The reliable and correct operation of the CA requires personnel to fulfill the following trusted roles (see the BlackBerry PKI Services Trusted Roles and Responsibilities).

5.2.1.1 CA Operations Manager

The CA Operations Manager provides administrative and management oversight of all CA operations. This role may involve assisting the CA Operators in the performance of their duties; however, this is discouraged. The CA Operations Manager is also responsible for reviewing and approving the audit log.

5.2.1.2 ZigBee Process Coordinator (ZPC)

The ZigBee Process Coordinator is responsible for managing the certificate life cycle processes, including interacting with applicants and customers, managing the certificate request queue and completing the certificate approval.

5.2.1.3 CA Internal Auditor

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

5.2.1.4 CA Operator

The CA Operator is responsible for vetting, key generation and key management. They are responsible for performing regular system backups and order fulfillment.

5.2.1.5 CA IT Configuration Administrator

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

5.2.1.6 CA Support Personnel

Customer support personnel serve in a trusted role. They are responsible for further investigation of issues encountered during the vetting or key generation procedures and vulnerability management as approved by the Policy Authority.

5.2.2 Number of Persons Required Per Task

The handling of CA Private Keys (throughout the entire CA key lifecycle) and the key activation material requires at least two people. The physical access controls placed upon this material ensure the involvement of at least two people. The logical access controls placed upon this material ensure the involvement of at least two people.

Certificate revocation requires the approval of the Policy Authority.

5.2.3 Identification and Authentication for Each Role

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

5.2.4 Roles Requiring Separation of Duties

See Section 5.2.1.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

All CA personnel are subject to all BlackBerry HR policies and terms of employment, including background screening.

5.3.2 Background Check Procedures

The background investigation includes the following checks:

- three professional references;
- criminal record check;
- check on academic and professional designations;
- proof that the prospective candidate is able to work in Canada (landed immigrant status, passport).

The background investigation and the hiring process are described in the BlackBerry PKI Services Personnel Hiring Procedure document.

5.3.3 Training Requirements

The training requirements for CA personnel are described in the Device CA Training and

Retraining Presentation.

5.3.4 Retraining Frequency and Requirements

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

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

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

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

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

Employees are given formal documentation of the violation and dismissal notice.

If severe, dismissal may be immediate. The employee's access credentials are removed, and under escort, the employee is allowed to remove personal belongings and leave the premises.

See the BlackBerry PKI Services Personnel Disciplinary Procedure.

5.3.7 Independent Contractor Requirements

See sections 5.3.1 and 5.3.2.

5.3.8 Documentation Supplied to Personnel

All CA personnel are provided copies of the CP, the relevant Subject CA CPSs, all CA Operations policies and procedures relevant to their trusted role, and all CA Operating Manuals.

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 are automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism is used.

All security audit logs, both electronic and non-electronic, are 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 Section 5.4.3, Retention Period for Audit Log, and 5.5.2, Retention Period for Archive.

5.4.1 Types of Events Recorded

The list of recorded events is contained in the Device CA Internal Audit Policy document.

5.4.2 Frequency of Processing Log

Refer to the Device CA Internal Audit Policy document.

5.4.3 Retention Period for Audit Log

Device CA Operations maintains its written monthly summaries of audit log reviews for a period not less than 7 years, or as necessary to comply with applicable laws. Audit logs are also kept until the completion of the next full accreditation audit.

5.4.4 Protection of Audit Log

The Device CA Personnel are obligated by this CP to keep the audit logging information generated by them on the CA until it is copied by the CA Configuration Administrator. Audit logs are retained on-site for at least two (2) months and are otherwise protected until after the next accreditation audit.

5.4.5 Audit Log Backup Procedures

Electronic audit logs follow the backup described in section 5.1.8.

Audit summaries are backed up at least monthly.

5.4.6 Audit Collection System (Internal vs. External)

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

Audit summary collection is external to the CA software and hardware.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

The Device CA PA will perform routine self-assessment of security controls.

5.5 Records Archival

5.5.1 Types of Records Archived

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

- Certificate Policy document
- Certification Practices Statement documents
- Contractual obligations
- Other agreements concerning operations of the CA
- Device CA baseline configuration (see the Device CA Configuration Management Policy)
- Modifications and updates to the Device CA baseline configuration (see the Device CA Configuration Management Policy)
- Certificate requests
- All certificates issued and/or published
- Audit log data (as described in section 5.4.1)
- Subscriber agreements
- Non-disclosure agreements
- Entity authentication data

- Enrollment forms
- Purchase orders
- All CRLs and CRLs issued and/or published
- Other data or applications to verify archive contents
- Documentation required by compliance auditors

In addition, CAs that retain subscriber private encryption keys for business continuity purposes shall archive such subscriber private keys.

5.5.2 Retention Period for Archive

The Device CA retains records of PKCs and the associated documentation (see section 5.5.1) for a term of no less than 7 years, unless otherwise stipulated as part of a third party agreement. Such agreements shall not override national laws.

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

5.5.3 Protection of Archive

Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction.

