BlackBerry | certicom

BlackBerry Certicom

Device CA X.509

Certification Practices Statement

Version 2.1

January 19, 2021

1 INTRODUCTION

The Device CA X.509 Certification Practices Statement (CPS) is targeted at applications requiring ECDSA and RSA based X.509 Public Key Certificates (PKCs) with a bias towards high-volume device manufacturing environments having bulk certificate requirements.

This document fulfills the Subject CA requirements placed upon X.509 Subject CAs by the Device CA Certificate Policy.

1.1 Overview

This CPS is written for PKCs targeted at 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 CPS 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 X.509 certificate types: CA, Subordinate CA (Sub-CA), and Administrative. It provides a root of trust for the Device CA Public Key Infrastructure (PKI). The Device CA PKI uses a hierachical trust model to fulfill Relying Party (RP) requirements for Sub-CA and Admininstrative PKCs.

An administrative PKC is an end entity certificate issued to individuals who are administering device PKCs on behalf of an organization.

This CPS contains information on the X.509 certificate types. The following CPs complement this document.

- Device CA Certificate Policy

  This CP provides additional information on X.509 CA, Sub-CA and Adminstrative PKCs.

The CP and this CPS govern the certificate life cycle for the Subject Cas described in this document.

1.2 Document name and identification

This CPS is known as the “Device CA X.509 CPS.” It uses the Object Identifier (OID) { 1.3.132.8.6 } to indicate the PKCs issued under this CPS.

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
11-08-2008	Updated with Administrative PKCs.	1.2
19-08-2008	CPS is now Certification Practices Statement everywhere.	1.3
7-Oct-08	Introduction of multiple administrative certificates for an organization.	1.4
30-Jan-2009	Updated method of destroying private keys. Now refers to IT Media Handling and Storage Procedures.	1.5
25-Mar-2010	Added point compression format, ASN.1 type and signature digest for administrative, certification authority, and subordinate certificate authority certificates. Corrected printed keys in ECDSA certificates. Added ASN.1 type and signature digest to RSA certificates and profiles.	1.6
14-Jun-2013	Updated practices on sub CA certificate expiry, renewal, enrollment processes. Updated Certificate Profile Validity.	1.7
18-Sept-2014	Changed BlackBerry to “BlackBerry” and removed details regarding fingerprint match.	1.8
24-Sept-2014	Cosmetic updates.	1.9
15-Feb-18	Updated URL for Device CA details on Certicom website. Removed RSA CA Certificate Profile, Certicom RSA-3027 ROOT CA Certificate Profile and Certicom sect163k1 Corporate ZigBee CA Certificate Profile (none of which were renewed). Updated details of Certificate Profiles that were renewed.	2.0
31-Mar-20	Updated logo and entity name from Certicom to BlackBerry Certicom.	2.1
19-Jan-21	Updated copyright.	2.1

1.3 PKI participants

1.3.1 Certification Authorities

The following CAs exist for issuing X.509 certificates:

- `Subject: CN=Certicom sect163k1 ROOT CA,O=Certicom Corp,C=CA`

  `Issuer: CN=Certicom sect163k1 ROOT CA,O=Certicom Corp,C=CA`

- `Subject: CN=Certicom sect163k1 Corporate Identity CA,O=Certicom Corp,C=CA`

  `Issuer: CN=Certicom sect163k1 ROOT CA,O=Certicom Corp,C=CA`

- `Subject: CN=Certicom secp384r1 ROOT CA,CA,O=Certicom Corp,C=CA`

  `Issuer: CN=Certicom secp384r1 ROOT CA,CA,O=Certicom Corp,C=CA`

1.3.2 Relying Parties

The CA and Sub-CA PKCs described in section 1.3.1 are publicly available at the following URL:
https://www.certicom.com/content/certicom/en/certificates/671-deviceca.html.

Administrative PKCs are not publicly available.

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

Administrative PKCs are limited to protecting the authenticity and confidentiality of requests for Device PKCs.

