COSE Working Group
Internet-Draft
Intended status: Informational
Expires: 23 April 2026

L. Liao
NIO
G. Selander
J. Preu Mattsson
Ericsson

20 October 2025

Test Vectors for CBOR Encoded X.509 (C509) Certificates
draft-lspm-cose-c509-test-vectors-00

Abstract

This document contains examples of CBOR encoded X.509 (C509) certificates, certificate (signing) requests, and certificate request templates.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 23 April 2026.

Copyright Notice

Table of Contents

1. Introduction

This document contains examples of X.509 certificates, certificate (signing) requests, and certificate request templates encoded in CBOR [RFC8949] according to the C509 specification [I-D.ietf-cose-cbor-encoded-cert]. This complements the C509 specification with many readable examples illustrating the encodings of the certificate and certificate request fields, and can be used for testing interoperability between C509 implementations.

Different encodings and formats of certificates and certificate requests are shown: X.509 certificates and certificate requests in PEM format, and C509 certificates and certificate requests in plain hex and in annotated form.

The examples include two types of C509 certificates, distinguished by the value of the c509CertificateType field (see [I-D.ietf-cose-cbor-encoded-cert]):

* c509CertificateType = 03 (here called type 3) is a reversible CBOR encoding of an X.509 certificate, where the issuerSignatureValue field of the C509 certificate contains the signatureValue field of the X.509 certificate, i.e., the digital signature computed upon the ASN.1 DER encoding.

* c509CertificateType = 02 (here called type 2) differs from type 3 only in this value, and that the issuerSignatureValue field of the C509 certificate contains the signature over the TBSCertificate of the C509 certificate, i.e., the digital signature computed upon the CBOR encoding.

The examples also include four types of C509 certificate requests (here called type 0, 1, 2 and 3) distinguished by the value of the c509CertificateRequestType field. This type indicates the format of the request as well as the format of the certificate being requested, see Figure 3 of [I-D.ietf-cose-cbor-encoded-cert].

Following [I-D.ietf-cose-cbor-encoded-cert], the C509 plain hex contains the ~C509Certificate, ~C509CertificateRequest and ~C509CertificateRequestTemplate, i.e. the unwrapped CBOR Sequence [RFC8742]. These can easily be converted into CBOR diagnostic notation (see Section 8 of [RFC8949]) using the CBOR Playground [CborMe]. (Note that CBOR sequences requires ticking the box 'cborseq' in the CBOR Playground.)

Private keys are also provided to enable the creation of signatures (and verification of the ECDH PoP). The keys printed in these examples cannot be considered secret and MUST NOT be used.

The examples are structured as follows:

* Section 2 contains a CA certificate used in later sections.

* Section 3 contains certificates with different types of subject public keys, including RSA, Weierstrass EC, Edwards EC, and Montgomery EC keys.

* Section 4 contains certificates with different types of signature and proof-of-possession algorithms, and references other sections where these algorithms are exemplified.

* Section 5 lists examples of subject attributes, and references other sections where the encoding of these attributes are exemplified.

* Section 6 lists examples of certificate extensions, and references other sections where the encoding of these extensions are exemplified.

* Section 7 gives examples of certificates with attributes or extensions for which no dedicated CBOR encoding has been defined and generic constructs, like CBOR OID [RFC9090], are used.

* Section 8 gives examples of certificate requests with different signature or proof-of-possession algorithms.

* Section 9 gives examples of certificate requests with different extensions.

* Section 10 gives examples of certificate request templates.

Editor's note: The current version does not contain any keys or signatures of post-quantum algorithms. This may be included in a future version or in a separate document.

1.1. Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Readers are expected to be familiar with C509 [I-D.ietf-cose-cbor-encoded-cert].

2. CA Certificate

* Use Ed25519 public key for the CA due to its small size in public key and signature value

* Self-signed

* Key: Ed25519

* Signature algorithm: Ed25519

* Signature algorithm: Ed25519

2.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VwBCIEILRAHe59PSDnJqhejd8oytYWP0L6SU8kMSRdxzbDybzG
-----END PRIVATE KEY-----
```

2.2. X.509 Certificate

PEM content (300 bytes):

```
-----BEGIN CERTIFICATE-----
MIIBKDCB26ADAgECAgEBMAUGAytlcDASMRAwDgYDVQQDDAd0ZXN0IGNhMB4XDTI1
MDEwMTAwMDAwMFoXDTI2MTIzMTIzNTk1OVowEjEQMA4GA1UEAwwHdGVzdCBjYTAq
MAUGAytlcAMhAFqUFKxW0bavDJZvxTuUdrXJXQ7qrvdk2e/obbcyDDbho1YwVDAd
BgNVHQ4EFgQUf824LQSVLho2uQrzejzxZtFe+SEwDgYDVR0PAQH/BAQDAgEGMBIG
A1UdEQQLMAmCB2FiYy5jb20wDwYDVR0TAQH/BAUwAwEB/zAFBgMrZXADQQA8bYD+
f1IDbzRAcw4R/HBfsyJ/Il0gf8SZ6RKvsFOMVdcAoLVAmEIZgV/5xxPGrnf3M5lo
DnmLRWMSIHZXricI
-----END CERTIFICATE-----
```

2.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 2.2.

* Compared to the C509 type 2 certificate, the only difference is the certificate type, the signature value, and the public key identifier.

Plain hex (161 bytes):

```
0341010CF61A677485801A6B36EC7F67746573742063610A58205A9414AC56D1B6AF
0C966FC53B9476B5C95D0EEAAEF764D9EFE86DB7320C36E18801547FCDB82D04952E
1A36B90AF37A3CF166D15EF9212118600367616263 2E636F6D232058403C6D80FE7F
52036F3440730E11FC705FB3227F225D207FC499E912AFB0538C55D700A0B5409842
19815FF9C713C6AE77F73399680E798B456312207657AE2708
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

2.4. C509 Type 2 Certificate

Plain hex (161 bytes):

```
0241010CF61A677485801A6B36EC7F67746573742063610A58205A9414AC56D1B6AF
0C966FC53B9476B5C95D0EEAAEF764D9EFE86DB7320C36E1880154C16DE726347331
107520B4ED9ED0088023A560332118600367616263 2E636F6D23205840AA0CF7A8B2
67EDE76B0C2CC0240A60587700D749A959EE3D96B59E13DEF9F137DC51FB9E460A5E
BF7F0C659365EBE32B44CCA4A2AC67E3D18A867C36400E2C01
```

Annotated hex:

```
     0: 02             # [0]. certificate type=2
     1: 41             # [1]. serial number=byte[1]
     2:   01
     3: 0C             # [2]. signature alg=12: Ed25519
     4: F6             # [3]. issuer=<null>
     5: 1A 67748580    # [4]. notBefore=1735689600: 2025-01-01T00:00:00Z
    10: 1A 6B36EC7F    # [5]. notAfter=1798761599: 2026-12-31T23:59:59Z
    15: 67             # [6]. subject=char[7]
    16:   74657374206361  # "test ca"
    23: 0A             # [7]. subjectPublicKeyAlg=10: Ed25519
    24: 58 20          # [8]. subject public key=byte[32]
    26:   5A9414AC56D1B6AF0C966FC53B9476B5C95D0EEAAEF764D9EFE86DB7320C
    56:   36E1
    58: 88             # [9]. extensions=array[8]
                         # extension[0]
    59:     01             # type=1: SubjectKeyIdentifier
    60:     54             # value=byte[20]
    61:       C16DE726347331107520B4ED9ED0088023A56033
                         # extension[1]
    81:     21             # type=-2: KeyUsage, critical
    82:     18 60          # value=96: [keyCertSign, cRLSign]
                         # extension[2]
    84:     03             # type=3: SubjectAlternativeName
    85:     67             # DNS, value=char[7]
    86:       6162632E636F6D  # "abc.com"
                         # extension[3]
    93:     23             # type=-4: BasicConstraints, critical
    94:     20             # value=-1: CA: true, pathLenConstraint:
                           # unlimited
    95: 58 40          # [10]. signature value=byte[64]
    97:   AA0CF7A8B267EDE76B0C2CC0240A60587700D749A959EE3D96B59E13DEF9
   127:   F137DC51FB9E460A5EBF7F0C659365EBE32B44CCA4A2AC67E3D18A867C36
   157:   400E2C01
```

3. Certificates With Different Subject Public Keys

3.1. RSA Public Key With Public Exponent 65537

* Self-signed

* RSA public key with public exponent = 65537 and 1024-bit modulus

* Signature algorithm: sha256WithRSAEncryption

* NotAfter: null

* Subject: only commonName of EUI-48

* Extensions: with only one non-critical extension keyUsage

3.1.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MIICdgIBADANBgkqhkiG9w0BAQEFAASCAmAwggJcAgEAAoGBALgJL28EcmqSHPqy
0xOunS8Bx85GX6t9pix6XHP6zl/7ovHdgKKa3EM5nPyiInm4miZIEOW5JrteDT9y
enY+FgE/ifj+rFnQ+91eiwxSgn5UkPE7hMNjTonG0XMa5fGmD4jtEY0IDhqyyqUy
0GwvfSoIdN7k5rblcoP2R42vQlPbAgMBAAECgYAfuNGYyMLyFLJzEhzpERmd7ygi
KaY2+KcKlqLWCP7Gs6jAGQahwKDD46voLghUQ9oqTBTBjDsdY9ZTv+dU91myXRnR
81QZxVmzFfZRZ1yNBZE7NctjH1UM1uejX08dp8ypFEZ8YUXydgwnVThyma6nwqeD
W2hAnP7S7LcisHs9/QJBAPJNe3l0Mqeq8Fwp4DL6opcnehT4qMe0d+/4nSIVodQc
iOJE752KYXs1GZ0/+ETWNoBn8L7ZFO9gjcd/xtlSAEUCQQDCcHyiGcuNRFx6vTGo
8Su460/PF8ViALOUAZwPiFO+Fxpx2kyWKk5DtKbCOXgeEPE2gcCFT1ztb/nusPJv
PJWfAkBM1rN0ZZv2veexYno90GulQZiec+iaRCnQyOeTuoZyTIZAMxpFvG+Dceho
jLO/qKrp94xKCW9xJg5wGJ5HppB9AkAVaK1Qa+att0k3en1tTKCzy7UN6GAjWlBr
i4HTc/9Efua6gn7MSfw0GEAEQq+nH9ZvWfoIs6RXwGyUi4cmGFWhAkEAjf207bsV
VUEhtJ3LEsgOaTGg+8VfHIZuXxNNwxxyIm2YacTXDXpvfslFWRuNxomp44dtPmmb
bqJRmhxWlrumnw==
-----END PRIVATE KEY-----
```

3.1.2. X.509 Certificate

PEM content (464 bytes):

```
-----BEGIN CERTIFICATE-----
MIIBzDCCATWgAwIBAgICEjQwDQYJKoZIhvcNAQELBQAwIjEgMB4GA1UEAwwXMTIt
MzQtNTYtRkYtRkUtNzgtOTAtQUIwIBcNMjUwMTAyMDAwMDAwWhgPOTk5OTEyMzEy
MzU5NTlaMCIxIDAeBgNVBAMMFzEyLTM0LTU2LUZGLUZFLTc4LTkwLUFCMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC4CS9vBHJqkhz6stMTrp0vAcfORl+rfaYs
elxz+s5f+6Lx3YCimtxDOZz8oiJ5uJomSBDluSa7Xg0/cnp2PhYBP4n4/qxZ0Pvd
XosMUoJ+VJDxO4TDY06JxtFzGuXxpg+I7RGNCA4assqlMtBsL30qCHTe5Oa25XKD
9keNr0JT2wIDAQABow8wDTALBgNVHQ8EBAMCB4AwDQYJKoZIhvcNAQELBQADgYEA
GBLBJZ3E5ChTAXQA4d/ZO6GbIyvogslssZnHA80bDbg03D8/6USiLw/Y3ETDc+CS
dWtBTRsVWLv9DTEMWu54D2UQnp9jgoiuouE+mCvAhC00DjCAizYJ5yDk5xN93Vik
7jHXYl9hrTw2ey826BOcyJuxlfUfN9GMGf7LHRYs6Ok=
-----END CERTIFICATE-----
```

3.1.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 3.1.2.

* Compared to the C509 type 2 certificate, the only difference is the certificate type, the signature value, and the public key identifier.

Plain hex (283 bytes):

```
0342123417F61A6775D700F6D830461234567890AB005880B8092F6F04726A921CFA
B2D313AE9D2F01C7CE465FAB7DA62C7A5C73FACE5FFBA2F1DD80A29ADC43399CFCA2
2279B89A264810E5B926BB5E0D3F727A763E16013F89F8FEAC59D0FBDD5E8B0C5282
7E5490F13B84C3634E89C6D1731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A
0874DEE4E6B6E57283F6478DAF4253DB0158801812C1259DC4E42853017400E1DFD9
3BA19B232BE882C96CB199C703CD1B0DB834DC3F3FE944A22F0FD8DC44C373E09275
6B414D1B1558BBFD0D310C5AEE780F65109E9F638288AEA2E13E982BC0842D340E30
808B3609E720E4E7137DDD58A4EE31D7625F61AD3C367B2F36E8139CC89BB195F51F
37D18C19FECB1D162CE8E9
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

3.1.4. C509 Type 2 Certificate

Plain hex (283 bytes):

```
0242123417F61A6775D700F6D830461234567890AB005880B8092F6F04726A921CFA
B2D313AE9D2F01C7CE465FAB7DA62C7A5C73FACE5FFBA2F1DD80A29ADC43399CFCA2
2279B89A264810E5B926BB5E0D3F727A763E16013F89F8FEAC59D0FBDD5E8B0C5282
7E5490F13B84C3634E89C6D1731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A
0874DEE4E6B6E57283F6478DAF4253DB015880371A7322CDD9DECB1F3B4851A18A47
B461A479C29DCE7397290C79DB95643A5C7FE2B1F02DB6AF5F0BCA9602D837F7EB3D
4AA28738CBCAD385043304E648022A1E9FE0FD19687839AC3EC7C7B6F6E5F85B4416
BA085D5C9E367A0B892829F2F3E4A31D3FDA0E58EA701A72CB3F1B4A06E3DF44F449
2FCFBD5C5F71F03340D7CA
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 17             # [2]. signature alg=23: sha256WithRSAEncryption
  5: F6             # [3]. issuer=<null>
  6: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 11: F6             # [5]. notAfter=<null>: 9999-12-31T23:59:59Z
 12: D8 30          # [6]. subject=tag(48)
 14:   46             # byte[6]
 15:     1234567890AB
 21: 00             # [7]. subjectPublicKeyAlg=0: RSA
 22: 58 80          # [8]. subject public key=byte[128]
 24:   B8092F6F04726A921CFAB2D313AE9D2F01C7CE465FAB7DA62C7A5C73FACE
 54:   5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5B926BB5E0D3F727A
 84:   763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C3634E89C6D1
114:   731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4E6B6E572
144:   83F6478DAF4253DB
152: 01             # [9]. extensions=1, KeyUsage: [digitalSignature]
153: 58 80          # [10]. signature value=byte[128]
155:   371A7322CDD9DECB1F3B4851A18A47B461A479C29DCE7397290C79DB9564
185:   3A5C7FE2B1F02DB6AF5F0BCA9602D837F7EB3D4AA28738CBCAD385043304
215:   E648022A1E9FE0FD19687839AC3EC7C7B6F6E5F85B4416BA085D5C9E367A
245:   0B892829F2F3E4A31D3FDA0E58EA701A72CB3F1B4A06E3DF44F4492FCFBD
275:   5C5F71F03340D7CA
```

3.2. RSA Public Key With Public Exponent 3

* Self-signed

* RSA public key with public exponent = 3 and 1024-bit modulus

* Signature algorithm: sha384WithRSAEncryption

* Subject: only commonName of EUI-64

* Extensions: with only one critical extension keyUsage

3.2.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MIICdQIBADANBgkqhkiG9w0BAQEFAASCAl8wggJbAgEAAoGBAIZ56wtPD8lB3+1N
CPeTMsFsl9/m19pL2/KKMzv8aLcXfFA5jVdfFOL0j6FKX9hDbeszEEFO6t6xId4G
ecaiqtlaRLr2pfE8nK1Oz7SM14dfn76HZv5tHsKr2wMxoOktKKvEdMNzeHAZlZW3
hvMfljyKbg9wu4LJ0A885zNTntMLAgEDAoGAFmmnLI0tTDWlUjeBfpiIdZIZT/vO
pGH5/cGzNKoRc9k/YrRCOTqDeyjCmuG6pAs8/IiCtY0nJR2FpQEUS8XHI/vL0Iuy
G1IFDuZfbXRfZPJARPELsaiAro3whb15hyQVANwajgt1RbYRziJyQAafvbUCFDAx
zXh7pirUIyerpw8CQQDCcHyiGcuNRFx6vTGo8Su460/PF8ViALOUAZwPiFO+Fxpx
2kyWKk5DtKbCOXgeEPE2gcCFT1ztb/nusPJvPJWfAkEAsQ1bDl+Bwzn3bdXyKan9
+TLREgkPGBn3xDZEsT9qlpOMKfsimI5/kXYaJp/62cbZFd/VykFVCXowTT1t9lxT
FQJBAIGgUxa73QjYPacoy8X2HSXyNTS6g5arImKrvV+wN9QPZvaRiGQcNC0jGdbQ
+r619iRWgFjfk0j1UUnLTEooY78CQHYI517qVoImpPPj9sZxU/t3NgwGChART9gk
Lct/nGRiXXFSFxBe/7ZOvBm//JEvO2PqjobWOLD8IDN+SU7oN2MCQQCy2Wpl7m7m
hErmI2k57QMUe7L1sqvIrMpGMpMIZAOgEIYXhNB1zN7krEry6AxihBUD/LEW5eUN
8a+sWQIF4SC6
-----END PRIVATE KEY-----
```

3.2.2. X.509 Certificate

PEM content (463 bytes):

```
-----BEGIN CERTIFICATE-----
MIIByzCCATSgAwIBAgICEjQwDQYJKoZIhvcNAQEMBQAwIjEgMB4GA1UEAwwXMTIt
MzQtNTYtNzgtOTAtQUItQ0QtRUYwHhcNMjUwMTAyMDAwMDAwWhcNMjYwMTAyMDAw
MDAwWjAiMSAwHgYDVQQDDBcxMi0zNC01Ni03OC05MC1BQi1DRC1FRjCBnTANBgkq
hkiG9w0BAQEFAAOBiwAwgYcCgYEAhnnrC08PyUHf7U0I95MywWyX3+bX2kvb8looz
O/xotxd8UDmNV18U4vSPoUpf2ENt6zMQQU7q3rEh3gZ5xqKq2VpEuval8TycrU7P
tIzXh1+fvodm/m0ewqvbAzGg6S0oq8R0w3N4cBmVlbeG8x+WPIpuD3C7gsnQDzzn
M1Oe0wsCAQOjEjAQMA4GA1UdDwEB/wQEAwIHgDANBgkqhkiG9w0BAQwFAAOBgQBE
lXlPBk0Q6anK6p9RBwjqp2RsUE0QA9lBrjaoxEuJbwNbfKFeujOr74EcQgYn9vRa
Tes3/2Wz62bNbdJpDy+HD+ENbAw6RYnD1ROThjb0wfeIUYpI1FToxZ28Oov+rpu1
buW5Yj9STo4p8X/0YZgiJE7fwePFzFkvA24+nt4aqA==
-----END CERTIFICATE-----
```

3.2.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 3.2.2.

Plain hex (293 bytes):

```
034212341818F61A6775D7001A69570A80D830481234567890ABCDEF008258808679
EB0B4F0FC941DFED4D08F79332C16C97DFE6D7DA4BDBF28A333BFC68B7177C50398D
575F14E2F48FA14A5FD8436DEB3310414EEADEB121DE0679C6A2AAD95A44BAF6A5F1
3C9CAD4ECFB48CD7875F9FBE8766FE6D1EC2ABDB0331A0E92D28ABC474C373787019
9595B786F31F963C8A6E0F70BB82C9D00F3CE733539ED30B4103205880449579 4F06
4D10E9A9CAEA9F510708EAA7646C504D1003D941AE36A8C44B896F035B7CA15EBA33
ABEF811C420627F6F45A4DEB37FF65B3EB66CD6DD2690F2F870FE10D6C0C3A4589C3
D513938636F4C1F788518A48D454E8C59DBC3A8BFEAE9BB56EE5B9623F524E8E29F1
7FF4619822244EDFC1E3C5CC592F036E3E9EDE1AA8
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

3.2.4. C509 Type 2 Certificate

Plain hex (293 bytes):

```
024212341818F61A6775D7001A69570A80D830481234567890ABCDEF008258808679
EB0B4F0FC941DFED4D08F79332C16C97DFE6D7DA4BDBF28A333BFC68B7177C50398D
575F14E2F48FA14A5FD8436DEB3310414EEADEB121DE0679C6A2AAD95A44BAF6A5F1
3C9CAD4ECFB48CD7875F9FBE8766FE6D1EC2ABDB0331A0E92D28ABC474C373787019
9595B786F31F963C8A6E0F70BB82C9D00F3CE733539ED30B4103205880511BFC472F
8DD672A522B24B33C971091CA3CA02699A813CC5931E1AD541338ABC1FF9883EC72E
9AF4F3B442C5FF5040231E1A6C1FF8CA3AA3F5CB1E743FD6C009D40692DBD8D5B7A9
1BB630EC18F1402DCCFFC1B67AC69DA5E4A8CCE0A3DF7396CDBA16C731370B8A96BF
62E67F93A56C74DA88F5F4DCC16FCF24C2D3B3192F
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 18 18          # [2]. signature alg=24: sha384WithRSAEncryption
  6: F6             # [3]. issuer=<null>
  7: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 12: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 17: D8 30          # [6]. subject=tag(48)
 19:   48             # byte[8]
 20:     1234567890ABCDEF
 28: 00             # [7]. subjectPublicKeyAlg=0: RSA
 29: 82             # [8]. subject public key=array[2]
 30:   58 80          # [0]=byte[128]
 32:     8679EB0B4F0FC941DFED4D08F79332C16C97DFE6D7DA4BDBF28A333BFC
 61:     68B7177C50398D575F14E2F48FA14A5FD8436DEB3310414EEADEB121DE
 90:     0679C6A2AAD95A44BAF6A5F13C9CAD4ECFB48CD7875F9FBE8766FE6D1E
119:     C2ABDB0331A0E92D28ABC474C3737870199595B786F31F963C8A6E0F70
148:     BB82C9D00F3CE733539ED30B
160:   41            # [1]=byte[1]
161:     03
162: 20            # [9]. extensions=-1, KeyUsage, critical:
                   #      [digitalSignature]
163: 58 80         # [10]. signature value=byte[128]
165:   511BFC472F8DD672A522B24B33C971091CA3CA02699A813CC5931E1AD541
195:   338ABC1FF9883EC72E9AF4F3B442C5FF5040231E1A6C1FF8CA3AA3F5CB1E
225:   743FD6C009D40692DBD8D5B7A91BB630EC18F1402DCCFFC1B67AC69DA5E4
255:   A8CCE0A3DF7396CDBA16C731370B8A96BF62E67F93A56C74DA88F5F4DCC1
285:   6FCF24C2D3B3192F
```

3.3. Weierstrass EC Public Key With secp256r1

* Self-signed

* EC key with curve secp256r1

* Signature algorithm: ecdsa-with-SHA256

* Subject: only commonName of even number of lowercase hex chars

* Extensions

  - Basic Constraints: CA, with no pathLen

  - Extended Key Usage: with only int usage

  - Subject Key Identifier

3.3.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MEECAQAwEwYHKoZIzj0CAQYIKoZIzj0DAQcEJzAlAgEBBCAMGYOct/eLyZgLXgeP
Q3jT81GUERXqvBvkzaxRD1pG7A==
-----END PRIVATE KEY-----
```

3.3.2. X.509 Certificate

PEM content (383 bytes):

```
-----BEGIN CERTIFICATE-----
MIIBezCCASCgAwIBAgICEjQwCgYIKoZIzj0EAwIwGzEZMBcGA1UEAwwQMTIzNDU2
Nzg5MGFiY2RlZjAeFw0yNTAxMDIwMDAwMDBaFw0yNjAxMDIwMDAwMDBaMBsxGTAX
BgNVBAMMEDEyMzQ1Njc4OTBhYmNkZWYwWTATBgcqhkjOPQIBBggqhkjOPQMBBwNC
AAT0E1lqhxJZlbTg2Le++8TW7bEfYa8IqzJAjU/5+QeN26s2Na/UltVlaiLv3D1Z
xEgqmYNrs1j79Mp405MENshXo1QwUjAdBgNVHQ4EFgQUB+EsTKzpXCKF7EpbBaSi
uw7IenowCwYDVR0PBAQDAgEGMA8GA1UdEwEB/wQFMAMBAf8wEwYDVR0lBAwwCgYI
KwYBBQUHAwEwCgYIKoZIzj0EAwIDSQAwRgIhAIol6Kq7pLGbjg0VlqR2wsQvUGj1
80V2BoBuLyhKIubnAiEAp5m4CfQ2QkbnoJOzzBDOKLXtmsX+4pVCSDuF5iQ7wT8=
-----END CERTIFICATE-----
```

3.3.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 3.3.2.

Plain hex (189 bytes):

```
0342123400F61A6775D7001A69570A80481234567890ABCDEF01584104F413596A87
125995B4E0D8B7BEFBC4D6EDB11F61AF08AB32408D4FF9F9078DDBAB3635AFD496D5
656A22EFDC3D59C4482A99836BB358FBF4CA78D3930436C85788015407E12C4CACE9
5C2285EC4A5B05A4A2BB0EC87A7A02186023200801584 08A25E8AABBA4B19B8E0D15
96A476C2C42F5068F5F3457606806E2F284A22E6E7A799B809F4364246E7A093B3CC
10CE28B5ED9AC5FEE29542483B85E6243BC13F
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, the signature value, and the public key identifier.

3.3.4. C509 Type 3 Certificate With Compressed EC Public Key

* C509 type 3 certificate with compressed EC public key converted from the X.509 certificate in Section 3.3.2.