The contents of the archive shall not be released except as follows.

(1) at the direction of the Device CA Operations Manager, or

(2) as required by law.

Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media shall be stored in a secure off-site location separate from the CA.

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time-Stamping of Records

CA archive records are time-stamped as they are created. The CA system clock is synchronized with an authoritative time standard as described in the Device CA Work

Instructions for Root and Subordinate Keying Ceremonies, Order Fulfillment, and Upgrades.

5.5.6 Archive Collection System (Internal or External)

The archive collection system is internal to the CA software.

Additional requirements are specified in the Subject CA CPS.

5.5.7 Procedures to Obtain and Verify Archive Information

The procedures detailing how to obtain, verify, package, transmit, and store the CA archive information are published in the IT Media Handling and Storage procedure.

Additional requirements are specified in the Subject CA CPS.

5.6 Key Changeover

To minimize risk from compromise of a CA's private signing key, that key may be changed frequently. The frequency of key changeover is specified in the Subject CA's CPS.

Following key changeover, only the new key will be used for certificate signing purposes. If the old private key is used to sign CRLs that contain certificates signed with that key, the old key must be retained and protected.

The CA's signing key shall have a validity period as described in Section 6.3.2.

5.7 Compromise and Disaster Recovery

The following describes the general principles applied to all CAs.

- The CA and supporting systems shall be deployed in accordance with customer agreements. The requirements of service levels will be specified in the Subject CA CPS.
- The CA shall implement features to provide high levels of reliability.
- 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.

The following subsections outline the policy for instances that may prevent such maintenance of reliability.

5.7.1 Incident and Compromise Handling Procedures

To maintain the integrity of its services, the Device CA PA implements data backup and recovery procedures. The Device CA PA has developed a Disaster Recovery and Business Continuity Plan (DRBCP). CAs are configured to meet individual SLAs as specified by their Subject CA CPS. The DRBCP and supporting procedures are reviewed and tested periodically (at least on an annual basis) and are revised and updated as needed.

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

CA personnel perform system back-ups on a regular basis. Back-up copies are made of CA Private Keys and are stored off-site in a secure location (see the Device CA Data Classification and Management Policy). In the event of a disaster whereby the primary and disaster recovery CA operations become inoperative at the primary facility and the Disaster Recovery / Mirror Site, the CA will re-initiate its operations on replacement hardware using backup copies of its software, data and CA private keys at a comparable, secured facility.

5.7.3 CA Private Key Compromise Procedures

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

Subscriber certificates may be renewed automatically by the CA under the new key pair, or the CA may require subscribers to repeat the initial certificate application process.

5.7.4 Business Continuity Plans After a Disaster

See Sections 5.7.1 through 5.7.3 above.

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

5.8 CA and RA Termination

In the event of termination of the CA operation, certificates signed by the CA shall be revoked. Prior to termination, the CA shall provide archived data to an archive facility as specified in the Subject CA CPS. As soon as possible, the CA will advise all other organizations to which it has issued certificates of its termination, using an agreed-upon method of communication specified in the Subject CA CPS.

The requirements of this article may be varied by contract, to the extent that such modifications affect only the contracting parties.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Cryptographic keying material used by CAs to sign certificates, CRLs or status information shall be generated in FIPS 140-2 validated cryptographic modules. For CAs that issue certificates to subordinate CAs, servers, code signing, and commercial non-repudiation, the module(s) shall meet FIPS 140-2, Level 3. For CAs that issue certificates for low risk end entity applications, the module(s) shall meet or exceed FIPS 140-2, Level 2. Multiparty control is required for CA key pair generation, as specified in Section 6.2.2.

CA key pair generation must 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. See the Device CA Internal Audit Policy document.

Subscriber key pair generation is subject to business agreements and performed in compliance with the Subject CA CPSs.

The protection of cryptographic keying material is described in the Device CA Access Control Policy.

The lifecycle of keys and certificates used in the administration of the business and administrative processes of the PKI shall conform to the CP and Subject CA CPS for the systems which constitute the CAs and RAs.

6.1.2 Private Key Delivery to Subscriber

Private Key generation for subscribers is subject to business agreements and performed in compliance with the Subject CA CPSs.

6.1.3 Public Key Delivery to Certificate Issuer

The lifecycle management of key pairs between CA and subscribers is subject to business agreements and performed in compliance with the Subject CA CPSs.

6.1.4 CA Public Key Delivery to Relying Parties

The delivery of CA PKCs to be installed in RP devices for trust path validation is subject to business agreements and performed in compliance with the Subject CA CPSs.

6.1.5 Key Sizes

This CP requires the use of RSA, ECDSA, or ECQV. Certificates, CRLs, and keys are generated according to the policies in this CP and the Subject CA CPS.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters are generated and checked in accordance with the standard that defines the cryptographic algorithm in which the parameters are to be used. Parameters specified in business agreement must be compatible with the CA system configuration and security policy.

For RSA, this includes PKCS #1, for ECDSA this includes ANSI X9.62-2005, and for ECQV this includes SEC4.