All permitted key usages are defined in section 6.1.6 are permitted.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Publication of Certification Information

Administrative PKCs are not published by the CA.

CA and Sub-CA PKCs are published at https://www.certicom.com/content/certicom/en/certificates/671-deviceca.html.

2.2 Time or Frequency of Publication

No stipulation.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

Within Device CA, the Certificate Subject Name 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
- Administrative PKC: CN=<common name defined by requestor>, O=<organization defined by requestor>, OU=<organizational unit defined by requestor>, C=<country defined by requestor>.

3.1.2 Meaningfulness

The Common Name (CN=), Organization (O=) and Organizational Unit (OU=) attributes in the Certificate Subject of Administrative PKCs unambigously and accurately identify the legal entity that is the subject of the certificate.

3.1.3 Uniqueness of Names

The uniqueness of the Common Name (CN=) of the Certificate Subject field of Administrative PKCs are not unique. The combination of Common Name (CN=), Organization (O=) and Organizational Unit (OU=) are unique in Administrative PKCs.

3.1.4 Recognition, Authentication, and Role of Trademarks

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

Sub-CAs issuing Administrative PKCs that include trademark-protected names must verify that applicant is authorized to request on behalf of the trademark owner. If the Administrative PKC includes an organizational unit name that is trademarked, then the applicant must be legally eligible to use that name in the PKC.

3.2 Initial identity validation

3.2.1 Authentication of Organization Identity

The following information is required to authenticate an organization.

1. The cryptographic fingerprint of the X.509 Administrative PKCS #10 certificate request.

3.2.2 Authentication of Individual Information

The following information is required to authenticate an individual.

1. An email or letter of authorization from the primary or alternative authorized and domain validated contact is required to authorize requests for Administrative PKCs within their organization.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application Processing

4.1.1 Performing Identification and Authentication Functions

Administrative identification and authentication functions are performed as described in section 3.

4.1.2 Enrollment Process and Responsibilities

The primary contact for an organization may authorize or designate company contacts for requesting an Administrative PKC or authorizing certificate handlers.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

No stipulation.

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Admininstrative PKCs are made available to the subscriber via FTP.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

No stipulation.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Acceptance of an Administrative PKC is shown through its use to request Device PKCs.

4.4.2 Publication of the Certificate by the CA

Administrative PKCs are not published by the CA.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers must use private keys only in accordance with the usages specified in their respective Subject CA CPS. See Sections 1.4.1 and 6.1.6.

4.5.2 Relying Party Public Key and Certificate Usage

RP use of a CA, Sub-CA, or Admininstrative PKCs is subject to all of the key usages presented with that PKC.

4.6 Certificate Renewal

4.6.1 Circumstances for Certificate Renewal

CA and Sub-CA PKCs renewal may occur at any time prior to expiry. Following renewal these certificates are made available to subscribers.

Administrative PKC renewal may occur any time prior to PKC expiry. Following expiry, re-enrollment is required via the initial identity validation described in the Device CA CP.

4.6.2 Who May Request a Certificate Renewal

The subscriber or authorized certificate handler of a licensed entity may request the renewal of an Administrative PKC.

4.6.3 Processing Certificate Renewal Requests

Administrative PKC renewal requests must be submitted by the subscriber whose name appears in the Certificate Subject (CN=).

4.6.4 Notification of New Certificate Issuance to Certificate Subject

The subscriber is provided download instructions for the Administrative PKCs.

4.6.5 Conduct Constituting Acceptance of Renewal Certificate

Acceptance of a renewed Administrative PKC is described in section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

Administrative PKCs are not published by the CA.

4.7 Certificate Re-Key

4.7.1 Circumstances for Certificate Re-Key

CA and Sub-CA PKCs may be re-keyed prior to expiry.

Administrative PKCs may be re-keyed if the owner or primary contract responsible for an Administrative PKC requests re-keying due to loss of their private key or password.

4.7.1 Who May Request Certification of a New Public Key

Re-key requests for CA and Sub-CA PKCs are requested by the Device CA PA.

