BlackBerry | certicom

BlackBerry V2X CA Certificates

4701 Tahoe Blvd., 5th Floor, Mississauga, Ontario, Canada, L4W 0B5

main 905-507-4220 • support 1-800-511-8011 • fax 905-507-4230

www.certicom.com

TABLE OF CONTENTS

1 ROOT CA CERTIFICATE PROFILE

The V2XCA Root CA Certificate is detailed below:

Name: rca.prod.v2xca.blackberry.com
Hash: 1346ddf49a7fe552e64c70c475c12a687128b6738a0ebd66f99af5239d8d7bbf
Start: 27 Feb 2018
Duration: 70 years
Certificate: rca.prod.v2xca.blackberry.com_certificate.b64
Details:

```
Sequence (ExplicitCertificate) {
   Integer (3)
   Enumerated (CertificateExplicit(0))
   Choice (IssuerIdentifier) :
      [1] Enumerated (SHA256(0))
   Sequence (ToBeSignedCertificate) {
      Choice (CertificateId) :
         [1] UTF8 "rca.prod.v2xca.blackberry.com"
      OctetString (
         00 00 00
      )
      Integer (0)
      Sequence (ValidityPeriod) {
         Integer (446837241)
         Choice (Duration) :
            [6] Integer (70)
      }
      Sequence (SequenceOfPsidSsp) {
         Sequence (PsidSsp) {

            Integer (35)
            Choice (ServiceSpecificPermissions) :
               [0] OctetString (
                  81 00 01
               )
      }
      Sequence (PsidSsp) {
         Integer (256)
         Choice (ServiceSpecificPermissions) :
            [0] OctetString (
               00 01 00 01 01 01 00
            )
      }
```

```
}
Sequence (SequenceOfPsidGroupPermissions) {
   Sequence (PsidGroupPermissions) {
      Choice (SubjectPermissions) :
         [1] Null
      Integer (3)
      Integer (-1)
      BitString (
         c0
      )
   }
   Sequence (PsidGroupPermissions) {
      Choice (SubjectPermissions) :
         [0] Sequence (SequenceOfPsidSspRange) {
            Sequence (PsidSspRange) {
               Integer (35)
            }
         }
      Integer (1)
      Integer (-1)
      BitString (
         c0
      )
   }
   Sequence (PsidGroupPermissions) {
      Choice (SubjectPermissions) :
         [0] Sequence (SequenceOfPsidSspRange) {
            Sequence (PsidSspRange) {
               Integer (38)
            }
         }
      Integer (1)
      Integer (-1)
      BitString (
         c0
      )
   }
   Sequence (PsidGroupPermissions) {
      Choice (SubjectPermissions) :
         [0] Sequence (SequenceOfPsidSspRange) {
            Sequence (PsidSspRange) {
               Integer (256)
            }
```

```
            }
          Integer (1)
          Integer (-1)
          BitString (
            c0
          )
        }
      }
      Choice (VerificationKeyIndicator) :
        [0] Choice (PublicVerificationKey) :
          [0] Choice (EccP256CurvePoint) :
            [2] OctetString (
              74 21 6d 1e 8b 12 8e 38    9c 83 e5 6b d9 4f 88 98
              d0 c2 c9 19 bd 79 41 e8    3d d4 a9 28 a9 15 65 f0
            )
    }
    Choice (Signature) :
      [0] Sequence (EcdsaP256Signature) {
        Choice (EccP256CurvePoint) :
          [0] OctetString (
            54 fe 55 3b 5c 5d d8 0a b6 14 18 0c 6b 40 07 ce
            98 0a 21 45 27 7b 1b 51 c3 77 66 2c 6f 68 b0 27
          )
        OctetString (
          b6 19 95 92 ee 73 79 6d 79 a1 3e 06 21 89 de 31
          eb 1a 94 e8 96 ab 6b 47 76 be 33 28 b0 76 11 d8
        )
      }
}
```

2 INTERMEDIATE CA CERTIFICATE

The ICA certificate is listed below.