6.1.7 Key Usage Purposes

Key usage values for each PKC are detailed in their respective Subject CA CPS.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules [FIPS 140-2]. The Device CA PA may determine that other comparable validation, certification, or verification standards are sufficient. The Device CA PA will publish these standards. Cryptographic modules shall be validated to a FIPS 140 level identified in this section, or validated, certified, or verified to requirements published by the Device CA PA.

See Section 6.1.1 for the current policy.

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

A single person is not permitted to invoke the complete CA signature process or access any cryptographic module containing the complete CA private signing key (see the Device CA Access Control Policy). CA signature keys are backed up under two-person control. Access to CA signing keys backed up for disaster recovery is under at least two-person control. CA Personnel required for two-person control are identified on the Permanent Authorized Access List. This list is available for inspection during compliance audits.

6.2.3 Private Key Escrow

CA private keys are not escrowed.

6.2.4 Private key Backup

Device CA's CA Private Keys are generated inside the HSM, which has been evaluated as specified in Section 6.1.1. These keys are encrypted and protected by multiple cryptographic tokens which enforce two-person control described in section 6.2.2. The backups are further encrypted and stored off-site for backup and disaster recovery purposes.

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

6.2.5 Private Key Archival

See Section 6.2.4.

CA and Sub-CA keys shall be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic token boundary.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

CA and Sub-CA private key archival is described in the Root and Subordinate CA Keying Ceremonies.

The method for subscriber key pair transfer shall be described in the Subject CA's CPS.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

The transfer of a private key into or from a cryptographic module is described in the Device CA Access Control Policy.

Subscriber keys shall be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic token boundary.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

6.2.7 Private Key Storage on Cryptographic Module

See Section 6.2.4.

6.2.8 Method of Activating Private Key

For certificates issued for use within the PKI and within the certificate fulfillment process specified in the business agreement, the subscriber must be authenticated to the cryptographic token before the activation of the associated private key(s). Acceptable means of authentication include but are not limited to pass-phrases, PINs or biometrics. Entry of activation data shall be protected from disclosure (i.e., the data should not be displayed while it is entered).

With regards to the certificates issued for the contracted certificates issued under an agreement, the subscribers are solely responsible for protection of the private keys. The CA maintains no involvement in the protection or distribution of such keys after they have been delivered to the subscriber.

6.2.9 Method of Deactivating Private Key

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

The HSM is to never be left in an unlocked, unattended state or otherwise left open to unauthorized access. After use, the cryptographic module is deactivated. CA activation data such as cryptographic tokens are removed and stored in secure tamper evident containers when not in use.

For PKCs issued for use in the Device CA PKI and within the certificate fulfillment process specified in the business agreement, the Subscribers should also deactivate their private keys via logout and token removal procedures when they are not in use.

6.2.10 Method of Destroying Private Key

Private signature keys are destroyed when they are no longer needed or when the certificates to which they correspond expire or are revoked as defined in the applicable CPS. In cases when this fails, Device CA must destroy the activation data such as any cryptographic tokens or passwords (see the Device CA Data Classification and Management Policy).

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

The CA retains copies of all Public Keys for archival in accordance with Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

All PKCs and corresponding keying materials have maximum validity periods (not exceeding) those recommended by NIST SP 800-57 unless otherwise stipulated in the Subject CA CPS.

The validity periods of each PKC is established by the Subject CA CPSs for the CAs.

Pursuant to Section 5.6, voluntarily retirement of CA Private Keys from signing subordinate certificates before the periods listed above to accommodate the key changeover process (i.e., the retiring CA Private Key is still used to sign CRLs to provide validation services for certificates issued with that retiring CA Private Key.)

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

All CA personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords according to the procedures set out in their Subject CA CPS (see the BlackBerry PKI Services Password Management Procedure)

6.4.2 Activation Data Protection

Data used to unlock private keys shall be protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data should be either biometric in nature or memorized (not written down). If written down, activation data shall be physically secured or encrypted under a FIPS approved cryptographic algorithm, and shall not be stored with the cryptographic module.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

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

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

Technical security controls on the Device CA Server and the separation of duties for PKI roles are described in the Device CA Access Control Policy.

When CA equipment is hosted on evaluated platforms in support of computer security assurance requirements, the system (hardware, software, operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as that which received the evaluation rating. The evaluation is performed in accordance with BlackBerry Certicom's Quality Assurance process.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Control

6.6.1 System Development Controls

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

- The CA shall use software that has been designed and developed under a formal, documented development methodology. This methodology is described in the Certicom Product Development Quality Manual.
- Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device). **BlackBerry Limited**

- Hardware and software developed specifically for the CA shall be developed in a controlled environment, and the development process shall be defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.

- The CA hardware and software shall be dedicated to performing one external task: the CA. There shall be no other applications, hardware devices, network connections, or component software installed that are not parts of the CA operation. Where the CA operation supports multiple CAs, the hardware platform can support multiple CAs.