Plain hex (157 bytes):

```
0342123400F61A6775D7001A69570A80481234567890ABCDEF015821FDF413596A87
125995B4E0D8B7BEFBC4D6EDB11F61AF08AB32408D4FF9F9078DDB88015407E12C4C
ACE95C2285EC4A5B05A4A2BB0EC87A7A0218602320080158408A25E8AABBA4B19B8E
0D1596A476C2C42F5068F5F3457606806E2F284A22E6E7A799B809F4364246E7A093
B3CC10CE28B5ED9AC5FEE29542483B85E6243BC13F
```

Annotated hex:

```
  0: 03             # [0]. certificate type=3
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 00             # [2]. signature alg=0: ecdsa-with-sha256
  5: F6             # [3]. issuer=<null>
  6: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 11: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 16: 48             # [6]. subject=byte[8]
 17:   1234567890ABCDEF
 25: 01             # [7]. subjectPublicKeyAlg=1: EC public key with
                    #      curve secp256r1
 26: 58 21          # [8]. subject public key=byte[33]
 28:   FDF413596A87125995B4E0D8B7BEFBC4D6EDB11F61AF08AB32408D4FF9F9
 58:   078DDB
 61: 88             # [9]. extensions=array[8]
                      # extension[0]
 62:     01             # type=1: SubjectKeyIdentifier
 63:     54             # value=byte[20]
 64:       07E12C4CACE95C2285EC4A5B05A4A2BB0EC87A7A
                    # extension[1]
 84:     02             # type=2: KeyUsage
 85:     18 60          # value=96: [keyCertSign, cRLSign]
                    # extension[2]
 87:     23             # type=-4: BasicConstraints, critical
 88:     20             # value=-1: CA: true, pathLenConstraint:
                        # unlimited
                    # extension[3]
 89:     08             # type=8: ExtendedKeyUsage
 90:     01             # 1: serverAuth
 91: 58 40          # [10]. signature value=byte[64]
 93:   8A25E8AABBA4B19B8E0D1596A476C2C42F5068F5F3457606806E2F284A22
123:   E6E7A799B809F4364246E7A093B3CC10CE28B5ED9AC5FEE29542483B85E6
153:   243BC13F
```

3.3.5. C509 Type 2 Certificate

Plain hex (189 bytes):

```
0242123400F61A6775D7001A69570A80481234567890ABCDEF01584104F413596A87
125995B4E0D8B7BEFBC4D6EDB11F61AF08AB32408D4FF9F9078DDBAB3635AFD496D5
656A22EFDC3D59C4482A99836BB358FBF4CA78D3930436C8578801541F3BC19DE194
830066C6EAE7CB9D211339EDD9420218602320080158408A25E8AABBA4B19B8E0D15
96A476C2C42F5068F5F3457606806E2F284A22E6E71EF91E63F35636A4D497E1FB4D
3C393ADCDB09D92E02E0194D703ECD98EB2D79
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 00             # [2]. signature alg=0: ecdsa-with-sha256
  5: F6             # [3]. issuer=<null>
  6: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 11: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 16: 48             # [6]. subject=byte[8]
 17:   1234567890ABCDEF
 25: 01             # [7]. subjectPublicKeyAlg=1: EC public key with
                    #      curve secp256r1
 26: 58 41          # [8]. subject public key=byte[65]
 28:   04F413596A87125995B4E0D8B7BEFBC4D6EDB11F61AF08AB32408D4FF9F9
 58:   078DDBAB3635AFD496D5656A22EFDC3D59C4482A99836BB358FBF4CA78D3
 88:   930436C857
 93: 88             # [9]. extensions=array[8]
                      # extension[0]
 94:     01             # type=1: SubjectKeyIdentifier
 95:     54             # value=byte[20]
 96:       1F3BC19DE194830066C6EAE7CB9D211339EDD942
                      # extension[1]
116:     02             # type=2: KeyUsage
117:     18 60          # value=96: [keyCertSign, cRLSign]
                      # extension[2]
119:     23             # type=-4: BasicConstraints, critical
120:     20             # value=-1: CA: true, pathLenConstraint:
                        # unlimited
                      # extension[3]
121:     08             # type=8: ExtendedKeyUsage
122:     01             # 1: serverAuth
123: 58 40          # [10]. signature value=byte[64]
125:   8A25E8AABBA4B19B8E0D1596A476C2C42F5068F5F3457606806E2F284A22
155:   E6E71EF91E63F35636A4D497E1FB4D3C393ADCDB09D92E02E0194D703ECD
185:   98EB2D79
```

3.4. Weierstrass EC Public Key With secp384r1

* Self-signed

* EC key with curve secp384r1

* Subject: only commonName with normal text

* Extensions

  - Basic Constraints: CA, with pathLen

  - Extended Key Usage: with only oid usage

  - Certificate Policies

  - Inhibit anyPolicy

3.4.1. Private Key

```
-----BEGIN PRIVATE KEY-----
ME4CAQAwEAYHKoZIzj0CAQYFK4EEACIENzA1AgEBBDA21kT4P50ZNXthip3vROKI
MkRC62+05D/N4Hr8iGcZ6gaS2DwnwNLOUYwYlY1pT3I=
-----END PRIVATE KEY-----
```

3.4.2. X.509 Certificate

PEM content (533 bytes):

```
-----BEGIN CERTIFICATE-----
MIICETCCAZegAwIBAgICEjQwCgYIKoZIzj0EAwMwHTEbMBkGA1UEAwwSc2VsZnNp
Z24tc2VjcDM4NHIxMB4XDTI1MDEwMjAwMDAwMFoXDTI2MDEwMjAwMDAwMFowHTEb
MBkGA1UEAwwSc2VsZnNpZ24tc2VjcDM4NHIxMHYwEAYHKoZIzj0CAQYFK4EEACID
YgAE3Wdi8DWJlFE3Ky/ptSqDFK0Q4sQ2PFpYSeKW/lGqub/QOrA40zQYoLzYMoCr
oL2RBAFxZcBItTRrVBCeRJ/MiJ5O6HC1+KLGPa5BTeGXVb4nihdeBA1KTBoO5G6S
Slwpo4GpMIGmMAsGA1UdDwQEAwIBBjASBgNVHRMBAf8ECDAGAQH/AgEBMGAGA1Ud
IARZMFcwCAYGZ4EMAQIDMEsGBFUdIAAwQzAaBggrBgEFBQcCARYOaHR0cDovL2Nw
cy51cmwwJQYIKwYBBQUHAgIwGQwXdGhpcyBpcyB0aGUgdXNlciBub3RpY2UwFQYD
VR0lBA4wDAYKKwYBBAGC41JjBDAKBgNVHTYEAwIBADAKBggqhkjOPQQDAwNoADBl
AjA0frXtSeH2U24qPztd8cEtm670QN+8Qr1F0x9LP9q9+p1oWoRYLZixskdCEPHH
hdoCMQCeIjIwB4iXmYgw4CLCIHCSStA6O5aWzSJ1Xc6GUy2rwR/SLg3Hk890DAmf
p3RoEgM=
-----END CERTIFICATE-----
```

3.4.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 3.4.2.

Plain hex (300 bytes):

```
0342123401F61A6775D7001A69570A807273656C667369676E2D7365637033383472
3102586104DD6762F035899451372B2FE9B52A8314AD10E2C4363C5A5849E296FE51
AAB9BFD03AB038D33418A0BCD83280ABA0BD9104017165C048B5346B54109E449FCC
889E4EE870B5F8A2C63DAE414DE19755BE278A175E040D4A4C1A0EE46E924A5C298A
021860230106830300840l6E687474703A2F2F6370732E75726C0277746869732069
732074686520757365726572206E6F74696365084A2B0601040182E3526304181E005860
347EB5ED49E1F6536E2A3F3B5DF1C12D9BAEF440DFBC42BD45D31F4B3FDABDFA9D68
5A84582D98B1B2474210F1C785DA9E22323007889799883OE022C22070924AD03A3B
9696CD22755DCE86532DABC11FD22E0DC793CF740C099FA774681203
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

3.4.4. C509 Type 2 Certificate

Plain hex (300 bytes):

```
0242123401F61A6775D7001A69570A807273656C667369676E2D7365637033383472
3102586104DD6762F035899451372B2FE9B52A8314AD10E2C4363C5A5849E296FE51
AAB9BFD03AB038D33418A0BCD83280ABA0BD9104017165C048B5346B54109E449FCC
889E4EE870B5F8A2C63DAE414DE19755BE278A175E040D4A4C1A0EE46E924A5C298A
021860230106830300840l6E687474703A2F2F6370732E75726C0277746869732069
732074686520757365726572206E6F74696365084A2B0601040182E3526304181E005860
347EB5ED49E1F6536E2A3F3B5DF1C12D9BAEF440DFBC42BD45D31F4B3FDABDFA9D68
5A84582D98B1B2474210F1C785DA99A28737A0AFB997FE5858C457570DF214A1688E
DE02740B32058B42C9CF6C559F1C7EB3EB75334496AD26BF589412C8
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 01             # [2]. signature alg=1: ecdsa-with-sha384
  5: F6             # [3]. issuer=<null>
  6: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 11: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 16: 72             # [6]. subject=char[18]
 17:   73656C667369676E2D73656370333834 # "selfsign-secp384"
 33:   7231                             # "r1"
 35: 02             # [7]. subjectPublicKeyAlg=2: EC public key with
                    #      curve secp384r1
 36: 58 61          # [8]. subject public key=byte[97]
 38:   04DD6762F035899451372B2FE9B52A8314AD10E2C4363C5A5849E296FE51
 68:   AAB9BFD03AB038D33418A0BCD83280ABA0BD9104017165C048B5346B5410
 98:   9E449FCC889E4EE870B5F8A2C63DAE414DE19755BE278A175E040D4A4C1A
128:   0EE46E924A5C29
```

```
   135: 8A             # [9]. extensions=array[10]
                         # extension[0]
   136:     02            # type=2: KeyUsage
   137:     18 60         # value=96: [keyCertSign, cRLSign]
                         # extension[1]
   139:     23            # type=-4: BasicConstraints, critical
   140:     01            # value=1: CA: true, pathLenConstraint: 1
                         # extension[2]
   141:     06            # type=6: CertificatePolicies
   142:     83            # value=array[3]
                            # CertificatePolicy[0]
   143:         03           # PolicyIdentifier=3:
                             # IndividualValidation
                            # CertificatePolicy[1]
   144:         00           # PolicyIdentifier=0: any
   145:         84           # PolicyQualifierInfos=array[4]
                               # PolicyQualifierInfo[0]
   146:             01           # policyQualifierId=1:
                                 # DomainValidation
   147:             6E           # qualifier=char[14]
   148:               687474703A2F2F6370732E75726C # "http://cps.url"
                               # PolicyQualifierInfo[1]
   162:             02           # policyQualifierId=2:
                                 # OrganizationValidation
   163:             77           # qualifier=char[23]
   164:               7468697320697320746865207573 # "this is the us"
   178:               6572206E6F74696365           # "er notice"
                         # extension[3]
   187:     08            # type=8: ExtendedKeyUsage
   188:     4A            # byte[10]:
   189:        2B0601040182E3526304 # oid: 1.3.6.1.4.1.45522.99.4
                         # extension[4]
   199:     18 1E         # type=30: InhibitAnyPolicy
   201:     00            # value=simple-uint(0)
   202: 58 60          # [10]. signature value=byte[96]
   204:   347EB5ED49E1F6536E2A3F3B5DF1C12D9BAEF440DFBC42BD45D31F4B3FDA
   234:   BDFA9D685A84582D98B1B2474210F1C785DA99A28737A0AFB997FE5858C4
   264:   57570DF214A1688EDE02740B32058B42C9CF6C559F1C7EB3EB75334496AD
   294:   26BF589412C8
```

3.5. Weierstrass EC Public Key With secp521r1

* Self-signed

* EC key with curve secp521r1

* Signature algorithm: ecdsa-with-SHA512

* Subject: empty

* Extensions

  - Basic Constraints: non-CA

  - Extended Key Usage: with usages of int and oid.

  - Subject Alt Name

3.5.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MGACAQAwEAYHKoZIzj0CAQYFK4EEACMESTBHAgEBBEIBTyH+UdnGf8eNYO8U2b7w
Z4A21kT4P50ZOUtjpDPxlkovVX2d6SpSsMn1njLAikYP2YOZwZZwd86lpB1+7sdS
a/Y=
-----END PRIVATE KEY-----
```

3.5.2. X.509 Certificate

PEM content (669 bytes):

```
-----BEGIN CERTIFICATE-----
MIICmTCCAfqgAwIBAgICEjQwCgYIKoZIzj0EAwQwADAeFw0yNTAxMDIwMDAwMDBa
Fw0yNjAxMDIwMDAwMDBaMAAwgZswEAYHKoZIzj0CAQYFK4EEACMDgYYABABVOM6P
fN4ikzXIWViqzQKd32XPwqcqdQVeY7j+WdB/tL3xDbe4un1XxcaR65bquXQRYVpq
Qw5ReHAxcZzrwwXmkgBwXMgouXVfj9U0Urd3pAy2eSVU5XGLq5HqPwMIakBypHBH
zuwkk8OEBF/Mbtjk90ilIjrxKQHrLhmmwoiVHJObBaOCAR8wggEbMAsGA1UdDwQE
AwIHgDCB3gYDVR0RBIHWMIHTpB4wHDELMAkGA1UEBgwCREUxDTALBgNVBAMMBFRl
c3SCB2FiYy5jb22BD2FiY0BleGFtcGxlLm9yZ6AiBggrBgEFBQcICaAWDBRzbXRw
dXRmOEBtYWlsYm94Lm9yZ4YVaHR0cDovL215dXJpbC5jb20vYWJjiAorBgEEAYLj
UmMIhwQRERERoBoGCisGAQQBguNSYwGgDAQKIiIiIiIiIiIqAuBggrBgEFBQcI
BKAiMCAGCisGAQQBguNSYwIEEgQQMzMzMzMzMzMzMzMzMzMzMzAMBgNVHRMBAf8E
AjAAMB0GA1UdJQQWMBQGCCsGAQUFBwMCBggrBgEFBQcDATAKBggqhkjOPQQDBAOB
jAAwgYgCQgEvg1j2RiHKaPfbZErv43lYBBpoZDavzt3nCs66c3RNcBR3hKQa1nZz
oe5bO5sag1FVOinoeBWr/MpdHeEJnyhLTAJCATuMwY1apn9zyoZAqNdUAYtNYbCU
YtnSPgnl6ltG8KOYo4KeYk9QJvjK8XMjP2dQlPLK+VAXz2p5oGENl8saf1ni
-----END CERTIFICATE-----
```

3.5.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 3.5.2.

Plain hex (457 bytes):

```
0342123402F61A6775D7001A69570A8080035885040055 38CE8F7CDE229335C85958
AACD029DDF65CFC2A72A75055E63B8FE59D07FB4BDF10DB7B8BA7D57C5C691EB96EA
B97411615A6A430E51787031719CEBC305E69200705CC828B9755F8FD53452B777A4
0CB6792554E5718BAB91EA3F03086A4072A47047CEEC2493C384045FCC6ED8E4F748
A5223AF12901EB2E19A6C288951C939B05880201039204840462445016454657374
02676162632E636F6D016F616263406578616D706C652E6F72672174736D74707574
6638406D61696C626F782E6F72670675687474703A2F2F6D797572696C2E636F6D2F
616263084A2B0601040182E3526308074411111111100824A2B0601040182E3526301
4C040A22222222222222222222220824A2B0601040182E35263025204103333333333
33333333333333333333332321088202015884012F8358F64621CA68F7DB644AEFE3
7958041A686436AFCEDDE70ACEBA73744D70147784A41AD67673A1EE5B3B9B1A8351
553A29E87815ABFCCA5D1DE1099F284B4C013B8CC18D5AA67F73CA8640A8D754018B
4D61B09462D9D23E09E5EA5B46F0A398A3829E624F5026F8CAF173233F675094F2CA
F95017CF6A79A0610D97CB1A7F59E2
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

3.5.4. C509 Type 2 Certificate

Plain hex (457 bytes):

```
0242123402F61A6775D7001A69570A8080035885040055 38CE8F7CDE229335C85958
AACD029DDF65CFC2A72A75055E63B8FE59D07FB4BDF10DB7B8BA7D57C5C691EB96EA
B97411615A6A430E51787031719CEBC305E69200705CC828B9755F8FD53452B777A4
0CB6792554E5718BAB91EA3F03086A4072A47047CEEC2493C384045FCC6ED8E4F748
A5223AF12901EB2E19A6C288951C939B05880201039204840462445016454657374
02676162632E636F6D016F616263406578616D706C652E6F72672174736D74707574
6638406D61696C626F782E6F72670675687474703A2F2F6D797572696C2E636F6D2F
616263084A2B0601040182E3526308074411111111100824A2B0601040182E3526301
4C040A22222222222222222222220824A2B0601040182E35263025204103333333333
33333333333333333333332321088202015884012F8358F64621CA68F7DB644AEFE3
7958041A686436AFCEDDE70ACEBA73744D70147784A41AD67673A1EE5B3B9B1A8351
553A29E87815ABFCCA5D1DE1099F284B4C01CDC0923D3297C17BB6EF9F5F14B090BD
CE0F5713A50EE5BB54FB208A95383BDCBEF2468346BAA70A85E8DF85E3FF5799DC2E
C913A1D560FAEB6142B396D46339A1
```

Annotated hex:

```
  0: 02            # [0]. certificate type=2
  1: 42            # [1]. serial number=byte[2]
  2:   1234
  4: 02            # [2]. signature alg=2: ecdsa-with-sha512
  5: F6            # [3]. issuer=<null>
  6: 1A 6775D700   # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 11: 1A 69570A80   # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
```

```
    16: 80             # [6]. subject=array[0], 0 attribute
    17: 03             # [7]. subjectPublicKeyAlg=3: EC public key with
                       #      curve secp521r1
    18: 58 85          # [8]. subject public key=byte[133]
    20:   04005538CE8F7CDE229335C85958AACD029DDF65CFC2A72A75055E63B8FE
    50:   59D07FB4BDF10DB7B8BA7D57C5C691EB96EAB97411615A6A430E51787031
    80:   719CEBC305E69200705CC828B9755F8FD53452B777A40CB6792554E5718B
   110:   AB91EA3F03086A4072A47047CEEC2493C384045FCC6ED8E4F748A5223AF1
   140:   2901EB2E19A6C288951C939B05
   153: 88             # [9]. extensions=array[8]
                         # extension[0]
   154:     02            # type=2: KeyUsage
   155:     01            # value=1: [digitalSignature]
                        # extension[1]
   156:     03            # type=3: SubjectAlternativeName
   157:     92            # value=array[18]
                           # GeneralName[0]
   158:         04          # GeneralNameType=4: directoryName
   159:         84          # GeneralNameValue=array[4], 2 attributes
                              # attribute[0]
   160:             04        # type=4: country
   161:             62        # value=char[2]
   162:               4445     # "DE"
                              # attribute[1]
   164:             01        # type=1: commonName
   165:             64        # value=char[4]
   166:               54657374  # "Test"
                           # GeneralName[1]
   170:         02            # GeneralNameType=2: dNSName
   171:         67            # GeneralNameValue=char[7]
   172:           6162632E636F6D  # "abc.com"
                           # GeneralName[2]
   179:         01            # GeneralNameType=1: rfc822Name
   180:         6F            # GeneralNameValue=char[15]
   181:           616263406578616D706C652E6F7267 # "abc@example.org"
                           # GeneralName[3]
   196:         21            # GeneralNameType=-2: on_smtpUTF8Mailbox
   197:         74            # GeneralNameValue=char[20]
   198:           736D747075746638406D61696C626F78 # "smtputf8@mailbox"
   214:           2E6F7267                       # ".org"
                           # GeneralName[4]
   218:         06            # GeneralNameType=6: uri
   219:         75            # GeneralNameValue=char[21]
   220:           687474703A2F2F6D797572696C2E636F # "http://myuril.co"
   236:           6D2F616263                     # "m/abc"
                           # GeneralName[5]
   241:         08            # GeneralNameType=8: registeredID
   242:         4A            # GeneralNameValue=byte[10]:
```

```
   243:            2B0601040182E3526308 # oid: 1.3.6.1.4.1.45522.99.8
                              # GeneralName[6]
   253:         07               # GeneralNameType=7: iPAddress
   254:         44               # GeneralNameValue=byte[4]
   255:           11111111
                              # GeneralName[7]
   259:         00               # GeneralNameType=0: otherName
   260:         82               # GeneralNameValue=array[2]
   261:           4A               # id=byte[10]:
   262:              2B0601040182E3526301 # oid: 1.3.6.1.4.1.45522.99.1
   272:           4C               # value=byte[12]
   273:             040A2222222222222222
                              # GeneralName[8]
   285:         20               # GeneralNameType=-1:
                                 # on_hardwareModuleName
   286:         82               # GeneralNameValue=array[2]
   287:           4A               # id=byte[10]:
   288:              2B0601040182E3526302 # oid: 1.3.6.1.4.1.45522.99.2
   298:           52               # value=byte[18]
   299:             0410333333333333333333333333333333
                         # extension[2]
   317:     23              # type=-4: BasicConstraints, critical
   318:     21              # value=-2: CA: false
                         # extension[3]
   319:     08              # type=8: ExtendedKeyUsage
   320:     82              # value=array[2]
   321:       02              # 2: clientAuth
   322:       01              # 1: serverAuth
   323: 58 84          # [10]. signature value=byte[132]
   325:   012F8358F64621CA68F7DB644AEFE37958041A686436AFCEDDE70ACEBA73
   355:   744D70147784A41AD67673A1EE5B3B9B1A8351553A29E87815ABFCCA5D1D
   385:   E1099F284B4C01CDC0923D3297C17BB6EF9F5F14B090BDCE0F5713A50EE5
   415:   BB54FB208A95383BDCBEF2468346BAA70A85E8DF85E3FF5799DC2EC913A1
   445:   D560FAEB6142B396D46339A1
```

3.6. Weierstrass EC Public Key With brainpoolP256r1

* Self-signed

* EC key with curve brainpoolP256r1

* Signature algorithm: ecdsa-with-shake128

* Subject:

  - country

  - state

- locality
- postalCode
- street

* Extensions:
  - IP Resources with IPAddressChoice of value "null"
  - IP Resources v2 with IPAddressChoice of value "null"
  - AS Resources
  - AS Resources v2

3.6.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MEICAQAwFAYHKoZIzj0CAQYJKyQDAwIIAQEHBCcwJQIBAQQgiOJE752KYXs1GZ0/
+ETWNoBn8L7ZFO9gjcd/xtlR/iE=
-----END PRIVATE KEY-----
```

3.6.2. X.509 Certificate

PEM content (644 bytes):

```
-----BEGIN CERTIFICATE-----
MIICgDCCAiegAwIBAgICEjQwCgYIKwYBBQUHBiAwgYUxITAfBgNVBAMMGHNlbGZz
aWduLWJyYWlucG9vbHAyNTZyMTELMAkGA1UEBgwCREUxFDASBgNVBAcMC215IGxv
Y2FsaXR5MREwDwYDVQQIDAhteSBzdGF0ZTESMBAGA1UECQwJbXkgc3RyZWV0MRYw
FAYDVQQRDA1teSBwb3N0YWxDb2RlMB4XDTI1MDEwMjAwMDAwMFoXDTI2MDEwMjAw
MDAwMFowgYUxITAfBgNVBAMMGHNlbGZzaWduLWJyYWlucG9vbHAyNTZyMTELMAkG
A1UEBgwCREUxFDASBgNVBAcMC215IGxvY2FsaXR5MREwDwYDVQQIDAhteSBzdGF0
ZTESMBAGA1UECQwJbXkgc3RyZWV0MRYwFAYDVQQRDA1teSBwb3N0YWxDb2RlMFow
FAYHKoZIzj0CAQYJKyQDAwIIAQEHA0IABHewd0Eu6YlQd57Ygv/LFkjgFCcjVEaW
JPW84vFPMkKtSsxWhqhlCNWftyn9wpgRGI2L8BbOSlFRBU2viIxI1e2jgYMwgYAw
CwYDVR0PBAQDAgeAMB4GCCsGAQUFBwEHBBIwEDAGBAIAAQUAMAYEAgACBQAwHQYI
KwYBBQUHAQgEETAPoA0wCwIBAjAGAgEDAgEGMB4GCCsGAQUFBwEcBBIwEDAGBAIA
AQUAMAYEAgACBQAwEgYIKwYBBQUHAR0EBjAEoAIFADAKBggrBgEFBQcGIANHADBE
AiBJk8WuMFasCrr1rN+G0vQIf+HPdH1s4tmjCKGGWbArFAIgSp0eiTNoEGMehnxx
f2FhP0AZwXUIF2N/BbJj8ZvtozM=
-----END CERTIFICATE-----
```

3.6.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 3.6.2.

Plain hex (259 bytes):

```
0342123403F61A6775D7001A69570A808C01781873656C667369676E2D627261696E
706F6F6C703235367231046244450 56B6D79206C6F63616C69747906686D79207374
61746507696D7920737472656574 0C6D6D7920706F7374616C436F64651818584104
77B077412EE98950779ED882FFCB1648E014272354469624F5BCE2F14F3242AD4ACC
5686A86508D59FB729FDC29811188D8BF016CE4A5151054DAF888C48D5ED8A020118
208401F602F6182182028201031822840 1F602F61823F658404993C5AE3056AC0ABA
F5ACDF86D2F4087FE1CF747D6CE2D9A308A18659B02B144A9D1E89336810631E867C
717F61613F4019C1750817637F05B263F19BEDA333
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

3.6.4. C509 Type 2 Certificate

Plain hex (259 bytes):

```
0242123403F61A6775D7001A69570A808C01781873656C667369676E2D627261696E
706F6F6C703235367231046244450 56B6D79206C6F63616C69747906686D79207374
61746507696D7920737472656574 0C6D6D7920706F7374616C436F64651818584104
77B077412EE98950779ED882FFCB1648E014272354469624F5BCE2F14F3242AD4ACC
5686A86508D59FB729FDC29811188D8BF016CE4A5151054DAF888C48D5ED8A020118
208401F602F6182182028201031822840 1F602F61823F658409CDE645DD8D02AA75B
6B773837DD8C6ABA2F07231569BAB5258BC4A0EC0E1EFB636B28E6BF1FD29522DD5C
20384BDCA1C35144440C5084E4A780CEEE84B06221
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 03             # [2]. signature alg=3: ecdsa-with-shake128
  5: F6             # [3]. issuer=<null>
  6: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 11: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 16: 8C             # [6]. subject=array[12], 6 attributes
                      # attribute[0]
 17:     01             # type=1: commonName
 18:     78 18          # value=char[24]
 20:       73656C667369676E2D627261696E706F # "selfsign-brainpo"
 36:       6F6C703235367231                 # "olp256r1"
                    # attribute[1]
 44:     04             # type=4: country
 45:     62             # value=char[2]
 46:       4445            # "DE"
```

```
                        # attribute[2]
    48:     05            # type=5: locality
    49:     6B            # value=char[11]
    50:       6D79206C6F63616C697479 # "my locality"
                        # attribute[3]
    61:     06            # type=6: state
    62:     68            # value=char[8]
    63:       6D79207374617465 # "my state"
                        # attribute[4]
    71:     07            # type=7: street
    72:     69            # value=char[9]
    73:       6D7920737472656574 # "my street"
                        # attribute[5]
    82:     0C            # type=12: postalCode
    83:     6D            # value=char[13]
    84:       6D7920706F7374616C436F6465 # "my postalCode"
    97: 18 18           # [7]. subjectPublicKeyAlg=24: EC public key with
                        #      curve brainpoolp256r1
    99: 58 41           # [8]. subject public key=byte[65]
   101:   0477B077412EE98950779ED882FFCB1648E014272354469624F5BCE2F14F
   131:   3242AD4ACC5686A86508D59FB729FDC29811188D8BF016CE4A5151054DAF
   161:   888C48D5ED
   166: 8A             # [9]. extensions=array[10]
                         # extension[0]
   167:     02            # type=2: KeyUsage
   168:     01            # value=1: [digitalSignature]
                        # extension[1]
   169:     18 20         # type=32: IPAddressBlocks
   171:     84            # value=array[4]
                            # IPAddrBlock[0]
   172:         01           # AFI=1: IPv4
                            # IPAddrBlock[1]
   173:         F6           # IPAddressChoice=<null>
                            # IPAddrBlock[2]
   174:         02           # AFI=2: IPv6
                            # IPAddrBlock[3]
   175:         F6           # IPAddressChoice=<null>
                        # extension[2]
   176:     18 21         # type=33: AutonomousSysIds
   178:     82            # value=array[2]
   179:       02            # id=2
   180:       82            # range=array[2]
   181:         01            # min=1
   182:         03            # max=3
                        # extension[3]
   183:     18 22         # type=34: IPAddressBlocksV2
   185:     84            # value=array[4]
                            # IPAddrBlock[0]
```

```
   186:         01             # AFI=1: IPv4
                              # IPAddrBlock[1]
   187:         F6             # IPAddressChoice=<null>
                              # IPAddrBlock[2]
   188:         02             # AFI=2: IPv6
                              # IPAddrBlock[3]
   189:         F6             # IPAddressChoice=<null>
                         # extension[4]
   190:     18 23            # type=35: AutonomousSysIdsV2
   192:     F6               # value=<null>
   193: 58 40           # [10]. signature value=byte[64]
   195:   9CDE645DD8D02AA75B6B773837DD8C6ABA2F07231569BAB5258BC4A0EC0E
   225:   1EFB636B28E6BF1FD29522DD5C20384BDCA1C35144440C5084E4A780CEEE
   255:   84B06221
```

3.7. Weierstrass EC Public Key With brainpoolP384r1

* Self-signed

* EC key with curve brainpoolP384r1

* Signature algorithm: ecdsa-with-sha384

* Subject:

  - surname

  - givenName

  - title

  - name

* Extensions:

  - IP Resources with non-null IPAddressChoice

  - IP Resources V2 with non-null IPAddressChoice

3.7.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MFICAQAwFAYHKoZIzj0CAQYJKyQDAwIIAQELBDcwNQIBAQQwgGfwvtkU72CNx3/G
2VH+IU85UqnWjleSVxt87bW/XLcURC4qRMOJB9G6KmsodzwN
-----END PRIVATE KEY-----
```

3.7.2. X.509 Certificate

PEM content (775 bytes):

```
-----BEGIN CERTIFICATE-----
MIIDAzCCAoqgAwIBAgICEjQwCgYIKoZIzj0EAwMwdDEhMB8GA1UEAwwYc2VsZnNp
Z24tYnJhaW5wb29scDM4NHIxMRMwEQYDVQQEDApteSBzdXJuYW1lMREwDwYDVQQM
DAhteSB0aXRsZTEVMBMGA1UEKgwMbXkgZ2l2ZW5OYW1lMRAwDgYDVQQpDAdteSBu
YW1lMB4XDTI1MDEwMjAwMDAwMFoXDTI2MDEwMjAwMDAwMFowdDEhMB8GA1UEAwwY
c2VsZnNpZ24tYnJhaW5wb29scDM4NHIxMRMwEQYDVQQEDApteSBzdXJuYW1lMREw
DwYDVQQMDAhteSB0aXRsZTEVMBMGA1UEKgwMbXkgZ2l2ZW5OYW1lMRAwDgYDVQQp
DAdteSBuYW1lMHowFAYHKoZIzj0CAQYJKyQDAwIIAQELA2IABGcJyZKRm0nEj9kx
0FxJfThl5ghMkd86TH54H0GFQ7Aj1Z6L8l0TP7GglOnULI+m7TtG6Yg6NavUsKnT
Cq79m36I7TgAVl0efwYzE01lGSktSb1V7DChZxl/7A90KYIrlaOB6jCB5zALBgNV
HQ8EBAMCB4AwawYIKwYBBQUHAQcEXzBdMCAEAgABMBoDBAQKAAADBAAKAAAwDAMF
AAoCAAADAwEKBDA5BAIAAjAzAwkAIAIAAQAAAAADCAAgAgACAAAAMBwDEQAgAgAD
AAAAAAAAAAAAAAAAAwcBIAIACAAAMGsGCCsGAQUFBwEcBF8wXTAgBAIAATAaAwQE
CgAAAwQACgAAMAwDBQAKAgAAAwMBCgQwOQQCAAIwMwMJACACAAEAAAAAAwgAIAIA
AgAAADAcAxEAIAIAAwAAAAAAAAAAAAAAAAMHASACAAgAADAKBggqhkjOPQQDAwNn
ADBkAjBnCcmSkZtJxI/ZMdBcSX04ZeYITJHfOkx+eB9BhUOwI9Wei/JdEz+xoJTp
1CyPpu0CMAwhL0vtg3X0tC2kZsuFMFJqzVUoJC5WuVi8M70+SXwg7a5KlP7bKZdu
1ULKnEDqoQ==
-----END CERTIFICATE-----
```

3.7.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 3.7.2.