4.7.2 Processing Certificate Re-Key Requests

CA and Sub-CA re-key requests are processed using the Device CA Work Instructions for the Root and Subordinate Keying Ceremonies.

4.7.3 Notification of New Certificate Issuance to Certificate Subject

No stipulation.

4.7.4 Conduct Constituting Acceptance of Re-Keyed Certificate

No stipulation.

4.7.5 Publication of the Re-Keyed Certificate by the CA

CA and Sub-CA PKCs are published as described in section 2.1.

4.8 Certificate Revocation and Suspension

4.8.1 Procedure for Revocation Request

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

X.509 PKCs are revoked whenever the binding between the Certificate Subject and the Certificate Subject's private key is no longer considered valid (e.g., comprise of the private key).

X.509 PKCs are revoked whenever the Device CA PA requests that it be revoked, when the PKC holder submits an authenticated revocation request, and when the CA determines that a situation has occurred that may affect the integrity of the PKC.

4.9.2 Who can Request Revocation

The Primary Contact or other appropriately authorized party can request revocation of an X.509 PKC. The revocation request must be received from the Primary Contact associated with the PKC application.

If the Primary Contact is not available the revocation request can be made by both the Billing and Technical Contact.

4.9.3 Procedure for Revocation Request

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

The operation of the CA complies with the policies and procedures provided to the Device CA Operations team. All policies and procedures used by this team are approved by the Device CA PA.

5.2 Audit Logging Procedures

5.2.1 Frequency of Processing Log

All audit logging data is reviewed monthly. (see /var/log/trustpoint.log, /var/log/fulllog monthly)

5.3 Records Archival

5.3.1 Archive Collection System (Internal or External)

No stipulation.

5.3.2 Procedures to Obtain and Verify Archive Information

No stipulation.

5.4 Key Changeover

Root CA keys will not be re-keyed. They will be renewed.

5.5 Compromise and Disaster Recovery

5.5.1 CA Private Key Compromise Procedures

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 (i.e. BlackBerry Certicom shipping procedures).

5.6 CA and RA Termination

The primary contact for each Administrative PKC is notified by telephone of CA or RA termination.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Administrative PKC key pair generation is performed using software called the "ca_reqtool". The User's Guide for this tool described how to generate a key pair.

6.1.2 Private Key Delivery to Subscriber

Private keys for Administrative PKCs are generated by the subscriber as described in section 6.1.1.

6.1.3 Public Key Delivery to Certificate Issuer

Administrative PKCs are provided to the person whose name appears in the primary contract of the enrollment form using BlackBerry Certicom's standard shipping method. This method includes FTP download of the PKC from a temporary account provided to the primary contact.

6.1.4 CA Public Key Delivery to Relying Parties

CA and Sub-CA PKCs needed to complete the chain of trust to an Administrative PKC are provided to the primary contact when they receive the "ca_reqtool".

CA and Sub-CA PKCs are also published as described in section 2.1.

6.1.5 Key Sizes

CA and Sub-CA key sizes are determined by the Device CA PA.

The key sizes and algorithms required by Administrative PKCs follow the recommendations of the User's Guide provided with the "ca_reqtool".

6.1.6 Key Usage Purposes

CA and Sub-CA PKCs have CRL signing and certificate signing key usages asserted as criticical.

Administrative PKCs have the digitial signature and key agreement key usage asserted as critical.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Private Key Archival

Private keying material for Administrative PKCs is not managed by the CA.

6.2.2 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 device according to the requirements described in the Device CA Data Classification and Management document.

6.2.3 Certificate Operational Periods and Key Pair Usage Periods

All PKCs and corresponding keying material has maximum validity periods (not exceeding) those recommended by NIST SP 800-57.

CA PKCs are valid for 10 year from the date of issue.

Sub-CA PKCs may be valid up to the date of issue of the CA less one month.

Administrative PKCs are valid for 5 calendar years from date of issue.