- Proper care shall be taken to prevent malicious software from being loaded onto the CA equipment. Only applications required to perform the operation of the CA shall be obtained from sources authorized by local policy. RA hardware and software shall be scanned for malicious code on first use and periodically thereafter.

Hardware and software updates shall be purchased or developed in the same manner as original equipment, and shall be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the CA system, in addition to any modifications and upgrades, is documented and controlled (see the Device CA Configuration Management Policy document). There is a mechanism for detecting unauthorized modification to the software or configuration. The CA software, when first loaded, is verified as being that supplied from the vendor, with no modifications, and the version intended for use. The CA shall periodically verify the integrity of the software as specified in the Subject CA CPS.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

The CA is not connected to an external network.

6.8 Time Stamping

See Section 5.5.5.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profiles

7.1.1 Root CA Profile

The Root CA PKC uses the X.509 v3 certificate profile as consistent with the IETF's RFC 5280. The CA uses the ITU X.509, version 3 standard to construct digital certificates for use within the PKI.

7.1.1.1 Subject Names

The subject follows the naming convention defined in Section 3.1.

7.1.1.2 Issuer Names

The issuer name exactly matches the subject name.

7.1.1.3 Serial Numbers

The serial number is unique, positive, and may be up to 20 octets in length.

7.1.1.4 Signature Values

The signature value is computed using the private key that matches the public key contained in the PKC.

The strength of the hash algorithm used to compute the signature value must match or exceed the strength of the public key contained in the PKC. The strength of the hash algorithm is determined using NIST SP 800-57.

7.1.1.5 Validity Period

The notBefore value is the date of certificate issuance.

The notAfter value is any value but should be upper bound by the expected life of the public key contained in the PKC by considering its strength and protection. The life expectancy of the key is determined using NIST SP 800-57

The notAfter value of subordinate PKCs may be subject to additional contraints. These constraints are described in the Subject CA CPS.

7.1.1.6 Unique Identifier

The unique identifier field is not included.

7.1.1.7 Key Usage Extension

The key usage extension is included and is marked as critical. The keyCertSign and cRLSign bits are set. No other bits are set.

7.1.1.8 Basic Constraints Extension

The basic constraints extension is included and is marked as critical. The cA boolean is set to true.

Inclusion of the pathLenConstraint is determined by the Subject CA CPS.

7.1.1.9 Certificate Policies Extension

The Certificate Policies extension is included. The criticality of this extension and the existance of any optional components is defined in the Subject CA CPS.

7.1.1.10 Policy Constraints Extension

CAs may assert policy constraints in CA certificates. Policy contraints are described in the Subject CA's CPS.

7.1.1.11 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.1.12 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.1.1.13 CRL Distribution Points Extension

The CRL distribution points extension and criticality of this extension is described in the Subject CA's CPS. If included, this extension contains one or more distributionPoint or cRLIssuer fields.

7.1.2 Sub CA Profile

The Sub CA Profile is identical to the Root CA Profile defined in section 7.1.1 with the following exceptions:

7.1.2.1 Issuer Names

The issuer name shall match exactly the subject name of a pre-existing Root CA or Sub CA as defined in section 7.1.1.1.

7.1.2.2 Signature Values

The signature value is computed using the private key that matches the public key contained in the PKC issuer name defined in section 7.1.2.1. The strength of the hash algorithm used to compute the signature value must match or exceed the strength of the public key contained in the PKC.

7.1.3 X.509 Certificate Profiles

The X.509 certificate profiles are identical to the Sub CA Profile defined in section 7.1.2 with the following exceptions:

7.1.3.1 Key Usage Extension

The key usage extension must be included and must be marked as critical. For ECC PKCs the keyAgreement bit must be set. For RSA PKCs the keyEncipherment bit must be set. All other bits may be defined by the Subject CA CPS.

7.1.3.2 Extended Key Usage Extension

The extended key usage extension and its associated criticality is optional and may be defined by the Subject CA CPS.

7.1.3.3 Basic Constraints Extension

The basic constraints extension is optional and may be defined by the Subject CA CPS. If included, the cA boolean value must be set to false.

7.1.3.4 Certificate Policies Extension

No stipulation.

7.1.3.5 CRL Distribution Points Extension

No stipulation.

7.2 CRL Profile

CRLs issued by a CA under this policy shall conform to RFC 5280.

7.2.1 Version Number(s)

If CRL are issued under a subject CPS it shall issue version two (2) CRLs (i.e. populated with integer "1"). CRLs conform to RFC 5280 and contain the basic fields listed below:

- Version
- Issuer Signature Algorithm (sha-1WithRSAEncryption {1 2 840 113549 1 1 5}) Issuer Distinguished Name
- thisUpdate (UTC format)
- nextUpdate (UTC format – thisUpdate plus 24 hours)
    - Revoked certificates list
    - Serial Number
- Revocation Date (see CRL entry extension for Reason Code below) Issuer's Signature

7.2.2 CRL and CRL Entry Extensions

CRL Number (monotonically increasing integer - never repeated)

Authority Key Identifier (same as Authority Key Identifier in certificates issued by CA)

CRL Entry Extensions

Invalidity Date (UTC - optional)

Reason Code (optional)

7.3 OCSP Profile

OCSP support, where supported, is stipulated in the Subject CA CPS .