Plain hex (504 bytes):

```
0342123401F61A6775D7001A69570A808A01781873656C667369676E2D627261696E
706F6F6C703338347231026A6D79207375726E616D650A686D79207469746C650D6C
6D7920676976656E4E616D651819676D79206E616D6518195861046709C992919B49
C48FD931D05C497D3865E6084C91DF3A4C7E781F418543B023D59E8BF25D133FB1A0
94E9D42C8FA6ED3B46E9883A35ABD4B0A9D30AAEFD9B7E88ED3800565D1E7F063313
4D6519292D49BD55EC30A167197FEC0F7429822B95860201482B0601050507010758
5F305D302004020001301A0304040A00000304000A0000300C0305000A0200000303
010A0430390402000230330309002002000100000000308002002000200000301C
0311002002000300000000000000000000000030701200200080000482B06010505
07011C585F305D302004020001301A0304040A00000304000A0000300C0305000A02
00000303010A0430390402000230330309002002000100000000308002002000200
0000301C0311002002000300000000000000000000000030701200200080000586O
6709C992919B49C48FD931D05C497D3865E6084C91DF3A4C7E781F418543B023D59E
8BF25D133FB1A094E9D42C8FA6ED0C212F4BED8375F4B42DA466CB8530526ACD5528
242E56B958BC33BD3E497C20EDAE4A94FEDB29976ED542CA9C40EAA1
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

3.7.4. C509 Type 2 Certificate

Plain hex (432 bytes):

```
0242123401F61A6775D7001A69570A808A01781873656C667369676E2D627261696E
706F6F6C703338347231026A6D79207375726E616D650A686D79207469746C650D6C
6D7920676976656E4E616D651819676D79206E616D6518195861046709C992919B49
C48FD931D05C497D3865E6084C91DF3A4C7E781F418543B023D59E8BF25D133FB1A0
94E9D42C8FA6ED3B46E9883A35ABD4B0A9D30AAEFD9B7E88ED3800565D1E7F063313
4D6519292D49BD55EC30A167197FEC0F7429822B9586020118208401854 30A000004
430A00000082440A020000420A040285482002000100000000004720020002000000
00825020020003000000000000000000000000046200200080000182284018543 0A00
0004430A00000082440A020000420A040285482002000100000000004720020002 00
0000008250200200030000000000000000000000004620020008000058606709C992
919B49C48FD931D05C497D3865E6084C91DF3A4C7E781F418543B023D59E8BF25D13
3FB1A094E9D42C8FA6ED4B168EF9239575AE498B2EC8E7169D69F29D3007733E80D1
EE1AAB99E6EED4D9A2E2129ACD422AF95986C94956D5CD67
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 01             # [2]. signature alg=1: ecdsa-with-sha384
  5: F6             # [3]. issuer=<null>
  6: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 11: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 16: 8A             # [6]. subject=array[10], 5 attributes
                      # attribute[0]
 17:     01             # type=1: commonName
 18:     78 18          # value=char[24]
 20:       73656C667369676E2D627261696E706F # "selfsign-brainpo"
 36:       6F6C703338347231                 # "olp384r1"
                      # attribute[1]
 44:     02             # type=2: surname
 45:     6A             # value=char[10]
 46:       6D79207375726E616D65 # "my surname"
                      # attribute[2]
 56:     0A             # type=10: title
 57:     68             # value=char[8]
 58:       6D79207469746C65 # "my title"
                      # attribute[3]
 66:     0D             # type=13: givenName
 67:     6C             # value=char[12]
 68:       6D7920676976656E4E616D65 # "my givenName"
```

```
                        # attribute[4]
    80:     18 19         # type=25: name
    82:     67            # value=char[7]
    83:       6D79206E616D65  # "my name"
    90: 18 19           # [7]. subjectPublicKeyAlg=25: EC public key with
                        #      curve brainpoolp384r1
    92: 58 61           # [8]. subject public key=byte[97]
    94:   046709C992919B49C48FD931D05C497D3865E6084C91DF3A4C7E781F4185
   124:   43B023D59E8BF25D133FB1A094E9D42C8FA6ED3B46E9883A35ABD4B0A9D3
   154:   0AAEFD9B7E88ED3800565D1E7F0633134D6519292D49BD55EC30A167197F
   184:   EC0F7429822B95
   191: 86             # [9]. extensions=array[6]
                         # extension[0]
   192:     02           # type=2: KeyUsage
   193:     01           # value=1: [digitalSignature]
                       # extension[1]
   194:     18 20         # type=32: IPAddressBlocks
   196:     84            # value=array[4]
                            # IPAddrBlock[0]
   197:         01           # AFI=1: IPv4
                            # IPAddrBlock[1]
   198:         85           # IPAddressChoice=array[5]
                               # IPAddressOrRange[0]=AddressPrefix
   199:             43           # Address=byte[3]
   200:               0A0000
   203:             04           # unusedBits=4
                               # IPAddressOrRange[1]=AddressPrefix
   204:             43           # Address=byte[3]
   205:               0A0000
   208:             00           # unusedBits=0
                               # IPAddressOrRange[2]=AddressRange
   209:             82           # array[2]
   210:               44           # min=byte[4]
   211:                 0A020000
   215:               42           # max=byte[2]
   216:                 0A04
                          # IPAddrBlock[2]
   218:         02           # AFI=2: IPv6
                            # IPAddrBlock[3]
   219:         85           # IPAddressChoice=array[5]
                               # IPAddressOrRange[0]=AddressPrefix
   220:             48           # Address=byte[8]
   221:               2002000100000000
   229:             00           # unusedBits=0
                               # IPAddressOrRange[1]=AddressPrefix
   230:             47           # Address=byte[7]
   231:               20020002000000
   238:             00           # unusedBits=0
```

```
                                # IPAddressOrRange[2]=AddressRange
   239:             82             # array[2]
   240:               50             # min=byte[16]
   241:                 20020003000000000000000000000000
   257:               46             # max=byte[6]
   258:                 200200080000
                       # extension[2]
   264:     18 22       # type=34: IPAddressBlocksV2
   266:     84          # value=array[4]
                          # IPAddrBlock[0]
   267:         01         # AFI=1: IPv4
                          # IPAddrBlock[1]
   268:         85         # IPAddressChoice=array[5]
                            # IPAddressOrRange[0]=AddressPrefix
   269:             43       # Address=byte[3]
   270:               0A0000
   273:             04       # unusedBits=4
                            # IPAddressOrRange[1]=AddressPrefix
   274:             43       # Address=byte[3]
   275:               0A0000
   278:             00       # unusedBits=0
                            # IPAddressOrRange[2]=AddressRange
   279:             82       # array[2]
   280:               44       # min=byte[4]
   281:                 0A020000
   285:               42       # max=byte[2]
   286:                 0A04
                          # IPAddrBlock[2]
   288:         02         # AFI=2: IPv6
                          # IPAddrBlock[3]
   289:         85         # IPAddressChoice=array[5]
                            # IPAddressOrRange[0]=AddressPrefix
   290:             48       # Address=byte[8]
   291:               2002000100000000
   299:             00       # unusedBits=0
                            # IPAddressOrRange[1]=AddressPrefix
   300:             47       # Address=byte[7]
   301:               20020002000000
   308:             00       # unusedBits=0
                            # IPAddressOrRange[2]=AddressRange
   309:             82       # array[2]
   310:               50       # min=byte[16]
   311:                 20020003000000000000000000000000
   327:               46       # max=byte[6]
   328:                 200200080000
   334: 58 60        # [10]. signature value=byte[96]
   336:   6709C992919B49C48FD931D05C497D3865E6084C91DF3A4C7E781F418543
   366:   B023D59E8BF25D133FB1A094E9D42C8FA6ED4B168EF9239575AE498B2EC8
```

```
   396:   E7169D69F29D3007733E80D1EE1AAB99E6EED4D9A2E2129ACD422AF95986
   426:   C94956D5CD67
```

3.8. Weierstrass EC Public Key With brainpoolP512r1

* Self-signed
* EC key with curve brainpoolp512r1
* Signature algorithm: ecdsa-with-SHAKE256
* Subject:
  - jurisdictionOfIncorporationCountryName
  - jurisdictionOfIncorporation StateOrProvinceName
  - jurisdictionOfIncorporationLocalityName
* Extensions:
  - Subject Directory Attributes
  - Subject Information Access
  - Policy Mappings

3.8.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MGICAQAwFAYHKoZIzj0CAQYJKyQDAwIIAQENBEcwRQIBAQRATzlSqdaOV5JXG3zt
tb9ctxRELipEw4kH0boqayh3PA02UW4leQ6yGuqx7iyWQKOzZYT5tnXlUqGh7jh/
+l3K8g==
-----END PRIVATE KEY-----
```

3.8.2. X.509 Certificate

PEM content (820 bytes):

```
-----BEGIN CERTIFICATE-----
MIIDMDCCApOgAwIBAgICEjQwCgYIKwYBBQUHBiEwgZExITAfBgNVBAMMGHNlbGZz
aWduLWJyYWlucG9vbHA1MTJyMTEsMCoGCysGAQQBgjc8AgEBDBtteSBqdXJJbmNv
cnBvcmF0aW9uTG9jYWxpdHkxKTAnBgsrBgEEAYI3PAIBAgwYbXkganVySW5jb3Jw
b3JhdGlvblN0YXRlMRMwEQYLKwYBBAGCNzwCAQMMAlNFMB4XDTI1MDEwMjAwMDAw
MFoXDTI2MDEwMjAwMDAwMFowgZExITAfBgNVBAMMGHNlbGZzaWduLWJyYWlucG9v
bHA1MTJyMTEsMCoGCysGAQQBgjc8AgEBDBtteSBqdXJJbmNvcnBvcmF0aW9uTG9j
YWxpdHkxKTAnBgsrBgEEAYI3PAIBAgwYbXkganVySW5jb3Jwb3JhdGlvblN0YXRl
MRMwEQYLKwYBBAGCNzwCAQMMAlNFMIGbMBQGByqGSM49AgEGCSskAwMCCAEBDQOB
ggAEbTJwZ9M0zlP6KTF6oge4XKI3Yj8ZoQxZS/Ak/D/+tk+rWITQ1EiicVUuAufP
RNi/EE2hgs7B3olchBi4Up2biyxLgKc23cVkcdalLGzkFOadVzVrFfwIpGth+lty
H6vHaTLzg22t5PcPbwysuNM1Gn61Tv8HfEAjaMSbtxW1NFijgZUwgZIwCwYDVR0P
BAQDAgeAMBoGA1UdCQQTMBEwDwYDVQQGMQgMAkRFDAJTRTA1BgNVHSEELjAsMBAG
BmeBDAECAgYGZ4EMAQIBMBgGCisGAQQBguNSYwYGCisGAQQBguNSYwcwMAYIKwYB
BQUHAQsEJDAiMCAGCCsGAQUFBzAChhRodHRwOi8vY2Fpc3N1ZXJzLnVybDAKBggr
BgEFBQcGIQOBigAwgYYCQQCnBF0wsdaruWFIYcEzCInuEsmfV/EyDlC9ZzYrmkDu
TEoIw5ylb6VfGGYepBJzMIVTK6aPmfzvIrV+R0OmWDPuAkEAgpwUKxkZxKd8wbvX
P/Mb8KLLJaq3LbzmEQDjdk3dv2RwyhoHemgE75t/eeuVJWYhveKNPor1VGgdaeM9
Bph4gA==
-----END CERTIFICATE-----
```

3.8.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 3.8.2.

Plain hex (434 bytes):

```
0342123404F61A6775D7001A69570A808801781873656C667369676E2D627261696E
706F6F6C70353132723113781B6D79206A7572496E636F72706F726174696F6E4C6F
63616C6974791478186D79206A7572496E636F72706F726174696F6E537461746515
625345181A5881046D327067D334CE53FA29317AA207B85CA237623F19A10C594BF0
24FC3FFEB64FAB5884D0D448A271552E02E7CF44D8BF104DA182CEC1DE895C8418B8
529D9B8B2C4B80A736DDC56471D6A52C6CE414E69D57356B15FC08A46B61FA5B721F
ABC76932F3836DADE4F70F6F0CACB8D3351A7EB54EFF077C402368C49BB715B53458
880201181882048262445625345181B8402014A2B0601040182E35263064A2B0601
040182E3526307181F820274687474703A2F2F6361697373756572732E75726C5880
A7045D30B1D6ABB9614861C1330889EE12C99F57F1320E50BD67362B9A40EE4C4A08
C39CA56FA55F18661EA412733085532BA68F99FCEF22B57E4743A65833EE829C142B
1919C4A77CC1BBD73FF31BF0A2CB25AAB72DBCE61100E3764DDDBF6470CA1A077A68
04EF9B7F79EB95256621BDE28D3E8AF554681D69E33D06987880
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

3.8.4. C509 Type 2 Certificate

Plain hex (434 bytes):

```
0242123404F61A6775D7001A69570A808801781873656C667369676E2D627261696E
706F6F6C70353132723113781B6D79206A7572496E636F72706F726174696F6E4C6F
63616C6974791478186D79206A7572496E636F72706F726174696F6E537461746515
625345181A5881046D327067D334CE53FA29317AA207B85CA237623F19A10C594BF0
24FC3FFEB64FAB5884D0D448A271552E02E7CF44D8BF104DA182CEC1DE895C8418B8
529D9B8B2C4B80A736DDC56471D6A52C6CE414E69D57356B15FC08A46B61FA5B721F
ABC76932F3836DADE4F70F6F0CACB8D3351A7EB54EFF077C402368C49BB715B53458
880201181882048262444562534518 1B8402014A2B0601040182E35263064A2B0601
040182E3526307181F820274687474703A2F2F6361697373756572732E75726C5880
9A23F973FF1BBBA49E4F05EC2DCCEA7C273CB4D65DDBDFA84DB103212859DBCB235D
187025B8C8F1F040F5590F05E47B65B2AE6A883FB96E9973D3BAB3B8CF41A6BDB83F
E998EFEE980DABD7B128C23F084724F718B5DCF2D3459D2BA9EFC53FAB140A8B5C1B
FC8D1F290E51320FE80DD46938CEF7BD6991D00732BF1189FF02
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 04             # [2]. signature alg=4: ecdsa-with-shake256
  5: F6             # [3]. issuer=<null>
  6: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 11: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 16: 88             # [6]. subject=array[8], 4 attributes
                      # attribute[0]
 17:     01           # type=1: commonName
 18:     78 18        # value=char[24]
 20:       73656C667369676E2D627261696E706F # "selfsign-brainpo"
 36:       6F6C703531327231                 # "olp512r1"
                    # attribute[1]
 44:     13           # type=19: jurIncorporationLocality
 45:     78 1B        # value=char[27]
 47:       6D79206A7572496E636F72706F726174 # "my jurIncorporat"
 63:       696F6E4C6F63616C697479           # "ionLocality"
                    # attribute[2]
 74:     14           # type=20: jurIncorporationState
 75:     78 18        # value=char[24]
 77:       6D79206A7572496E636F72706F726174 # "my jurIncorporat"
 93:       696F6E5374617465                 # "ionState"
                    # attribute[3]
101:     15           # type=21: jurIncorporationCountry
102:     62           # value=char[2]
103:       5345          # "SE"
105: 18 1A         # [7]. subjectPublicKeyAlg=26: EC public key with
```

```
                    #      curve brainpoolp512r1
  107: 58 81        # [8]. subject public key=byte[129]
  109:   046D327067D334CE53FA29317AA207B85CA237623F19A10C594BF024FC3F
  139:   FEB64FAB5884D0D448A271552E02E7CF44D8BF104DA182CEC1DE895C8418
  169:   B8529D9B8B2C4B80A736DDC56471D6A52C6CE414E69D57356B15FC08A46B
  199:   61FA5B721FABC76932F3836DADE4F70F6F0CACB8D3351A7EB54EFF077C40
  229:   2368C49BB715B53458
  238: 88           # [9]. extensions=array[8]
                      # extension[0]
  239:     02           # type=2: KeyUsage
  240:     01           # value=1: [digitalSignature]
                      # extension[1]
  241:     18 18        # type=24: SubjectDirectoryAttributes
  243:     82           # value=array[2], 1 Attribute
  244:       04           # attributeType=4: country
  245:       82           # attributeValue=array[2]
  246:         62           # attributeValue[0]=char[2]
  247:           4445          # "DE"
  249:         62           # attributeValue[1]=char[2]
  250:           5345          # "SE"
                      # extension[2]
  252:     18 1B        # type=27: PolicyMappings
  254:     84           # value=array[4]
                        # policyMapping[0]
  255:         02           # issuerDomainPolicy=2:
                            # OrganizationValidation
  256:         01           # subjectDomainPolicy=1: DomainValidation
                        # policyMapping[1]
  257:         4A           #  issuerDomainPolicy=byte[10]:
  258:            2B0601040182E3526306 # oid: 1.3.6.1.4.1.45522.99.6
  268:         4A           # subjectDomainPolicy=byte[10]:
  269:            2B0601040182E3526307 # oid: 1.3.6.1.4.1.45522.99.7
                      # extension[3]
  279:     18 1F        # type=31: SubjectInfoAccess
  281:     82           # value=array[2]
                        # AccessDescription[0]
  282:         02           # accessMethod=2: CAIssuers
  283:         74           # uri=char[20]
  284:           687474703A2F2F636169737375657273 # "http://caissuers"
  300:           2E75726C                         # ".url"
  304: 58 80        # [10]. signature value=byte[128]
  306:   9A23F973FF1BBBA49E4F05EC2DCCEA7C273CB4D65DDBDFA84DB103212859
  336:   DBCB235D187025B8C8F1F040F5590F05E47B65B2AE6A883FB96E9973D3BA
  366:   B3B8CF41A6BDB83FE998EFEE980DABD7B128C23F084724F718B5DCF2D345
  396:   9D2BA9EFC53FAB140A8B5C1BFC8D1F290E51320FE80DD46938CEF7BD6991
  426:   D00732BF1189FF02
```

3.9. Weierstrass EC Public Key With frp256v1

* Self-signed
* EC key with curve frp256v1
* Signature algorithm: ecdsa-with-SHA1
* Subject:
  - emailAddress
  - telephoneNumber
  - businessCategory
* Extensions:
  - Policy Constraints with only requireExplicitPolicy
  - Name Constraints with only permittedSubTrees

3.9.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MEMCAQAwFQYHKoZIzj0CAQYKKoF6AYFfZYIAAQQnMCUCAQEEIIjiRO+dimF7NRmd
P/hE1jaAZ/C+2RTvYI3Hf8bZUf4h
-----END PRIVATE KEY-----
```

3.9.2. X.509 Certificate

PEM content (560 bytes):

```
-----BEGIN CERTIFICATE-----
MIICLDCCAdOgAwIBAgICEjQwCQYHKoZIzj0EATB3MR4wHAYJKoZIhvcNAQkBFg9h
YmNAZXhhbXBsZS5vcmcxGjAYBgNVBAMMEXNlbGZzaWduLWZycDI1NnYxMRwwGgYD
VQQPDBNteSBidXNpbmVzc0NhdGVnb3J5MRswGQYDVQQUDBJteSB0ZWxlcGhvbmVO
dW1iZXIwHhcNMjUwMTAyMDAwMDAwWhcNMjYwMTAyMDAwMDAwWjB3MR4wHAYJKoZI
hvcNAQkBFg9hYmNAZXhhbXBsZS5vcmcxGjAYBgNVBAMMEXNlbGZzaWduLWZycDI1
NnYxMRwwGgYDVQQPDBNteSBidXNpbmVzc0NhdGVnb3J5MRswGQYDVQQUDBJteSB0
ZWxlcGhvbmVOdW1iZXIwWzAVBgcqhkjOPQIBBgoqgXoBgV9lggABA0IABDeNLSih
9lRxJPLbakL2ORW/ovZTeuIM8EF9Z1++ZgPagKTPPx5DYzNDqzvoAVDsBOlkndYn
BbwFW9zaeR6yUGKjTjBMMAsGA1UdDwQEAwIHgDAvBgNVHR4EKDAmoCQwEIIOcGVy
bWl0dGVkLmRuczEwEIIOcGVybWl0dGVkLmRuczIwDAYDVR0kBAUwA4ABATAJBgcq
hkjOPQQBA0gAMEUCIDeNLSih9lRxJPLbakL2ORW/ovZTeuIM8EF9Z1++ZgPaAiEA
ogGOHd9Lkh+8Ri65sQWgBuzhQld/WYPdk4ewEgtjBW0=
-----END CERTIFICATE-----
```

3.9.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 3.9.2.

Plain hex (276 bytes):

```
0342123438FEF61A6775D7001A69570A8088006F616263406578616D706C652E6F72
67017173656C667369676E2D667270323536763 76310B736D7920627573696E65737343
617465676F7279181A726D792074656C6570686F6E654E756D626572181B58410437
8D2D28A1F6547124F2DB6A42F63915BFA2F6537AE20CF0417D675FBE6603DA80A4CF
3F1E43633343AB3BE80150EC04E9649DD62705BC055BDCDA791EB25062860201181A
8284026E7065726D69747465642E646E7331026E7065726D69747465642E646E7332
F6181C8201F65840378D2D28A1F6547124F2DB6A42F63915BFA2F6537AE20CF0417D
675FBE6603DAA2018E1DDF4B921FBC462EB9B105A006ECE142577F5983DD9387B012
0B63056D
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

3.9.4. C509 Type 2 Certificate

Plain hex (276 bytes):

```
0242123438FEF61A6775D7001A69570A8088006F616263406578616D706C652E6F72
67017173656C667369676E2D667270323536763 76310B736D7920627573696E65737343
617465676F7279181A726D792074656C6570686F6E654E756D626572181B58410437
8D2D28A1F6547124F2DB6A42F63915BFA2F6537AE20CF0417D675FBE6603DA80A4CF
3F1E43633343AB3BE80150EC04E9649DD62705BC055BDCDA791EB25062860201181A
8284026E7065726D69747465642E646E7331026E7065726D69747465642E646E7332
F6181C8201F65840378D2D28A1F6547124F2DB6A42F63915BFA2F6537AE20CF0417D
675FBE6603DAB6D89694165C9C5BD7A30A7D81A2F52E94193A740E445EA2041751E9
040DAFFB
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 38 FE          # [2]. signature alg=-255: ecdsa-with-sha1
  6: F6             # [3]. issuer=<null>
  7: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 12: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 17: 88             # [6]. subject=array[8], 4 attributes
                      # attribute[0]
 18:     00             # type=0: emailAddress
```

```
    19:     6F             # value=char[15]
    20:       616263406578616D706C652E6F7267 # "abc@example.org"
                         # attribute[1]
    35:     01             # type=1: commonName
    36:     71             # value=char[17]
    37:       73656C667369676E2D66727032353676 # "selfsign-frp256v"
    53:       31                               # "1"
                         # attribute[2]
    54:     0B             # type=11: businessCategory
    55:     73             # value=char[19]
    56:       6D7920627573696E6573734361746567 # "my businessCateg"
    72:       6F7279                           # "ory"
                         # attribute[3]
    75:     18 1A          # type=26: telephoneNumber
    77:     72             # value=char[18]
    78:       6D792074656C6570686F6E654E756D62 # "my telephoneNumb"
    94:       6572                             # "er"
    96: 18 1B          # [7]. subjectPublicKeyAlg=27: EC public key with
                       #      curve frp256v1
    98: 58 41          # [8]. subject public key=byte[65]
   100:   04378D2D28A1F6547124F2DB6A42F63915BFA2F6537AE20CF0417D675FBE
   130:   6603DA80A4CF3F1E43633343AB3BE80150EC04E9649DD62705BC055BDCDA
   160:   791EB25062
   165: 86            # [9]. extensions=array[6]
                        # extension[0]
   166:     02           # type=2: KeyUsage
   167:     01           # value=1: [digitalSignature]
                      # extension[1]
   168:     18 1A        # type=26: NameConstraints
   170:     82           # value=array[2]
   171:       84           # permittedSubtrees=array[4]
                             # GeneralName[0]
   172:           02           # GeneralNameType=2: dNSName
   173:           6E           # GeneralNameValue=char[14]
   174:             7065726D69747465642E646E7331 # "permitted.dns1"
                             # GeneralName[1]
   188:           02           # GeneralNameType=2: dNSName
   189:           6E           # GeneralNameValue=char[14]
   190:             7065726D69747465642E646E7332 # "permitted.dns2"
   204:       F6           # excludedSubtrees=<null>
                      # extension[2]
   205:     18 1C        # type=28: PolicyConstraints
   207:     82           # value=array[2]
   208:       01           # requireExplicitPolicy=1
   209:       F6           # inhibitPolicyMapping=<null>
   210: 58 40         # [10]. signature value=byte[64]
   212:   378D2D28A1F6547124F2DB6A42F63915BFA2F6537AE20CF0417D675FBE66
   242:   03DAB6D89694165C9C5BD7A30A7D81A2F52E94193A740E445EA2041751E9
```

272: 040DAFFB

3.10. Weierstrass EC Public Key With sm2p256v1

* Self-signed
* EC key with curve sm2p256v1
* Signature algorithm: sm2-with-sm3
* Subject:
  - serialNumber
  - organization
  - organizationalUnit
  - organizationIdentifier
* Extensions:
  - Policy Constraints with only inhibitPolicyMapping
  - Name Constraints with only excludedSubTrees

3.10.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MEECAQAwEwYHKoZIzj0CAQYIKoEcz1UBgi0EJzAlAgEBBCDyTXt5dDKnqvBcKeAy
+qKXJ3oU+KjHtHfv+J0iFaHUHA==
-----END PRIVATE KEY-----
```

3.10.2. X.509 Certificate

PEM content (621 bytes):

```
-----BEGIN CERTIFICATE-----
MIICaTCCAg6gAwIBAgICEjQwCgYIKoEcz1UBg3UwgZUxGzAZBgNVBAMMEnNlbGZz
aWduLXNtMnAyNTZ2MTEYMBYGA1UEBQwPbXkgc2VyaWFsTnVtYmVyMRgwFgYDVQQK
DA9teSBvcmdhbml6YXRpb24xHjAcBgNVBAsMFW15IG9yZ2FuaXphdGlvbmFsVW5p
dDEiMCAGA1UEYQwZbXkgb3JnYW5pemF0aW9uSWRlbnRpZmllcjAeFw0yNTAxMDIw
MDAwMDBaFw0yNjAxMDIwMDAwMDBaMIGVMRswGQYDVQQDDBJzZWxmc2lnbi1zbTJw
MjU2djExGDAWBgNVBAUMD215IHNlcmlhbE51bWJlcjEYMBYGA1UECgwPbXkgb3Jn
YW5pemF0aW9uMR4wHAYDVQQLDBVteSBvcmdhbml6YXRpb25hbFVuaXQxIjAgBgNV
BGEMGW15IG9yZ2FuaXphdGlvbklkZW50aWZpZXIwWTATBgcqhkjOPQIBBggqgRzP
VQGCLQNCAASV//S+hhHIFJyBrewUEl2synRqLz/jjNLqtxHoyZ8QH7tEhCPxZvn/
2Y8OMhWXuzlINab7JAM3o4kSkHoiw/BKo0wwSjALBgNVHQ8EBAMCB4AwLQYDVR0e
BCYwJKEiMA+CDWV4Y2x1ZGVkLmRuczEwD4INZXhjbHVkZWQuZG5zMjAMBgNVHSQE
BTADgQECMAoGCCqBHM9VAYN1A0kAMEYCIQDFPvnlhkfEPEAwGHIamRTHlPvXqLAt
VJ9kSJUNq8i9BAIhAMNuRdx7agBuEj9/n8YTo8BkIBwDmcdOs+kHr9cAnf8a
-----END CERTIFICATE-----
```

3.10.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 3.10.2.

