BlackBerry Certicom

Device CA
ZigBee Smart Energy Profile
Certification Practices Statement

Version 2.1

March 31, 2020

BlackBerry Limited – Subject to Change without notice.

1 INTRODUCTION 4
1.1 Overview 4
1.2 Document name and identification 5
1.2.1 Revision History 5
1.3 PKI participants 6
1.3.1 Certification Authorities 6
1.3.2 Relying Parties 6
1.4 Certificate Usage 6
1.4.1 Appropriate certificate uses 6
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES 7
3 IDENTIFICATION AND AUTHENTICATION 7
3.1 Naming 7
3.1.1 Types of Names 7
3.1.2 Meaningfulness 7
3.1.3 Uniqueness of Names 7
3.1.4 Recognition, Authentication, and Role of Trademarks 7
3.2 Initial identity validation 7
3.2.1 Method to Prove Possession of Private Key 7
3.2.2 Authentication of Organization Identity 7
3.2.3 Authentication of Individual Information 7
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 8
4.1 Certificate Application Processing 8
4.1.1 Performing Identification and Authentication Functions 8
4.1.2 Enrollment Process and Responsibilities 8
4.2 Certificate Issuance 8
4.2.1 CA Actions During Certificate Issuance 8
4.2.2 Notification to Subscriber by the CA of Issuance of Certificate 8
4.3 Certificate Acceptance 8
4.3.1 Conduct Constituting Certificate Acceptance 8
4.3.2 Publication of the Certificate by the CA 9
4.4 Key Pair and Certificate Usage 9
4.4.1 Subscriber Private Key and Certificate Usage 9
4.4.2 Relying Party Public Key and Certificate Usage 9
4.5 Certificate Renewal 9
4.5.1 Circumstances for Certificate Renewal 9
4.5.2 Who May Request a Certificate Renewal 9
4.6 Certificate Re-Key 9
4.6.1 Circumstances for Certificate Re-Key 9
4.7 Certificate Revocation and Suspension 9
4.7.1 Circumstances for Revocation 9
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 10
5.1 Physical Controls 10
5.2 Audit Logging Procedures 10
5.2.1 Frequency of Processing Log 10
5.3 Records Archival 10
5.3.1 Archive Collection System (Internal or External) 10
5.3.2 Procedures to Obtain and Verify Archive Information 10

5.4 Key Changeover 10
5.5 Compromise and Disaster Recovery 10
5.5.1 CA Private Key Compromise Procedures 10
5.6 CA and RA Termination 10
6 TECHNICAL SECURITY CONTROLS 11
6.1 Key Pair Generation and Installation 11
6.1.1 Key Pair Generation 11
6.1.2 Private Key Delivery to Subscriber 11
6.1.3 Public Key Delivery to Certificate Issuer 11
6.1.4 CA Public Key Delivery to Relying Parties 11
6.1.5 Key Sizes 11
6.1.6 Key Usage Purposes 11
6.2 Private Key Protection and Cryptographic Module Engineering Controls 12
6.2.1 Private Key Archival 12
6.2.2 Method of Destroying Private Key 12
6.2.3 Certificate Operational Periods and Key Pair Usage Periods 12
6.3 Activation Data 12
6.3.1 Activation Data Generation and Installation 12
6.4 Life Cycle Technical Control 12
6.4.1 Security Management Controls 12
7 CERTIFICATE, CRL, AND OCSP PROFILES 13
7.1.1 Root CA Profile 13
7.1.2 ZigBee Smart Energy Profile 13
8 OTHER BUSINESS AND LEGAL MATTERS 15
8.1 Fees 15
8.1.1 Certificate Issuance or Renewal Fees 15
9 Certificate Profiles 16
9.1 Certicom sect163k1 ZigBee CA Certificate Profile 16
9.2 ZigBee Smart Energy Certificate Profile 17

1 INTRODUCTION

The Device CA ZigBee Smart Energy Certification Practices Statement (CPS) is targeted at applications requiring Device Certificates (PKCs) with a bias towards high-volume device manufacturing environments having bulk certificate requirements based upon the ZigBee Smart Energy Profile.