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices specified in this CP have been designed to meet or exceed the requirements of generally accepted and developing industry standards including ISO 27001, ISO 17799, the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79/ISO 21188 PKI Practices and Policy Framework ("CA WebTrust/ISO 21188"), and other industry standards related to the operation of CA's.

8.1 Frequency or Circumstances of Assessment

An annual audit is performed by an independent external auditor to assess CA compliance with this CP.

8.2 Identity & Qualifications of Assessor

(1) 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.

(2) 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.

(3) Rules and standards: The individual or group must conform to applicable standards, rules, and best practices promulgated by the American Institute of Certified Public Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA), 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.

(4) Reputation: The firm must have a reputation for conducting its auditing business competently and correctly.

(5) 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. The assessor shall maintain a high standard of ethics designed to ensure impartiality and the exercise of independent professional judgment, subject to disciplinary action by its licensing body.

8.4 Topics Covered By Assessment

Topics covered by the annual CA audit 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.

8.5 Actions Taken As A Result of Deficiency

If an audit reports any material noncompliance with applicable law, this CP, or any other 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 Device CA 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, then the Device CA PA may instruct Operations Manager to revoke the certificates affected by such non-compliance.

8.6 Communication of Results

The results of any inspection or audit are reported to the management, acting as the Device CA PA, and any appropriate entities, as may be required by law, regulation or agreement. At its option, the CA will 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 9.3.

9 OTHER BUSINESS AND LEGAL MATTERS

This part describes the legal representations, warranties and limitations associated with each of Device CA's digital certificates.

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

All fees charged by Device CA certificate services are subject to business agreements unless stipulated in a Subject CA CPS.

9.1.2 Certificate Access Fees

No stipulations.

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

No stipulations. Subject to business agreements.

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

Device CA keeps the following types of information confidential and maintains reasonable controls to prevent the exposure of such records to unauthorized personnel.

- All private keys
- Any activation data used to access private keys or gain access to the CA system
- Any business continuity incident response, contingency, and disaster recovery plans
- Any other security practices, measures, mechanisms, plans, or procedures used to protect the confidentiality, integrity or availability of information
- Any information held by Device CA as private information in accordance with Section 9.4
- Any transactional, audit log and archive record identified in Section 5.4 or 5.5 including certificate application records and documentation submitted in support of certificate applications whether successful or rejected.
- Transaction records, financial audit records and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CP)

9.3.2 Information Not Within the Scope of Confidential Information

No stipulation.

9.3.3 Responsibility to Protect Confidential Information

Device CA observe applicable rules on the protection of personal data deemed by law or the Device CA privacy policy (see Section 9.4 of this CP) to be confidential.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

No stipulation.

9.4.2 Information Treated as Private

No stipulation.

9.4.3 Information Not Deemed Private

Certificates, CRLs, and personal or corporate information appearing in them are not considered private.

9.4.4 Responsibility to Protect Private Information

Each party shall 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 shall 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.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Device CA shall 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 Device CA owes a duty to keep information confidential.
- The party requesting such information.
- A 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, US and European law concerning the protection of personal data.

9.5 Intellectual Property Rights

Device CA, its strategic partners, and other business associates, each own all their respective intellectual property rights associated with their databases, web sites, Device CA digital certificates and any other publication originating from Device CA including this CP.

The word "Device CA" is a registered trademark of BlackBerry Limited. BlackBerry may have other trade and service marks that have not been registered, but that nonetheless are and shall remain its property.

Certificates are the exclusive property of Device CA. Device CA gives permission to reproduce and distribute certificates according to business agreement, on a royalty-free basis, provided that they are reproduced and distributed in full. Device CA reserves the right to revoke the certificate at any time and at its sole discretion.

Private and public keys are the property of the Subscribers under the terms of valid business agreements.

All secret shares (distributed elements) of the Device CA private keys remain the respective property of Device CA.

9.6 Representations and warranties

9.6.1 CA Representations and Warranties

Except as expressly stated in this CP, BlackBerry Certicom makes no representations or warranties regarding its Device CA service. BlackBerry Certicom reserves its right to modify such representations as it sees fit, at its sole discretion, or as required by law or valid business agreements.

Only to the extent specified in the relevant sections of this CP, BlackBerry Certicom shall:

- Comply with this CP and its internal or published policies and procedures.
- Comply with applicable laws and regulations.
- Provide infrastructure and certification services.
- Provide trust mechanisms including a key generation mechanism, key protection, and secret sharing procedures regarding its own infrastructure.
- Provide prompt notice in case of compromise of its private key(s).
- Provide and validate application procedures for the various types of certificates that it may make commercially available.
- Issue digital certificates in accordance with this CP and fulfill its obligations presented herein.
- Provide support to Subscribers and Relying Parties as described in this CP.
- Revoke certificates according to this CP.
- Provide for the expiration and renewal of certificates according to this CP.

