AutoCrypt V2X PKI Root CA Certificate

AUTOCRYPT

Root CA Certificate

Root CA Certificate Overview

- Name : rootca.autocrypt.io
- Hash : DE7A4877FEF79C3611130D4566D4B75B17FDCF873EC3216B5372B2F4DA77ADE6
- Start : 2022-07-08T07:34:41 (UTC)
- Duration : 17 years

Details

```
Sequence (ExplicitCertificate) {
  Integer (3)
  Enumerated (CertificateExplicit(0))
  Choice (IssuerIdentifier) :
    [1] Enumerated (SHA256(0))
   Sequence (ToBeSignedCertificate) {
        Choice (CertificateId) :
      [1] UTF8 "rootca.autocrypt.io"
    OctetString (
      00 00 00
    )
    Integer (0)
    Sequence (ValidityPeriod) {
                  Integer (584350486)
                  Choice (Duration) :
        [6] Integer (17)
    }
    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 02 00 02 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) :
            [3] OctetString (
              32 ed ca cc 4c d7 ee 89 ff ea 7e 05 a0 a6 05 c1
              3e ae f7 08 48 62 fd bd b8 22 53 03 90 c2 77 e5
            )
  }
  Choice (Signature) :
    [0] Sequence (EcdsaP256Signature) {
          Choice (EccP256CurvePoint) :
          [0] OctetString (
            2f dd 11 ea aa e5 b2 32 02 a7 42 b2 40 48 a5 45
            ef f1 71 48 c7 e3 00 c4 0b 72 35 50 93 10 9 c72
          )
          OctetString (
            1a cd ff d7 5e cd f5 b2 47 78 0a ae 79 f4 8f 10
            97 46 16 3a 76 a2 4d 6c 55 1d 06 cb 01 90 26 b4
        )
    }
}
```