6.3 Activation Data

6.3.1 Activation Data Generation and Installation

The creation of passwords to protect CA and Sub-CA private keys is described in the Device CA Access Control Policy and the BlackBerry PKI Services Password Management Procedure.

The creation of passwords to protect Administrative PKC private keys is described in the User's Guide provided with the "ca_reqtool".

6.4 Life Cycle Technical Control

6.4.1 Security Management Controls

The integrity of the CA software is verified prior to each software upgrade. Verification of said software requires the execution of the BlackBerry Certicom Software Development Lifecycle, as specified in the BlackBerry Certicom Product Development Quality Manual.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1.1 Root CA Profile

The Root CA and Sub-CA PKCs use the X.509 v3 certificate profile as consistent with the IETF's RFC 3280 (http://www.ietf.org/rfc/rfc3280.txt). Device CA uses the ITU X.509, version 3 standard to construct digital certificates for use within the Device CA PKI.

7.1.1.1 Basic Constraints Extension

CA and Sub-CA PKCs do not assert the pathLenConstraint extension.

7.1.1.2 Certificate Policies Extension

This extension is not critical.

No optional components are asserted in any PKC issued under this CPS.

7.1.1.3 Policy Constraints Extension

No policy constraints are asserted in any PKC issued under this CPS.

7.1.1.4 CRL Distribution Points Extension

This extension is not included in an PKC issued under this CPS.

8 OTHER BUSINESS AND LEGAL MATTERS

8.1 Fees

8.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9 X.509 Certificate Profiles

9.1 CA Certificate Profile

Field	Content
Version	v3
Serial Number	<set by CA>
Signature Algorithm	<set by CA>
Issuer	CN=<set by CA>, O=Certicom Corp, C=CA
Validity:	
Not Before	<set to date of issue>
Not After	<set to 10 years after date of issue>
Subject	CN=<set to issuer>, O=Certicom Corp, C=CA
Public Key:	
Algorithm Identifier	<set by requester>
ECParameters (namedCurve)	<set by requester>
ECPoint	<set by requester>
Point Compressions Format	Uncompressed
Extensions:	
Key Usage (critical)	Certificate Signing, CRL Signing
Basic Constraints (critical)	Subject Type=CA (No Path Length Constraint specified.)
ASN.1 Type:	UTF-8
Signature Digest:	<set by CA>
Other Information:	
"Official" Filename	<set by Device CA PA>

9.1.1 BlackBerry Certicom sect163k1 ROOT CA Certificate Profile

Field	Content
Version	v3
Serial Number	10390645
Signature Algorithm	ecdsa-with-sha1
Issuer	CN=Certicom sect163k1 ROOT CA, O=Certicom Corp, C=CA

Validity:	
Not Before	2017/06/14 18:01:01
Not After	2037/12/31 23:59:59
Subject	CN= Certicom sect163k1 ROOT CA, O=Certicom Corp, C=CA
Public Key:	
Algorithm Identifier	id-eccPublicKey
ECParameters (namedCurve)	sect163k1
ECPoint	0406F3BB0F49E25AE7C7F331C230B287492B6926FE80020D6D36737C9B6A44D86D207827C67A160D7A443B
Point Compression Format	Uncompressed
Extensions:	
Key Usage (critical)	Certificate Signing, CRL Signing
Basic Constraints (critical)	Subject Type=CA (No Path Length Constraint specified.)
ASN.1 Type:	UTF-8
Signature Digest:	SHA-1
Other Information:	
"Official" Filename	cic_ecc_sect163k1_root_cert.pem

9.1.2 BlackBerry Certicom secp384r1 ROOT CA Certificate Profile

Field	Content
Version	v3
Serial Number	103906468
Signature Algorithm	ecdsa-with-sha1
Issuer	CN=Certicom secp384r1 ROOT CA, O=Certicom Corp, C=CA
Validity:	
Not Before	2017/06/14 18:33:09
Not After	2037/12/31 12:59:59
Subject	CN= Certicom secp384r1 ROOT CA, O=Certicom Corp, C=CA
Public Key:	