- Make available extracts of this CP and applicable CPSs as attachments to business agreements.

- Warrant the accuracy of information published on a Certificate issued pursuant to the requirements and specifications of a business agreement.

The Subscriber also acknowledges that BlackBerry Certicom has no further obligations under this CP unless stipulated in a valid business agreement.

Except as it may have otherwise been stated in a subject CPS or valid business agreement, BlackBerry Certicom:

- Does not warrant the accuracy, authenticity, completeness or fitness of any unverified information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of BlackBerry Certicom except as it may be stated in the relevant product description contained in this CP.

- Shall incur no liability for representations of information contained in a certificate except as it may be stated in the relevant product description in this CP.

- Does not warrant the quality, functions or performance of any software or hardware device.

- Shall have no liability if it cannot execute the revocation of a certificate for reasons outside its own control.

9.6.2 RA representations and Warranties

No stipulation.

9.6.3 Subscriber Representations and Warranties

Unless otherwise stated in this CP or the applicable CPS and valid business agreements, Subscribers shall exclusively be responsible:

- To minimize internal risk of private key compromise by ensuring that they and their agents have adequate knowledge and training.

- Where applicable, to generate a secure private / public key pair to be used in association with the certificate request submitted to Device CA.

- Where applicable, ensure that the public key submitted to Device CA is the correct one and corresponds with the private key used.

- Provide correct and accurate information in communications with Device CA and alert Device CA if any information originally submitted has changed since it was submitted to Device CA.

- Read, understand and agree with all terms and conditions in this CP and associated policies published in the Device CA Repository at https://blackberry.certicom.com/en/products/zigbee-certicom-device-authentication-service.

- Use Device CA certificates for legal and authorized purposes in accordance with the terms and conditions expressed in the subject business agreement.

- Cease using the certificate if any information in it becomes misleading, obsolete or invalid.

- Cease using the certificate if it is expired and remove it from any applications and/or devices it has been installed on.

- Make reasonable efforts to prevent the compromise, loss, disclosure, modification, or otherwise unauthorized use of the private key corresponding to the public key published in a Device CA certificate.

- Request the revocation of a certificate in case of any occurrence that might materially affect the integrity of the certificate.

- For acts and omissions of partners and agents they use to generate, retain, escrow, or destroy their private keys

Without limiting other Subscriber obligations stated in this CP, Subscribers are solely liable for any misrepresentations they make in certificates to third parties that reasonably rely on the representations contained therein.

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

- 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 Certicom.

- The Subscriber retains control of the Subscriber's private key, uses a trustworthy system, and takes reasonable precautions to prevent its loss, disclosure, modification, or unauthorized use and that no unauthorized person has ever had access to the Subscriber's private key.

- All representations made by the Subscriber to BlackBerry Certicom regarding the information contained in the certificate are accurate and true to the best of the Subscriber's knowledge or to the extent that the Subscriber receives notice of such information, the Subscriber shall act promptly to notify BlackBerry Certicom of any material inaccuracies contained in the certificate.

- The certificate is used exclusively for authorized and legal purposes consistent with this CP, the subject CPS and the valid business agreement under which the certificate is issued.

- The Subscriber agrees with the terms and conditions of this CP and other Device CA agreements and policy statements which is part of a valid business agreement under which the certificate is issued.

- The Subscriber abides by the laws applicable to the country or territory in which the certificate is used, including those related to intellectual property protection, fair trade practices and computer fraud and abuse.

- The Subscriber complies with all export laws and regulations for dual usage goods as may be applicable.

9.6.4 Relying Party Representations and Warranties

If applicable, a Relying Party accepts that in order to reasonably rely on a Device CA certificate, the Relying Party must:

- Study the limitations to the usage of digital certificates and be aware through the Relying Party Agreement of the limitations of liability of BlackBerry Certicom for reliance on a Device CA issued certificate.

- Read and agree with the terms of the Device CA Relying Party Agreement.

- Verify the Device CA certificates by referring to the relevant CRL and also the CRLs of any intermediate CA or root CA as available through Device CA's repository.

- Trust a Device CA certificate only if it is valid and has not been revoked or has expired.

- Take any other reasonable steps to minimize the risk of relying on a digital signature created by an invalid, revoked, expired or rejected certificate; and finally,

- Rely on a Device CA certificate, only as may be reasonable under the

- circumstances, given:

    - any legal requirements for the identification of a party, the protection of the confidentiality or privacy of information, or the legal enforceability of the transaction in accordance with any laws that may apply;

    - all facts listed in the Certificate, or of which the Relying Party has or should have notice including this CP;

- the economic value of the transaction or communication, if applicable;
- the potential losses or damage which might be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction or communication;
- the applicability of the laws of a particular jurisdiction including the jurisdiction specified in an agreement with the Subscriber or in this CP;
- the Relying Party's previous course of dealing with the Subscriber, if any;
- usage of trade including experience with computer-based methods of trade; and
- any other indications of reliability or unreliability, or other facts of which the Relying Party knows or has notice, pertaining to the Subscriber and/or the application, communication or transaction.