Plain hex (301 bytes):

```
03421234182DF61A6775D7001A69570A808A017273656C667369676E2D736D327032
35367631036F6D792073657269616C4E756D626572086F6D79206F7267616E697A61
74696F6E09756D79206F7267616E697A6174696F6E616C556E69741278196D79206F
7267616E697A6174696F6E4964656E746966696572181C58410495FFF4BE8611C814
9C81ADEC14125DACCA746A2F3FE38CD2EAB711E8C99F101FBB448423F166F9FFD98F
0E321597BB394835A6FB240337A38912907A22C3F04A860201181A82F684026D6578
636C756465642E646E7331026D6578636C756465642E646E7332181C82F6025840C5
3EF9E58647C43C403018721A9914C794FBD7A8B02D549F6448950DABC8BD04C36E45
DC7B6A006E123F7F9FC613A3C064201C0399C74EB3E907AFD7009DFF1A
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

3.10.4. C509 Type 2 Certificate

Plain hex (301 bytes):

```
02421234182DF61A6775D7001A69570A808A017273656C667369676E2D736D327032
35367631036F6D792073657269616C4E756D626572086F6D79206F7267616E697A61
74696F6E09756D79206F7267616E697A6174696F6E616C556E69741278196D79206F
7267616E697A6174696F6E4964656E746966696572181C58410495FFF4BE8611C814
9C81ADEC14125DACCA746A2F3FE38CD2EAB711E8C99F101FBB448423F166F9FFD98F
0E321597BB394835A6FB240337A38912907A22C3F04A860201181A82F684026D6578
636C756465642E646E7331026D6578636C756465642E646E7332181C82F60258400E
6F4EDA275E22D67E72278FD0959B2CA3B02BEBDC2FE677B75AB629D160FC8AE1A98C
366FA988A058A8804FD99448988891C2CC78FE71367A5DB24E1707ABA1
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 18 2D          # [2]. signature alg=45: sm2-with-sm3
  6: F6             # [3]. issuer=<null>
  7: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 12: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 17: 8A             # [6]. subject=array[10], 5 attributes
                      # attribute[0]
 18:     01           # type=1: commonName
 19:     72           # value=char[18]
 20:       73656C667369676E2D736D3270323536 # "selfsign-sm2p256"
 36:       7631                           # "v1"
                    # attribute[1]
 38:     03           # type=3: serialNumber
 39:     6F           # value=char[15]
 40:       6D792073657269616C4E756D626572 # "my serialNumber"
                    # attribute[2]
 55:     08           # type=8: organization
 56:     6F           # value=char[15]
 57:       6D79206F7267616E697A6174696F6E # "my organization"
                    # attribute[3]
 72:     09           # type=9: organizationalUnit
 73:     75           # value=char[21]
 74:       6D79206F7267616E697A6174696F6E61 # "my organizationa"
 90:       6C556E6974                     # "lUnit"
                    # attribute[4]
 95:     12           # type=18: organizationIdentifier
 96:     78 19        # value=char[25]
 98:       6D79206F7267616E697A6174696F6E49 # "my organizationI"
114:       64656E746966696572             # "dentifier"
123: 18 1C          # [7]. subjectPublicKeyAlg=28: EC public key with
                    #      curve sm2p256v1
125: 58 41          # [8]. subject public key=byte[65]
127:   0495FFF4BE8611C8149C81ADEC14125DACCA746A2F3FE38CD2EAB711E8C9
157:   9F101FBB448423F166F9FFD98F0E321597BB394835A6FB240337A3891290
```

```
   187:   7A22C3F04A
   192: 86             # [9]. extensions=array[6]
                         # extension[0]
   193:     02             # type=2: KeyUsage
   194:     01             # value=1: [digitalSignature]
                         # extension[1]
   195:     18 1A          # type=26: NameConstraints
   197:     82             # value=array[2]
   198:       F6             # permittedSubtrees=<null>
   199:       84             # excludedSubtrees=array[4]
                               # GeneralName[0]
   200:           02             # GeneralNameType=2: dNSName
   201:           6D             # GeneralNameValue=char[13]
   202:             6578636C756465642E646E7331 # "excluded.dns1"
                               # GeneralName[1]
   215:           02             # GeneralNameType=2: dNSName
   216:           6D             # GeneralNameValue=char[13]
   217:             6578636C756465642E646E7332 # "excluded.dns2"
                         # extension[2]
   230:     18 1C          # type=28: PolicyConstraints
   232:     82             # value=array[2]
   233:       F6             # requireExplicitPolicy=<null>
   234:       02             # inhibitPolicyMapping=2
   235: 58 40          # [10]. signature value=byte[64]
   237:   0E6F4EDA275E22D67E72278FD0959B2CA3B02BEBDC2FE677B75AB629D160
   267:   FC8AE1A98C366FA988A058A8804FD99448988891C2CC78FE71367A5DB24E
   297:   1707ABA1
```

3.11. Montgomery EC Public Key With X25519

* X25519 public key

* Extensions

  - authorityKeyIdentifier with only the field keyIdentifier

  - authorityInfoAccess

  - issuerAltName

3.11.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VuBCIEIPJNe3l0Mqeq8Fwp4DL6opcnehT4qMe0d+/4nSIVodQc
-----END PRIVATE KEY-----
```

3.11.2. X.509 Certificate

* Issued by the CA in Section 2.2.

PEM content (678 bytes):

```
-----BEGIN CERTIFICATE-----
MIICojCCAlSgAwIBAgICEjQwBQYDK2VwMBIxEDAOBgNVBAMMB3Rlc3QgY2EwHhcN
MjUwMTAyMDAwMDAwWhcNMjYwMTAyMDAwMDAwWjAUMRIwEAYDVQQDDAllZS14MjU1
MTkwKjAFBgMrZW4DIQCK/1FvrHEkQVDnD5J39K33+yn0GnpKiCi9R2ci/Bt/CKOC
AcowggHGMAsGA1UdDwQEAwIDKDAfBgNVHSMEGDAWgBR/zbgtBJUuGja5CvN6PPFm
0V75ITCCAZQGCCsGAQUFBwEBBIIBhjCCAYIwIwYIKwYBBQUHMAGGF2h0dHA6Ly9v
Y3NwLmV4YW1wbGUub3JnMCgGCCsGAQUFBzAChhxodHRwOi8vY2Fpc3N1ZXJzLmV4
YW1wbGUub3JnMCsGCCsGAQUFBzAFhh9odHRwOi8vY2FyZXBvc2l0b3J5LmV4YW1w
bGUub3JnMCsGCCsGAQUFBzADhh9odHRwOi8vdGltZXN0YW1waW5nLmV4YW1wbGUu
b3JnMCsGCCsGAQUFBzAFhh9odHRwOi8vY2FyZXBvc2l0b3J5LmV4YW1wbGUub3Jn
MCsGCCsGAQUFBzAKhh9odHRwOi8vcnBraW1hbmlmZXN0LmV4YW1wbGUub3JnMCsG
CCsGAQUFBzALhh9odHRwOi8vc2lnbmVkb2JqZWN0LmV4YW1wbGUub3JnMCkGCCsG
AQUFBzANhh1odHRwOi8vcnBraW5vdGlmeS5leGFtcGxlLm9yZzAlBgorBgEEAYLj
UmMDhhdodHRwOi8vMTIzNC5leGFtcGxlLm9yZzAFBgMrZXADQQBKpB8Pwf95Vu15
Aad3ppKqsr9gRSbySGCIYrfoXAnoYe4MfhpPS281JSOsDo+v4avGxIQLYFKBWXLv
B7YjfB8N
-----END CERTIFICATE-----
```

3.11.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 3.11.2.

Plain hex (454 bytes):

```
034212340C67746573742063611A6775D7001A69570A806965652D78323535313908
58208AFF516FAC71244150E70F9277F4ADF7FB29F41A7A4A8828BD476722FC1B7F08
86021407547FCDB82D04952E1A36B90AF37A3CF166D15EF92109920177687474703A
2F2F6F6373702E6578616D706C652E6F726702781C687474703A2F2F636169737375
6572732E6578616D706C652E6F726705781F687474703A2F2F63617265706F736974
6F72792E6578616D706C652E6F726703781F687474703A2F2F74696D657374616D70
696E672E6578616D706C652E6F726705781F687474703A2F2F63617265706F736974
6F72792E6578616D706C652E6F72670A781F687474703A2F2F72706B696D616E6966
6573742E6578616D706C652E6F72670B781F687474703A2F2F7369676E65646F626A
6563742E6578616D706C652E6F72670D781D687474703A2F2F72706B696E6F746966
792E6578616D706C652E6F72674A2B0601040182E3526037687474703A2F2F3132
33342E6578616D706C652E6F726758404AA41F0FC1FF7956ED7901A777A692AAB2BF
604526F248608862B7E85C09E861EE0C7E1A4F4B6F352523AC0E8FAFE1ABC6C4840B
6052815972EF07B6237C1F0D
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

3.11.4. C509 Type 2 Certificate

* Issued by the CA in Section 2.4.

Plain hex (464 bytes):

```
024212340C67746573742063611A6775D7001A69570A806965652D78323535313908
58208AFF516FAC71244150E70F9277F4ADF7FB29F41A7A4A8828BD476722FC1B7F08
8802140754C16DE726347331107520B4ED9ED0088023A56033099201776874703A
2F2F6F6373702E6578616D706C652E6F726702781C687474703A2F2F636169737375
6572732E6578616D706C652E6F726705781F687474703A2F2F63617265706F736974
6F72792E6578616D706C652E6F726703781F687474703A2F2F74696D657374616D70
696E672E6578616D706C652E6F726705781F687474703A2F2F63617265706F736974
6F72792E6578616D706C652E6F72670A781F687474703A2F2F72706B696D616E6966
6573742E6578616D706C652E6F72670B781F687474703A2F2F7369676E65646F626A
6563742E6578616D706C652E6F72670D781D687474703A2F2F72706B696E6F746966
792E6578616D706C652E6F72674A2B0601040182E3526303776874703A2F2F3132
33342E6578616D706C652E6F72671819676162632E636F6D584057C96B7C203A3242
0856F76986B40965A5C9FEB926014FB0D9FF0C9A409F6DDBF1502B6CF8A5427E40C5
95338DD17386B25D817AF441DF020751EEAF3E8BFF0E
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 0C             # [2]. signature alg=12: Ed25519
  5: 67             # [3]. issuer=char[7]
  6:   74657374206361  # "test ca"
 13: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 18: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 23: 69             # [6]. subject=char[9]
 24:   65652D783235353139 # "ee-x25519"
 33: 08             # [7]. subjectPublicKeyAlg=8: X25529
 34: 58 20          # [8]. subject public key=byte[32]
 36:   8AFF516FAC71244150E70F9277F4ADF7FB29F41A7A4A8828BD476722FC1B
 66:   7F08
 68: 88             # [9]. extensions=array[8]
                      # extension[0]
 69:     02             # type=2: KeyUsage
 70:     14             # value=20: [keyEncipherment, keyAgreement]
                      # extension[1]
 71:     07             # type=7: AuthorityKeyIdentifier
 72:     54             # value=byte[20]
 73:       C16DE726347331107520B4ED9ED0088023A56033
```

```
                      # extension[2]
    93:     09          # type=9: AuthorityInfoAccess
    94:     92          # value=array[18]
                          # AccessDescription[0]
    95:         01          # accessMethod=1: OCSP
    96:         77          # uri=char[23]
    97:           687474703A2F2F6F6373702E6578616D # "http://ocsp.exam"
   113:           706C652E6F7267                  # "ple.org"
                          # AccessDescription[1]
   120:         02          # accessMethod=2: CAIssuers
   121:         78 1C       # uri=char[28]
   123:           687474703A2F2F636169737375657273 # "http://caissuers"
   139:           2E6578616D706C652E6F7267         # ".example.org"
                          # AccessDescription[2]
   151:         05          # accessMethod=5: CARepository
   152:         78 1F       # uri=char[31]
   154:           687474703A2F2F63617265706F736974 # "http://careposit"
   170:           6F72792E6578616D706C652E6F7267   # "ory.example.org"
                          # AccessDescription[3]
   185:         03          # accessMethod=3: timeStamping
   186:         78 1F       # uri=char[31]
   188:           687474703A2F2F74696D657374616D70 # "http://timestamp"
   204:           696E672E6578616D706C652E6F7267   # "ing.example.org"
                          # AccessDescription[4]
   219:         05          # accessMethod=5: CARepository
   220:         78 1F       # uri=char[31]
   222:           687474703A2F2F63617265706F736974 # "http://careposit"
   238:           6F72792E6578616D706C652E6F7267   # "ory.example.org"
                          # AccessDescription[5]
   253:         0A          # accessMethod=10: RPKIManifest
   254:         78 1F       # uri=char[31]
   256:           687474703A2F2F72706B696D616E6966 # "http://rpkimanif"
   272:           6573742E6578616D706C652E6F7267   # "est.example.org"
                          # AccessDescription[6]
   287:         0B          # accessMethod=11: signedObject
   288:         78 1F       # uri=char[31]
   290:           687474703A2F2F7369676E65646F626A # "http://signedobj"
   306:           6563742E6578616D706C652E6F7267   # "ect.example.org"
                          # AccessDescription[7]
   321:         0D          # accessMethod=13: RPKINotify
   322:         78 1D       # uri=char[29]
   324:           687474703A2F2F72706B696E6F746966 # "http://rpkinotif"
   340:           792E6578616D706C652E6F7267       # "y.example.org"
                          # AccessDescription[8]
   353:         4A          # accessMethod=byte[10]:
   354:            2B0601040182E3526303 # oid: 1.3.6.1.4.1.45522.99.3
   364:         77          # uri=char[23]
   365:           687474703A2F2F313233342E6578616D # "http://1234.exam"
```

```
   381:           706C652E6F7267                  # "ple.org"
                        # extension[3]
   388:     18 19          # type=25: IssuerAlternativeName
   390:     67             # DNS, value=char[7]
   391:       6162632E636F6D  # "abc.com"
   398: 58 40          # [10]. signature value=byte[64]
   400:   57C96B7C203A32420856F76986B40965A5C9FEB926014FB0D9FF0C9A409F
   430:   6DDBF1502B6CF8A5427E40C595338DD17386B25D817AF441DF020751EEAF
   460:   3E8BFF0E
```

3.12. Montgomery Public Key With X448

* X448 public key

* Extensions:

  - authorityKeyIdentifier with all fields

  - crlDistributionPoints

  - freshestCRL

3.12.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MEYCAQAwBQYDK2VvBDoEOPJNe3l0Mqeq8Fwp4DL6opcnehT4qMe0d+/4nSIVodQc
iOJE752KYXs1GZ0/+ETWNoBn8L7ZFO9g
-----END PRIVATE KEY-----
```

3.12.2. X.509 Certificate

* Issued by the CA in Section 2.2.

PEM content (407 bytes):

```
-----BEGIN CERTIFICATE-----
MIIBkzCCAUWgAwIBAgICEjQwBQYDK2VwMBIxEDAOBgNVBAMMB3Rlc3QgY2EwHhcN
MjUwMTAyMDAwMDAwWhcNMjYwMTAyMDAwMDAwWjASMRAwDgYDVQQDDAdlZS14NDQ4
MEIwBQYDK2VvAzkAHDfvq+qShHs28mSJCu/byWQDnFxhoxEcCQvk0KQpeaZmfitk
J1dg/2/U/wP8WWa1Dj2aqstI9DujgaYwgaMwCwYDVR0PBAQDAgMoMCcGA1UdHwQg
MB4wHKAaoBiGFmh0dHA6Ly9jcmwuZXhhbXBsZS5vcmcwOgYDVR0jBDMwMYAUf824
LQSVLho2uQrzejzxZtFe+SGhFqQUMBIxEDAOBgNVBAMMB3Rlc3QgY2GCAQEwLwYD
VR0uBCgwJjAkoCKgIIYeaHR0cDovL2ZyZXNoZXN0Y3JsLmV4YW1wbGUub3JnMAUG
AytlcANBABxt9FhGnYY5ENyTkCCOE5ZagJMI7q13ntyJhAa4HDOE1n7FNktLrWxe
LO6x1MlPj7SLHg35j18CG/2FdwHhGQo=
-----END CERTIFICATE-----
```

3.12.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 3.12.2.

Plain hex (254 bytes):

```
034212340C67746573742063611A6775D7001A69570A806765652D78343438095838
1C37EFABEA92847B36F264890AEFDBC964039C5C61A3111C090BE4D0A42979A6667E
2B64275760FF6FD4FF03FC5966B50E3D9AAACB48F43B880214058176687474703A2F
2F63726C2E6578616D706C652E6F72670783547FCDB82D04952E1A36B90AF37A3CF1
66D15EF92182046774657374206361410118 1D81781E687474703A2F2F6672657368
65737463726C2E6578616D706C652E6F726758401C6DF458469D863910DC9390208E
13965A809308EEAD779EDC898406B81C3384D67EC5364B4BAD6C5E2CEEB1D4C94F8F
B48B1E0DF98F5F021BFD857701E1190A
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

3.12.4. C509 Type 2 Certificate

* Issued by the CA in Section 2.4.

Plain hex (254 bytes):

```
024212340C67746573742063611A6775D7001A69570A806765652D78343438095838
1C37EFABEA92847B36F264890AEFDBC964039C5C61A3111C090BE4D0A42979A6667E
2B64275760FF6FD4FF03FC5966B50E3D9AAACB48F43B880214058176687474703A2F
2F63726C2E6578616D706C652E6F7267078354C16DE726347331107520B4ED9ED008
8023A560338204677465737420636141011 81D81781E687474703A2F2F6672657368
65737463726C2E6578616D706C652E6F72675840BA9C332169D5278EB1151DDF914A
12468229C3212994749BE368CB29F09F8A78BDD3A86097D9C414EEBEAA89B9DC9655
4644089C420B23C3000F6A3B83D3340E
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 0C             # [2]. signature alg=12: Ed25519
  5: 67             # [3]. issuer=char[7]
  6:   74657374206361  # "test ca"
 13: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 18: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 23: 67             # [6]. subject=char[7]
 24:   65652D78343438  # "ee-x448"
 31: 09             # [7]. subjectPublicKeyAlg=9: X448
 32: 58 38          # [8]. subject public key=byte[56]
 34:   1C37EFABEA92847B36F264890AEFDBC964039C5C61A3111C090BE4D0A429
 64:   79A6667E2B64275760FF6FD4FF03FC5966B50E3D9AAACB48F43B
 90: 88             # [9]. extensions=array[8]
                      # extension[0]
 91:     02             # type=2: KeyUsage
 92:     14             # value=20: [keyEncipherment, keyAgreement]
                      # extension[1]
 93:     05             # type=5: CRLDistributionPoints
 94:     81             # value=array[1]
 95:       76             # [0]=char[22]
 96:         687474703A2F2F63726C2E6578616D70 # "http://crl.examp"
112:         6C652E6F7267                     # "le.org"
                      # extension[2]
118:     07             # type=7: AuthorityKeyIdentifier
119:     83             # value=array[3]
120:       54             # [0]=byte[20]
121:         C16DE726347331107520B4ED9ED0088023A56033
141:       82             # [1]=array[2]
142:         04             # [0]=simple-uint(4)
143:         67             # [1]=char[7]
144:           74657374206361  # "test ca"
151:       41             # [2]=byte[1]
152:         01
                      # extension[3]
153:     18 1D          # type=29: FreshestCRL
155:     81             # value=array[1]
156:       78 1E          # [0]=char[30]
158:         687474703A2F2F667265736865737463 # "http://freshestc"
174:         726C2E6578616D706C652E6F7267     # "rl.example.org"
188: 58 40         # [10]. signature value=byte[64]
190:   BA9C332169D5278EB1151DDF914A12468229C3212994749BE368CB29F09F
220:   8A78BDD3A86097D9C414EEBEAA89B9DC96554644089C420B23C3000F6A3B
250:   83D3340E
```

3.13. Edwards EC Public Key With ED25519

* Self-signed
* EC key with curve ed25519
* Signature algorithm: Ed25519
* Subject:
  - domainComponent
  - dnQualifier
  - dmdName
  - unstructuredName
  - unstructuredAddress
  - generationQualifier
* Extensions:
  - Policy Constraints with both requireExplicitPolicy and inhibitPolicyMapping
  - Name Constraints with both permittedSubTrees and excludedSubTrees

3.13.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MC4CAQAwBQYDK2VwBCIEIPJNe3l0Mqeq8Fwp4DL6opcnehT4qMe0d+/4nSIVodQc
-----END PRIVATE KEY-----
```

3.13.2. X.509 Certificate

PEM content (733 bytes):

```
-----BEGIN CERTIFICATE-----
MIIC2TCCAougAwIBAgICEjQwBQYDK2VwMIHZMRkwFwYDVQQDDBBzZWxmc2lnbi1l
ZDI1NTE5MR8wHQYDVQQsDBZteSBnZW5lcmF0aW9uUXVhbGlmaWVyMRcwFQYDVQQu
DA5teSBkblF1YWxpZmllcjEiMCAGCgmSJomT8ixkARkWEm15IGRvbWFpbkNvbXBv
bmVudDETMBEGA1UENgwKbXkgZG1kTmFtZTEiMCAGCSqGSIb3DQEJAgwTbXkgdW5z
dHJ1Y3R1cmVkTmFtZTElMCMGCSqGSIb3DQEJCAwWbXkgdW5zdHJ1Y3R1cmVkQWRk
cmVzczAeFw0yNTAxMDIwMDAwMDBaFw0yNjAxMDIwMDAwMDBaMIHZMRkwFwYDVQQD
DBBzZWxmc2lnbi1lZDI1NTE5MR8wHQYDVQQsDBZteSBnZW5lcmF0aW9uUXVhbGlm
aWVyMRcwFQYDVQQuDA5teSBkblF1YWxpZmllcjEiMCAGCgmSJomT8ixkARkWEm15
IGRvbWFpbkNvbXBvbmVudDETMBEGA1UENgwKbXkgZG1kTmFtZTEiMCAGCSqGSIb3
DQEJAgwTbXkgdW5zdHJ1Y3R1cmVkTmFtZTElMCMGCSqGSIb3DQEJCAwWbXkgdW5z
dHJ1Y3R1cmVkQWRkcmVzczAqMAUGAytlcAMhAEYnCuwPMoN+Eod50wsknFMdbULB
rCnkAjKO3Hn6wr6Vo3UwczALBgNVHQ8EBAMCB4AwUwYDVR0eBEwwSqAkMBCCDnBl
cm1pdHRlZC5kbnMxMBCCDnBlcm1pdHRlZC5kbnMyoSIwD4INZXhjbHVkZWQuZG5z
MTAPgg1leGNsdWRlZC5kbnMyMA8GA1UdJAQIMAaAAQGBAQIwBQYDK2VwA0EAOXvc
HHvzKL/9iuCTu4w3/AZ1C9bcJxBXN/MR2vM02IwCJbH0RDXyLSRWv6zIJsoiE5aa
RiibuQhT5WLQnJExAg==
-----END CERTIFICATE-----
```

3.13.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 3.13.2.