Algorithm Identifier	id-eccPublicKey
ECParameters (namedCurve)	Secp384r1
ECPoint	047DA28060809C165F746167CC541691B9A6D497DE4C7D9602A4 FD9AA7FCFDC3324CDA3B8CB510C8ADA9FB25E829646759FF1494 9946191471EAE32FC29C4C6D4CD7383E94AAEB9B851364E4A3D9 6B248DE1A94CAE1FA6D865898449A1D3FBB9EF
Point Compression Format	Uncompressed
Extensions:	
Key Usage (critical)	Certificate Signing, CRL Signing
Basic Constraints (critical)	Subject Type=CA (No Path Length Constraint specified.)
ASN.1 Type:	UTF-8
Signature Digest:	SHA-384
Other Information:	
"Official" Filename	cic_ecc_secp384r1_root_cert.pem

9.2 Sub-CA Certificate Profile

Field	**Content**
Version	v3
Serial Number	<set by CA>
Signature Algorithm	<set by CA>
Issuer	CN=<set by CA>, O=Certicom Corp, C=CA
Validity:	
Not Before	<set to date of issue>
Not After	<set to 5 years after date of issue or as required by Subject CA CPS>
Subject	CN=<set by requester>, O=<set by requester>, C=<set by requester>
Public Key:	
Algorithm Identifier	<set by requester>
ECParameters (namedCurve)	<set by requester>
ECPoint	<set by requester>
Point Compression Format	<set by requester>
Extensions:	

Key Usage (critical)	Certificate Signing, CRL Signing
Basic Constraints (critical)	Subject Type=CA (No Path Length Constraint specified.)
ASN.1 Type:	UTF-8
Signature Digest:	<set by CA>
Other Information:	
"Official" Filename	<set by Device CA PA>

9.2.1 BlackBerry Certicom sect163k1 Corporate Identity CA Certificate Profile

Field	**Content**
Version	v3
Serial Number	103906466
Signature Algorithm	ecdsa-with-sha1
Issuer	CN= Certicom sect163k1 ROOT CA, O=Certicom Corp, C=CA
Validity:	
Not Before	2017/06/14 18:06:56
Not After	2027/12/31 23:59:59
Subject	CN= Certicom sect163k1 Corporate Identity CA, O=Certicom Corp, C=CA
Public Key:	
Algorithm Identifier	id-eccPublicKey
ECParameters (namedCurve)	Sect163k1
ECPoint	0404F476BB7D4D499B7FD24F6FEE85809032EA4AC0E2033 0C4ED1DD675DF57243992024930952 92C7978B8
Point Compression Format	Uncompressed
Extensions:	
Key Usage (critical)	Certificate Signing, CRL Signing
Basic Constraints (critical)	Subject Type=CA (No Path Length Constraint specified.)
Extended Key Usage (critical)	Server Authentication, Client Authentication, Code Signing, Email Protection
ASN.1 Type:	UTF-8
Signature Digest:	SHA-1
Other Information:	

"Official" Filename	cic_ecc_sect163k1_corpid_cert.pem

9.3 Administrative Certificate Profile

Field	**Content**
Version	v3
Serial Number	<set by CA>
Signature Algorithm	ecdsa-with-sha1
Issuer	CN= Certicom sect163k1 Corporate Identity CA, O=Certicom Corp, C=CA
Validity:	
Not Before	<set to by CA date of issue>
Not After	<set to by CA 5 years subsequent to date of issue>
Subject	CN=<provided by requestor>, O=<provided by requestor>, OU=<provided by requestor (mandatory if multiple administrative certificates exist for this organization)> C=<provided by requestor>
Public Key:	
Algorithm Identifier	id-ecPublicKey
ECParameters (namedCurve)	sect163k1
ECPoint	<elliptic curve public key provided in certification request>
Point Compression Format	Uncompressed
Extensions:	
Key Usage (critical)	Digital Signature and Key Agreement
ASN.1 Type:	UTF-8
Signature Digest:	SHA-1