9.6.5 Representations and Warranties of Other Participants

Not applicable.

9.7 Disclaimers of Warranties

BlackBerry Certicom disclaims all warranties and obligations of any type including any warranty of fitness for a particular purpose, and any warranty of the accuracy of unverified information provided, save as contained herein and as cannot be excluded at law. In no event and under no circumstances (except for fraud or willful misconduct) shall BlackBerry Certicom be liable for any or all of the following and the results thereof:

- Any indirect incidental or consequential damages.
- Any costs, expenses, or loss of profits.
- Any death or personal injury.
- Any loss of data.
- Any other indirect, consequential or punitive damages arising from or in connection with the use, delivery, license, performance or non-performance of certificates or digital signatures.
- Any other transactions or services offered within the framework of this CP.
- Any other damages except for those due to reliance, on the information featured on a certificate, or on the verified information in a certificate.

- Any liability incurred in this case or any other case if the fault in this verified information is due to fraud or willful misconduct of the applicant.
- Any liability that arises from the usage of a certificate that has not been issued or used in conformance with this CP.
- Any liability that arises from the usage of a certificate that is not valid.
- Any liability that arises from usage of a certificate that exceeds the limitations in usage and value and transactions stated upon it or in this CP.
- Any liability that arises from security, usability, integrity of products including hardware and software a Subscriber uses.
- Any liability that arises from compromise of a Subscriber's private key.

9.8 Limitations of Liability

BLACKBERRY CERTICOM CERTIFICATES MAY ONLY BE USED IN CONNECTION WITH DATA TRANSFER AND TRANSACTIONS HAVING A VALUE OF LESS THAN $1 MILLION. IN NO EVENT AND UNDER NO CIRCUMSTANCES (EXCEPT FOR FRAUD OR WILLFUL MISCONDUCT) WILL THE AGGREGATE LIABILITY OF BLACKBERRY CERTICOM, WHETHER JOINTLY OR SEVERALLY, TO ALL PARTIES INCLUDING WITHOUT ANY LIMITATION A SUBSCRIBER, AN APPLICANT, A RECIPIENT, OR A RELYING PARTY FOR ALL DIGITAL SIGNATURES AND TRANSACTIONS RELATED TO SUCH CERTIFICATE EXCEED THE LOWER OF THE AMOUNT PAID BY THE SUBSCRIBER TO BLACKBERRY CERTICOM IN THE PRIOR 12 MONTH AND $1 MILLION. DAMAGES ARE LIMITED TO DIRECT, PROVABLE DAMAGES ONLY AND IN NO EVENT WILL EITHER PARTY BE LIABLE UNDER THIS AGREEMENT FOR ANY SPECIAL, INDIRECT, CONSEQUENTIAL, OR PUNITIVE DAMAGES INCLUDING, WITHOUT LIMITATION, DAMAGES WHICH REFLECT LOST BUSINESS, PROFITS OR REVENUE OBTAINED OR LOST, OR THE COSTS OF RECONSTRUCTING DATA OR REBUILDING DEVICES, WHETHER DAMAGES OF THIS NATURE WERE FORESEEABLE OR NOT, AND EVEN IF THAT PARTY HAD BEEN ADVISED THAT DAMAGES OF THIS NATURE WERE POSSIBLE.

9.9 Indemnities

By accepting or using a certificate, each Subscriber and Relying Party agrees to indemnify and hold BlackBerry Certicom, as well as any of its respective parent companies, subsidiaries, directors, officers, employees, agents, and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind including reasonable attorneys' fees, that BlackBerry Certicom, and/or the above mentioned parties may incur, that are caused by the use or publication of a certificate, and

that arises from that party's: (i) misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional; (ii) violation of the Subscriber Agreement, Relying Party Agreement, this CP, or any applicable law; (iii) compromise or unauthorized use of a Certificate or Private Key caused by the negligence of that party and not by BlackBerry Certicom (unless prior to such unauthorized use BlackBerry Certicom has received an authenticated request to revoke the Certificate); or (iv) misuse of the Certificate or Private Key.

9.10 Term and Termination

9.10.1 Term

This CP and any amendments hereto shall become effective upon publication in the Repository or as part of a valid business agreement, and shall remain in effect perpetually until terminated in accordance with this Section 9.10.

9.10.2 Termination

This CP as amended from time to time shall remain in force until it is replaced by a new version or is otherwise terminated in accordance with this Section 9.10.

9.10.3 Effect of Termination and Survival

The conditions and effect resulting from termination of this document will be communicated via the Device CA Repository and in accordance with stipulations in valid business agreements upon termination. That communication will outline the provisions that may survive termination of this CP and remain in force. The responsibilities for protecting business confidential and private personal information shall survive termination, and the terms and conditions for all existing Certificates shall remain valid for the remainder of the Validity Periods of such Certificates.