Plain hex (331 bytes):

```
034212340CF61A6775D7001A69570A808E017073656C667369676E2D656432353531
390F766D792067656E65726174696F6E5175616C6966696572106E6D7920646E5175
616C696669657216726D7920646F6D61696E436F6D706F6E656E74181B6A6D792064
6D644E616D65181D736D7920756E737472756374757265644E616D65181E766D7920
756E737472756374757265644164646726573730A582046270AEC0F32837E128779D3
0B249C531D6D42C1AC29E402328EDC79FAC2BE95860201181A8284026E7065726D69
747465642E646E7331026E7065726D69747465642E646E733284026D6578636C7564
65642E646E7331026D6578636C756465642E646E7332181C8201025840397BDC1C7B
F328BFFD8AE093BB8C37FC06750BD6DC27105737F311DAF334D88C0225B1F44435F2
2D2456BFACC826CA2213969A46289BB90853E562D09C913102
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

3.13.4. C509 Type 2 Certificate

Plain hex (331 bytes):

```
024212340CF61A6775D7001A69570A808E017073656C667369676E2D656432353531
390F766D792067656E65726174696F6E5175616C6966696572106E6D7920646E5175
616C696669657216726D7920646F6D61696E436F6D706F6E656E74181B6A6D792064
6D644E616D65181D736D7920756E737472756374757265644E616D65181E766D7920
756E737472756374757265644164647265730A582046270AEC0F32837E128779D3
0B249C531D6D42C1AC29E402328EDC79FAC2BE95860201181A8284026E7065726D69
747465642E646E7331026E7065726D69747465642E646E733284026D6578636C7564
65642E646E7331026D6578636C756465642E646E7332181C82010258403894B5785C
EA7A3BDA00D7E0D9AF5C3CA005AB6A753A58A472BE4BE9C65BAA844BD97B0E8CD212
0B17BD7AC3DDDE97FB40B3D89A64A13222337AA4BF6BA2E809
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 0C             # [2]. signature alg=12: Ed25519
  5: F6             # [3]. issuer=<null>
  6: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 11: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 16: 8E             # [6]. subject=array[14], 7 attributes
                      # attribute[0]
 17:     01             # type=1: commonName
 18:     70             # value=char[16]
 19:       73656C667369676E2D65643235353139 # "selfsign-ed25519"
                      # attribute[1]
 35:     0F             # type=15: generationQualifier
 36:     76             # value=char[22]
 37:       6D792067656E65726174696F6E517561 # "my generationQua"
 53:       6C6966696572                     # "lifier"
                      # attribute[2]
 59:     10             # type=16: DNQualifier
 60:     6E             # value=char[14]
 61:       6D7920646E5175616C6966696572 # "my dnQualifier"
                      # attribute[3]
 75:     16             # type=22: domainComponent
 76:     72             # value=char[18]
 77:       6D7920646F6D61696E436F6D706F6E65 # "my domainCompone"
 93:       6E74                             # "nt"
                      # attribute[4]
 95:     18 1B          # type=27: DMDName
 97:     6A             # value=char[10]
 98:       6D7920646D644E616D65 # "my dmdName"
                      # attribute[5]
108:     18 1D          # type=29: unstructuredName
110:     73             # value=char[19]
111:       6D7920756E737472756374757265644E # "my unstructuredN"
127:       616D65                           # "ame"
```

```
                        # attribute[6]
   130:     18 1E          # type=30: unstructuredAddress
   132:     76             # value=char[22]
   133:       6D7920756E737472756374572656441 # "my unstructuredA"
   149:       646472657373                    # "ddress"
   155: 0A             # [7]. subjectPublicKeyAlg=10: Ed25519
   156: 58 20          # [8]. subject public key=byte[32]
   158:   46270AEC0F32837E128779D30B249C531D6D42C1AC29E402328EDC79FAC2
   188:   BE95
   190: 86             # [9]. extensions=array[6]
                          # extension[0]
   191:     02             # type=2: KeyUsage
   192:     01             # value=1: [digitalSignature]
                        # extension[1]
   193:     18 1A          # type=26: NameConstraints
   195:     82             # value=array[2]
   196:       84             # permittedSubtrees=array[4]
                               # GeneralName[0]
   197:            02             # GeneralNameType=2: dNSName
   198:            6E             # GeneralNameValue=char[14]
   199:              7065726D69747465642E646E7331 # "permitted.dns1"
                               # GeneralName[1]
   213:            02             # GeneralNameType=2: dNSName
   214:            6E             # GeneralNameValue=char[14]
   215:              7065726D69747465642E646E7332 # "permitted.dns2"
   229:       84             # excludedSubtrees=array[4]
                               # GeneralName[0]
   230:            02             # GeneralNameType=2: dNSName
   231:            6D             # GeneralNameValue=char[13]
   232:              6578636C756465642E646E7331 # "excluded.dns1"
                               # GeneralName[1]
   245:            02             # GeneralNameType=2: dNSName
   246:            6D             # GeneralNameValue=char[13]
   247:              6578636C756465642E646E7332 # "excluded.dns2"
                        # extension[2]
   260:     18 1C          # type=28: PolicyConstraints
   262:     82             # value=array[2]
   263:       01             # requireExplicitPolicy=1
   264:       02             # inhibitPolicyMapping=2
   265: 58 40          # [10]. signature value=byte[64]
   267:   3894B5785CEA7A3BDA00D7E0D9AF5C3CA005AB6A753A58A472BE4BE9C65B
   297:   AA844BD97B0E8CD2120B17BD7AC3DDDE97FB40B3D89A64A13222337AA4BF
   327:   6BA2E809
```

3.14. Edwards EC Public Key With ED448

* Self-signed

* EC key with curve ed448
* Signature algorithm: ED448
* Subject:
  - initials
  - pseudonym
  - userid
* Extensions:
  - Precertificate Signing Certificate
  - OCSP No Check
  - TLS Features
  - Signed Certificate Timestamp List

3.14.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MEcCAQAwBQYDK2VxBDsEOfJNe3l0Mqeq8Fwp4DL6opcnehT4qMe0d+/4nSIVodQc
iOJE752KYXs1GZ0/+ETWNoBn8L7ZFO9gjQ==
-----END PRIVATE KEY-----
```

3.14.2. X.509 Certificate

PEM content (787 bytes):

```
-----BEGIN CERTIFICATE-----
MIIDDzCCAo+gAwIBAgICEjQwBQYDK2VxMGExFzAVBgNVBAMMDnNlbGZzaWduLWVk
NDQ4MRQwEgYDVQQrDAtteSBpbml0aWFsczEVMBMGA1UEQQwMbXkgcHNldWRvbnlt
MRkwFwYKCZImiZPyLGQBAQwJbXkgdXNlcmlkMB4XDTI1MDEwMjAwMDAwMFoXDTI2
MDEwMjAwMDAwMFowYTEXMBUGA1UEAwwOc2VsZnNpZ24tZWQ0NDgxFDASBgNVBCsM
C215IGluaXRpYWxzMRUwEwYDVQRBDAxteSBwc2V1ZG9ueW0xGTAXBgoJkiaJk/Is
ZAEBDAlteSB1c2VyaWQwQzAFBgMrZXEDOgCMNeSR21hwLXuZFnwZ+Gsmgeol0h+D
rG7HgECpBBFPyx3PI59sTYRRR/fiJ5Ookan5yl0eIKc5jICjggFQMIIBTDALBgNV
HQ8EBAMCB4AwggECBgorBgEEAdZ5AgQCBIHzBIHwAO4AdQAiIiIiIiIiIiIiIiIi
IiIiIiIiIiIiIiIiIiIiIiIgAAAZQkT7DxAAAEAwBGMEQCIEBAQEBAQEBAQEBA
QEBAQEBAQEBAQEBAQEBAQEBAAiBAQEBAQEBAQEBAQEBAQEBAQEBAQEBA
QEBAQEBAB1ACIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiIiAAABlCRP
/w8AAAQDAEYwRAIgQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAQEACIEBA
QEBAQEBAQEBAQEBAQEBAQEBAQEBAQEBAMA8GCSsGAQUFBzABBQQCBQAw
EAYKKwYBBAHWeQIEAwQCBQAwFAYIKwYBBQUHARgECDAGAgEsAgEQMAUGAytlcQNz
ADhF10+BlgrM/99q64XWTGMFU+rHwIEZRvv2XV5GiQqci8Xi1xrmzYbwHZqsNTgP
LSuK4H137SjrgCxJdp5lX/NmtZ3JQBFzBFdH4R75UKgNquhl/IDVl0hmDWhWT8k5
I1G60ik75/eSKtUC2oOm8FUoAA==
-----END CERTIFICATE-----
```

3.14.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 3.14.2.

Plain hex (473 bytes):

```
034212340DF61A6775D7001A69570A8088016E73656C667369676E2D65643434380E
6B6D7920696E697469616C73116C6D792070736575646F6E796D181C696D79207573
657269640B58398C35E491DB58702D7B99167C19F86B2681EA25D21F83AC6EC78040
A904114FCB1DCF239F6C4D845147F7E22793A891A9F9CA5D1E20A7398C808A02010A
8858202222222222222222222222222222222222222222222222222222222222222
2239270E00584040404040404040404040404040404040404040404040404040404
4040404040404040404040404040404040404040404040404040404040404040404
4040405820222222222222222222222222222222222222222222222222222222222
22222219270F00584040404040404040404040404040404040404040404040404040
4040404040404040404040404040404040404040404040404040404040404040404
40404040401824F61825F6182682182C1058723845D74F81960ACCFFDF6AEB85D64C
630553EAC7C0811946FBF65D5E46890A9C8BC5E2D71AE6CD86F01D9AAC35380F2D2B
8AE07D77ED28EB802C49769E655FF366B59DC9401173045747E11EF950A80DAAE865
FC80D59748660D68564FC9392351BAD2293BE7F7922AD502DA83A6F0552800
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

3.14.4. C509 Type 2 Certificate

Plain hex (473 bytes):

```
024212340DF61A6775D7001A69570A8088016E73656C667369676E2D65643434380E
6B6D7920696E697469616C73116C6D792070736575646F6E796D181C696D79207573
657269640B58398C35E491DB58702D7B99167C19F86B2681EA25D21F83AC6EC78040
A904114FCB1DCF239F6C4D845147F7E22793A891A9F9CA5D1E20A7398C808A02010A
8858202222222222222222222222222222222222222222222222222222222222222
2239270E00584040404040404040404040404040404040404040404040404040404
4040404040404040404040404040404040404040404040404040404040404040404
4040405820222222222222222222222222222222222222222222222222222222222
22222219270F00584040404040404040404040404040404040404040404040404040
4040404040404040404040404040404040404040404040404040404040404040404
40404040401824F61825F6182682182C105872ED25FBBD003303D2680C385B159FE4
6C26CB81E8368A24B038B8048E0FF8BC44F1F0825A5945152E24992F696A90BA0DAE
59E3713264CFE38026AB8D8D64B8DE1194C23D0FB19CDD4E2B581AC75CBBF9FAD253
14B75462DB8CDFBCE5C832D4137410CB5A948CB1EE1575C95066CC47951000
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 0D             # [2]. signature alg=13: Ed448
  5: F6             # [3]. issuer=<null>
  6: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 11: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 16: 88             # [6]. subject=array[8], 4 attributes
                      # attribute[0]
 17:     01           # type=1: commonName
 18:     6E           # value=char[14]
 19:       73656C667369676E2D6564343438 # "selfsign-ed448"
                      # attribute[1]
 33:     0E           # type=14: initials
 34:     6B           # value=char[11]
 35:       6D7920696E697469616C73 # "my initials"
                      # attribute[2]
 46:     11           # type=17: pseudonym
 47:     6C           # value=char[12]
 48:       6D792070736575646F6E796D # "my pseudonym"
                      # attribute[3]
 60:     18 1C        # type=28: userID
 62:     69           # value=char[9]
 63:       6D7920757365726964 # "my userid"
 72: 0B             # [7]. subjectPublicKeyAlg=11: Ed448
 73: 58 39          # [8]. subject public key=byte[57]
 75:   8C35E491DB58702D7B99167C19F86B2681EA25D21F83AC6EC78040A90411
```

```
   105:   4FCB1DCF239F6C4D845147F7E22793A891A9F9CA5D1E20A7398C80
   132: 8A             # [9]. extensions=array[10]
                         # extension[0]
   133:     02             # type=2: KeyUsage
   134:     01             # value=1: [digitalSignature]
                         # extension[1]
   135:     0A             # type=10: SignedCertificateTimestampList
   136:     88             # value=array[8]
                             # SignedCertificateTimestamp[0]
   137:         58 20          # logID=byte[32]
   139:           2222222222222222222222222222222222222222222222222222
   165:           222222222222
   171:         39 270E        # timestamp=-9999
   174:         00             # sigAlg=0: ecdsa-with-sha256
   175:         58 40          # sigValue=byte[64]
   177:           4040404040404040404040404040404040404040404040404040
   203:           4040404040404040404040404040404040404040404040404040
   229:           40404040404040404040
                             # SignedCertificateTimestamp[1]
   241:         58 20          # logID=byte[32]
   243:           2222222222222222222222222222222222222222222222222222
   269:           222222222222
   275:         19 270F        # timestamp=9999
   278:         00             # sigAlg=0: ecdsa-with-sha256
   279:         58 40          # sigValue=byte[64]
   281:           4040404040404040404040404040404040404040404040404040
   307:           4040404040404040404040404040404040404040404040404040
   333:           40404040404040404040
                         # extension[2]
   345:     18 24          # type=36: OCSPNoCheck
   347:     F6             # value=<null>
                         # extension[3]
   348:     18 25          # type=37: PreCertificate
   350:     F6             # value=<null>
                         # extension[4]
   351:     18 26          # type=38: TLSFeatures
   353:     82             # value=array[2]
   354:       18 2C          # value=44: cookie
   356:       10             # value=16: application layer protocol
                             # negotiation
   357: 58 72          # [10]. signature value=byte[114]
   359:   ED25FBBD003303D2680C385B159FE46C26CB81E8368A24B038B8048E0FF8
   389:   BC44F1F0825A5945152E24992F696A90BA0DAE59E3713264CFE38026AB8D
   419:   8D64B8DE1194C23D0FB19CDD4E2B581AC75CBBF9FAD25314B75462DB8CDF
   449:   BCE5C832D4137410CB5A948CB1EE1575C95066CC47951000
```

4. Certificates with Different Signature Algorithms

4.1. RSASSA-PKCS1-v1_5 With SHA-1

* Self-signed

* Signature algorithm: sha1WithRSAEncryption

4.1.1. Private Key

See Section 3.1.1.

4.1.2. X.509 Certificate

PEM content (463 bytes):

```
-----BEGIN CERTIFICATE-----
MIIByzCCATSgAwIBAgICEjQwDQYJKoZIhvcNAQEFBQAwITEfMB0GA1UEAwwWc2Vs
ZnNpZ24tcnNhLXdpdGgtc2hhMTAeFw0yNTAxMDIwMDAwMDBaFw0yNjAxMDIwMDAw
MDBaMCExHzAdBgNVBAMMFnNlbGZzaWduLXJzYS13aXRoLXNoYTEwgZ8wDQYJKoZI
hvcNAQEBBQADgY0AMIGJAoGBALgJL28EcmqSHPqy0xOunS8Bx85GX6t9pix6XHP6
zl/7ovHdgKKa3EM5nPyiInm4miZIEOW5JrteDT9yenY+FgE/ifj+rFnQ+91eiwxS
gn5UkPE7hMNjTonG0XMa5fGmD4jtEY0IDhqyyqUy0GwvfSoIdN7k5rblcoP2R42v
QlPbAgMBAAGjEjAQMA4GA1UdDwEB/wQEAwIHgDANBgkqhkiG9w0BAQUFAAOBgQBy
vlKYpmd/Cnh0eiiaEvGVVbFQY6Qx95k5BpyVL+Wp2K5oB/WZ5fwP/mf/w8viB7hc
rTO02AaTvv5NJNyt3ubIwV1UBn1MX+OWC43HH6GRH+6cndHiE/2cAKRoGMBA3xKp
4YMRr/kweqpFcIWfFObSWJ4aWdmw/6eg5e3uPIhd/A==
-----END CERTIFICATE-----
```

4.1.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 4.1.2.

Plain hex (302 bytes):

```
0342123438FFF61A6775D7001A69570A807673656C667369676E2D7273612D776974
682D73686131005880B8092F6F04726A921CFAB2D313AE9D2F01C7CE465FAB7DA62C
7A5C73FACE5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5B926BB5E0D3F72
7A763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C3634E89C6D1731AE5
F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4E6B6E57283F6478DAF4253
DB20588072BE5298A6677F0A78747A289A12F19555B15063A431F79939069C952FE5
A9D8AE6807F599E5FC0FFE67FFC3CBE207B85CAD33B4D80693BEFE4D24DCADDEE6C8
C15D54067D4C5FE3960B8DC71FA1911FEE9C9DD1E213FD9C00A46818C040DF12A9E1
8311AFF9307AAA4570859F14E6D2589E1A59D9B0FFA7A0E5EDEE3C885DFC
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

4.1.4. C509 Type 2 Certificate

Plain hex (302 bytes):

```
0242123438FFF61A6775D7001A69570A807673656C667369676E2D7273612D776974
682D73686131005880B8092F6F04726A921CFAB2D313AE9D2F01C7CE465FAB7DA62C
7A5C73FACE5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5B926BB5E0D3F72
7A763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C3634E89C6D1731AE5
F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4E6B6E57283F6478DAF4253
DB2058800150926C5642D9CB2AAA27A17B68FBBFC9F47AA42CD9E6779B4E9A7A81C7
60589C53AC23BAD6A94F5A6B275BE292B79BA9CB59D045E44809353DCE73C936A06E
C20D51AE24C559DDB02EBF4B0838F515328058F601D91F6DAE5BFF55DC78DEB80970
D2F74757FC5F96BE6F217825DC8286D9446CCA0C9AF257FCE66CD963F891
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 38 FF          # [2]. signature alg=-256: sha1WithRSAEncryption
  6: F6             # [3]. issuer=<null>
  7: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 12: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 17: 76             # [6]. subject=char[22]
 18:   73656C667369676E2D7273612D776974 # "selfsign-rsa-wit"
 34:   682D73686131                     # "h-sha1"
 40: 00             # [7]. subjectPublicKeyAlg=0: RSA
 41: 58 80          # [8]. subject public key=byte[128]
 43:   B8092F6F04726A921CFAB2D313AE9D2F01C7CE465FAB7DA62C7A5C73FACE
 73:   5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5B926BB5E0D3F727A
103:   763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C3634E89C6D1
133:   731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4E6B6E572
163:   83F6478DAF4253DB
171: 20             # [9]. extensions=-1, KeyUsage, critical:
                    #      [digitalSignature]
172: 58 80          # [10]. signature value=byte[128]
174:   0150926C5642D9CB2AAA27A17B68FBBFC9F47AA42CD9E6779B4E9A7A81C7
204:   60589C53AC23BAD6A94F5A6B275BE292B79BA9CB59D045E44809353DCE73
234:   C936A06EC20D51AE24C559DDB02EBF4B0838F515328058F601D91F6DAE5B
264:   FF55DC78DEB80970D2F74757FC5F96BE6F217825DC8286D9446CCA0C9AF2
294:   57FCE66CD963F891
```

4.2. ECDSA With SHA1

* Signature algorithm: ecdsa-with-sha1

See Section 3.9.

4.3. ECDSA With SHA256

* Signature algorithm: ecdsa-with-sha256

See Section 3.3.

4.4. ECDSA With SHA384

* Signature algorithm: ecdsa-with-sha384

See Section 3.4.

4.5. ECDSA With SHA512

* Signature algorithm: ecdsa-with-SHA512

See Section 3.5.

4.6. ECDSA With SHAKE128

* Signature algorithm: ecdsa-with-shake128

See Section 3.6.

4.7. ECDSA With SHAKE256

* Signature algorithm: ecdsa-with-shake256

See Section 3.8.

4.8. Ed25519

* Signature algorithm: ed25519

See Section 3.13.

4.9. Ed448

* Signature algorithm: ed448

See Section 3.14.

4.10. ECDH PoP With SHA-256 And HMAC-SHA256

* Signature algorithm sa-ecdhPop-sha256-hmac-sha256

See Section 8.2.

4.11. ECDH PoP With SHA-384 And HMAC-SHA384

* Signature algorithm: sa-ecdhPop-sha384-hmac-sha384

See Section 8.3.

4.12. ECDH PoP With SHA-512 And HMAC-SHA512

* Signature algorithm: sa-ecdhPop-sha512-hmac-sha512f

See Section 8.4.

4.13. RSASSA-PKCS1-v1_5 With SHA-256

* Signature algorithm sha256WithRSAEncryption

See Section 3.1.

4.14. RSASSA-PKCS1-v1_5 With SHA-384

* Signature algorithm: sha384WithRSAEncryption

See Section 3.2.

4.15. RSASSA-PKCS1-v1_5 With SHA-512

* Self-signed
* Signature algorithm: sha512WithRSAEncryption

4.15.1. Private Key

See Section 3.1.1.

4.15.2. X.509 Certificate

PEM content (467 bytes):

```
-----BEGIN CERTIFICATE-----
MIIBzzCCATigAwIBAgICEjQwDQYJKoZIhvcNAQENBQAwIzEhMB8GA1UEAwwYc2Vs
ZnNpZ24tcnNhLXdpdGgtc2hhNTEyMB4XDTI1MDEwMjAwMDAwMFoXDTI2MDEwMjAw
MDAwMFowIzEhMB8GA1UEAwwYc2VsZnNpZ24tcnNhLXdpdGgtc2hhNTEyMIGfMA0G
CSqGSIb3DQEBAQUAA4GNADCBiQKBgQC4CS9vBHJqkhz6stMTrp0vAcfORl+rfaYs
elxz+s5f+6Lx3YCimtxDOZz8oiJ5uJomSBDluSa7Xg0/cnp2PhYBP4n4/qxZ0Pvd
XosMUoJ+VJDxO4TDY06JxtFzGuXxpg+I7RGNCA4assqlMtBsL30qCHTe5Oa25XKD
9keNr0JT2wIDAQABoxIwEDAOBgNVHQ8BAf8EBAMCB4AwDQYJKoZIhvcNAQENBQAD
gYEAJAbODIhhp4VHV8H6LZ5YI4CFgBdOg8lrlnTBlpBetrwI7NCEha/22u5epjzv
ZvdYOXLcsvKhqhS2hMGjOVS7R6ffu/9N/nUSa9341ocG/SbeZuXL8Ba12faHGMq2
6yK9i42EI91vKGuHIXw6WONk8GAXXFHdH6xgTJ/1U2krm+4=
-----END CERTIFICATE-----
```

4.15.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 4.15.2.

Plain hex (305 bytes):

```
034212341819F61A6775D7001A69570A80781873656C667369676E2D7273612D7769
74682D736861353132005880B8092F6F04726A921CFAB2D313AE9D2F01C7CE465FAB
7DA62C7A5C73FACE5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5B926BB5E
0D3F727A763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C3634E89C6D1
731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4E6B6E57283F6478D
AF4253DB2058802406CE0C8861A7854757C1FA2D9E5823808580174E83C96B9674C1
96905EB6BC08ECD08485AFF6DAEE5EA63CEF66F7583972DCB2F2A1AA14B684C1A339
54BB47A7DFBBFF4DFE75126BDDF8D68706FD26DE66E5CBF016B5D9F68718CAB6EB22
BD8B8D8423DD6F286B87217C3A58E364F060175C51DD1FAC604C9FF553692B9BEE
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

4.15.4. C509 Type 2 Certificate

Plain hex (305 bytes):

```
024212341819F61A6775D7001A69570A80781873656C667369676E2D7273612D7769
74682D736861353132005880B8092F6F04726A921CFAB2D313AE9D2F01C7CE465FAB
7DA62C7A5C73FACE5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5B926BB5E
0D3F727A763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C3634E89C6D1
731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4E6B6E57283F6478D
AF4253DB205880B5D4C31502957FBEE2E4DED7E45E723A8B9A86A46E9FEA1D878178
08D1ACE802370B91718755F101FFB3B971816120BE5CC05D2EE866422D78EF7D16AA
78CE4011E4DC92AE1C7DA3C7831773A44A7B2F5BAFED5D2B8A6A4E6E49638B3335DC
68B596AE5FC48360E1C7DD50BD457CF2CFDCF56F98BE1EA3103B12DD5B6221DB21
```

Annotated hex:

```
  0: 02            # [0]. certificate type=2
  1: 42            # [1]. serial number=byte[2]
  2:   1234
  4: 18 19         # [2]. signature alg=25: sha512WithRSAEncryption
  6: F6            # [3]. issuer=<null>
  7: 1A 6775D700   # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 12: 1A 69570A80   # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 17: 78 18         # [6]. subject=char[24]
 19:   73656C667369676E2D7273612D776974 # "selfsign-rsa-wit"
 35:   682D736861353132                 # "h-sha512"
 43: 00            # [7]. subjectPublicKeyAlg=0: RSA
 44: 58 80         # [8]. subject public key=byte[128]
 46:   B8092F6F04726A921CFAB2D313AE9D2F01C7CE465FAB7DA62C7A5C73FACE
 76:   5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5B926BB5E0D3F727A
106:   763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C3634E89C6D1
136:   731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4E6B6E572
166:   83F6478DAF4253DB
174: 20            # [9]. extensions=-1, KeyUsage, critical:
                   #      [digitalSignature]
175: 58 80         # [10]. signature value=byte[128]
177:   B5D4C31502957FBEE2E4DED7E45E723A8B9A86A46E9FEA1D87817808D1AC
207:   E802370B91718755F101FFB3B971816120BE5CC05D2EE866422D78EF7D16
237:   AA78CE4011E4DC92AE1C7DA3C7831773A44A7B2F5BAFED5D2B8A6A4E6E49
267:   638B3335DC68B596AE5FC48360E1C7DD50BD457CF2CFDCF56F98BE1EA310
297:   3B12DD5B6221DB21
```

4.16. RSASSA-PSS With SHA-256

* Self-signed

* Signature algorithm: rsassa-pss-with-sha256

4.16.1. Private Key

See Section 3.1.1.

4.16.2. X.509 Certificate

PEM content (575 bytes):

```
-----BEGIN CERTIFICATE-----
MIICOzCCAXCgAwIBAgICEjQwQQYJKoZIhvcNAQEKMDSgDzANBglghkgBZQMEAgEF
AKEcMBoGCSqGSIb3DQEBCDANBglghkgBZQMEAgEFAKIDAgEgMCUxIzAhBgNVBAMM
GnNlbGZzaWduLXJzYXNzYS1wc3Mtc2hhMjU2MB4XDTI1MDEwMjAwMDAwMFoXDTI2
MDEwMjAwMDAwMFowJTEjMCEGA1UEAwwac2VsZnNpZ24tcnNhc3NhLXBzcy1zaGEy
NTYwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALgJL28EcmqSHPqy0xOunS8B
x85GX6t9pix6XHP6zl/7ovHdgKKa3EM5nPyiInm4miZIEOW5JrteDT9yenY+FgE/
ifj+rFnQ+91eiwxSgn5UkPE7hMNjTonG0XMa5fGmD4jtEY0IDhqyyqUy0GwvfSoI
dN7k5rblcoP2R42vQlPbAgMBAAGjEjAQMA4GA1UdDwEB/wQEAwIHgDBBBgkqhkiG
9w0BAQowNKAPMA0GCWCGSAFlAwQCAQUAoRwwGgYJKoZIhvcNAQEIMA0GCWCGSAFl
AwQCAQUAogMCASADgYEAaxYseZDcSnGCKNIuIk3zWqHnUZIwyOtSrx6iG2RBexZj
Hr8Gp9Anfzk5p8iw//TcfIkbJ119gfUpdZhxvMQjqq6NRqD1Hj/gte0npsFtSojF
7zIGqFbtuwbnr3PUKXa8Y/Yu0QBRvw3bZCVNxeixHr1O71t6oJLfEHm6QSXQv+c=
-----END CERTIFICATE-----
```

4.16.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 4.16.2.

Plain hex (307 bytes):

```
03421234181AF61A6775D7001A69570A80781A73656C667369676E2D727361737361
2D7073732D736861323536005880B8092F6F04726A921CFAB2D313AE9D2F01C7CE46
5FAB7DA62C7A5C73FACE5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5B926
BB5E0D3F727A763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C3634E89
C6D1731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4E6B6E57283F6
478DAF4253DB2058806B162C7990DC4A718228D22E224DF35AA1E7519230C8EB52AF
1EA21B64417B16631EBF06A7D0277F3939A7C8B0FFF4DC7C891B275D7D81F5297598
71BCC423AAAE8D46A0F51E3FE0B5ED27A6C16D4A88C5EF3206A856EDBB06E7AF73D4
2976BC63F62ED10051BF0DDB64254DC5E8B11EBD4EEF5B7AA092DF1079BA4125D0BF
E7
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

4.16.4. C509 Type 2 Certificate

Plain hex (307 bytes):

```
02421234181AF61A6775D7001A69570A80781A73656C667369676E2D727361737361
2D7073732D736861323536005880B8092F6F04726A921CFAB2D313AE9D2F01C7CE46
5FAB7DA62C7A5C73FACE5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5B926
BB5E0D3F727A763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C3634E89
C6D1731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4E6B6E57283F6
478DAF4253DB2058804D8FB6928B9C34EF6E53A22DE2BED6579A58FB990CED4C7CC5
B0227CBB210741B3C3DA6A72CFA764CEF937DABC9C373776FD882ABBD052936D6B4A
14A12E628AF43CA89A6CAAC11513AA9C4438C668447FFF7497F32BE445B58A4EA2E4
0E30C32165558EFB66E2B17640B93B061BD8BF5812818B318415E9F20FFE5EA50C9D
39
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 18 1A          # [2]. signature alg=26: rsassa-pss-with-sha256
  6: F6             # [3]. issuer=<null>
  7: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 12: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 17: 78 1A          # [6]. subject=char[26]
 19:   73656C667369676E2D7273617373612D # "selfsign-rsassa-"
 35:   7073732D736861323536             # "pss-sha256"
 45: 00             # [7]. subjectPublicKeyAlg=0: RSA
 46: 58 80          # [8]. subject public key=byte[128]
 48:   B8092F6F04726A921CFAB2D313AE9D2F01C7CE465FAB7DA62C7A5C73FACE
 78:   5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5B926BB5E0D3F727A
108:   763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C3634E89C6D1
138:   731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4E6B6E572
168:   83F6478DAF4253DB
176: 20             # [9]. extensions=-1, KeyUsage, critical:
                    #      [digitalSignature]
177: 58 80          # [10]. signature value=byte[128]
179:   4D8FB6928B9C34EF6E53A22DE2BED6579A58FB990CED4C7CC5B0227CBB21
209:   0741B3C3DA6A72CFA764CEF937DABC9C373776FD882ABBD052936D6B4A14
239:   A12E628AF43CA89A6CAAC11513AA9C4438C668447FFF7497F32BE445B58A
269:   4EA2E40E30C32165558EFB66E2B17640B93B061BD8BF5812818B318415E9
299:   F20FFE5EA50C9D39
```

4.17. RSASSA-PSS With SHA-384

* Self-signed

* Signature algorithm: rsassa-pss-with-sha384

4.17.1. Private Key

See Section 3.1.1.