This document fulfills the Subject CA requirements placed upon ZigBee Smart Energy Subject CAs by the Device CA Certificate Policy.

1.1 Overview

This CPS is written for PKCs targeted at devices supporting ZigBee Smart Energy Profile certificate profiles. ZigBee Smart Energy Profile certificate profiles are consistent with the Smart Energy Profile Specification ZigBee Profile 0x0109, ZigBee Document 075356r12ZB and subsequent versions of the ZigBee Profile 0x109 “Smart Energy” specification.

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 ECQV certificate types: Device PKCs. It provides a root of trust for the Device CA Public Key Infrastructure (PKI). The Device CA PKI uses an implicit trust model to fulfill Relying Party (RP) requirements Device PKCs. This implicit trust model relies upon a known and trusted CA public key and the ECQV implicit certificate algorithm.

This CPS contains information on the ZigBee Smart Energy 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.

- Device CA X.509 Certificate Practice Statement

  This CPS provides information on Administrative PKCs.

The above documents 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 ZigBee Smart Energy Profile CPS." It uses the Object Identifier (OID) { 1.3.132.8.7 } 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 Device PKCs.	1.2
19-08-2008	CPS is now Certification Practices Statement everywhere.	1.3
8-Oct-2008	Addressed compliance issues between CP and CPS.	1.4
30-Jan-2009	Updated method of destroying private keys. Now refers to IT Media Handling and Storage Procedures.	1.5
1-April-2009	Added point compression format, ANS.1 type and signature digest specification to ZigBee CA certificate.	1.6
15-Oct-2009	Updated Overview and Certificate Usage sections based upon input from legal.	1.7
25-Mar-2010	Minor editorial changes.	1.8
14-Jun-2013	Updated to address modified practices including key renewal for sub CA, changed BlackBerry to "BlackBerry."	1.9
15-Feb-18	Updated URL for Device CA details on Certicom website. Modified frequency of audit logging data review to monthly per current process. Updated details of Certicom sect163k1 ZigBee CA Certificate Profile.	2.0
31-Mar-20	Updated logo and entity name from Certicom to BlackBerry Certicom.	2.1

1.3 PKI participants

1.3.1 Certification Authorities

The following CAs exist for issuing ZigBee Smart Energy Profile PKCs:

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

  `Issuer: CN=Certicom sect163k1 ZigBee 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.

Device PKCs are not publicly available.

1.4 Certificate Usage

1.4.1 Appropriate certificate uses

Device PKCs usage is limited to devices from ZigBee Smart Energy Certified device manufacturers with products that comply with the ZigBee Smart Energy Profile.

All permitted key usages are defined in section 6.1.6.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

Device PKCs and their revocation information are not published by the CA.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

Within Device CA, the Certificate Subject Name is an 64-bit IEEE MAC address carried in the PKC and bound to the physical address of the Device itself.

3.1.2 Meaningfulness

Certificate Subject Name is a valid MAC address.

3.1.3 Uniqueness of Names

The MAC address in a Device PKC is unique.

3.1.4 Recognition, Authentication, and Role of Trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to Prove Possession of Private Key

The method used by a subscriber to decrypt and verify the Device PKC and the device keying material is described in the "ca_reqtool" User's Guide. The request tool uses subscriber administrative certificates to validate bulk certificate requests.

3.2.2 Authentication of Organization Identity

No stipulation.

3.2.3 Authentication of Individual Information

Only an authorized representative of the subscriber company whose name appears in the Certificate Subject (CN=) of an Administrative PKC is permitted to request a Device PKC. This subscriber must follow the procedures for requesting Device PKCs described in the "ca_reqtool" User's Guide.

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 3.2.