9.11 Individual Notices and Communications with Participants

BlackBerry Certicom accepts notices related to this CP by means messages addressed to the locations specified in Section 2.2 of this CP. Upon receipt of a valid “acknowledgment of receipt” from BlackBerry Certicom, the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed to the street address specified in Section 2.2.

9.12 Amendments

9.12.1 Procedure for Amendment

Revisions not denoted "significant" shall be those deemed by the Device CA Policy Authority to have minimal or no impact on Subscribers and Relying Parties using certificates and CRLs issued by Device CA. Such revisions may be made without notice to users of this CP and without changing the version number of this CP. Controls are in place to reasonably ensure that the Device CA CP is not amended and published without the prior authorization of the Device CA Policy Authority.

9.12.2 Notification Mechanism and Period

No stipulation.

9.12.3 Circumstances Under which OID Must be Changed

If a change in Device CA Certificate Policy or Certification Practices Statement is determined by the Device CA Policy Authority to warrant a change in the currently specified OID for a particular type of certificate, then the revised version of this CP or subject CPS will also contain a revised OID for that type of certificate.

9.13 Dispute Resolution Provisions

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, mediation, umpire, binding expert's advice, co-operation monitoring and normal expert's advice) the parties agree to notify BlackBerry Certicom of the dispute with a view to seek dispute resolution.

9.14 Governing Law

This CP is governed by, and construed in accordance with the law of Ontario. This choice of law is made to ensure uniform interpretation of this CP, regardless of the place of residence or place of use of Device CA digital certificates or other products and services. Ontario law applies in all of BlackBerry Certicom's commercial or contractual relationships in which this CP may apply or quoted implicitly or explicitly in relation to Device CA products and services where BlackBerry Certicom acts as a provider, supplier, beneficiary receiver or otherwise.

Each party including BlackBerry Certicom, Subscribers and Relying Parties, irrevocably agree that a tribunal (court or arbitration body) located in Ontario shall have exclusive jurisdiction to hear and decide any suit, action or proceedings, and to settle any disputes, which may arise out of or in connection with this CP or the provision of Device CA PKI services.

9.15 Compliance with Applicable Law

This CP shall be subject to applicable national, province, local and foreign laws, rules, regulations, ordinances, decrees and orders including but not limited to restrictions on exporting or importing software, hardware or technical information.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CP shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances, and intended usage of the product or service described herein. In interpreting this CP the parties shall also take into account the international scope and application of the services and products of BlackBerry Certicom as well as the principle of good faith as it is applied in commercial transactions.

The headings, subheadings, and other captions in this CP are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CP.

Appendices and definitions to this CP are for all purposes an integral and binding part of the CP. If/when this CP conflicts with other rules, guidelines, or contracts, this CP shall prevail and bind the Subscriber and other parties. If there is any conflict between the sections of this CP and any other document that relate to Device CA, then the sections benefiting BlackBerry Certicom and preserving BlackBerry Certicom's best interests, at BlackBerry Certicom's sole determination, shall prevail and bind the applicable parties.

9.16.2 Assignment

Parties to this CP may not assign any of their rights or obligations under this CP or applicable agreements without the written consent of BlackBerry Certicom.

9.16.3 Severability

If any provision of this CP or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CP (and the application of the invalid or unenforceable provision to other persons or circumstances) shall remain in full force and effect and shall be interpreted in such a manner as to implement the original intention of the parties to the fullest extent possible.

Each and every provision of this CP that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

9.16.4 Enforcement (Attorneys' Fees and Waiver Of Rights)

BlackBerry Certicom reserves the right to seek indemnification and attorneys' fees from any party related to that party's conduct described in Section 9.9. Except where an express time frame is set forth in this CP, no delay or omission by any party to exercise any right, remedy or power it has under this CP shall impair or be construed as a waiver of such right, remedy or power. A waiver by any party of any breach or covenant in this CP shall not be construed to be a waiver of any other or succeeding breach or covenant. Bilateral agreements between BlackBerry Certicom and the parties to this CP may contain additional provisions governing enforcement.

9.16.5 Force Majeure

BLACKBERRY CERTICOM INCURS NO LIABILITY IF IT IS PREVENTED, FORBIDDEN OR DELAYED FROM PERFORMING, OR OMITS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF: ANY PROVISION OF ANY APPLICABLE LAW, REGULATION OR ORDER; CIVIL, GOVERNMENTAL OR MILITARY AUTHORITY; THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEM OPERATED BY ANY OTHER PARTY OVER WHICH IT HAS NO CONTROL; FIRE, FLOOD, OR OTHER EMERGENCY CONDITION; STRIKE; ACTS OF TERRORISM OR WAR; ACT OF GOD; OR OTHER SIMILAR CAUSES BEYOND ITS REASONABLE CONTROL AND WITHOUT ITS FAULT OR NEGLIGENCE.

9.17 Other provisions

This CP shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties that this CP applies to. The rights and obligations detailed in this CP are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this CP articles on termination or cessation of operations, and provided that such assignment does not effect a negation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.