4.17.2. X.509 Certificate

PEM content (575 bytes):

```
-----BEGIN CERTIFICATE-----
MIICOzCCAXCgAwIBAgICEjQwQQYJKoZIhvcNAQEKMDSgDzANBglghkgBZQMEAgIF
AKEcMBoGCSqGSIb3DQEBCDANBglghkgBZQMEAgIFAKIDAgEwMCUxIzAhBgNVBAMM
GnNlbGZzaWduLXJzYXNzYS1wc3Mtc2hhMzg0MB4XDTI1MDEwMjAwMDAwMFoXDTI2
MDEwMjAwMDAwMFowJTEjMCEGA1UEAwwac2VsZnNpZ24tcnNhc3NhLXBzcy1zaGEz
ODQwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALgJL28EcmqSHPqy0xOunS8B
x85GX6t9pix6XHP6zl/7ovHdgKKa3EM5nPyiInm4miZIEOW5JrteDT9yenY+FgE/
ifj+rFnQ+91eiwxSgn5UkPE7hMNjTonG0XMa5fGmD4jtEY0IDhqyyqUy0GwvfSoI
dN7k5rblcoP2R42vQlPbAgMBAAGjEjAQMA4GA1UdDwEB/wQEAwIHgDBBBgkqhkiG
9w0BAQowNKAPMA0GCWCGSAFlAwQCAgUAoRwwGgYJKoZIhvcNAQEIMA0GCWCGSAFl
AwQCAgUAogMCATADgYEAqVzA6vSrfxLlxmScZDh63L2urQ7spjsiVkW6EQFEZvUT
eJBArUoQh+skNokj0K/ThgT0Ivh2hFgrvWx69/t4h9JAy2OMGj3sAHGH8HlgsqG4
glCKKGyhsXJqPEtOSAilslD7s5zI1xhmToKQ5ZqZVkXSSph5+rZkwKjRO67tv64=
-----END CERTIFICATE-----
```

4.17.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 4.17.2.

Plain hex (307 bytes):

```
03421234181BF61A6775D7001A69570A80781A73656C667369676E2D727361737361
2D7073732D736861333834005880B8092F6F04726A921CFAB2D313AE9D2F01C7CE46
5FAB7DA62C7A5C73FACE5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5B926
BB5E0D3F727A763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C3634E89
C6D1731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4E6B6E57283F6
478DAF4253DB205880A95CC0EAF4AB7F12E5C6649C64387ADCBDAEAD0EECA63B2256
45BA11014466F513789040AD4A1087EB24368923D0AFD38604F422F87684582BBD6C
7AF7FB7887D240CB638C1A3DEC007187F07960B2A1B882508A286CA1B1726A3C4B4E
4808A5B250FBB39CC8D718664E8290E59A995645D24A9879FAB664C0A8D13BAEEDBF
AE
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

4.17.4. C509 Type 2 Certificate

Plain hex (307 bytes):

```
02421234181BF61A6775D7001A69570A80781A73656C667369676E2D727361737361
2D7073732D736861333834005880B8092F6F04726A921CFAB2D313AE9D2F01C7CE46
5FAB7DA62C7A5C73FACE5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5B926
BB5E0D3F727A763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C3634E89
C6D1731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4E6B6E57283F6
478DAF4253DB20588062E00951C6AC6536337911F5568E8FCB79440A0A7A59EA7EEF
FC20CD8A85E2111502116A040D14A209602BCD8F635D9B91689429F8B43D35FC79A4
B3AE34824D41B56D9472513673F7D13B2F77B81992B205DDFF91088CCDF03E85A7F0
7471EFF6549AF07A77BBAE313D1B909DDF2EC94C67E0F20A342CC25CFFF87A820CE9
DC
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 18 1B          # [2]. signature alg=27: rsassa-pss-with-sha384
  6: F6             # [3]. issuer=<null>
  7: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 12: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 17: 78 1A          # [6]. subject=char[26]
 19:   73656C667369676E2D7273617373612D # "selfsign-rsassa-"
 35:   7073732D736861333834             # "pss-sha384"
 45: 00             # [7]. subjectPublicKeyAlg=0: RSA
 46: 58 80          # [8]. subject public key=byte[128]
 48:   B8092F6F04726A921CFAB2D313AE9D2F01C7CE465FAB7DA62C7A5C73FACE
 78:   5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5B926BB5E0D3F727A
108:   763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C3634E89C6D1
138:   731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4E6B6E572
168:   83F6478DAF4253DB
176: 20             # [9]. extensions=-1, KeyUsage, critical:
                    #      [digitalSignature]
177: 58 80          # [10]. signature value=byte[128]
179:   62E00951C6AC6536337911F5568E8FCB79440A0A7A59EA7EEFFC20CD8A85
209:   E2111502116A040D14A209602BCD8F635D9B91689429F8B43D35FC79A4B3
239:   AE34824D41B56D9472513673F7D13B2F77B81992B205DDFF91088CCDF03E
269:   85A7F07471EFF6549AF07A77BBAE313D1B909DDF2EC94C67E0F20A342CC2
299:   5CFFF87A820CE9DC
```

4.18. RSASSA-PSS With SHA-512

* Self-signed

* RSA public key with 1536-bit modulus

* Signature algorithm: rsassa-pss-with-sha512

4.18.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MIIDlgIBADANBgkqhkiG9w0BAQEFAASCA4AwggN8AgEAAoHBALURcpGG7cAbIzXs
fkarHPOzH7jUYTPONQWI79he0IdlaLe+AGzjUnq6ZDobD4+l7FQCIpYwRCz84wUI
BMsD+pnlvD+NSLPuqUtCDCb43se3joWAp54prqDcm9xZc/idmz236LvrC/01fOcQ
2e855Ktii4YShduQk58NL9AdjpvJcXz0xOQvsX3MUixCqfoACwX/+6niTuZLmRwe
AYJKnVr9w36hHIGvKh+oK9WJQK19TbYfjcaIxIpobEWxBlYm0wIDAQABAoHAGnwr
BXVhPmnZxyVIvT6B6sr8ggpyuLivZxgGI+COi6zThJjisrViQaMU+QOEowQ9TXZ4
fP53YnCP0RMWBw9rGcARvpFZx+lKKGtzSpoO6tNYd1eqbPH3jKkS6p1yX18cxXKv
IXDGNeaHkrMAzUrFnyAdp84N4py6ilwe4GFSXoXsY+hUFqf2ndLnrdbtutorPOSb
OoAkSha26343TA4KbWSSjzIBdFrevSdVJKPhyXTMM7kzl8rT5ZVq6A5FxkeJAmEA
8k17eXQyp6rwXCngMvqilyd6FPiox7R37/idIhWh1ByI4kTvnYphezUZnT/4RNY2
gGfwvtkU72CNx3/G2VH+IU85UqnWjleSVxt87bW/XLcURC4qRMOJB9G6Kmsodz6Z
AmEAv03NHUsQ+DtA0quYuttBDJYzatVELoR0DINO9uUl7b6kpOeVrHHDqrnKaUKK
NSw7MU2jjGxUlDYblX/CfRFbGi26jefCDHRCJNBdK7XDEobcuWiR3N5G3v5RALyP
71BLAmA1TWg5Op+eFNOVYrzoWgyEdfG8RUtTy1aLGsTuZ5XXBIP0Srfvjy6MnQzK
c/UYp4sLylHCmhyp4DKwTWKgEhJ2n2f70FLbs1YFBY4A+Pdk3P1/ViyEPgOaDcAH
btVTDhkCYQC+HmjpYs/TkreCZszbbsi/5Inm81nWTQYz5U9VqTe/hcaEqC6keU82
3XuejmViILoW7ozKImMQBJH3SkgUGWqLosSTAK9lxyhxA66EoRfj0qmLjbPgZ/rQ
5LfF3p/A+u8CYHb/ZTlM+RxAgAJ7bsxrUKJrkM4yRz7YXNcXZH4N6A+s4HzY1+Y/
aKaI5NsOmVR3Gr2OzpxQwALgD+Xo6hzyBPQ2gbozBA2VQ38zwt3M4dU6clFcc9R1
q1jQfu4/j1hEEg==
-----END PRIVATE KEY-----
```

4.18.2. X.509 Certificate

PEM content (703 bytes):

```
-----BEGIN CERTIFICATE-----
MIICuzCCAbCgAwIBAgICEjQwQQYJKoZIhvcNAQEKMDSgDzANBglghkgBZQMEAgMF
AKEcMBoGCSqGSIb3DQEBCDANBglghkgBZQMEAgMFAKIDAgFAMCUxIzAhBgNVBAMM
GnNlbGZzaWduLXJzYXNzYS1wc3Mtc2hhNTEyMB4XDTI1MDEwMjAwMDAwMFoXDTI2
MDEwMjAwMDAwMFowJTEjMCEGA1UEAwwac2VsZnNpZ24tcnNhc3NhLXBzcy1zaGE1
MTIwgd8wDQYJKoZIhvcNAQEBBQADgc0AMIHJAoHBALURcpGG7cAbIzXsfkarHPOz
H7jUYTPONQWI79he0IdlaLe+AGzjUnq6ZDobD4+l7FQCIpYwRCz84wUIBMsD+pnl
vD+NSLPuqUtCDCb43se3joWAp54prqDcm9xZc/idmz236LvrC/01fOcQ2e855Kti
i4YShduQk58NL9AdjpvJcXz0xOQvsX3MUixCqfoACwX/+6niTuZLmRweAYJKnVr9
w36hHIGvKh+oK9WJQK19TbYfjcaIxIpobEWxBlYm0wIDAQABoxIwEDAOBgNVHQ8B
Af8EBAMCB4AwQQYJKoZIhvcNAQEKMDSgDzANBglghkgBZQMEAgMFAKEcMBoGCSqG
SIb3DQEBCDANBglghkgBZQMEAgMFAKIDAgFAA4HBAColIqgyLpIBpUstLLEaPeNe
NpA9ZibWHKT+HrHFhINsWmg6SNYDrn4/XA1j/1II9nlCvq8oq2HnHr6IUqIe6tpd
YSA5sNiAdqzSDdWRmpzpGCBzCZoxrxT3mtZ7NPqmOKYj9xRGhyrRyHB9VnEbaWXt
r2Tyr3LI6dmUsRkh+jjW31NeaLl2YAPkqsMqiXBaxiIkaYs+CwQ6UIwiy8wcdqKC
K3F9aMjdTyyfZOdSU8YqONqQbmZPJSuBAHxVgrumyQ==
-----END CERTIFICATE-----
```

4.18.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 4.18.2.

Plain hex (435 bytes):

```
03421234181CF61A6775D7001A69570A80781A73656C667369676E2D727361737361
2D7073732D7368613531320058C0B511729186EDC01B2335EC7E46AB1CF3B31FB8D4
6133CE350588EFD85ED0876568B7BE006CE3527ABA643A1B0F8FA5EC540222963044
2CFCE3050804CB03FA99E5BC3F8D48B3EEA94B420C26F8DEC7B78E8580A79E29AEA0
DC9BDC5973F89D9B3DB7E8BBEB0BFD357CE710D9EF39E4AB628B861285DB90939F0D
2FD01D8E9BC9717CF4C4E42FB17DCC522C42A9FA000B05FFFBA9E24EE64B991C1E01
824A9D5AFDC37EA11C81AF2A1FA82BD58940AD7D4DB61F8DC688C48A686C45B10656
26D32058C02A2522A8322E9201A54B2D2CB11A3DE35E36903D6626D61CA4FE1EB1C5
84836C5A683A48D603AE7E3F5C0D63FF5208F67942BEAF28AB61E71EBE8852A21EEA
DA5D612039B0D88076ACD20DD5919A9CE9182073099A31AF14F79AD67B34FAA638A6
23F71446872AD1C8707D56711B6965EDAF64F2AF72C8E9D994B11921FA38D6DF535E
68B9766003E4AAC32A89705AC62224698B3E0B043A508C22CBCC1C76A2822B717D68
C8DD4F2C9F64E75253C62A38DA906E664F252B81007C5582BBA6C9
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

4.18.4. C509 Type 2 Certificate

Plain hex (435 bytes):

```
02421234181CF61A6775D7001A69570A80781A73656C667369676E2D727361737361
2D7073732D7368613531320058C0B511729186EDC01B2335EC7E46AB1CF3B31FB8D4
6133CE350588EFD85ED0876568B7BE006CE3527ABA643A1B0F8FA5EC540222963044
2CFCE3050804CB03FA99E5BC3F8D48B3EEA94B420C26F8DEC7B78E8580A79E29AEA0
DC9BDC5973F89D9B3DB7E8BBEB0BFD357CE710D9EF39E4AB628B861285DB90939F0D
2FD01D8E9BC9717CF4C4E42FB17DCC522C42A9FA000B05FFFBA9E24EE64B991C1E01
824A9D5AFDC37EA11C81AF2A1FA82BD58940AD7D4DB61F8DC688C48A686C45B10656
26D32058C0A2218182F9D326F7A5164835FF9B2D24927A5277D9482AB0A729D4321D
66365D58A0DFADDABB6D6D57FF358CFB090DFDFE12EA0D1FCA209808AAFAD0DC4F24
F1ACA12B364B6922B93DD574737BA10B77B1BFF69512C4A35692C03565E19EB8F312
3A3B07063783A08F9AB93FEDCEAB7C2295F47226D4B6ED536E71BB7E671DD9D9BCC9
BF592353C9BCEFFC0B78BC1615F4C53C6B8EF403B606E6D89A3458AA16C786609F35
3E40F8EB5BACDA815B1BDDA10132BC8642EBBF6FF5D9AB1A11D272
```

Annotated hex:

```
     0: 02             # [0]. certificate type=2
     1: 42             # [1]. serial number=byte[2]
     2:   1234
     4: 18 1C          # [2]. signature alg=28: rsassa-pss-with-sha512
     6: F6             # [3]. issuer=<null>
     7: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
    12: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
    17: 78 1A          # [6]. subject=char[26]
    19:   73656C667369676E2D7273617373612D # "selfsign-rsassa-"
    35:   7073732D736861353132             # "pss-sha512"
    45: 00             # [7]. subjectPublicKeyAlg=0: RSA
    46: 58 C0          # [8]. subject public key=byte[192]
    48:   B511729186EDC01B2335EC7E46AB1CF3B31FB8D46133CE350588EFD85ED0
    78:   876568B7BE006CE3527ABA643A1B0F8FA5EC5402229630442CFCE3050804
   108:   CB03FA99E5BC3F8D48B3EEA94B420C26F8DEC7B78E8580A79E29AEA0DC9B
   138:   DC5973F89D9B3DB7E8BBEB0BFD357CE710D9EF39E4AB628B861285DB9093
   168:   9F0D2FD01D8E9BC9717CF4C4E42FB17DCC522C42A9FA000B05FFFBA9E24E
   198:   E64B991C1E01824A9D5AFDC37EA11C81AF2A1FA82BD58940AD7D4DB61F8D
   228:   C688C48A686C45B1065626D3
   240: 20             # [9]. extensions=-1, KeyUsage, critical:
                       #      [digitalSignature]
   241: 58 C0          # [10]. signature value=byte[192]
   243:   A2218182F9D326F7A5164835FF9B2D24927A5277D9482AB0A729D4321D66
   273:   365D58A0DFADDABB6D6D57FF358CFB090DFDFE12EA0D1FCA209808AAFAD0
   303:   DC4F24F1ACA12B364B6922B93DD574737BA10B77B1BFF69512C4A35692C0
   333:   3565E19EB8F3123A3B07063783A08F9AB93FEDCEAB7C2295F47226D4B6ED
   363:   536E71BB7E671DD9D9BCC9BF592353C9BCEFFC0B78BC1615F4C53C6B8EF4
   393:   03B606E6D89A3458AA16C786609F353E40F8EB5BACDA815B1BDDA10132BC
   423:   8642EBBF6FF5D9AB1A11D272
```

4.19. RSASSA-PSS With SHAKE128

* Self-signed

* Signature algorithm: rsassa-pss-with-shake128

4.19.1. Private Key

See Section 3.1.1.

4.19.2. X.509 Certificate

PEM content (469 bytes):

```
-----BEGIN CERTIFICATE-----
MIIB0TCCAT2gAwIBAgICEjQwCgYIKwYBBQUHBh4wJzElMCMGA1UEAwwcc2VsZnNp
Z24tcnNhc3NhLXBzcy1zaGFrZTEyODAeFw0yNTAxMDIwMDAwMDBaFw0yNjAxMDIw
MDAwMDBaMCcxJTAjBgNVBAMMHHNlbGZzaWduLXJzYXNzYS1wc3Mtc2hha2UxMjgw
gZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALgJL28EcmqSHPqy0xOunS8Bx85G
X6t9pix6XHP6zl/7ovHdgKKa3EM5nPyiInm4miZIEOW5JrteDT9yenY+FgE/ifj+
rFnQ+91eiwxSgn5UkPE7hMNjTonG0XMa5fGmD4jtEY0IDhqyyqUy0GwvfSoIdN7k
5rblcoP2R42vQlPbAgMBAAGjEjAQMA4GA1UdDwEB/wQEAwIHgDAKBggrBgEFBQcG
HgOBgQByM9xppigNp+i9m2mNiHR93BfwLhn0bn9889MUt+khw3LvDPUWnbqUVAj8
DwAFBzSHsZlDFI1gdkEH69Ruu/+fij6pDCjoMyCset+RWZwOWdyP2bHx/JWncxj1
5lAouomFNeD+ixv2eI/sJfiA0nGaVwOJmzrs5cC3wY1MzlW3GQ==
-----END CERTIFICATE-----
```

4.19.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 4.19.2.

Plain hex (309 bytes):

```
03421234181DF61A6775D7001A69570A80781C73656C667369676E2D727361737361
2D7073732D7368616B65313238005880B8092F6F04726A921CFAB2D313AE9D2F01C7
CE465FAB7DA62C7A5C73FACE5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5
B926BB5E0D3F727A763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C363
4E89C6D1731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4E6B6E572
83F6478DAF4253DB2058807233DC69A6280DA7E8BD9B698D88747DDC17F02E19F46E
7F7CF3D314B7E921C372EF0CF5169DBA945408FC0F0005073487B19943148D607641
07EBD46EBBFF9F8A3EA90C28E83320AC7ADF91599C0E59DC8FD9B1F1FC95A77318F5
E65028BA898535E0FE8B1BF6788FEC25F880D2719A5703899B3AECE5C0B7C18D4CCE
55B719
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

4.19.4. C509 Type 2 Certificate

Plain hex (309 bytes):

```
02421234181DF61A6775D7001A69570A80781C73656C667369676E2D727361737361
2D7073732D7368616B65313238005880B8092F6F04726A921CFAB2D313AE9D2F01C7
CE465FAB7DA62C7A5C73FACE5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5
B926BB5E0D3F727A763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C363
4E89C6D1731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4E6B6E572
83F6478DAF4253DB20588006B4F24DEFA5DC3C58E8C0B8E30A03C43A43A42B6EAD06
458EE0FFB5EAA443204DA030DFD19BCDCA2D5C0B4D6C848B5F9EC444C39CDF4C7263
887D922AE17D8989A5F2046E6B4D2D9F114BA960DC55DFFFF775F9481F580DAD43A9
84BAE37A650297C563C9AAA24CBFC3086BBCD6CAEE405E23EDC9104DD16F653B47C9
EB6B31
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 18 1D          # [2]. signature alg=29: rsassa-pss-with-shake128
  6: F6             # [3]. issuer=<null>
  7: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 12: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 17: 78 1C          # [6]. subject=char[28]
 19:   73656C667369676E2D7273617373612D # "selfsign-rsassa-"
 35:   7073732D7368616B65313238         # "pss-shake128"
 47: 00             # [7]. subjectPublicKeyAlg=0: RSA
 48: 58 80          # [8]. subject public key=byte[128]
 50:   B8092F6F04726A921CFAB2D313AE9D2F01C7CE465FAB7DA62C7A5C73FACE
 80:   5FFBA2F1DD80A29ADC43399CFCA22279B89A264810E5B926BB5E0D3F727A
110:   763E16013F89F8FEAC59D0FBDD5E8B0C52827E5490F13B84C3634E89C6D1
140:   731AE5F1A60F88ED118D080E1AB2CAA532D06C2F7D2A0874DEE4E6B6E572
170:   83F6478DAF4253DB
178: 20             # [9]. extensions=-1, KeyUsage, critical:
                    #      [digitalSignature]
179: 58 80          # [10]. signature value=byte[128]
181:   06B4F24DEFA5DC3C58E8C0B8E30A03C43A43A42B6EAD06458EE0FFB5EAA4
211:   43204DA030DFD19BCDCA2D5C0B4D6C848B5F9EC444C39CDF4C7263887D92
241:   2AE17D8989A5F2046E6B4D2D9F114BA960DC55DFFFF775F9481F580DAD43
271:   A984BAE37A650297C563C9AAA24CBFC3086BBCD6CAEE405E23EDC9104DD1
301:   6F653B47C9EB6B31
```

4.20. RSASSA-PSS With SHAKE256

* Self-signed

* Signature algorithm: rsassa-pss-with-shake256

4.20.1. Private Key

See Section 4.18.1.

4.20.2. X.509 Certificate

PEM content (597 bytes):

```
-----BEGIN CERTIFICATE-----
MIICUTCCAX2gAwIBAgICEjQwCgYIKwYBBQUHBh8wJzElMCMGA1UEAwwcc2VsZnNp
Z24tcnNhc3NhLXBzcy1zaGFrZTI1NjAeFw0yNTAxMDIwMDAwMDBaFw0yNjAxMDIw
MDAwMDBaMCcxJTAjBgNVBAMMHHNlbGZzaWduLXJzYXNzYS1wc3Mtc2hha2UyNTYw
gd8wDQYJKoZIhvcNAQEBBQADgc0AMIHJAoHBALURcpGG7cAbIzXsfkarHPOzH7jU
YTPONQWI79he0IdlaLe+AGzjUnq6ZDobD4+l7FQCIpYwRCz84wUIBMsD+pnlvD+N
SLPuqUtCDCb43se3joWAp54prqDcm9xZc/idmz236LvrC/01fOcQ2e855Ktii4YS
hduQk58NL9AdjpvJcXz0xOQvsX3MUixCqfoACwX/+6niTuZLmRweAYJKnVr9w36h
HIGvKh+oK9WJQK19TbYfjcaIxIpobEWxBlYm0wIDAQABoxIwEDAOBgNVHQ8BAf8E
BAMCB4AwCgYIKwYBBQUHBh8DgcEAjurY2mbPMZ4lE99aj8wWiiQhOvUIfCaGVyTW
sYWSkNvvtn/SuszOwwD3u4GCIH7fP66LRYWthFw/3ZTpT82lqdJSfrJe1BnZ7a0r
aarrQN1eJEdJNpeF7GdJinsRXUzgDpVCYifjiBnufr3gE3Eygsso/Pr1Q/XvQ/OK
nnCj+vQQDSOXCkEuTHGZ9cgc9kczlvP3MZmg6OLZ2KgtdgFzRJCT39JeD3p3lyn7
j/mfBk9ZxL3vWY2gR5eDwgXvIdmK
-----END CERTIFICATE-----
```

4.20.3. C509 Type 3 Certificate

* C509 type 3 certificate converted from the X.509 certificate in Section 4.20.2.

Plain hex (437 bytes):

```
03421234181EF61A6775D7001A69570A80781C73656C667369676E2D727361737361
2D7073732D7368616B653235360058C0B511729186EDC01B2335EC7E46AB1CF3B31F
B8D46133CE350588EFD85ED0876568B7BE006CE3527ABA643A1B0F8FA5EC54022296
30442CFCE3050804CB03FA99E5BC3F8D48B3EEA94B420C26F8DEC7B78E8580A79E29
AEA0DC9BDC5973F89D9B3DB7E8BBEB0BFD357CE710D9EF39E4AB628B861285DB9093
9F0D2FD01D8E9BC9717CF4C4E42FB17DCC522C42A9FA000B05FFFBA9E24EE64B991C
1E01824A9D5AFDC37EA11C81AF2A1FA82BD58940AD7D4DB61F8DC688C48A686C45B1
065626D32058C08EEAD8DA66CF319E2513DF5A8FCC168A24213AF5087C26865724D6
B1859290DBEFB67FD2BACCCEC300F7BB8182207EDF3FAE8B4585AD845C3FDD94E94F
CDA5A9D2527EB25ED419D9EDAD2B69AAEB40DD5E244749369785EC67498A7B115D4C
E00E95426227E38819EE7EBDE013713282CB28FCFAF543F5EF43F38A9E70A3FAF410
0D23970A412E4C7199F5C81CF6473396F3F73199A0E8E2D9D8A82D760173449093DF
D25E0F7A779729FB8FF99F064F59C4BDEF598DA0479783C205EF21D98A
```

Annotated hex:

* See the annotated hex of the C509 type 2 certificate. The only difference is the certificate type, and the signature value.