Intermediate CA
Name: ica.prod.v2xca.blackberry.com
Hash: 60bbf7a7a4923404587f6cc3efe57f4687be4030cc2ff44fdc17996c9e02eabd
Start: 27 Feb 2018
Duration: 50 years
Certificate:ica.prod.v2xca.blackberry.com_certificate.b64
Details:

```
Sequence (ExplicitCertificate) {
```

```
Integer (3)
Enumerated (CertificateExplicit(0))
Choice (IssuerIdentifier) :
   [0] OctetString (
      f9 9a f5 23 9d 8d 7b bf
   )
Sequence (ToBeSignedCertificate) {
   Choice (CertificateId) :
      [1] UTF8 "ica.prod.v2xca.blackberry.com"
   OctetString (
      8d 7b bf
   )
   Integer (2)
   Sequence (ValidityPeriod) {
      Integer (446851539)
      Choice (Duration) :
         [6] Integer (50)
   }
   Choice (GeographicRegion) :
      [3] Sequence (SequenceOfIdentifiedRegion) {
         Choice (IdentifiedRegion) :
            [0] Integer (124)
         Choice (IdentifiedRegion) :
            [0] Integer (484)
         Choice (IdentifiedRegion) :
            [0] Integer (840)
      }
   Sequence (SequenceOfPsidSsp) {
      Sequence (PsidSsp) {
         Integer (35)
         Choice (ServiceSpecificPermissions) :
            [0] OctetString (
               83 00 01
            )
      }
   }
   Sequence (SequenceOfPsidGroupPermissions) {
      Sequence (PsidGroupPermissions) {
         Choice (SubjectPermissions) :
            [1] Null
         Integer (2)
         Integer (0)
         BitString (
```

```
            c0
          )
        }
        Sequence (PsidGroupPermissions) {
          Choice (SubjectPermissions) :
            [0] Sequence (SequenceOfPsidSspRange) {
              Sequence (PsidSspRange) {
                Integer (35)
                Choice (SspRange) :
                  [1] Null
              }
              Sequence (PsidSspRange) {
                Integer (256)
                Choice (SspRange) :
                  [1] Null
              }
            }
          Integer (1)
          Integer (-1)
          BitString (
            c0
          )
        }
      }
      Choice (VerificationKeyIndicator) :
        [0] Choice (PublicVerificationKey) :
          [0] Choice (EccP256CurvePoint) :
            [3] OctetString (
              a5 8f 20 eb 8f d4 20 7e 60 97 49 74 eb 82 cc 4e
              0f 7a 92 59 c1 56 7e 1b 42 30 18 51 06 e5 ff 30
            )
    }
    Choice (Signature) :
      [0] Sequence (EcdsaP256Signature) {
        Choice (EccP256CurvePoint) :
          [0] OctetString (
            a6 07 60 bd 6d 98 8e 90 b5 2c e9 83 43 fa d8 dd
            23 2f e9 0d 8c 0a d7 23 cc 84 6c 66 a6 b3 c7 0e
          )
        OctetString (
          12 23 f2 7b 09 bd 45 8e    a1 0e 7c 4b 8b 51 d6 67
          ad 55 15 8e 5c ba 96 61    70 3f 1b ac 78 51 ba 33
        )
```

```
        }
    }
```

3 ENROLLMENT CA (ECA) CERTIFICATE

The ECA certificate is listed below.

```
Enrolment CA
Name: eca.prod.v2xca.blackberry.com
Hash: b1024f6bddd4d14e8562589ece27f010d37ec7bc5fb937f4694543befd05dba4
Start: October 4, 2018
Duration: 40 years
Certificate: eca.prod.v2xca.blackberry.com_certificate.b64
Details:
Sequence (ExplicitCertificate) {
   Integer (3)
   Enumerated (CertificateExplicit(0))
   Choice (IssuerIdentifier) :
      [0] OctetString (
         dc 17 99 6c 9e 02 ea bd
      )
   Sequence (ToBeSignedCertificate) {
      Choice (CertificateId) :
         [1] UTF8 "eca.prod.v2xca.blackberry.com"
      OctetString (
         8d 7b bf
      )
      Integer (2)
      Sequence (ValidityPeriod) {
         Integer (465762046)
         Choice (Duration) :
            [6] Integer (40)
      }
      Choice (GeographicRegion) :
         [3] Sequence (SequenceOfIdentifiedRegion) {
            Choice (IdentifiedRegion) :
               [0] Integer (124)
            Choice (IdentifiedRegion) :
               [0] Integer (484)
            Choice (IdentifiedRegion) :
               [0] Integer (840)
         }
      Sequence (SequenceOfPsidSsp) {
         Sequence (PsidSsp) {
            Integer (35)
            Choice (ServiceSpecificPermissions) :
               [0] OctetString (
```

```
                84 00 01
              )
          }
        }
        Sequence (SequenceOfPsidGroupPermissions) {
          Sequence (PsidGroupPermissions) {
            Choice (SubjectPermissions) :
              [1] Null
            Integer (1)
            Integer (0)
            BitString (
              40
            )
          }
        }
        Sequence (PublicEncryptionKey) {
          Enumerated (AES_128_CCM(0))
          Choice (BasePublicEncryptionKey) :
            [0] Choice (EccP256CurvePoint) :
              [3] OctetString (
                95 77 0f 72 2f 7a ce 40    a0 33 0e 86 9a ce 9b 27
                a2 4d 0c 95 d4 00 56 f1    19 cf b0 fe 54 a9 7d 21
              )
        }
        Choice (VerificationKeyIndicator) :
          [0] Choice (PublicVerificationKey) :
            [0] Choice (EccP256CurvePoint) :
              [2] OctetString (
                a5 d6 94 88 db df 63 4b    52 a5 21 54 f5 11 b3 09
                b1 ee aa 60 e0 1d 3d f0    1e c8 eb 4e b3 c2 97 e5
              )
      }
      Choice (Signature) :
        [0] Sequence (EcdsaP256Signature) {
          Choice (EccP256CurvePoint) :
            [0] OctetString (
              cc 03 9d dc 45 c5 04 cb    aa c9 d4 d8 c4 e3 53 8c
              98 6d ed e6 98 91 17 21    6b 5a 1f 20 95 ec c0 62
            )
          OctetString (
            69 d4 4b 01 5a 8b 1e 50    01 08 f2 25 29 44 a2 f3
            c5 05 76 d9 26 dc 61 9d    08 ba cd 94 03 c7 b7 9f
          )
        }
    }
```