Device certification requests are signed with the Administrative PKC owned by the subscriber making the request. They are encrypted with the following PKC:

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

Subject: C=CA,O=Certicom Corp,OU=TrustPoint,CN=Certicom Corp
sect163k1 ZigBee Corporate Identity
```

4.1.2 Enrollment Process and Responsibilities

Anyone within an organization possessing a valid Administrative PKC may request a Device PKC for that organization.

4.2 Certificate Issuance

4.2.1 CA Actions During Certificate Issuance

Device PKCs are encrypted using the Admininstrative PKC of the subscriber requesting the PKCs and signed by the the following PKC:

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

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

4.2.2 Notification to Subscriber by the CA of Issuance of Certificate

No stipulation.

4.3 Certificate Acceptance

4.3.1 Conduct Constituting Certificate Acceptance

Acceptance of a Device PKC is shown through download of the PKCs by the subscriber using the instructions provided with the shipping notice.

4.3.2 Publication of the Certificate by the CA

Device PKCs are not published by the CA.

4.4 Key Pair and Certificate Usage

4.4.1 Subscriber Private Key and Certificate Usage

Subscribers must use private keys only in accordance with the usages specified sections 1.4.1 and 6.1.6.

4.4.2 Relying Party Public Key and Certificate Usage

RP use of a public key in a Device PKC is subject to all of the key usages presented with that PKC. Use of a public key reconstructed from the Device PKC requires possession of the public key that issued the Device PKC.

4.5 Certificate Renewal

4.5.1 Circumstances for Certificate Renewal

The ZigBee Sub-CA identified in section 9.1 can be renewed.

Device PKCs are not renewed.

4.5.2 Who May Request a Certificate Renewal

The Device CA PA can request the renewal of the ZigBee Sub-CA identified in section 1.3.1.

4.6 Certificate Re-Key

4.6.1 Circumstances for Certificate Re-Key

The ZigBee Sub-CA identified section 9.1 cannot be re-keyed.

Device PKCs are not re-keyed.

4.7 Certificate Revocation and Suspension

4.7.1 Circumstances for Revocation

Device PKCs are not revoked.

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 Policy Authority.

5.2 Audit Logging Procedures

5.2.1 **Frequency of Processing Log**

All audit logging data is reviewed 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

ZigBee Sub-CA key changeover is not performed.

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 such as standard 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

Device PKC key pair generation is performed using software called the “ca_reqtool”. The “ca_reqtool” User’s Guide describes how to generate a key pair or request the CA to perform key pair generation.

6.1.2 Private Key Delivery to Subscriber

Private keys for Device PKCs that are generated by the CA are encrypted using the Administrative PKC owned by the subscriber requesting the Device PKC and signed using the PKC identified in section 4.1.1.

6.1.3 Public Key Delivery to Certificate Issuer

Device PKCs are provided to the primary contact 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 certificates needed to complete the chain of trust to a Device PKC are provided to authorized subscriber contacts when they receive the “ca_reqtool”.

6.1.5 Key Sizes

CA and Sub-CA key sizes are determined by the ZigBee Security Specification.

The key sizes and algorithms required by Device PKCs use the ECQV and the sect163k1 named elliptic curve.

6.1.6 Key Usage Purposes

Device PKCs are issued with both the digital signature and the key agreement key usages asserted.

Pre-Certified Device PKCs are issued with the pre-certified key usages asserted.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Private Key Archival

Private keying material for Device PKCs is encrypted using the Administrative PKC belonging to the subscriber requesting the Device PKC. They are stored by the CA.

The CA cannot access the private keying material once encrypted. Loss of the Administrative private key results in the loss of the Device PKC private keying material.

6.2.2 Method of Destroying Private Key

Private keys are destroyed as described in the Device CA Data Classification and Management document.

6.2.3 Certificate Operational Periods and Key Pair Usage Periods

Device PKCs do not expire.