4.20.4. C509 Type 2 Certificate

Plain hex (437 bytes):

```
02421234181EF61A6775D7001A69570A80781C73656C667369676E2D727361737361
2D7073732D7368616B653235360058C0B511729186EDC01B2335EC7E46AB1CF3B31F
B8D46133CE350588EFD85ED0876568B7BE006CE3527ABA643A1B0F8FA5EC54022296
30442CFCE3050804CB03FA99E5BC3F8D48B3EEA94B420C26F8DEC7B78E8580A79E29
AEA0DC9BDC5973F89D9B3DB7E8BBEB0BFD357CE710D9EF39E4AB628B861285DB9093
9F0D2FD01D8E9BC9717CF4C4E42FB17DCC522C42A9FA000B05FFFBA9E24EE64B991C
1E01824A9D5AFDC37EA11C81AF2A1FA82BD58940AD7D4DB61F8DC688C48A686C45B1
065626D32058C03C5A7DBA06D0918EB0397D881C60312E0668171E2644F9E30E05DC
76231AF177C8E1B460A763B31B7B869F2070602BB5749D627A7074973D4D49ADF9A2
82C506101713DD246B92AD47D2A8A914891538670F8F38F32B4C39A87C5B4FF1DFBF
7F00A6353F199F885EA95172C334B61335A46D9DE493D2A1DB40B7CF7F39E6297D95
1CC35D459B911A591EF16511D9470C861320B6559A138D1F4AE6B4FF8E493A3B9C51
50B123FEB2FB84B5FDE60CE4FBC5FA74E4E1B9CCDAA8F2A8D4CF574263
```

Annotated hex:

```
  0: 02             # [0]. certificate type=2
  1: 42             # [1]. serial number=byte[2]
  2:   1234
  4: 18 1E          # [2]. signature alg=30: rsassa-pss-with-shake256
  6: F6             # [3]. issuer=<null>
  7: 1A 6775D700    # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 12: 1A 69570A80    # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 17: 78 1C          # [6]. subject=char[28]
 19:   73656C667369676E2D7273617373612D # "selfsign-rsassa-"
 35:   7073732D7368616B65323536         # "pss-shake256"
 47: 00             # [7]. subjectPublicKeyAlg=0: RSA
 48: 58 C0          # [8]. subject public key=byte[192]
 50:   B511729186EDC01B2335EC7E46AB1CF3B31FB8D46133CE350588EFD85ED0
 80:   876568B7BE006CE3527ABA643A1B0F8FA5EC5402229630442CFCE3050804
110:   CB03FA99E5BC3F8D48B3EEA94B420C26F8DEC7B78E8580A79E29AEA0DC9B
140:   DC5973F89D9B3DB7E8BBEB0BFD357CE710D9EF39E4AB628B861285DB9093
170:   9F0D2FD01D8E9BC9717CF4C4E42FB17DCC522C42A9FA000B05FFFBA9E24E
200:   E64B991C1E01824A9D5AFDC37EA11C81AF2A1FA82BD58940AD7D4DB61F8D
230:   C688C48A686C45B1065626D3
242: 20             # [9]. extensions=-1, KeyUsage, critical:
                    #      [digitalSignature]
243: 58 C0          # [10]. signature value=byte[192]
245:   3C5A7DBA06D0918EB0397D881C60312E0668171E2644F9E30E05DC76231A
275:   F177C8E1B460A763B31B7B869F2070602BB5749D627A7074973D4D49ADF9
305:   A282C506101713DD246B92AD47D2A8A914891538670F8F38F32B4C39A87C
335:   5B4FF1DFBF7F00A6353F199F885EA95172C334B61335A46D9DE493D2A1DB
365:   40B7CF7F39E6297D951CC35D459B911A591EF16511D9470C861320B6559A
395:   138D1F4AE6B4FF8E493A3B9C5150B123FEB2FB84B5FDE60CE4FBC5FA74E4
425:   E1B9CCDAA8F2A8D4CF574263
```

4.21. SM2 With SM3

* Signature algorithm: sm2-with-sm3

See Section 3.10.

5. Certificates With Different Subject Attributes

5.1. One Attribute CommonName With EUI-48

* Subject: with only one attribute commonName consisting of even number of EUI-48.

See Section 3.1.

5.2. One Attribute CommonName With EUI-64

* Subject: with only one attribute commonName consisting of even number of EUI-64.

See Section 3.2.

5.3. One Attribute CommonName With Even Number Of Lowercase Hex Letters

* Subject: with only one attribute commonName consisting of even number of lowercase hex letters

See Section 3.3.

5.4. One Attribute CommonName With Other Text

* Subject: with only one attribute commonName consisting of text other than EUI-48, EUR-64 and even number of lowercase hex letters

See Section 3.4.

5.5. Empty Subject

* Subject: empty subject.

See Section 3.5.

5.6. Subject With Attribute Business Category

* Subject: with attribute business category

See Section 3.9.

5.7. Subject With Attribute Country

* Subject: with attribute country

See Section 3.6.

5.8. Subject With Attribute Directory Management Domain Name

* Subject: with attribute directory magement domain name

See Section 3.13.

5.9. Subject With Attribute DN Qualifier

* Subject: with attribute DN Qualifier

See Section 3.13.

5.10. Subject With Attribute Domain Component

* Subject: with attribute domain component

See Section 3.13.

5.11. Subject With Attribute Email Address

* Subject: with attribute email address

See Section 3.9.

5.12. Subject With Attribute Generation Qualifier

* Subject: with attribute generation qualifier

See Section 3.13.

5.13. Subject With Attribute Given Name

* Subject: with attribute given name

See Section 3.7.

5.14. Subject With Attribute Initials

* Subject: with attribute initials

See Section 3.14.

5.15. Subject With Attribute Incorporation Country

* Subject: with attribute incorporation country

See Section 3.8.

5.16. Subject With Attribute Incorporation Locality

* Subject: with attribute incorporation locality

See Section 3.8.

5.17. Subject With Attribute Incorporation State Or Province

* Subject: with attribute incorporation State or province

See Section 3.8.

5.18. Subject With Attribute Locality

* Subject: with attribute locality

See Section 3.6.

5.19. Subject With Attribute Name

* Subject: with attribute name

See Section 3.7.

5.20. Subject With Attribute Organization

* Subject: with attribute organization

See Section 3.10.

5.21. Subject With Attribute Organizational Unit

* Subject: with attribute organizational unit

See Section 3.10.

5.22. Subject With Attribute Organization Identifier

* Subject: with attribute organization identifier

See Section 3.10.

5.23. Subject With Attribute Postal Code

* Subject: with attribute postal code

See Section 3.6.

5.24. Subject With Attribute Pseudonym

* Subject: with attribute pseudonym

See Section 3.14.

5.25. Subject With Attribute Serial Number

* Subject: with attribute serial number

See Section 3.10.

5.26. Subject With Attribute State

* Subject: with attribute state

See Section 3.6.

5.27. Subject With Attribute Street

* Subject: with attribute street

See Section 3.6.

5.28. Subject With Attribute Surname

* Subject: with attribute surname

See Section 3.7.

5.29. Subject With Attribute Telephone Number

* Subject: with attribute telephone number

See Section 3.9.

5.30. Subject With Attribute Title

* Subject: with attribute title

See Section 3.7.

5.31. Subject With Attribute Unstructured Name

* Subject: with attribute unstructured name

See Section 3.13.

5.32. Subject With Attribute Unstructured Address

* Subject: with attribute unstructured address

See Section 3.13.

5.33. Subject With Attribute userid

* Subject: with attribute userid

See Section 3.14.

6. Certificates With Different Extensions

6.1. Empty extensions

* Extensions: no extensions.

Not applied to certificate, see Section 8.4 for examples in certificate requests.

6.2. One Extension: Non-critical Extension keyUsage

* Extensions: with only one extension: non-critical extension keyUsage

See Section 3.1.

6.3. One Extension: Critical Extension keyUsage

* Extensions: with only one extension: critical extension keyUsage

See Section 3.2.

6.4. Authority Information Access

See Section 3.11.

6.5. Authority Key Identifier

* With only the field KeyIdentifier

  See Section 3.11.

* With all fields

  See Section 3.12.

6.6. AS Resources And AS Resources v2

* With null ASIdentifiers

* With non-empty array of ASIdOrRange

See Section 3.6.

6.7. Basic Constraints

* With CA = true and absent pathLen

  See Section 3.3.

* With CA = true and present pathLen

  See Section 3.4.

* With CA = false

  See Section 3.5.

6.8. Certificate Policies

See Section 3.4.

6.9. Challenge Password

Not applied to certificates. See Section 8.1.

6.10. CRL Distribution Points and Freshest CRL

See Section 3.12.

6.11. Extended Key Usage

* With usages identified by int

  See Section 3.3.

* With usages identified by ~oid

  See Section 3.4.

* With usages identified by int and ~oid

  See Section 3.5.

6.12. Inhibit anyPolicy

See Section 3.4.

6.13. Issuer Alternative Name

See Section 3.11.

6.14. IP Resources and IP Resources V2

* With IPAddressOrRange of "null"

  See Section 3.6.

* With IPAddressOrRange of non-null

  See Section 3.6.

6.15. Name Constraints

* With only PermittedSubTree

  See Section 3.9.

* With only ExcludedSubTree

  See Section 3.10.

* With both PermittedSubTree and ExcludedSubTree

  See Section 3.13.

6.16. OCSP No Check

See Section 3.14.

6.17. Policy Constraints

* With only RequireExplicitPolicy

  See Section 3.9.

* With only InhibitPolicyMapping

  See Section 3.10.

* With both Require and Inhibit

  See Section 3.13.

6.18. Policy Mappings

See Section 3.8.

6.19. PreCertificate Signing Certificate

See Section 3.14.

6.20. Signed Certificate Timestamp List

See Section 3.14.

6.21. Subject Alternative Name

See Section 3.5.

6.22. Subject Directory Attributes

See Section 3.8.

6.23. Subject Information Access

See Section 3.8.

6.24. Subject Key Identifier

See Section 3.3.

6.25. TLS Features

See Section 3.14.

7. X.509 Certificate With Unconvertible Attributes And Extensions

* Common Name: subject with text not of types PrintableString and UTF8String.
* Subject Public Key Algorithm: EC public key with unknown curve OID in the "parameters" field.
* Extension AS Resources: ASIdentifiers with the "rdi" field.
* Extension CRL Distribution Points: with the "reasons" field in DistributionPoint.
* Extension IP Resources: SAFI is present.

* Extension Name Constraints: with Option Directory Name with IA5String.

* Extension Signed Certificate Timestamp List: with the "extensions" field.

7.1. Private Key

See Section 3.3.1.

7.2. X.509 Certificate

PEM content (614 bytes)

```
-----BEGIN CERTIFICATE-----
MIICYjCCAgigAwIBAgIBATAKBggqhkjOPQQDAjAiMSAwHgYDVQQDFhdBbiBJQTVT
dHJpbmcgQ29tbW9uTmFtZTAeFw0yNTAxMDIwMDAwMDBaFw0yNjAxMDIwMDAwMDBa
MCIxIDAeBgNVBAMWF0FuIElBNVN0cmluZyBDb21tb25OYW1lMFswFQYHKoZIzj0C
AQYKKwYBBAGC41JjBQNCAAT0E1lqhxJZlbTg2Le++8TW7bEfYa8IqzJAjU/5+QeN
26s2Na/UltVlaiLv3D1ZxEgqmYNrs1j79Mp405MENshXo4IBKzCCAScwEgYIKwYB
BQUHAQgEBjAEoQIFADAtBgNVHR8EJjAkMCKgHKAahhhodHRwOi8vZHVtbXkuZXhh
bXBsZS5vcmeBAgZAMBoGCCsGAQUFBwEHAQH/BAswCTAHBAMAAQEFADAzBgNVHR4E
LDAqoCgwJqQkMCIxIDAeBgNVBAMWF0FuIElBNVN0cmluZyBDb21tb25OYW1lMIGQ
BgorBgEEAdZ5AgQCBIGBBH8AfQB7ABERERERERERERERERERERERERERERERERER
ERERERERAAABlCRP2+cABgABAgMEBQQDAEYwRAIgEhISEhISEhISEhISEhISEhIS
EhISEhISEhISEhICIBISEhISEhISEhISEhISEhISEhISEhISEhISEhISEhISEhIS
MAoGCCqGSM49BAMCA0gAMEUCIQCKJeiqu6Sxm44NFZakdsLEL1Bo9fNFdgaAbi8o
SiLm5wIgSlObrR2qhbXa62NKc6edLBFIg8qIE/w/oYc153i+sUg=
-----END CERTIFICATE-----
```

Text representation:

```
Certificate:
  Data:
    Version: v3 (2)
    Serial Number:
      01
    Issuer: CN=An IA5String CommonName
    Validity:
      Not Before: Thu Jan 02 01:00:00 CET 2025
      Not After : Fri Jan 02 01:00:00 CET 2026
    Subject: CN=An IA5String CommonName
    Subject Public Key Info:
      Public Key Algorithm: 1.2.840.10045.2.1
      Pub:
        04:f4:13:59:6a:87:12:59:95:b4:e0:d8:b7:be:fb:c4:d6:ed:
        b1:1f:61:af:08:ab:32:40:8d:4f:f9:f9:07:8d:db:ab:36:35:
        af:d4:96:d5:65:6a:22:ef:dc:3d:59:c4:48:2a:99:83:6b:b3:
```

```
          58:fb:f4:ca:78:d3:93:04:36:c8:57
      X509v3 extensions:
        X509v3 sbgp-autonomousSysNum:
          Routing Domain Identifier (RDI): inherit
        X509v3 cRLDistributionPoints:
          Reasons: [keyCompromise]
          Full Name:
            URI: http://dummy.example.org
        X509v3 sbgp-ipAddrBlock: critical
          IPv4 unicast: inherit
        X509v3 nameConstraints:
          Permitted
            Directory Name: CN=An IA5String CommonName
        X509v3 CT Precertificate SCTs:
          Signed Certificate Timestamp:
            Version:    v1(0)
            Log ID:
              11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:
              11:11:11:11:11:11:11:11:11:11:11:11:11:11:11:11
            Timestamp:  2025-01-02T00:00:00.999Z
            Extensions:
              00:01:02:03:04:05
            Signature:  ecdsa-with-sha256
              30:44:02:20:12:12:12:12:12:12:12:12:12:12:12:12:
              12:12:12:12:12:12:12:12:12:12:12:12:12:12:12:12:
              12:12:12:12:02:20:12:12:12:12:12:12:12:12:12:12:
              12:12:12:12:12:12:12:12:12:12:12:12:12:12:12:12:
              12:12:12:12:12:12
    Signature Algorithm: SHA256WITHECDSA
    Signature Value:
      30:45:02:21:00:8a:25:e8:aa:bb:a4:b1:9b:8e:0d:15:96:a4:
      76:c2:c4:2f:50:68:f5:f3:45:76:06:80:6e:2f:28:4a:22:e6:
      e7:02:20:4a:53:9b:ad:1d:aa:85:b5:da:eb:63:4a:73:a7:9d:
      2c:11:48:83:ca:88:13:fc:3f:a1:87:35:e7:78:be:b1:48
```

7.3. C509 Type 3 Certificate

* C509 type 3 certificated converted from the X.509 certificate in Section 7.2.

Plain hex (465 bytes):

```
03410100F61A6775D7001A69570A8082435504035819161741 6E2049413553747269
6E6720436F6D6D6F6E4E616D6582472A8648CE3D02014C060A2B0601040182E35263
05584104F413596A87125995B4E0D8B7BEFBC4D6EDB11F61AF08AB32408D4FF9F907
8DDBAB3635AFD496D5656A22EFDC3D59C4482A99836BB358FBF4CA78D3930436C857
8B482B060105050701084630 04A102050043551D1F582630243022A01CA01A861868
7474703A2F2F64756D6D792E6578616D706C652E6F726781020640482B0601050507
0107F54B3009300704030001010500181A828204824355040358191617416E204941
35537472696E6720436F6D6D6F6E4E616D65F64A2B06010401D6790204025881047F
007D007B00111111111111111111111111111111111111111111111111111111111
11111100000194244FDBE70006000102030405040300463044022012121212121212
12121212121212121212121212121212121212121212121212121202201212121212121212
12121212121212121212121212121212121212121212121212121258408A25E8AABBA4B1
9B8E0D1596A476C2C42F5068F5F3457606806E2F284A22E6E74A539BAD1DAA85B5DA
EB634A73A79D2C114883CA8813FC3FA18735E778BEB148
```

Annotated hex:

```
  0: 03            # [0]. certificate type=3
  1: 41            # [1]. serial number=byte[1]
  2:   01
  3: 00            # [2]. signature alg=0: ecdsa-with-sha256
  4: F6            # [3]. issuer=<null>
  5: 1A 6775D700   # [4]. notBefore=1735776000: 2025-01-02T00:00:00Z
 10: 1A 69570A80   # [5]. notAfter=1767312000: 2026-01-02T00:00:00Z
 15: 82            # [6]. subject=array[2], 1 attribute
                     # attribute[0]
 16:     43          # type=byte[3]:
 17:        550403     # oid: 2.5.4.3 (commonName)
 20:     58 19        # value=byte[25]
 22:       1617416E20494135537472696E6720436F6D6D6F6E4E616D65
 47: 82            # [7]. subjectPublicKeyAlg=array[2]
 48:   47            # algorithm=byte[7]:
 49:      2A8648CE3D0201 # oid: 1.2.840.10045.2.1
 56:   4C            # parameters=byte[12]
 57:     060A2B0601040182E3526305
 69: 58 41         # [8]. subject public key=byte[65]
 71:   04F413596A87125995B4E0D8B7BEFBC4D6EDB11F61AF08AB32408D4FF9F9
101:   078DDBAB3635AFD496D5656A22EFDC3D59C4482A99836BB358FBF4CA78D3
131:   930436C857
136: 8B            # [9]. extensions=array[11]
                     # extension[0]
137:     48          # type=byte[8]:
138:        2B06010505070108 # oid: 1.3.6.1.5.5.7.1.8
                              # (AutonomousSysIds)
146:     46          # value=byte[6]
147:       3004A1020500
                     # extension[1]
153:     43          # type=byte[3]:
```

```
   154:        551D1F        # oid: 2.5.29.31 (CRLDistributionPoints)
   157:     58 26          # value=byte[38]
   159:       30243022A01CA01A8618687474703A2F2F64756D6D792E6578616D70
   187:       6C652E6F726781020640
                         # extension[2]
   197:     48              # type=byte[8]:
   198:        2B06010505070107 # oid: 1.3.6.1.5.5.7.1.7
                              # (IPAddressBlocks)
   206:     F5              # critical
   207:     4B              # value=byte[11]
   208:       300930070403000101050O
                         # extension[3]
   219:     18 1A           # type=26: NameConstraints
   221:     82              # value=array[2]
   222:       82              # permittedSubtrees=array[2]
                                # GeneralName[0]
   223:           04            # GeneralNameType=4: directoryName
   224:           82            # GeneralNameValue=array[2], 1
                                # attribute
                                  # attribute[0]
   225:              43           # type=byte[3]:
   226:                 550403       # oid: 2.5.4.3 (commonName)
   229:              58 19        # value=byte[25]
   231:                1617416E20494135537472696E6720436F6D6D6F6E4E61
   254:                6D65
   256:       F6              # excludedSubtrees=<null>
                          # extension[4]
   257:     4A              # type=byte[10]:
   258:        2B06010401D679020402 # oid: 1.3.6.1.4.1.11129.2.4.2
                                    # (SignedCertificateTimestampList)
   268:     58 81           # value=byte[129]
   270:       047F007D007B001111111111111111111111111111111111111111111111
   298:       111111111111111111111100000194244FDBE7000600010203040504
   326:       0300463044022012121212121212121212121212121212121212121212
   354:       121212121212121212121202201212121212121212121212121212121212
   382:       12121212121212121212121212121212
   399: 58 40          # [10]. signature value=byte[64]
   401:   8A25E8AABBA4B19B8E0D1596A476C2C42F5068F5F3457606806E2F284A22
   431:   E6E74A539BAD1DAA85B5DAEB634A73A79D2C114883CA8813FC3FA18735E7
   461:   78BEB148
```

8. Certificate Requests With Different Signature Algorithms

8.1. ECDSA With SHA256

* Signature algorithm: ecdsa-with-SHA256

* Extensions: normal extension subjectAltName

8.1.1. Private Key

See Section 3.3.1.

8.1.2. X.509 Certificate Request

PEM content (244 bytes):

```
-----BEGIN CERTIFICATE REQUEST-----
MIHxMIGXAgEAMBAxDjAMBgNVBAMMBWVjZHNhMFkwEwYHKoZIzj0CAQYIKoZIzj0D
AQcDQgAE9BNZaocSWZW04Ni3vvvE1u2xH2GvCKsyQI1P+fkHjdurNjWv1JbVZWoi
79w9WcRIKpmDa7NY+/TKeNOTBDbIV6AlMCMGCSqGSIb3DQEJDjEWMBQwEgYDVR0R
BAswCYIHYWJjLmNvbTAKBggqhkjOPQQDAgNJADBGAiEAiiXoqruksZuODRWWpHbC
xC9QaPXzRXYGgG4vKEoi5ucCIQDaqB1FnHgqK1QEkIkfSu0+NwXG++EDSqigH4kj
F8jfAg==
-----END CERTIFICATE REQUEST-----
```

Text representation:

```
Certificate Request:
  Data:
    Version: v1 (0)
    Subject: CN=ecdsa
    Subject Public Key Info:
      Public Key Algorithm: EC/SECP256R1
      Pub:
        04:f4:13:59:6a:87:12:59:95:b4:e0:d8:b7:be:fb:c4:d6:ed:
        b1:1f:61:af:08:ab:32:40:8d:4f:f9:f9:07:8d:db:ab:36:35:
        af:d4:96:d5:65:6a:22:ef:dc:3d:59:c4:48:2a:99:83:6b:b3:
        58:fb:f4:ca:78:d3:93:04:36:c8:57
    Attributes:
      X509v3 extensions:
        X509v3 subjectAlternativeName:
          DNS: abc.com
  Signature Algorithm: SHA256WITHECDSA
  Signature Value:
    30:46:02:21:00:8a:25:e8:aa:bb:a4:b1:9b:8e:0d:15:96:a4:
    76:c2:c4:2f:50:68:f5:f3:45:76:06:80:6e:2f:28:4a:22:e6:
    e7:02:21:00:da:a8:1d:45:9c:78:2a:2b:54:04:90:89:1f:4a:
    ed:3e:37:05:c6:fb:e1:03:4a:a8:a0:1f:89:23:17:c8:df:02
```

8.1.3. C509 Type 3 Certificate Request

* C509 type 3 certificate request converted from the X.509 certificate request in Section 8.1.2.

Plain hex (152 bytes):

```
030065656364736101584104F413596A87125995B4E0D8B7BEFBC4D6EDB11F61AF08
AB32408D4FF9F9078DDBAB3635AFD496D5656A22EFDC3D59C4482A99836BB358FBF4
CA78D3930436C8578203676162632E636F6D58408A25E8AABBA4B19B8E0D1596A476
C2C42F5068F5F3457606806E2F284A22E6E7DAA81D459C782A2B540490891F4AED3E
3705C6FBE1034AA8A01F892317C8DF02
```

Annotated hex:

* See the annotated hex of the C509 type 0 certificate request. The only difference is the certificate request type, and the signature value.

8.1.4. C509 Type 1 Certificate Request

* C509 type 1 certificate request converted from the X.509 certificate request in Section 8.1.2.

Plain hex (152 bytes):

```
010065656364736101584104F413596A87125995B4E0D8B7BEFBC4D6EDB11F61AF08
AB32408D4FF9F9078DDBAB3635AFD496D5656A22EFDC3D59C4482A99836BB358FBF4
CA78D3930436C8578203676162632E636F6D58408A25E8AABBA4B19B8E0D1596A476
C2C42F5068F5F3457606806E2F284A22E6E7DAA81D459C782A2B540490891F4AED3E
3705C6FBE1034AA8A01F892317C8DF02
```

Annotated hex:

* See the annotated hex of the C509 type 0 certificate request. The only difference is the certificate request type, and the signature value.

8.1.5. C509 Type 2 Certificate Request

Plain hex (152 bytes):

```
020065656364736101584104F413596A87125995B4E0D8B7BEFBC4D6EDB11F61AF08
AB32408D4FF9F9078DDBAB3635AFD496D5656A22EFDC3D59C4482A99836BB358FBF4
CA78D3930436C8578203676162632E636F6D58408A25E8AABBA4B19B8E0D1596A476
C2C42F5068F5F3457606806E2F284A22E6E790455A15E702657A93E9B1DDCD3298A6
239162E674A110CF7DF2AD6902006CB5
```

Annotated hex:

* See the annotated hex of the C509 type 0 certificate request. The only difference is the certificate request type, and the signature value.