4 PSEUDONYM CA (PCA) CERTIFICATE

The PCA certificate is listed below.

Pseudonym CA
Name: pca.prod.v2xca.blackberry.com
Hash: 60d01c31b65ef1f1e765de4d6cf341713c06c957fb131fe284657773f307ea42
Start: October 4, 2018
Duration: 4 years
Certificate: pca.prod.v2xca.blackberry.com_certificate.b64
Details:

```
Sequence (ExplicitCertificate) {
   Integer (3)
   Enumerated (CertificateExplicit(0))
   Choice (IssuerIdentifier) :
      [0] OctetString (
         dc 17 99 6c 9e 02 ea bd
      )
   Sequence (ToBeSignedCertificate) {
      Choice (CertificateId) :
         [1] UTF8 "pca.prod.v2xca.blackberry.com"
      OctetString (
         8d 7b bf
      )
      Integer (2)
      Sequence (ValidityPeriod) {
         Integer (465762114)
         Choice (Duration) :
            [6] Integer (4)
      }
      Choice (GeographicRegion) :
         [3] Sequence (SequenceOfIdentifiedRegion) {
            Choice (IdentifiedRegion) :
               [0] Integer (124)
            Choice (IdentifiedRegion) :
               [0] Integer (484)
            Choice (IdentifiedRegion) :
               [0] Integer (840)
         }
      Sequence (SequenceOfPsidSsp) {
         Sequence (PsidSsp) {
            Integer (35)
            Choice (ServiceSpecificPermissions) :
               [0] OctetString (
                  85 00 01
               )
         }
      }
      Sequence (SequenceOfPsidGroupPermissions) {
```

```
            Sequence (PsidGroupPermissions) {
               Choice (SubjectPermissions) :
                  [1] Null
               Integer (1)
               Integer (0)
               BitString (
                  80
               )
            }
         }
         Sequence (PublicEncryptionKey) {
            Enumerated (AES_128_CCM(0))
            Choice (BasePublicEncryptionKey) :
               [0] Choice (EccP256CurvePoint) :
                  [2] OctetString (
                     d0 8c 0e cd f7 81 44 2c    47 ae d0 8c ea 14 83 ce
                     50 16 42 f3 ce 90 26 e1    56 bd d4 07 6b ff 2a b4
                  )
         }
         Choice (VerificationKeyIndicator) :
            [0] Choice (PublicVerificationKey) :
               [0] Choice (EccP256CurvePoint) :
                  [3] OctetString (
                     40 7e b0 a7 98 10 b1 61    5b 90 52 aa c4 49 65 c4
                     f9 ae 5c 60 ae 4b 03 76    cf 26 4d 19 29 c7 5a 9e
                  )
      }
      Choice (Signature) :
         [0] Sequence (EcdsaP256Signature) {
            Choice (EccP256CurvePoint) :
               [0] OctetString (
                  1a f2 27 7a 47 57 a0 5e    fd 77 11 8a 3e 47 b8 0c
                  fd 47 d1 fe 28 fe 53 4a    e5 c6 3f fc 1f aa c1 03
               )
            OctetString (
               92 3c c1 7e 9b 9c 44 c4    82 a6 ef 48 dd 9f ba 32
               72 40 66 a1 b6 84 7c 9a    81 09 cd 55 36 6d d8 16
            )
         }
}
```