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 Device CA Password Construction Guidelines document.

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 Sub-CA PKC uses the X.509 v3 certificate profile as consistent with the IETF's RFC 5280. 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 Validity Period

The notAfter attribute for the validity period of the ZigBee Sub-CA PKC is 5 years or less after the notBefore value.

Device PKCs do have a validity period.

7.1.1.2 Basic Constraints Extension

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

7.1.1.3 Certificate Policies Extension

This extension is not critical.

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

7.1.1.4 Policy Constraints Extension

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

7.1.1.5 CRL Distribution Points Extension

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

7.1.2 ZigBee Smart Energy Profile

The ZigBee Smart Energy Profile is defined by the ZigBee Alliance in the document Advanced Metering Initiative Profile 1.0 and 1.1 Specifications (ZigBee Document 075356ro8ZB). This profile contains fields for issuer, subject, key data, and profile attribute data. These are defined below.

7.1.2.1 Issuer Value

The issuer value is a unique 64-bit IEEE MAC address defining the device address. This value is implicitly associated with a pre-existing Root CA or Sub CA public key.

7.1.2.2 Subject Value

The subject value is a unique 64-bit IEEE device address. This value is associated with the device to which the certificate was issued.

7.1.2.3 Key Data

This is 21 bytes of public key reconstruction data computed using the private key that matches the public key identified by the issuer value defined in secion 7.1.4.1 of this document.

7.1.2.4 Profile Identifier

The two bytes ‘x01’ and ‘x09’ which identify the ZigBee Smart Energy Profile.

7.1.2.5 Certificate Version

The one byte ‘x10’ which identifies the certificate version.

7.1.2.6 Cert/Key Usage

The one byte ‘x83’ for “Pre-Certified ZigBee Smart Energy v1.0”, or ‘x03’ for “ZigBee Smart Energy v 1.0”.

7.1.2.7 Manufacturer ID

The two-byte ZigBee Alliance Manufacturer ID.

7.1.2.8 Profile Data

Four bytes for which no stipulation is made.

8 OTHER BUSINESS AND LEGAL MATTERS

8.1 Fees

8.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9 Certificate Profiles

9.1 BlackBerry Certicom sect163k1 ZigBee CA Certificate Profile

The public key provided in this certificate contains the trusted CA key used by relying parties with Device PKCs.

Verification of this certificate using the issuer certificate and a comparison of the public key contained within this provides assurance that the CA key provided with Device PKCs is legitimate.

Field	**Content**
Version	v3
Serial Number	103906467
Signature Algorithm	ecdsa-with-sha1

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

Validity:	
Not Before	2017/06/14 18:13:12
Not After	2027/12/31 23:59:59

Subject	CN= Certicom sect163k1 ZigBee CA,
	O=Certicom Corp,
	C=CA

Public Key:	
Algorithm Identifier	id-eccPublicKey
ECParameters (namedCurve)	sect163k1
ECPoint	0202264C5E4CBFA186A6B925B966B5B3A4D7A390344E
Point Compression Format	Compressed
Extensions:	
Key Usage (critical)	Certificate Signing, CRL Signing
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=0
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_zigbee_cert.pem

9.2 ZigBee Smart Energy Certificate Profile

For Device PKCs conforming to the ZigBee Smart Energy Profile, the Issuer ID: 8 bytes, Certicom ZigBee UI64 / MAC address (bound to BlackBerry Certicom ZigBee Smart Energy private key).

For 10 bytes of "Profile Attribute Data" for ZigBee Smart Energy Version 1.0 (and pre-certified).

Offset	Size	Name	Description
0	2	Profile ID	Defined by the ZigBee Alliance—For the ZigBee Smart Energy Profile v 1.0 = 0x0109—**SET BY MFG.**
2	1	Version/Reserved	Upper 4-bits indicate version of PKC, lower 4 bits are reserved and must be zero filled. For ZigBee Smart Energy Profile v1.0 = 0x10—**SET BY CA.**
3	1	Key/Cert Usage	A bit field that indicates the key usage set by CA 0 = digital signatures 1 = key agreement 2 – 6 = reserved must be zero 7 = pre-certified device For ZigBee Smart Energy v 1.0 = 0x03 For Pre-Certified ZigBee Smart Energy v1.0 = 0x83 **SET BY CA**
4	2	Manufacturer ID	2-byte ZigBee Alliance Manufacturer ID Must match manufacturer ID of customer SET BY MFG - VETTED BY CERTICOM VETTING
6	4		Undefined: manufacturer specified or all 0's