8.1.6. C509 Type 0 Certificate Request

Plain hex (152 bytes):

```
00006565636473610158410F413596A87125995B4E0D8B7BEFBC4D6EDB11F61AF08
AB32408D4FF9F9078DDBAB3635AFD496D5656A22EFDC3D59C4482A99836BB358FBF4
CA78D3930436C8578203676162632E636F6D58408A25E8AABBA4B19B8E0D1596A476
C2C42F5068F5F3457606806E2F284A22E6E7C2AEF4221B91E3D99BCE70E3755804EA
B51D78CD76355F13448D9D5FC4EC35BC
```

Annotated hex:

```
  0: 00             # [0]. c509CertificateRequestType=0
  1: 00             # [1]. subjectSignatureAlgorithm=0:
                    #      ecdsa-with-sha256
  2: 65             # [2]. subject=char[5]
  3:   6563647361      # "ecdsa"
  8: 01             # [3]. subjectPublicKeyAlg=1: EC public key with
                    #      curve secp256r1
  9: 58 41          # [4]. subject public key=byte[65]
 11:   04F413596A87125995B4E0D8B7BEFBC4D6EDB11F61AF08AB32408D4FF9F9
 41:   078DDBAB3635AFD496D5656A22EFDC3D59C4482A99836BB358FBF4CA78D3
 71:   930436C857
 76: 82             # [5]. extensions=array[2]
                      # extension[0]
 77:     03             # type=3: SubjectAlternativeName
 78:     67             # DNS, value=char[7]
 79:       6162632E636F6D  # "abc.com"
 86: 58 40          # [6]. signature value=byte[64]
 88:   8A25E8AABBA4B19B8E0D1596A476C2C42F5068F5F3457606806E2F284A22
118:   E6E7C2AEF4221B91E3D99BCE70E3755804EAB51D78CD76355F13448D9D5F
148:   C4EC35BC
```

8.2. ECDH PoP with SHA-256 and HMAC-SHA256

* Signature algorithm: sa-ecdhPop-sha256-hmac-sha256

* Signature value: with only hashValue field

* Extensions: challenge password with printable String

8.2.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MEECAQAwEwYHKoZIzj0CAQYIKoZIzj0DAQcEJzAlAgEBBCAuLpSUUN6u6VJJyQvn
Nyvkz9ca/kKUfUPG7W+OGX6ZCQ==
-----END PRIVATE KEY-----
```

8.2.2. X.509 Certificate Request

* The private key and certificate of the peer are in Section 3.3.1 and Section 3.3.2.

PEM content (206 bytes):

```
-----BEGIN CERTIFICATE REQUEST-----
MIHLMIGVAgEAMBcxFTATBgNVBAMMDGRoc2lnLXNoYTI1NjBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABMTUozeP7JAAXLsNPq8TCbSCkpr1ZhSvJqnyLbg8TzR3sLqX
Et+CE3SfkY1979+zKmxD3wlxXQDke+BRnSDksxSgHDAaBgkqhkiG9w0BCQcxDRML
bXkgcGFzc3dvcmQwCgYIKwYBBQUHBhoDJQAwIgQgyKNiK7fmJtuRHFcWHh/I/loi
lrthHNVPkHXMolbgdFQ=
-----END CERTIFICATE REQUEST-----
```

Text representation:

```
-----BEGIN CERTIFICATE REQUEST-----
MIHLMIGVAgEAMBcxFTATBgNVBAMMDGRoc2lnLXNoYTI1NjBZMBMGByqGSM49AgEG
CCqGSM49AwEHA0IABMTUozeP7JAAXLsNPq8TCbSCkpr1ZhSvJqnyLbg8TzR3sLqX
Et+CE3SfkY1979+zKmxD3wlxXQDke+BRnSDksxSgHDAaBgkqhkiG9w0BCQcxDRML
bXkgcGFzc3dvcmQwCgYIKwYBBQUHBhoDJQAwIgQgyKNiK7fmJtuRHFcWHh/I/loi
lrthHNVPkHXMolbgdFQ=
-----END CERTIFICATE REQUEST-----
```

8.2.3. C509 Type 3 Certificate Request

* C509 type 3 certificate request converted from the X.509 certificate request in Section 8.2.2.

Plain hex (132 bytes):

```
030E6C64687369672D736861323536015841 04C4D4A3378FEC90005CBB0D3EAF1309
B482929AF56614AF26A9F22DB83C4F3477B0BA9712DF8213749F918D7DEFDFB32A6C
43DF09715D00E47BE0519D20E4B3148238FE6B6D792070617373776F72645820C8A3
622BB7E626DB911C57161E1FC8FE5A2296BB611CD54F9075CCA256E07454
```

Annotated hex:

* See the annotated hex of the C509 type 0 certificate request. The only difference is the certificate request type, and the signature value.

8.2.4. C509 Type 1 Certificate Request

* C509 type 1 certificate request converted from the X.509 certificate request in Section 8.2.2.

Plain hex (132 bytes):

```
010E6C64687369672D736861323536015841 04C4D4A3378FEC90005CBB0D3EAF1309
B482929AF56614AF26A9F22DB83C4F3477B0BA9712DF8213749F918D7DEFDFB32A6C
43DF09715D00E47BE0519D20E4B3148238FE6B6D792070617373776F72645820C8A3
622BB7E626DB911C57161E1FC8FE5A2296BB611CD54F9075CCA256E07454
```

Annotated hex:

* See the annotated hex of the C509 type 0 certificate request. The only difference is the certificate request type, and the signature value.

8.2.5. C509 Type 2 Certificate Request

* The private key and certificate of the peer are in Section 3.3.1 and Section 3.3.5.

Plain hex (132 bytes):

```
020E6C64687369672D736861323536015841 04C4D4A3378FEC90005CBB0D3EAF1309
B482929AF56614AF26A9F22DB83C4F3477B0BA9712DF8213749F918D7DEFDFB32A6C
43DF09715D00E47BE0519D20E4B3148238FE6B6D792070617373776F726458203126
94C8B2D2BA20E953D5CCAA080FE5181C67D829C9A3271297AF54BB926B06
```

Annotated hex:

* See the annotated hex of the C509 type 0 certificate request. The only difference is the certificate request type, and the signature value.

8.2.6. C509 Type 0 Certificate Request

* The private key and certificate of the peer are in Section 3.3.1 and Section 3.3.5.

Plain hex (132 bytes):

```
000E6C64687369672D736861323536015841 04C4D4A3378FEC90005CBB0D3EAF1309
B482929AF56614AF26A9F22DB83C4F3477B0BA9712DF8213749F918D7DEFDFB32A6C
43DF09715D00E47BE0519D20E4B3148238FE6B6D792070617373776F7264582075C8
DBD5BCD0F132162BFDE3DED7C3C3C9556EACB4BAF4C5EB6204790923FCA8
```

Annotated hex:

```
     0: 00             # [0]. c509CertificateRequestType=0
     1: 0E             # [1]. subjectSignatureAlgorithm=14:
                       #      sa-ecdhPop-sha256-hmac-sha256
     2: 6C             # [2]. subject=char[12]
     3:   64687369672D736861323536 # "dhsig-sha256"
    15: 01             # [3]. subjectPublicKeyAlg=1: EC public key with
                       #      curve secp256r1
    16: 58 41          # [4]. subject public key=byte[65]
    18:   04C4D4A3378FEC90005CBB0D3EAF1309B482929AF56614AF26A9F22DB83C
    48:   4F3477B0BA9712DF8213749F918D7DEFDFB32A6C43DF09715D00E47BE051
    78:   9D20E4B314
    83: 82             # [5]. extensions=array[2]
                         # extension[0]
    84:     38 FE        # type=-255: ChallengePassword,
                         # printableString
    86:     6B           # value=char[11]
    87:       6D792070617373776F7264 # "my password"
    98: 58 20          # [6]. signature
                       #      value=DhSigStatic.hashValue=byte[32]
   100:   75C8DBD5BCD0F132162BFDE3DED7C3C3C9556EACB4BAF4C5EB6204790923
   130:   FCA8
```

8.3. ECDH PoP With SHA-384 And HMAC-SHA384

* Signature algorithm: sa-ecdhPop-sha384-hmac-sha384

* Signature value: with all fields

* Extensions: challenge password with UTF8 String

8.3.1. Private Key

```
-----BEGIN PRIVATE KEY-----
ME4CAQAwEAYHKoZIzj0CAQYFK4EEACIENzA1AgEBBDBUbYpmsdFTjH5242lnccrR
+S9hKNFLUk7CGvyvn2qPBrvxTwFk0g+y5Kb0yGm9mFc=
-----END PRIVATE KEY-----
```

8.3.2. X.509 Certificate Request

* The private key and certificate of the peer are in Section 3.4.1 and Section 3.4.2.

PEM content (289 bytes):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBHTCBsgIBADAXMRUwEwYDVQQDDAxkaHNpZy1zaGEzODQwdjAQBgcqhkjOPQIB
BgUrgQQAIgNiAAQKxeNs56ZnUpvRp6BZmvKELxvkk9P+0gApVXSg2LvxoQfBSIrP
CZoyRp67HFpzLWnC+TVnIoaHKc6IeEx72NBX1j4l/dDyjDWbpsWMJXHYxoOIaqaj
ift9JLlim5l0N3WgHDAaBgkqhkiG9w0BCQcxDQwLbXkgcGFzc3dvcmQwCgYIKwYB
BQUHBhsDWgAwVzAjMB0xGzAZBgNVBAMMEnNlbGZzaWduLXNlY3AzODRyMQICEjQE
MNBiezUC+UP6T/S/CXa+xQDhh4xmQCv1nBGFZeEU/mmxRTBMMUBWttUcKm1uDZqZ
ZQ==
-----END CERTIFICATE REQUEST-----
```

Text representation:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBHTCBsgIBADAXMRUwEwYDVQQDDAxkaHNpZy1zaGEzODQwdjAQBgcqhkjOPQIB
BgUrgQQAIgNiAAQKxeNs56ZnUpvRp6BZmvKELxvkk9P+0gApVXSg2LvxoQfBSIrP
CZoyRp67HFpzLWnC+TVnIoaHKc6IeEx72NBX1j4l/dDyjDWbpsWMJXHYxoOIaqaj
ift9JLlim5l0N3WgHDAaBgkqhkiG9w0BCQcxDQwLbXkgcGFzc3dvcmQwCgYIKwYB
BQUHBhsDWgAwVzAjMB0xGzAZBgNVBAMMEnNlbGZzaWduLXNlY3AzODRyMQICEjQE
MNBiezUC+UP6T/S/CXa+xQDhh4xmQCv1nBGFZeEU/mmxRTBMMUBWttUcKm1uDZqZ
ZQ==
-----END CERTIFICATE REQUEST-----
```

8.3.3. C509 Type 3 Certificate Request

* C509 type 3 certificate request converted from the X.509 certificate request in Section 8.3.2.

Plain hex (203 bytes):

```
030F6C64687369672D736861333834025861040AC5E36CE7A667529BD1A7A0599AF2
842F1BE493D3FED200295574A0D8BBF1A107C1488ACF099A32469EBB1C5A732D69C2
F9356722868729CE88784C7BD8D057D63E25FDD0F28C359BA6C58C2571D8C683886A
A6A389FB7D24B9629B997437758218FF6B6D792070617373776F7264837273656C66
7369676E2D736563703338347231421234583 0D0627B3502F943FA4FF4BF0976BEC5
00E1878C66402BF59C118565E114FE69B145304C314056B6D51C2A6D6E0D9A9965
```

Annotated hex:

* See the annotated hex of the C509 type 0 certificate request. The only difference is the certificate request type, and the signature value.

8.3.4. C509 Type 1 Certificate Request

* C509 type 1 certificate request converted from the X.509 certificate request in Section 8.3.2.

Plain hex (203 bytes):

```
010F6C64687369672D736861333834025861040AC5E36CE7A667529BD1A7A0599AF2
842F1BE493D3FED200295574A0D8BBF1A107C1488ACF099A32469EBB1C5A732D69C2
F9356722868729CE88784C7BD8D057D63E25FDD0F28C359BA6C58C2571D8C683886A
A6A389FB7D24B9629B997437758218FF6B6D792070617373776F7264837273656C66
7369676E2D736563703338347231421234583 0D0627B3502F943FA4FF4BF0976BEC5
00E1878C66402BF59C118565E114FE69B145304C314056B6D51C2A6D6E0D9A9965
```

Annotated hex:

* See the annotated hex of the C509 type 0 certificate request. The only difference is the certificate request type, and the signature value.

8.3.5. C509 Type 2 Certificate Request

* The private key and certificate of the peer are in Section 3.4.1 and Section 3.4.4.

Plain hex (203 bytes):

```
020F6C64687369672D736861333834025861040AC5E36CE7A667529BD1A7A0599AF2
842F1BE493D3FED200295574A0D8BBF1A107C1488ACF099A32469EBB1C5A732D69C2
F9356722868729CE88784C7BD8D057D63E25FDD0F28C359BA6C58C2571D8C683886A
A6A389FB7D24B9629B997437758218FF6B6D792070617373776F7264837273656C66
7369676E2D736563703338347231421234583 0736D7BA3F79CC16A2A58F88AFD6DC8
2BCDBB3A8E8A5B7B105D8DA6B9545EC5B99B90F4812FFC703EB28E2B47F5FF69AA
```

Annotated hex:

* See the annotated hex of the C509 type 0 certificate request. The only difference is the certificate request type, and the signature value.

8.3.6. C509 Type 0 Certificate Request

* The private key and certificate of the peer are in Section 3.4.1 and Section 3.4.4.

Plain hex (203 bytes):

```
000F6C64687369672D736861333834025861040AC5E36CE7A667529BD1A7A0599AF2
842F1BE493D3FED200295574A0D8BBF1A107C1488ACF099A32469EBB1C5A732D69C2
F9356722868729CE88784C7BD8D057D63E25FDD0F28C359BA6C58C2571D8C683886A
A6A389FB7D24B9629B997437758218FF6B6D792070617373776F7264837273656C66
7369676E2D736563703338347231421234583 0E127E66463CC079A637DA971D8ED64
70A004B9165910885CB044538F93C23E0819483823F8D9AF55BFFA3E53CEBE36B9
```

Annotated hex:

```
     0: 00             # [0]. c509CertificateRequestType=0
     1: 0F             # [1]. subjectSignatureAlgorithm=15:
                       #      sa-ecdhPop-sha384-hmac-sha384
     2: 6C             # [2]. subject=char[12]
     3:   64687369672D736861333834 # "dhsig-sha384"
    15: 02             # [3]. subjectPublicKeyAlg=2: EC public key with
                       #      curve secp384r1
    16: 58 61          # [4]. subject public key=byte[97]
    18:   040AC5E36CE7A667529BD1A7A0599AF2842F1BE493D3FED200295574A0D8
    48:   BBF1A107C1488ACF099A32469EBB1C5A732D69C2F9356722868729CE8878
    78:   4C7BD8D057D63E25FDD0F28C359BA6C58C2571D8C683886AA6A389FB7D24
   108:   B9629B99743775
   115: 82             # [5]. extensions=array[2]
                         # extension[0]
   116:     18 FF        # type=255: ChallengePassword
   118:     6B           # value=char[11]
   119:       6D792070617373776F7264 # "my password"
   130: 83             # [6]. signature value=DhSigStatic=array[3]
   131:   72             # issuer=char[18]
   132:     73656C667369676E2D73656370333834 # "selfsign-secp384"
   148:     7231                             # "r1"
   150:   42             # serialNumber=byte[2]
   151:     1234
   153:   58 30          # hashValue=byte[48]
   155:     E127E66463CC079A637DA971D8ED6470A004B9165910885CB044538F93
   184:     C23E0819483823F8D9AF55BFFA3E53CEBE36B9
```

8.4. ECDH PoP With SHA-512 And HMAC-SHA512

* Signature algorithm: sa-ecdhPop-sha512-hmac-sha512

* Signature value: with all fields

* Extensions: empty

8.4.1. Private Key

```
-----BEGIN PRIVATE KEY-----
MF8CAQAwEAYHKoZIzj0CAQYFK4EEACMESDBGAgEBBEGYAuJjVrO97/rkH82IyZSy
71Rtimax0VONomS0XClgUOA1+6U8bwhyjFiEMQSJC5mrLpJeuO5Z6IGl/uwnS5It
LA==
-----END PRIVATE KEY-----
```

8.4.2. X.509 Certificate Request

* The private key and certificate of the peer are in Section 3.5.1 and Section 3.5.2.

PEM content (286 bytes):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBvAIBADAXMRUwEwYDVQQDDAxkaHNpZy1zaGE1MTIwgZswEAYHKoZIzj0C
AQYFK4EEACMDgYYABAForTEuNgFjmmHiGcPDj768sqCrVOaYYW88gPqP9et8WCn8
TPILotzY/IQV0uf+a5KoRHQNfOpLnpJPAQ6l0Jf7jQCBOWzQvsXh2AFUdvWHzndS
5L1WKiYOyqL3CuTNL02dv0dKWJjFWj/bc27z8ftrjLbG2OSj33K2rYutzXyocWjg
36AAMAoGCCsGAQUFBwYcA00AMEowBjAAAgISNARAz1DjPK3P00YBfYL1yp36GGHE
8Ihna+i0ibvntapED7K4iyjdyUMKikRMyIvB9vLWNia/xQ8L0/9FQWls5FhECA==
-----END CERTIFICATE REQUEST-----
```

Text representation:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBGjCBvAIBADAXMRUwEwYDVQQDDAxkaHNpZy1zaGE1MTIwgZswEAYHKoZIzj0C
AQYFK4EEACMDgYYABAForTEuNgFjmmHiGcPDj768sqCrVOaYYW88gPqP9et8WCn8
TPILotzY/IQV0uf+a5KoRHQNfOpLnpJPAQ6l0Jf7jQCBOWzQvsXh2AFUdvWHzndS
5L1WKiYOyqL3CuTNL02dv0dKWJjFWj/bc27z8ftrjLbG2OSj33K2rYutzXyocWjg
36AAMAoGCCsGAQUFBwYcA00AMEowBjAAAgISNARAz1DjPK3P00YBfYL1yp36GGHE
8Ihna+i0ibvntapED7K4iyjdyUMKikRMyIvB9vLWNia/xQ8L0/9FQWls5FhECA==
-----END CERTIFICATE REQUEST-----
```

8.4.3. C509 Type 3 Certificate Request

* C509 type 3 certificate request converted from the X.509 certificate request in Section 8.4.2.

Plain hex (223 bytes):

```
03106C64687369672D736861353132035885040168AD312E3601639A61E219C3C38F
BEBCB2A0AB54E698616F3C80FA8FF5EB7C5829FC4CF20BA2DCD8FC8415D2E7FE6B92
A844740D7CEA4B9E924F010EA5D097FB8D0081396CD0BEC5E1D8015476F587CE7752
E4BD562A260ECAA2F70AE4CD2F4D9DBF474A5898C55A3FDB736EF3F1FB6B8CB6C6D8
E4A3DF72B6AD8BADCD7CA87168E0DF8083804212345840CF50E33CADCFD346017D82
F5CA9DFA1861C4F088676BE8B489BBE7B5AA440FB2B88B28DDC9430A8A444CC88BC1
F6F2D63626BFC50F0BD3FF4541696CE4584408
```

Annotated hex:

* See the annotated hex of the C509 type 0 certificate request. The only difference is the certificate request type, and the signature value.

8.4.4. C509 Type 1 Certificate Request

* C509 type 1 certificate request converted from the X.509 certificate request in Section 8.4.2.

Plain hex (223 bytes):

```
01106C64687369672D736861353132035885040168AD312E3601639A61E219C3C38F
BEBCB2A0AB54E698616F3C80FA8FF5EB7C5829FC4CF20BA2DCD8FC8415D2E7FE6B92
A844740D7CEA4B9E924F010EA5D097FB8D0081396CD0BEC5E1D8015476F587CE7752
E4BD562A260ECAA2F70AE4CD2F4D9DBF474A5898C55A3FDB736EF3F1FB6B8CB6C6D8
E4A3DF72B6AD8BADCD7CA87168E0DF8083804212345840CF50E33CADCFD346017D82
F5CA9DFA1861C4F088676BE8B489BBE7B5AA440FB2B88B28DDC9430A8A444CC88BC1
F6F2D63626BFC50F0BD3FF4541696CE4584408
```

Annotated hex:

* See the annotated hex of the C509 type 0 certificate request. The only difference is the certificate request type, and the signature value.

8.4.5. C509 Type 2 Certificate Request

* The private key and certificate of the peer are in Section 3.5.1 and Section 3.5.4.

Plain hex (223 bytes):

```
02106C64687369672D736861353132035885040168AD312E3601639A61E219C3C38F
BEBCB2A0AB54E698616F3C80FA8FF5EB7C5829FC4CF20BA2DCD8FC8415D2E7FE6B92
A844740D7CEA4B9E924F010EA5D097FB8D0081396CD0BEC5E1D8015476F587CE7752
E4BD562A260ECAA2F70AE4CD2F4D9DBF474A5898C55A3FDB736EF3F1FB6B8CB6C6D8
E4A3DF72B6AD8BADCD7CA87168E0DF8083804212345840 61D337C6DBF89F04E02072
8F37C6F42A9B9AF25ADF51B334D1F8AF26BCB048DF3896097FA1FAEA65DC34B945C2
022AA3727BD75A75F557370250C05E9DE6B0D7
```

Annotated hex:

* See the annotated hex of the C509 type 0 certificate request. The only difference is the certificate request type, and the signature value.

8.4.6. C509 Type 0 Certificate Request

* The private key and certificate of the peer are in Section 3.5.1 and Section 3.5.4.

Plain hex (223 bytes):

```
00106C64687369672D736861353132035885040168AD312E3601639A61E219C3C38F
BEBCB2A0AB54E698616F3C80FA8FF5EB7C5829FC4CF20BA2DCD8FC8415D2E7FE6B92
A844740D7CEA4B9E924F010EA5D097FB8D0081396CD0BEC5E1D8015476F587CE7752
E4BD562A260ECAA2F70AE4CD2F4D9DBF474A5898C55A3FDB736EF3F1FB6B8CB6C6D8
E4A3DF72B6AD8BADCD7CA87168E0DF8083804212345840 64C41B84A6267F63C32972
7D62CB3C35BB76E47EFD329D0CC0EDFD8DA95BF86E35E907869D3173BBC8E39B42F6
A02653E658D301A426FC3F85EECD55777FF53A
```

Annotated hex:

```
  0: 00             # [0]. c509CertificateRequestType=0
  1: 10             # [1]. subjectSignatureAlgorithm=16:
                    #      sa-ecdhPop-sha512-hmac-sha512
  2: 6C             # [2]. subject=char[12]
  3:   64687369672D736861353132 # "dhsig-sha512"
 15: 03             # [3]. subjectPublicKeyAlg=3: EC public key with
                    #      curve secp521r1
 16: 58 85          # [4]. subject public key=byte[133]
 18:   040168AD312E3601639A61E219C3C38FBEBCB2A0AB54E698616F3C80FA8F
 48:   F5EB7C5829FC4CF20BA2DCD8FC8415D2E7FE6B92A844740D7CEA4B9E924F
 78:   010EA5D097FB8D0081396CD0BEC5E1D8015476F587CE7752E4BD562A260E
108:   CAA2F70AE4CD2F4D9DBF474A5898C55A3FDB736EF3F1FB6B8CB6C6D8E4A3
138:   DF72B6AD8BADCD7CA87168E0DF
151: 80             # [5]. extensions=array[0]
152: 83             # [6]. signature value=DhSigStatic=array[3]
153:   80             # issuer=array[0], 0 attribute
154:   42             # serialNumber=byte[2]
155:     1234
157:   58 40          # hashValue=byte[64]
159:     64C41B84A6267F63C329727D62CB3C35BB76E47EFD329D0CC0EDFD8DA9
188:     5BF86E35E907869D3173BBC8E39B42F6A02653E658D301A426FC3F85EE
217:     CD55777FF53A
```

9. Certificate Requests With Different Extensions

9.1. With Normal Extensions

* Extensions: extensions except challengePassword

See Section 8.1.

9.2. With Extension Challenge Password

* Extensions: extension challege pasword of type Printable String

See Section 8.2.

* Extensions: extension challege pasword of type UTF8String String

See Section 8.3.

9.3. With Empty Extensions

* Extensions: no extensions

See Section 8.4.

10. Certificate Request Templates

10.1. All Fields Of Value "undefined" (If Possible)

* c509CertificateRequestType: undefined
* subjectSignatureAlgorithm: undefined
* subject: empty array
* subjectPublicKeyAlgorithm: undefined
* subjectPublicKey: undefined
* extensionsRequest: empty array

Plain hex (7 bytes):

00F7F780F7F780

Annotated hex:

```
0: 00             # [0]. c509CertificateRequestTemplateType=0
1: F7             # [1]. c509CertificateRequestType=<undefined>
2: F7             # [2]. subjectSignatureAlgorithm=<undefined>
3: 80             # [3]. subject=array[0], 0 attribute
4: F7             # [4]. subjectPublicKeyAlgorithm=<undefined>
5: F7             # [5]. subjectPublicKey=<undefined>
6: 80             # [6]. extensions=array[0]
```

10.2. With 1 Element In Fields

* c509CertificateRequestType: 1 element
* subjectSignatureAlgorithm: 1 element
* subject: 1 element
* subjectPublicKeyAlgorithm: 1 element

* extensionsRequest: 1 element

Plain hex (14 bytes):

```
00810081008201F78101F78203F7
```

Annotated hex:

```
 0: 00             # [0]. c509CertificateRequestTemplateType=0
 1: 81             # [1]. c509CertificateRequestType=array[1]
 2:   00             # 0
 3: 81             # [2]. subjectSignatureAlgorithm=array[1]
 4:   00             # [0]=0: ecdsa-with-sha256
 5: 82             # [3]. subject=array[2], 1 attribute
                     # attribute[0]
 6:     01             # type=1: commonName
 7:     F7             # value=<undefined>
 8: 81             # [4]. subjectPublicKeyAlgorithm=array[1]
 9:   01             # [0]=1: EC public key with curve secp256r1
10: F7             # [5]. subjectPublicKey=<undefined>
11: 82             # [6]. extensions=array[2]
                     # extension[0]
12:     03             # type=3: SubjectAlternativeName
13:     F7             # value=<undefined>
```

10.3. Complex Template

* c509CertificateRequestType: multiple types

* subjectSignatureAlgorithm: all choices

* subjectPublicKeyAlgorithm: all choices

* subject

  - choice (int, Defined)

  - choice (int, undefined)

  - choice (~oid, Defined)

  - choice (~oid, undefined)

* extensions

  - choice (int, Defined)

  - choice (int, undefined)

- choice (~oid, Defined)

- choice (~oid, undefined)

Plain hex (150 bytes):

```
008400010203830 14A2B0601040182E3526309824A2B0601040182E352630A420500
8801F7236244454A2B0601040182E352630BF74A2B0601040182E352630C4D0C0B63
6F6E73742D76616C756583014A2B0601040182E3526309824A2B0601040182E35263
0A420500F78808F72118604A2B0601040182E352630DF74A2B0601040182E352630E
4D0C0B636F6E73742D76616C7565
```

Annotated hex:

```
  0: 00             # [0]. c509CertificateRequestTemplateType=0
  1: 84             # [1]. c509CertificateRequestType=array[4]
  2:   00             # 0
  3:   01             # 1
  4:   02             # 2
  5:   03             # 3
  6: 83             # [2]. subjectSignatureAlgorithm=array[3]
  7:   01             # [0]=1: ecdsa-with-sha384
  8:   4A             # [1]=byte[10]:
  9:      2B0601040182E3526309 # oid: 1.3.6.1.4.1.45522.99.9
 19:   82             # [2]=array[2]
 20:     4A             # algorithm=byte[10]:
 21:        2B0601040182E352630A # oid: 1.3.6.1.4.1.45522.99.10
 31:     42             # parameters=byte[2]
 32:       0500
 34: 88             # [3]. subject=array[8], 4 attributes
                      # attribute[0]
 35:     01             # type=1: commonName
 36:     F7             # value=<undefined>
                      # attribute[1]
 37:     23             # type=-4: country, Printable String
 38:     62             # value=char[2]
 39:       4445            # "DE"
                      # attribute[2]
 41:     4A             # type=byte[10]:
 42:        2B0601040182E352630B # oid: 1.3.6.1.4.1.45522.99.11
 52:     F7             # value=<undefined>
                      # attribute[3]
 53:     4A             # type=byte[10]:
 54:        2B0601040182E352630C # oid: 1.3.6.1.4.1.45522.99.12
 64:     4D             # value=byte[13]
 65:       0C0B636F6E73742D76616C7565
 78: 83             # [4]. subjectPublicKeyAlgorithm=array[3]
 79:   01             # [0]=1: EC public key with curve secp256r1
```

```
 80:   4A             # [1]=byte[10]:
 81:      2B0601040182E3526309 # oid: 1.3.6.1.4.1.45522.99.9
 91:   82             # [2]=array[2]
 92:     4A             # algorithm=byte[10]:
 93:        2B0601040182E352630A # oid: 1.3.6.1.4.1.45522.99.10
103:     42             # parameters=byte[2]
104:       0500
106: F7             # [5]. subjectPublicKey=<undefined>
107: 88             # [6]. extensions=array[8]
                      # extension[0]
108:     08             # type=8: ExtendedKeyUsage
109:     F7             # value=<undefined>
                      # extension[1]
110:     21             # type=-2: KeyUsage, critical
111:     18 60          # value=96: [keyCertSign, cRLSign]
                      # extension[2]
113:     4A             # type=byte[10]:
114:        2B0601040182E352630D # oid: 1.3.6.1.4.1.45522.99.13
124:     F7             # value=<undefined>
                      # extension[3]
125:     4A             # type=byte[10]:
126:        2B0601040182E352630E # oid: 1.3.6.1.4.1.45522.99.14
136:     4D             # value=byte[13]
137:       0C0B636F6E73742D76616C7565
```

11. Security Considerations

The private keys printed in these examples cannot be considered secret and MUST NOT be used.

12. Privacy Considerations

There are no privacy considerations.

13. IANA Considerations

There are no IANA considerations.

14. References

14.1. Normative References

[I-D.ietf-cose-cbor-encoded-cert]
Mattsson, J. P., Selander, G., Raza, S., Hglund, J., and M. Furuhed, "CBOR Encoded X.509 Certificates (C509 Certificates)", Work in Progress, Internet-Draft, draft-ietf-cose-cbor-encoded-cert-15, 18 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-cose-cbor-encoded-cert-15>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8742] Bormann, C., "Concise Binary Object Representation (CBOR) Sequences", RFC 8742, DOI 10.17487/RFC8742, February 2020, <https://www.rfc-editor.org/rfc/rfc8742>.

[RFC8949] Bormann, C. and P. Hoffman, "Concise Binary Object Representation (CBOR)", STD 94, RFC 8949, DOI 10.17487/RFC8949, December 2020, <https://www.rfc-editor.org/rfc/rfc8949>.

[RFC9090] Bormann, C., "Concise Binary Object Representation (CBOR) Tags for Object Identifiers", RFC 9090, DOI 10.17487/RFC9090, July 2021, <https://www.rfc-editor.org/rfc/rfc9090>.

14.2. Informative References

[CborMe] Bormann, C., "CBOR Playground", May 2018, <https://cbor.me/>.

Appendix A. Acknowledgments

Authors' Addresses

Lijun Liao
NIO
Email: lijun.liao@nio.io

Gran Selander
Ericsson
Email: goran.selander@ericsson.com

John Preu Mattsson
Ericsson
Email: john.mattsson@ericsson.com